

D-Link NetXtreme[®] DGE-560SX User Guide

Gigabit Fiber (LC) PCI Express Server Adapter

Index

Chapter 1: Introduction	5
1.1 Functionality and Features:.....	5
1.1.1 Features.....	5
1.1.2 Supported Operating Environments	6
1.2 Teaming	7
1.2.1 Overview	7
1.2.2 Load Balancing and Fault Tolerance.....	7
1.3 Virtual LANs	12
1.3.1 VLAN Overview	12
1.3.2 Adding VLANs to Teams	14
1.4 SNMP Management	14
Chapter 2: Installing the Hardware	17
2.1 System Requirements	17
2.1.1 Hardware Requirements	17
2.1.2 Operating System Requirements	17
2.2 Safety Precautions.....	18
2.3 Preinstallation Checklist	18
2.4 Installing the Adapter.....	19
Chapter 3: Installing the Driver Software.....	20
3.1 Creating a Driver Disk.....	20
3.2 Broadcom Boot Agent Driver Software.....	20
3.2.1 Overview	21
3.2.2 Setting Up MBA in a Client Environment	22
3.2.3 Setting Up MBA in a Server Environment	25
3.3 NDIS2 Driver Software	26
3.3.1 Preinstallation Requirements.....	26
3.3.2 Installing the NDIS2 Driver Software for Use on MS-DOS Platforms ..	26
3.3.3 Installing the DOS NDIS2 Driver Software on the Hard Disk.....	31
3.3.4 Configuring the NDIS2 Driver Software	32
3.3.5 Using Keywords for the B57.dos Drivers.....	34
3.4 ODI Driver Software	35
3.4.1 Installing the Driver Software	35
3.4.2 Configuring Parameters for the B57.com Driver (in the Net.cfg file)..	37
3.5 Linux Driver Software.....	38
3.5.1 Limitations.....	38
3.5.2 Packaging	38

3.5.3	Installing TG3 Driver Software	39
3.5.4	Network Installations	41
3.5.5	Patching PCI Files (Optional)	41
3.5.6	Unloading/Removing the TG3 Driver	41
3.5.7	Driver Messages	42
3.5.8	Teaming with Channel Bonding	43
3.6	NetWare Driver Software	43
3.6.1	NetWare Core Driver Software	43
3.6.2	Broadcom Advanced Server Program Driver Software (NetWare)	54
3.6.3	SNMP Agent	71
3.7	Windows Driver Software	71
3.7.1	Installing the Driver Software	71
3.7.2	Updating the Driver Software	74
3.7.3	Viewing or Changing the Properties of the Controller	74
3.7.4	Setting Power Management Options	75
3.7.5	Removing the Device Drivers	76
Chapter 4:	Installing Management Applications	77
4.1	Installing Broadcom Advanced Control Suite and Related Management Applications	77
4.1.1	Using the Installer	77
4.1.2	Using Silent Installation	78
4.2	Modifying Management Applications	79
4.3	Repairing Management Applications	80
4.4	Removing Management Applications	80
Chapter 5:	Using Broadcom Advanced Control Suite 4	81
5.1	Broadcom Advanced Control Suite Overview	81
5.2	Starting Broadcom Advanced Control Suite	81
5.3	Using Broadcom Advanced Control Suite	81
5.3.1	BACS Interface	82
5.3.2	Configuring Preferences	85
5.3.3	Connecting to a Host	85
5.3.4	Managing the Host	86
5.3.5	Managing the Network Adapter	88
5.4	Configuring Teaming	104
5.4.1	Using the Broadcom Teaming Wizard	107
5.4.2	Using Expert Mode	116
Chapter 6:	User Diagnostics	127
6.1	Introduction	127

6.2 System Requirements	127
6.3 Running D-Link NetXtreme User Diagnostics.....	128
6.4 Diagnostic Test Descriptions	131
6.5 Diagnostic Test Messages.....	136
Chapter 7: Troubleshooting	139
7.1 Hardware Diagnostics	140
7.1.1 BACS Diagnostic Tests Failures	140
7.1.2 BACS Network Test Failures.....	140
7.2 Troubleshooting Checklist	141
7.3 Checking for Network Link and Activity	142
7.4 Checking if Current Drivers are Loaded	142
7.5 Testing Network Connectivity	143
7.6 Software Problems and Solutions	144
7.6.1 How to Add a Third-Party OEM Network Adapter to a RIS Installation	144
7.6.2 RIPREP Utility Problem.....	145
7.6.3 Linux and ASFIPMon	147
7.6.4 Broadcom Boot Agent.....	147
7.6.5 Broadcom Advanced Server Program (BASP).....	147
7.6.6 Miscellaneous	148

Information in this document is subject to change without notice.

© 2011 Broadcom Corporation. All rights reserved.

Broadcom, the pulse logo, Connecting everything, the Connecting everything logo, NetXtreme, Ethernet@Wirespeed, LiveLink, and Smart Load Balancing are among the trademarks of Broadcom Corporation and/or its affiliates in the United States, certain other countries, and/or the EU. Microsoft and Windows are trademarks of Microsoft Corporation. Linux is a trademark of Linus Torvalds. NetWare is a trademark of Novell Corporation. Intel is a trademark of Intel Corporation. Magic Packet is a trademark of Advanced Micro Devices, Inc. Red Hat is a trademark of Red Hat, Inc. PCI Express is a trademark of PCI-SIG. Any other trademarks or trade names mentioned are the property of their respective owners.

Chapter 1: Introduction

1.1 Functionality and Features:

D-Link NetXtreme Gigabit Ethernet adapters connect a PCI Express™ compliant system to a Gigabit Ethernet network.

D-Link NetXtreme Gigabit Ethernet adapters target the increased congestion experienced at the backbone and system in today's networks and provide a future upgrade path for systems that require more bandwidth than Fast Ethernet can provide.

Using the Broadcom teaming software, you can split your network into virtual LANs (VLANs) as well as group multiple network adapters together into teams to provide network load balancing and fault tolerance functionality. See Teaming and Broadcom Gigabit Ethernet Teaming Services for detailed information about teaming. See Virtual LANs for a description of VLANs. See Configuring Teaming for instructions on configuring teaming and creating VLANs on Windows and NetWare operating systems.

1.1.1 Features

The following is a list of the D-Link NetXtreme Gigabit Ethernet adapter features for all supported operating systems:

- Gigabit Ethernet (IEEE Std 802.3-1999)
- Logical Link Control (IEEE Std 802.2)
- Flow Control (IEEE Std 802.3x)
- Standard Ethernet frame size (1518 bytes)
- Jumbo frames (up to 9 KB)
- NetWare 5.1 does not support Jumbo frames.
- Layer-2 Priority Encoding (IEEE 802.1p)
- High-speed on-chip RISC processor
- Adaptive interrupt frequency
- Up to 4 classes of service (CoS)

- Up to 4 send rings and receive rings
- Integrated 96 KB frame buffer memory
- GMI/MII Management Interface
- Statistics for SNMP MIB II, Ethernet-like MIB, and Ethernet MIB (IEEE Std 802.3z, Clause 30)
- 4 unique MAC unicast addresses
- Support for multicast addresses via 128 bits hashing hardware function
- Serial EEPROM or serial NVRAM flash memory
- Supports PXE 2.1 specification (Linux Red Hat PXE Server, Windows 2000 Server, Windows Server 2003, Intel APITEST, DOS UNDI)
- JTAG support
- ACPI
- LiveLink™ (supported in both the 32-bit and 64-bit Windows operating systems)
- Self boot

Adaptive Interrupt Frequency

The adapter driver intelligently adjusts host interrupt frequency based on traffic conditions, to increase overall application throughput. When traffic is light, the adapter driver interrupts the host for each received packet, minimizing latency. When traffic is heavy, the adapter issues one host interrupt for multiple, back-to-back incoming packets, preserving host CPU cycles.

Broadcom Advanced Control Suite

Broadcom Advanced Control Suite (BACS), a component of the Broadcom teaming software, is an integrated utility that provides useful information about each network adapter that is installed in your system. The BACS utility also enables you to perform detailed tests, diagnostics, and analyses on each adapter, as well as to modify property values and view traffic statistics for each adapter. BACS is used on Windows operating systems to configure teaming and to add VLANs. See Using Broadcom Advanced Control Suite for detailed information and instructions.

1.1.2 Supported Operating Environments

The D-Link NetXtreme Gigabit Ethernet adapter has software support for the following operating systems:

- Microsoft® Windows® (32-bit and 64-bit extended)
- Linux® (32-bit and 64-bit extended)
- MS-DOS®
- NetWare®

1.2 Teaming

1.2.1 Overview

Adapter teaming allows you to group network adapters together to function as a team. The benefits of teaming include allowing membership to VLANs, providing load balancing between adapters, and offering fault tolerance. These benefits can be combined such that you can couple the functionality of load balancing for the load balance members and the capability of employing a failover with having the team participate on different VLANs.

Broadcom Advanced Server Program (BASP) is the Broadcom teaming software for Windows Server 2003, Windows Server 2008, and NetWare operating systems. For Windows operating systems, BASP is configured through the Broadcom Advanced Control Suite (BACS) utility. For NetWare operating systems, teams are configured by loading BASP with all the necessary frames for the team. For Linux operating systems, teaming is done with channel bonding.

BASP supports four types of load balancing teams:

- Smart Load Balancing and Failover
- Link Aggregation (802.3ad)
- Generic Trunking (FEC/GEC)/802.3ad-Draft Static
- SLB (Auto-Fallback Disable)

 **NOTE:** Enabling Windows Server 2003 built-in bridging is not advisable when you are using teaming software.

1.2.2 Load Balancing and Fault Tolerance

Teaming provides traffic load balancing and fault tolerance (redundant adapter operation in the event that a network connection fails). When multiple adapters are installed in the same system, they can be grouped with up to four teams.

Each team can consist of up to eight adapters, with one adapter used as a standby for Smart Load Balancing and Failover (SLB) or SLB (Auto-Fallback Disabled) team types. If traffic is not identified on any of the adapter team member connections due to failure of the adapter, cable, or switch, the load will be distributed to the remaining team members with an active connection. In the event that all primary adapters fail, traffic will be distributed to the standby adapter. Existing sessions are maintained with no impact on the user.

Types of Teams

The available types of teams for the supported operating systems are shown in the following table:

Table 1. Types of Teams	
Operating System	Available Types of Teams
Windows Server 2003 Windows Server 2008	Smart Load Balancing and Failover Link Aggregation (802.3ad) Generic Trunking (FEC/GEC)/802.3ad-Draft Static SLB (Auto-Fallback Disable)
Linux	Team adapters using the bonding kernel module and a channel bonding interface. See your Red Hat documentation for more information.
NetWare	Smart Load Balancing Link Aggregation (802.3ad) Generic Trunking

Smart Load Balancing™ and Failover

Smart Load Balancing™ and Failover is the Broadcom implementation of load balancing based on IP flow. This feature supports balancing IP traffic across multiple adapters (team members) in a bidirectional manner. In this type of team, all adapters in the team have separate MAC addresses. This type of team provides automatic fault detection and dynamic failover to other team member or to a hot standby member. This is done independently of Layer 3 protocol (IP, IPX, NetBEUI); rather, it works with existing Layer 2 and Layer 3 switches. No switch configuration (such as trunk, link aggregation) is necessary for this type of team to work.

NOTES:

- If you do not enable LiveLink™ when configuring SLB teams, disabling Spanning Tree Protocol (STP) at the switch or port is recommended. This

minimizes the downtime due to spanning tree loop determination when failing over. LiveLink mitigates such issues.

- IPX balances only on the transmit side of the team; other protocols are limited to the primary adapter.
- If a team member is linked at 1000 Mbit/s and another team member is linked at 100 Mbit/s, most of the traffic is handled by the 1000 Mbit/s team member.

Link Aggregation (802.3ad)

This mode supports link aggregation and conforms to the IEEE 802.3ad (LACP) specification. Configuration software allows you to dynamically configure which adapters you want to participate in a given team. If the link partner is not correctly configured for 802.3ad link configuration, errors are detected and noted. With this mode, all adapters in the team are configured to receive packets for the same MAC address. The outbound load-balancing scheme is determined by our BASP driver. The team link partner determines the load-balancing scheme for inbound packets. In this mode, at least one of the link partners must be in active mode.

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

The Generic Trunking (FEC/GEC)/802.3ad-Draft Static type of team is very similar to the Link Aggregation (802.3ad) type of team in that all adapters in the team are configured to receive packets for the same MAC address. The Generic Trunking (FEC/GEC)/802.3ad-Draft Static) type of team, however, does not provide LACP or marker protocol support. This type of team supports a variety of environments in which the adapter link partners are statically configured to support a proprietary trunking mechanism. For instance, this type of team could be used to support Lucent's OpenTrunk or Cisco's Fast EtherChannel (FEC). Basically, this type of team is a light version of the Link Aggregation (802.3ad) type of team. This approach is much simpler, in that there is not a formalized link aggregation control protocol (LACP). As with the other types of teams, the creation of teams and the allocation of physical adapters to various teams is done statically through user configuration software.

The Generic Trunking (FEC/GEC/802.3ad-Draft Static) type of team supports load balancing and failover for both outbound and inbound traffic.

SLB (Auto-Fallback Disable)

The SLB (Auto-Fallback Disable) type of team is identical to the Smart Load Balancing and Failover type of team, with the following exception—when the standby member is active, if a primary member comes back on line, the team continues using the standby member, rather than switching back to the primary member.

If any primary adapter assigned to a team is disabled, the team functions as a Smart Load Balancing and Failover type of team in which auto-fallback occurs.

All primary interfaces in a team participate in load-balancing operations by sending and receiving a portion of the total traffic. Standby interfaces take over in the event that all primary interfaces have lost their links.

Failover teaming provides redundant adapter operation (fault tolerance) in the event that a network connection fails. If the primary adapter in a team is disconnected because of failure of the adapter, cable, or switch port, the secondary team member becomes active, redirecting both inbound and outbound traffic originally assigned to the primary adapter. Sessions will be maintained, causing no impact to the user.

Limitations of Smart Load Balancing and Failover/SLB (Auto-Fallback Disable) Types of Teams

Smart Load Balancing™ (SLB) is a protocol-specific scheme. The level of support for IP, IPX, and NetBEUI protocols is listed below.

Table 2. Smart Load Balancing						
Operating System	Failover/Fallback—All Broadcom			Failover/Fallback—Multivendor		
Protocol	IP	IPX	NetBEUI	IP	IPX	NetBEUI
Windows Server 2003	Y	Y	N/S	Y	N	N/S
Windows Server 2008	Y	Y	N/S	Y	N	N/S
NetWare 5.1/6.5	Y	Y	N/S	Y	N	N/S
Red Hat Linux 3 and 4	Y	N/S	N/S	Y	N/S	N/S
Operating System	Load Balance—All Broadcom			Load Balance—Multivendor		
Protocol	IP	IPX	NetBEUI	IP	IPX	NetBEUI
Windows Server	Y	Y	N/S	Y	N	N/S

2003						
Windows Server 2008	Y	Y	N/S	Y	N	N/S
NetWare 5.1/6.5	Y	Y	N/S	Y	Y	N/S
Red Hat Linux 3 and 4	Y	N/S	N/S	Y	N/S	N/S

Legend: Y = yes

N = no

N/S = not supported

Drivers for third-party network adapters must be NetWare Event Service Layer (NESL) compliant for NetWare to be fault-tolerant and load-balanced in a multivendor team.

The Smart Load Balancing type of team works with all Ethernet switches without having to configure the switch ports to any special trunking mode. Only IP traffic is load-balanced in both inbound and outbound directions. IPX traffic is load-balanced in the outbound direction only. Other protocol packets are sent and received through one primary interface only. Failover for non-IP traffic is supported only for Broadcom network adapters. The Generic Trunking type of team requires the Ethernet switch to support some form of port trunking mode (for example, Cisco's Gigabit EtherChannel or other switch vendor's Link Aggregation mode). The Generic Trunking type of team is protocol-independent, and all traffic should be load-balanced and fault-tolerant.

 **NOTE:** If you do not enable LiveLink™ when configuring teams, disabling Spanning Tree Protocol (STP) at the switch is recommended. This minimizes the downtime due to the spanning tree loop determination when failing over. LiveLink mitigates such issues.

LiveLink™ Functionality

LiveLink™ functionality is a feature of BASP that is available only for the Smart Load Balancing™ and Failover type of teaming. The purpose of LiveLink is to detect network connectivity beyond the switch and to route traffic only through team members that have a live link. This function is accomplished through the teaming software. The teaming software periodically probes (issues a link packet from each team member) one or more specified target network adapter(s). The probe target(s) responds when it receives the link packet. If a team member does not detect a response within a specified amount of time after a specified number of retries, the teaming software discontinues passing traffic through that team

member. Later, if that team member begins to detect a response from a probe target, this indicates that the link has been restored, and the teaming software automatically resumes passing traffic through that team member. LiveLink works only with TCP/IP.

LiveLink™ functionality is supported in both 32-bit and 64-bit Windows operating systems, but is not supported in NetWare systems. For similar functionality in Linux operating systems, refer to Channel Bonding in your Red Hat documentation.

Teaming and Large Send Offload/Checksum Offload Support

Large Send Offload (LSO) and Checksum Offload are enabled for a team only when all of the members support and are configured for the feature.

1.3 Virtual LANs

1.3.1 VLAN Overview

Virtual LANs (VLANs) allow you to split your physical LAN into logical parts, to create logical segmentation of workgroups, and to enforce security policies for each logical segment. Each defined VLAN behaves as its own separate network with its traffic and broadcasts isolated from the others, increasing bandwidth efficiency within each logical group. Up to 64 VLANs (63 tagged and 1 untagged) can be defined for each Broadcom adapter on your server, depending on the amount of memory available in your system.

VLANs can be added to a team to allow multiple VLANs with different VLAN IDs. A virtual adapter is created for each VLAN added.

Although VLANs are commonly used to create individual broadcast domains and/or separate IP subnets, it is sometimes useful for a server to have a presence on more than one VLAN simultaneously. Broadcom adapters support multiple VLANs on a per-port or per-team basis, allowing very flexible network configurations.

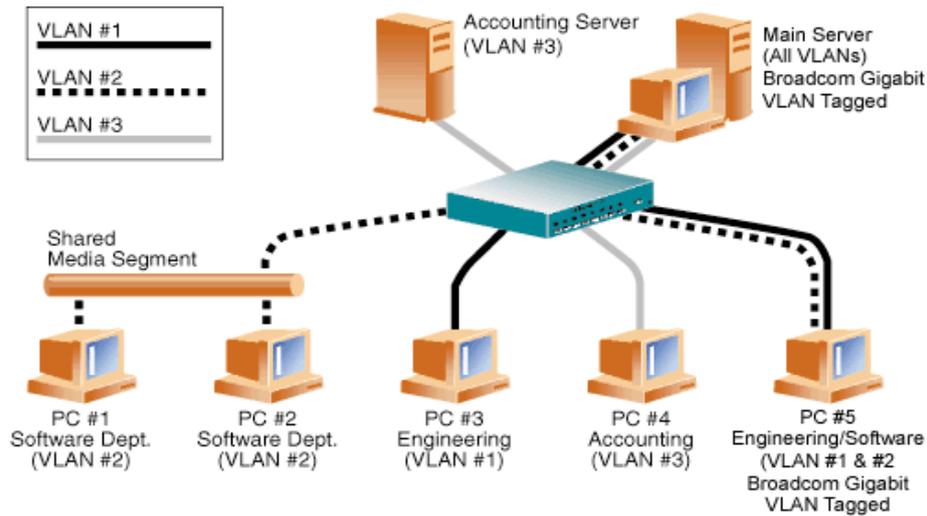


Figure 1: Example of Servers Supporting Multiple VLANs with Tagging

Figure 1 shows an example network that uses VLANs. In this example network, the physical LAN consists of a switch, two servers, and five clients. The LAN is logically organized into three different VLANs, each representing a different IP subnet. The features of this network are described in Table 1:

Table 1: Example VLAN Network Topology	
Component	Description
VLAN #1	An IP subnet consisting of the Main Server, PC #3, and PC #5. This subnet represents an engineering group.
VLAN #2	Includes the Main Server, PCs #1 and #2 via shared media segment, and PC #5. This VLAN is a software development group.
VLAN #3	Includes the Main Server, the Accounting Server and PC #4. This VLAN is an accounting group.
Main Server	A high-use server that needs to be accessed from all VLANs and IP subnets. The Main Server has a Broadcom adapter installed. All three IP subnets are accessed via the single physical adapter interface. The server is attached to one of the switch ports, which is configured for VLANs #1, #2, and #3. Both the adapter and the connected switch port have tagging turned on. Because of the tagging VLAN capabilities of both devices, the server is able to communicate on all three IP subnets in this network, but continues to maintain broadcast separation between all of them.
Accounting Server	Available to VLAN #3 only. The Accounting Server is isolated from all traffic on VLANs #1 and #2. The switch port connected to the server has tagging turned off.
PCs #1 and	Attached to a shared media hub that is then connected to the switch. PCs #1

#2	and #2 belong to VLAN #2 only, and are logically in the same IP subnet as the Main Server and PC #5. The switch port connected to this segment has tagging turned off.
PC #3	A member of VLAN #1, PC #3 can communicate only with the Main Server and PC #5. Tagging is not enabled on PC #3 switch port.
PC #4	A member of VLAN #3, PC #4 can only communicate with the servers. Tagging is not enabled on PC #4 switch port.
PC #5	A member of both VLANs #1 and #2, PC #5 has a Broadcom adapter installed. It is connected to switch port #10. Both the adapter and the switch port are configured for VLANs #1 and #2 and have tagging enabled.

 **NOTE:** VLAN tagging is only required to be enabled on switch ports that create trunk links to other switches, or on ports connected to tag-capable end-stations, such as servers or workstations with Broadcom adapters.

1.3.2 Adding VLANs to Teams

Each team supports up to 64 VLANs (63 tagged and 1 untagged). Note that only Broadcom adapters and Alteon® AceNIC adapters can be part of a team with VLANs. With multiple VLANs on an adapter, a server with a single adapter can have a logical presence on multiple IP subnets. With multiple VLANs in a team, a server can have a logical presence on multiple IP subnets and benefit from load balancing and failover. For instructions on adding a VLAN to a team, see Adding a VLAN for Windows operating systems or see Configuring VLANs for NetWare operating systems.

 **NOTE:** Adapters that are members of a failover team can also be configured to support VLANs. Because VLANs are not supported for an Intel LOM, if an Intel LOM is a member of a failover team, VLANs cannot be configured for that team.

1.4 SNMP Management

BASP Subagent

The BASP subagent, baspmgmt.dll, is designed for the Windows Server 2003, and Windows Server 2008 SNMP service. It is required to install the SNMP service before installing the BASP subagent.

The BASP subagent allows an SNMP manager software to actively monitor the configurations and performance of the Broadcom Advanced Server features. The subagent also provides an alarm trap to an SNMP manager to inform the manager of any changes to the conditions of the BASP component.

The BASP subagent allows monitoring of the configurations and statistics for the BASP teams, the physical NIC adapters participating in a team, and the virtual NIC adapters created as the result of teaming. Non-teamed NIC adapters are not monitored at this time. The BASP configuration data includes information such as team IDs, physical/virtual/VLAN/team adapter IDs, physical/virtual/VLAN/team/ adapter descriptions, and MAC addresses of the adapters.

The statistics include detailed information such as data packets transmitted and received for the physical/virtual/VLAN/team adapters.

The alarm trap forwards information about the changes in configuration of the physical adapters participating in a team, such as physical adapter link up/down, and adapter installed/removed events.

To monitor this information, an SNMP manager must load the Broadcom BASP MIB database files to allow monitoring of the information described above. These files, which are shown below, are included with the installation CD:

baspcfg.mib

baspcfg.mib

baspcfg.mib

BASP Extensible-Agent

The D-Link NetXtreme Gigabit Ethernet Controller Extended Information SNMP extensible-agent, bcmif.dll, is designed for Windows Server 2003, and Windows Server 2008 SNMP service.

The extensible-agent allows the SNMP manager software to actively monitor the configurations of the D-Link NetXtreme adapter. It is intended to supplement the information already provided by the standard SNMP Management Network Interface information.

The extensible-agent provides in-depth information about a D-Link NetXtreme adapter such as:

- MAC address
- Bound IP address
- IP subnet mask
- Physical link status
- Adapter state
- Line speed
- Duplex mode
- Memory range
- Interrupt setting
- Bus number
- Device number
- Function number

To monitor this information, a SNMP manager needs to load the Broadcom Extended information MIB file to allow monitoring of the information described above. This file, `bcmif.mib`, is included on the D-Link NetXtreme adapter installation CD.

The monitored workstation requires the installation of the Broadcom Extended Information SNMP extensible-agent, `bcmif.dll`, and requires the Windows Server 2003, and Windows Server 2008 SNMP service to be installed and loaded.

Chapter 2: Installing the Hardware

2.1 System Requirements

Before you install the D-Link NetXtreme Gigabit Ethernet adapter, verify that your system meets the requirements listed for your operating system:

2.1.1 Hardware Requirements

- Pentium-based system that meets operating system requirements
- One open 32-bit or 64-bit PCI Express slot
- 128-MB RAM (minimum) for Windows and Linux. 64-MB RAM (minimum) for NetWare

2.1.2 Operating System Requirements

General

- PCI Express 2.0 Host Interface

Microsoft Windows

One of the following versions of Microsoft Windows:

- Windows Server 2003 Family
- Windows Server 2008 Family

Novell NetWare

One of the following versions of Novell NetWare: NetWare 4.2, NetWare 5.1, NetWare 6.0, or NetWare 6.5, with the latest support pack.

Linux

 **NOTE:** The current version of the adapter driver has been tested on the latest Red Hat, SuSE, and other Linux distributions for i386, ia64, and x86_64 CPU architectures using 2.4.x and 2.6.x kernels. The driver has been tested up to kernel version 2.4.33 and 2.6.13. The driver should work on other little endian or big endian CPU architectures, but only very limited

testing has been done on some of these machines. The Makefile may have to be modified to include architecture-specific compile switches, and some minor changes in the source files may also be required. On these machines, patching the driver into the kernel is recommended.

2.2 Safety Precautions

 CAUTION! The adapter is being installed in a system that operates with voltages that can be lethal. Before you remove the cover of your system, you must observe the following precautions to protect yourself and to prevent damage to the system components:

- Remove any metallic objects or jewelry from your hands and wrists.
- Make sure to use only insulated or nonconducting tools.
- Verify that the system is powered OFF and unplugged before you touch internal components.
- Install or remove adapters in a static-free environment. The use of a properly grounded wrist strap or other personal antistatic devices and an antistatic mat is strongly recommended.

2.3 Preinstallation Checklist

1. Verify that your server meets the hardware and software requirements listed under System Requirements.
2. Verify that your server is using the latest BIOS.

 **NOTE:** If you acquired the adapter software on a floppy disk or from the Broadcom support website (http://www.broadcom.com/support/ethernet_nic/downloaddrivers.php), verify the path to the adapter driver files.

3. If your system is active, shut it down.
4. When system shutdown is complete, turn off the power and unplug the power cord.
5. Holding the adapter card by the edges, remove it from its shipping package and place it on an antistatic surface.

6. Check the adapter for visible signs of damage, particularly on the card edge connector. Never attempt to install any damaged adapter.

2.4 Installing the Adapter

The following instructions apply to installing the D-Link NetXtreme Gigabit Ethernet adapter (add-in NIC) in most servers. Refer to the manuals that were supplied with your server for details about performing these tasks on your particular server.

1. Review the Safety Precautions and Preinstallation Checklist. Before installing the adapter, ensure the system power is OFF and unplugged from the power outlet, and that proper electrical grounding procedures have been followed.
2. Open the system case, and select any empty PCI Express slot. If you do not know how to identify any of these PCI slots, refer to your system documentation.
3. Remove the blank cover-plate from the slot that you selected.
4. Align the adapter connector edge with the connector slot in the system.
5. Applying even pressure at both corners of the card, push the adapter card into the slot until it is firmly seated. When the adapter is properly seated, the adapter port connectors are aligned with the slot opening, and the adapter faceplate is flush against the system chassis.

 **CAUTION! Do not use excessive force when seating the card as this may damage the system or the adapter. If you have difficulty seating the adapter, remove it, realign it, and try again.**

6. Secure the adapter with the adapter clip or screw.
7. Close the system case and disconnect any personal antistatic devices.

Chapter 3: Installing the Driver Software

3.1 Creating a Driver Disk

Create driver disks using the Broadcom MakeDisk utility (Setup.exe file). This utility runs under Windows and allows you to create disks with the following drivers:

- Windows Server 2003 (IA32, IA64, X64 (AMD64))
- NetWare 5.x/6
- NetWare BASP
- MS-DOS Open Data-Link Interface (ODI)

To create a driver disk or file

1. Insert a 3.5-inch disk into drive A (default) or create a folder on your hard disk.
2. Insert the installation CD into your system CD-ROM drive.
3. If the CD does not automatically run, then browse to the MakeDisk folder on the CD and double-click **Setup.exe**.
4. Follow the onscreen instructions.
5. Select the driver or drivers of choice. Note that selecting multiple drivers results in creating multiple disks.
6. Click **Next**.
7. Click **OK**.
8. If more than one driver was selected, **Setup Needs the Next Disk** is displayed again. Insert another 3.5-inch disk or browse to another folder and click **OK**.

When all driver disks have been created, an information screen is displayed confirming that the disks were successfully created. Click **OK**.

3.2 Broadcom Boot Agent Driver Software

3.2.1 Overview

D-Link NetXtreme Gigabit Ethernet adapters support Preboot Execution Environment (PXE), Remote Program Load (RPL), and Bootstrap Protocol (BootP). Multi-Boot Agent (MBA) is a software module that allows your networked system to boot with the images provided by remote systems across the network. The Broadcom MBA driver complies with the PXE 2.1 specification and is released with both monolithic and split binary images. This provides flexibility to users in different environments where the motherboard may or may not have built-in base code.

The MBA module operates in a client/system environment. A network consists of one or more boot systems that provide boot images to multiple systems through the network. The Broadcom implementation of the MBA module has been tested successfully in the following environments:

- **Linux® Red Hat® PXE Server.** Broadcom PXE clients are able to remotely boot and use network resources (NFS mount, and so forth) and to perform Linux installations. In the case of a remote boot, the Linux universal driver binds seamlessly with the Broadcom Universal Network Driver Interface (UNDI) and provides a network interface in the Linux remotely-booted client environment.
- **Intel® APITEST.** The Broadcom PXE driver passes all API compliance test suites.
- **MS-DOS UNDI.** The MS-DOS Universal Network Driver Interface (UNDI) seamlessly binds with the Broadcom UNDI to provide a network device driver interface specification (NDIS2) interface to the upper layer protocol stack. This allows systems to connect to network resources in an MS-DOS environment.
- **Remote Installation Service (RIS).** The Broadcom PXE clients are able to remotely boot to a Windows 2000 Server or a Windows Server 2003 (SP1 and older) system running RIS to initialize and install Windows Server 2003 and prior operating systems.
- **Windows Deployment Service (WDS).** For Windows Server 2003 SP2, RIS was replaced by WDS, which offers a Broadcom PXE client to install Windows operating systems, including Windows Vista and Windows Server 2008.
- **Automated Deployment Service (ADS).** The Broadcom PXE client can connect to a Windows Server 2003 system and run a deployment agent that allows one to perform some administrative functions, including, but not limited to, deploying a Windows Server 2003 image.

3.2.2 Setting Up MBA in a Client Environment

Use the following procedure for add-in NICs. For LOMs, refer to your computer's system guide.

Setting up MBA in a client environment involves the following steps:

1. Enabling the MBA driver.
2. Configuring the MBA driver.
3. Setting up the BIOS for the boot order.

Enabling the MBA Driver

To enable or disable the MBA driver:

1. Insert the driver source media in the CD-ROM drive and boot up in DOS mode.
2. Type:

```
drive: \dos\utility
```

where

drive is the drive letter of the CD-ROM drive.

 NOTE: The B57udiag.exe file is on the installation CD.

3. Type:

```
b57udiag -mba [ 0-disable | 1-enable ] -c devnum
```

where

devnum is the specific device(s) number (0,1,2, ...) to be programmed.

Specifying the MBA Protocol

To specify the MBA protocol:

1. Place the driver source media in the CD-ROM drive and boot up in DOS mode.
2. Type:

```
drive: \dos\utility
```

where

drive is the drive letter of the CD-ROM drive.

3. Type:

```
b57udiag -mbap [ 0-pxe | 1-rpl | 2-bootp ] -c devnum
```

where

devnum is the specific device(s) number (0,1,2,...) to be programmed.

Forcing the MBA to a Specific Speed

To force the MBA to a specific speed

1. Place the driver source media in the CD-ROM drive and boot up in DOS mode.

2. Type:

```
drive:\dos\utility
```

where

drive is the drive letter of the CD-ROM drive.

3. Type:

```
b57udiag -mbas [ 0-Auto | 1-10HD | 2-10FD | 3-100H | 4-100F ] -c  
devnum
```

where

devnum is the specific device(s) number (0,1,2,...) to be programmed.

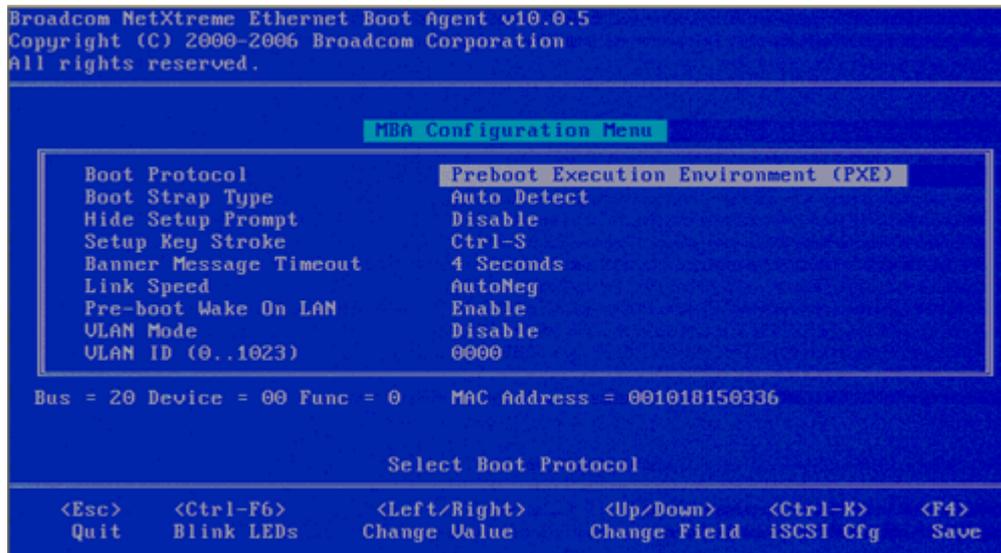
Configuring the MBA Driver

 **NOTE:** You can use the MBA Configuration Menu to configure the MBA driver one adapter at a time as described below, or you can use the D-Link NetXtreme User Diagnostics MS-DOS based application to simultaneously configure the MBA driver for multiple adapters.

1. Restart your system.

2. Press CTRL+S within 4 seconds after you are prompted to do so.

 NOTE: The message prompting you to press CTRL+S is displayed once for each D-Link NetXtreme Gigabit Ethernet adapter you have in your system. The messages are displayed in the same order as the assigned adapter device number.



- Use the UP ARROW and DOWN ARROW keys to move to the Boot Protocol menu item. Then use the RIGHT ARROW or LEFT ARROW key to select the boot protocol of choice if other boot protocols besides Preboot Execution Environment (PXE) are available. If available, other boot protocols include Remote Program Load (RPL) and Bootstrap Protocol (BOOTP).

 NOTE: If you have multiple adapters in your system and you are unsure which adapter you are configuring, press CTRL+F6, which causes the port LEDs on the adapter to start blinking.

- Use the UP ARROW, DOWN ARROW, LEFT ARROW, and RIGHT ARROW keys to move to and change the values for other menu items, as desired.
- Press F4 to save your settings.
- Press ESC when you are finished.

Setting Up the BIOS

To boot from the network with the MBA, make the MBA enabled adapter the first bootable device under the BIOS. This procedure depends on the system BIOS implementation. Refer to the user manual for the system for instructions.

3.2.3 Setting Up MBA in a Server Environment

Linux Red Hat PXE Server

The Red Hat Enterprise Linux has PXE Server support. It allows users to remotely perform a complete Linux installation over the network. The distribution comes with the boot images boot kernel (vmlinuz) and initial ram disk (initrd), which are located on the Red Hat disk#1:

```
/images/pxeboot/vmlinuz
```

```
/images/pxeboot/initrd.img
```

Refer to the Red Hat documentation for instructions on how to install PXE Server on Linux.

The Initrd.img file distributed with Red Hat 8.0, however, does not have a Linux network driver for the D-Link NetXtreme Gigabit Ethernet adapter.

This version requires drivers that are not part of the standard distribution. You can create a driver disk for the D-Link NetXtreme Gigabit Ethernet adapter using files obtained from the support website. NetXtreme Refer to the Linux Readme.txt file for more information.

A remote boot does not require a standard Linux network driver for the D-Link NetXtreme Gigabit Ethernet adapter. After the PXE client downloads the Linux kernel and initial ram disk, the Linux universal driver that came with the Linux distribution binds with the UNDI code of the PXE to form a Linux network driver.

 **NOTE:** Refer to the Distrib.txt file on the installation CD for a list of the specific Linux distributions on which the driver has been tested.

Windows Server 2003

The current version of Windows Server 2003 does not include the latest released network driver for the D-Link NetXtreme Gigabit Ethernet adapter. You can create a driver disk for the adapter using files obtained from the support website. To perform remote installations with PXE, include a network driver for the NetXtreme Gigabit Ethernet adapter as a part of the client installation image on the server. Refer to Microsoft Knowledge Base Article, "How to Add Third-Party OEM Network Adapters to RIS Installations." See also Troubleshooting for details.

DOS UNDI/Intel APITEST

To boot in DOS mode and connect to a network for the DOS environment, download the Intel PXE PDK from the Intel website. This PXE PDK comes with a TFTP/ProxyDHCP/Boot server. The PXE PDK can be downloaded from Intel at <http://downloadcenter.intel.com/default.aspx>.

3.3 NDIS2 Driver Software

3.3.1 Preinstallation Requirements

Before you can successfully install the NDIS2 driver software, the Broadcom network adapter must be physically installed in the server. Networking software that is appropriate to the operating system (such as Microsoft LAN Manager 2.2 for MS-DOS) must already be running on your server.

3.3.2 Installing the NDIS2 Driver Software for Use on MS-DOS Platforms

The NDIS2 driver software can be run from an MS-DOS startup disk using Microsoft Network Client 3.0 or from the hard disk using Microsoft LAN Manager 2.2.

Creating a Startup Disk to Run Microsoft Network

Client

To perform this installation you must have the following items:

- Windows NT Server 4.0 CD-ROM
- A blank MS-DOS system disk (3.5" high-density floppy disk)
- Access to the Broadcom NDIS2 driver file (B57.dos). This file is located on the installation CD.

NOTES:

- **Windows NT Server 4.0 users.** When running **Setup for Microsoft Network Client v3.0 for MS-DOS**, click any network card from the list (**NE2000 Compatible**, for example) to create the startup disk.
- After creating the startup disk, follow the instructions in **Modifying the Startup Disk**.

To create a startup disk

1. Create a folder called NCADMIN in the root of the C drive.
2. Copy the NCADMIN.CN_, NCADMIN.EX_, and NCADMIN.HL_ files from the I386 folder on the Windows NT Server 4.0 CD-ROM.
3. Open a command prompt window and change the directory to C:\NCADMIN.
4. Type **expand -r ncdadmin.*** and press ENTER.
5. Close the command prompt window by typing exit and then pressing **ENTER**.
6. Start Windows Explorer.
7. Open the NCADMIN folder and double-click **ncadmin.exe**.
8. Follow the on-screen instructions to make the network startup disk (choose **NE2000 Compatible** from the list of adapters).

Modifying the Startup Disk

To modify the startup disk

1. Edit A:\Net\Protocol.ini with Notepad or a similar text editor.
 - a. Change DriverName=\$ to DriverName=B57\$.
 - b. Remove all other parameter entries under the [MS\$NE2CLONE] or equivalent section such as IOBASE=0x300 or INTERRUPT=3, and so on.

Example Protocol.ini file for IP

```
[network.setup]
version=0x3110
netcard=ms$ne2clone,1,MS$NE2CLONE,1
transport=tcPIP,TCPiP
lana0=ms$ne2clone,1,tcPIP
[MS$NE2CLONE]
DriverName=B57$
[protman]
DriverName=PROTMAN$
PRIORITY=MS$NDISHLP
[tcPIP]
NBSessions=6
```

```

DefaultGateway=0
SubNetMask=255 0 0 0
IPAddress=192 168 0 1
DisableDHCP=0
DriverName=TCP/IP$
BINDINGS=MS$NE2CLONE
LANABASE=0

```

Example: Protocol.ini file for IPX

```

[network.setup]
version=0x3110
netcard=ms$ne2clone,1,MS$NE2CLONE,1
transport=ms$ndishlp,MS$NDISHLP
transport=ms$nwlink,MS$NWLINK
lana0=ms$ne2clone,1,ms$nwlink
lana1=ms$ne2clone,1,ms$ndishlp
[MS$NE2CLONE]
DriverName=B57$
[protman]
DriverName=PROTMAN$
PRIORITY=MS$NDISHLP
[MS$NDISHLP]
DriverName=ndishlp$
BINDINGS=ms$ne2clone
[ms$nwlink]
DriverName=nwlink$
FRAME=Ethernet_802.2
BINDINGS=MS$NE2CLONE
LANABASE=0

```

Example Protocol.ini file for NetBEUI

```

[network.setup]
version=0x3110
netcard=ms$ne2clone,1,MS$NE2CLONE,1
transport=ms$ndishlp,MS$NDISHLP
transport=ms$netbeui,MS$NETBEUI
lana0=ms$ne2clone,1,ms$ndishlp

```

```
lanal=ms$ne2clone,1,ms$netbeui
[MS$NE2CLONE]
DriverName=B57$
[protman]
DriverName=PROTMAN$
PRIORITY=MS$NDISHLP
[MS$NDISHLP]
DriverName=ndishlp$
BINDINGS=MS$NE2CLONE
[MS$NETBEUI]
DriverName=netbeui$
SESSIONS=10
NCBS=12
BINDINGS=MS$NE2CLONE
LANABASE=0
```

2. Edit A:\Net\System.ini.
 - a. Change netcard= to netcard=b57.dos.
 - b. Check for references to C:\NET and change C:\NET to A:\NET if necessary.

Example System.ini file

```
[network]
sizworkbuf=1498
filesharing=no
printsharing=no
autologon=yes
computername=MYPC
lanroot=A:\NET
username=USER1
workgroup=WORKGROUP
reconnect=yes
dospophotkey=N
lmlogon=0
logondomain=
preferredredir=basic
autostart=basic
maxconnections=8
```

```
[network drivers]
netcard=B57.dos
transport=ndishlp.sys,*netbeui
devdir=A:\NET
LoadRMDrivers=yes
```

3. Copy B57.dos to A:\Net.
4. Create the appropriate Autoexec.bat file in drive A for the chosen protocol as shown below.

For TCP/IP

```
path=a:\net
a:\net\net initialize
a:\net\netbind.com
a:\net\umb.com
a:\net\tcptsr.exe
a:\net\tinyrfc.exe
a:\net\nmtsrx.exe
a:\net\emsbfr.exe
a:\net\net start basic
net use z: \\SERVERNAME\SHARENAME
```

For IPX

```
SET PATH=A:\NET
A:\NET\net initialize
A:\NET\nwlink
A:\NET\NET START BASIC
net use z: \\SERVERNAME\SHARENAME
```

For NetBEUI

```
SET PATH=A:\NET
A:\NET\NET START BASIC
net use z: \\SERVERNAME\SHARENAME
```

5. Create a Config.sys file on the startup disk in drive A as shown below.

```
files=30
```

```
device=a:\net\ifshlp.sys  
lastdrive=z
```

3.3.3 Installing the DOS NDIS2 Driver Software on the Hard Disk

To install the DOS NDIS2 Driver Software on the hard disk

1. Verify that the system has Microsoft LAN Manager 2.2 installed, with a protocol such as NetBEUI configured.
2. Create a folder on your hard disk to store the NDIS 2.01 driver.

Example: C:\LANMAN

3. Copy the B57.dos file to this folder.
4. Edit the Config.sys file by adding the following lines:

```
DEVICE = C:\LANMAN\PROTMAN.DOS  
DEVICE = C:\LANMAN\B57.DOS  
DEVICE = C:\LANMAN\NETBEUI.DOS
```

5. Edit the Autoexec.bat file by adding the following lines:

```
C:\LANMAN\NETBIND.EXE  
C:\LANMAN\NET START WORKSTATION  
C:\LANMAN\NET USE drive letter: \\server name\resource name
```

6. Edit the Protocol.ini file (located in C:\LANMAN) to configure the driver to bind with NetBEUI or any other protocols.

Example:

```
[PROTOCOL MANAGER]  
DriverName = PROTMAN$  
[NETBEUI_XIF]  
DriverName = netbeui$  
BINDINGS = B57  
[B57]  
DriverName = "B57$"
```

7. Restart the computer to complete the installation.

 NOTE: The driver loads during system configuration and displays the Broadcom banner, controller name, MAC address, IRQ number, detected line speed, and the controller BusNum and DevNum. If the driver fails to load, an *initialization fail* message is displayed.

3.3.4 Configuring the NDIS2 Driver Software

The NDIS2 driver software can be configured by adding specific optional keywords to the Protocol.ini file. If multiple (or multiport) D-Link NetXtreme Gigabit Ethernet adapters are installed in a system, the NDIS2 driver software loads by default on the adapter/port that has a good link. If 2 or more adapters have a good link, the NDIS2 driver software loads on the adapter having the latest Device ID. If 2 or more adapters that have a good link have the same Device ID, the NDIS2 driver software loads on the adapter that is located in the slot having the lowest bus number.

 NOTE: On MS-DOS platforms, it is not recommended to load the NDIS2 driver software on more than 1 adapter; the required NDIS2 protocol manager that supports multiple binds is not available in the MS-DOS environment.

If it is necessary to have the NDIS2 driver load on certain adapters in a certain order, the BusNum, DevNum, and FuncNum keywords can be used. Do not use these keywords unless you know how to configure PCI devices.

The **BusNum** keyword value, which represents the PCI bus number in which the adapter is located, is a decimal number ranging from 0 to 255.

The **FuncNum** keyword value, which represents the function (port) number of a multiport adapter, is a decimal number, with 0 representing the first port, and 1 representing the second port.

The **DevNum** keyword value, which represents the assigned device number, is a decimal number ranging from 0 to 31.

 NOTE: At the end of the NDIS2 driver software installation process, note the BusNum and DevNum values that are displayed. Alternatively, use Broadcom Advanced Control Suite (see Broadcom Advanced Control Suite) to view the bus number, function (port) number, and device number assigned to each adapter (Windows users only).

Example BusNum, DevNum, and FuncNum keyword entries for loading the NDIS2 driver on multiple adapters in a certain order are shown below:

```
[B57]
DRIVERNAME = B57$
BUSNUM = 3
DEVNUM = 10
[B57_2]
DRIVERNAME = B572$
BUSNUM 3
DEVNUM 11
[B57_3]
DRIVERNAME = B573$
BUSNUM 3
DEVNUM 12
[B57_4]
DRIVERNAME = B574$
BUSNUM 3
DEVNUM 13
```

The LineSpeed keyword is used to force the speed of the network connection. The LineSpeed keyword requires a decimal number and of either 10, 100, or 1000. Technically, a line speed of 1000 Mbit/s cannot be forced and can be achieved only through auto-negotiation. For the sake of simplicity, the driver performs auto-negotiation when the line speed is set to a value of 1000. Forced 1000 Mbit/s speed is not needed for copper links; auto-negotiation is the proper supported configuration under the IEEE Ethernet specification.

The Duplex keyword is used to force the duplex mode of the adapter. The Duplex keyword requires a text string of either HALF or FULL. When the Duplex keyword is used, the LineSpeed keyword must also be used. If neither keyword is used, the network adapter defaults to auto-negotiation mode.

The NodeAddress keyword specifies the network address used by the adapter. If a multicast address or a broadcast address is specified, the adapter uses the default MAC address.

The FixChecksumOff keyword turns off the driver workaround for the TCP/IP stack to recognize the ones complement version of the checksum.

Example entries for the LineSpeed, Duplex, and NodeAddress keywords are shown below:

```
[B57]
DRIVERNAME = B57$
```

```
BUSNUM = 3  
DEVNUM = 10  
PORTNUM = 0  
LINESPEED = 100  
DUPLEX = FULL  
NODEADDRESS = "001020304050"
```

3.3.5 Using Keywords for the B57.dos Drivers

The Protocol.ini file contains certain keywords that are used by the B57.dos drivers. These keywords are listed below:

BusNum. Specifies the number of the PCI bus on which the network adapter is located. Requires a decimal number having a value ranging from 0 to 255.

DevNum. Specifies the device number assigned to the network adapter when it is configured by the PCI BIOS. Requires a decimal number having a value ranging from 0 to 255.

FuncNum or PortNum. Specifies the PCI function or port number assigned to the network controller. Requires a decimal number having a value ranging from 0 to 7.

 **NOTE:** These keywords, **BusNum**, **DevNum**, and **FuncNum** (or **PortNum**), are needed when multiple adapters are installed in the server and when a specific controller must be loaded in a certain order. These keywords are used concurrently and are included for manufacturing purposes. Do not use them unless you are familiar with how to configure PCI devices. A PCI device scan utility is needed to find this information.

LineSpeed. Specifies the speed of the network connection in Mbit/s. Requires the decimal number **10**, **100**, or **1000**. Technically, a line speed of 1000 Mbit/s cannot be forced and is achievable only through auto-negotiation. For the sake of simplicity, the driver performs auto-negotiation when the line speed is set to a value of 1000.

Duplex. Specifies the duplex mode of the network adapter. Requires a setting of either **Half** or **Full**. When this keyword is used, the **LineSpeed** keyword must also be used. If neither keyword is used, the network adapter defaults to auto-negotiation mode.

NodeAddress. Specifies the network address used by the network adapter. If a multicast address or a broadcast address is specified, the adapter uses the default MAC address.

Example:

```
[B57]
DriverName = "B57$"
BusNum = 3
DevNum = 14
PortNum = 2
LineSpeed = 1000
Duplex = Full
NodeAddress = 001020304050
```

3.4 ODI Driver Software

The Open Data-Link Interface (ODI) driver software allows LAN drivers to work together irrespective of differences between the hardware and/or the protocol stacks of communicating systems. An intervening layer, called the link support layer (LSL), is responsible for routing different packet types between LAN drivers and protocol stacks.

3.4.1 Installing the Driver Software

Installing the ODI driver software involves the following steps:

1. Verify that the MS-DOS operating system files are installed on your system hard disk or are available on a removable storage device.
2. Install the ODI driver software in the MS-DOS environment.
3. If necessary, reconfigure the driver software after installation.

Preinstallation Requirements

Verify that the D-Link NetXtreme Gigabit Ethernet adapter driver software has been installed on your system. If it has not, install it (see Installing the Driver Software). Otherwise, you cannot use a D-Link NetXtreme Gigabit Ethernet adapter in the MS-DOS environment.

 **NOTE:** To be able to successfully install the adapter driver in the MS-DOS environment, the adapter must be installed before you install the adapter driver.

Installing the ODI Driver in the MS-DOS 6.22

Environment

1. Copy the ODI driver file (B57.com) to the root directory of the hard disk (the B57.com file is on the installation CD).
2. Copy the Lsl.com, Ipxodi.com, and Vlm.com files to the same directory (these files are provided by Novell).
3. Edit the Autoexec.bat file by adding the following lines:

```
C:\LSL
```

```
C:\B57
```

```
C:\IPXODI
```

```
C:\VLM
```

4. Edit the Net.cfg file and place the file in the same location as the Autoexec.bat file (located in drive C) to configure the driver to bind with different frame types.

```
LINK DRIVER B57
```

```
FRAME ETHERNET_802.2
```

```
FRAME ETHERNET_802.3
```

```
FRAME ETHERNET_II
```

```
FRAME ETHERNET_SNAP
```

```
NetWare DOS Requester
```

```
FIRST NETWORK DRIVE=F
```

```
NETWARE PROTOCOL=NDS BIND
```

```
PROTOCOL IPXODI
```

5. Restart the computer to complete the install.
6. As the files are being loaded, the computer attempts to attach to a NetWare server using the frame types specified in Net.cfg. If the connection is successful, a dialog box appears.
7. Change to drive F and log on to the NetWare server.

 **NOTE:** The driver loads during system configuration, and the Broadcom banner, the adapter name, the MAC address, the IRQ number, the detected line speed, and the BUSNUM and DEVNUM of the adapter are displayed. If the driver fails to load, an initialization fail message appears.

3.4.2 Configuring Parameters for the B57.com Driver (in the Net.cfg file)

The following are optional custom keywords used in the Net.cfg file:

BUSNUM

DEVNUM

FUNNUM

SUBVID

MODEL

The first two keywords (BUSNUM and DEVNUM) are used concurrently and have been included for manufacturing purposes. Do not use them unless you are familiar with PCI device configuration. These two keywords are needed if multiple D-Link NetXtreme Gigabit Ethernet adapters are installed in a system, and each adapter must be loaded in a specific order.

BUSNUM specifies the PCI bus number and DEVNUM specifies the device number that is assigned to the adapter when it is configured by the PCI BIOS.

The values for these adapter parameters are displayed in hexadecimal notation when the driver loads (the Net.cfg file expects hexadecimal values). A PCI device scan utility can also be used to find this information. If the driver loads on a single adapter, the displayed values can be used in the Net.cfg file.

If a PCI scan utility displays adapter 1 at bus 4 and device 11 (hexadecimal), and adapter 3 at bus 3 and device 13 (hexadecimal), the following load instructions are written to the Net.cfg file (load adapter 3 first, and optionally load adapter 1 second):

```
LINK DRIVER B57
BUSNUM 3
DEVNUM 13 (13 hex = 19 decimal)
LINK DRIVER B57
BUSNUM 4
DEVNUM 11 (11 hex = 17 decimal)
```

The FUNNUM keyword is used to determine which function/port the driver is to load on when using a multifunction (multiport) adapter. Function number values are limited to 0 and 1, for the first and second ports of the adapter.

The SUBVID keyword is used to for load the driver only on the first adapter found that has a subvendor ID (SVID) that matches the one set in Net.cfg. The driver ignores all other adapters that do not have a matching SVID. SUBVID expects a hexadecimal number.

Example:

```
LINK DRIVER B57  
SUBVID 14E4
```

SUBVID cannot be used with BUSNUM, DEVNUM or FUNNUM.

The MODEL keyword is for loading the driver only on the first adapter found that has a subvendor ID (SVID) that matches the one set in MODEL. The driver ignores all other adapters that do not have a matching SVID. MODEL expects a decimal number.

Example:

```
LINK DRIVER B44  
MODEL 534
```

3.5 Linux Driver Software

3.5.1 Limitations

The current version of the adapter driver has been tested on the latest Red Hat, SuSE, and other Linux distributions for i386, ia64, and x86_64 CPU architectures using 2.4.x and 2.6.x kernels. The driver has been tested up to kernel version 2.4.33 and 2.6.13. The driver should work on other little endian or big endian CPU architectures, but only very limited testing has been done on some of these machines. The Makefile may have to be modified to include architecture-specific compile switches, and some minor changes in the source files may also be required. On these machines, patching the driver into the kernel is recommended.

3.5.2 Packaging

The Linux TG3 driver is released in the following packaging formats (file names):

- Source RPM (*tg3-version.src.rpm*)
- Supplemental (*tg3_sup-version.tar.gz*)
- Compressed tar (*tg3-version.tar.gz*)

Identical source files to build the driver are included in both RPM and TAR source packages. The tar file contains additional utilities such as patches and driver disk images for network installation.

3.5.3 Installing TG3 Driver Software

Installing the Source RPM Package

1. Install the source RPM package.

```
rpm -ivh tg3-version.src.rpm
```

2. Change the directory to the RPM path and build the binary driver for your kernel (the RPM path is different for different Linux distributions).

```
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)
```

 **NOTE:** During your attempt to install a source RPM package, the following message may be displayed:

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

The most likely cause of the error is that the rpm-build package has not been installed. Locate the rpm-build package on the Linux installation media and install it using the following command:

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

Complete the installation of the source RPM.

3. Install the newly-built package (driver and man page).

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

Depending on the kernel, the driver is installed to one of the following paths:

2.4.x kernels:

```
/lib/modules/kernel_version/kernel/drivers/net/tg3.o
```

2.4.x kernels with the tg3 driver patched in:

```
/lib/modules/kernel_version/kernel/drivers/addon/tg3/tg3.o
```

2.6.x kernels:

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

4. Load the driver.

```
modprobe tg3
```

To configure the network protocol and address, refer to the Linux version-specific documentation.

Building the Driver from the Source TAR File

1. Create a directory (*tg3-version*) and extract the TAR files to the directory.

```
tar xvzf tg3-version.tgz
```

2. Build the driver *tg3.o* as a loadable module for the running kernel.

```
CD tg3-version  
make clean  
make; make install
```

3. Test the driver by loading it.

```
rmmod tg3  
modprobe tg3
```

No message should be returned if this command runs properly.



NOTE: See the RPM instructions above for the location of the installed driver.

4. To configure network protocol and address, refer to the manuals supplied with your operating system.

3.5.4 Network Installations

For network installations through NFS, FTP, or HTTP (using a network boot disk or PXE), a driver disk that contains the tg3 driver may be needed. The driver disk images for the most recent Red Hat versions are included. Boot drivers for other Linux versions can be compiled by modifying the Makefile and the make environment. Further information is available from the Red Hat website, <http://www.redhat.com>.

To create the driver disk, select the appropriate image file (located in `tg3_sup-version.tar.gz`) and type the following:

```
dd if=<version>.dd.img of=/dev/fd0
```

3.5.5 Patching PCI Files (Optional)

For hardware detection utilities such as Red Hat kudzu to properly identify tg3 supported devices, a number of files containing PCI vendor and device information may need to be updated.

Apply the updates by running the scripts provided in the Supplemental tar file. For example, on Red Hat Enterprise Linux, apply the updates by doing the following:

```
./patch_pcitbl.sh /usr/share/hwdata/pcitable pci.updates  
/usr/share/hwdata/pcitable.new  
./patch_pciids.sh /usr/share/hwdata/pci.ids pci.updates  
/usr/share/hwdata/pci.ids.new
```

Next, the old files can be backed up and the new files can be renamed for use.

```
cp /usr/share/hwdata/pci.ids /usr/share/hwdata/old.pci.ids  
cp /usr/share/hwdata/pci.ids.new /usr/share/hwdata/pci.ids  
cp /usr/share/hwdata/pcitable /usr/share/hwdata/old.pcitable  
cp /usr/share/hwdata/pcitable.new /usr/share/hwdata/pcitable
```

 **NOTE:** The paths above are for Red Hat distributions. These paths may be different on other distributions.

3.5.6 Unloading/Removing the TG3 Driver

Unloading/Removing the Driver from an RPM

Installation

To unload the driver, use **ifconfig** to bring down all *ethX* interfaces opened by the driver, and then type the following:

```
rmmod tg3
```

If the driver was installed using **rpm**, do the following to remove it:

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

Removing the Driver from a TAR Installation

If the driver was installed using make install from the tar file, the tg3.o driver file has to be manually deleted from the operating system. See Installing the Source RPM Package for the location of the installed driver.

If there is an interface configuration that is related to the tg3 driver, then bring the interface down first by using **ifconfig ethx down** and then **rmod tg3**.

3.5.7 Driver Messages

The following are the most common sample messages that may be logged in the */var/log/messages* file. Use **dmesg -n/level** to control the level at which messages appear on the console. Most systems are set to level 6 by default.

Driver Sign on

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

NIC Detected

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

Flow Control

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

Link Up and Speed Indication

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

Link Down Indication

tg3: eth#: Link is down.

3.5.8 Teaming with Channel Bonding

With the TG3 driver, you can team adapters together using the bonding kernel module and a channel bonding interface. Refer to your Red Hat documentation for more information on Linux Channel Bonding.

3.6 NetWare Driver Software

3.6.1 NetWare Core Driver Software

Preinstallation Requirements

A network device driver must be installed before the D-Link NetXtreme Gigabit Ethernet adapter can be used with your Novell NetWare system.

Before you can successfully install the adapter driver for Novell NetWare, the adapter card must be physically installed in the system and, typically, NetWare operating system software must already be running on the system. Make sure that your system meets the hardware and operating system software requirements described in *Installing the Hardware*.

To enable the D-Link NetXtreme adapter to function correctly, you must install the latest Novell NetWare support pack files. The NetWare support pack or patch file(s) needed for the operating system running on your server are indicated below:

Table 1: NetWare Support Files		
NetWare Version	Support Pack	Files to be Installed
NetWare 5.1	Latest support	The latest support pack can be found at: http://download.novell.com/index.jsp?product_id=&search=Sea

	pack	rch&families=2639&version=8130&date_range=&keywords=&sort_by=&x=25&y=8
NetWare 6.0	Latest support pack	The latest support pack can be found at: http://download.novell.com/index.jsp?product_id=&search=Search&families=2639&version=7486&date_range=&keywords=&sort_by=&x=17&y=7
NetWare 6.5	Latest support pack	The latest support pack can be found at: http://download.novell.com/index.jsp?product_id=&search=Search&families=2639&version=12127&date_range=&keywords=&sort_by=&x=32&y=4

NOTES:

- **NetWare 5.1/6.0/6.5.** If you are installing NetWare 5.1/6.0/6.5 for the first time on a system, the driver is installed during the operating system installation process. Install the NetWare support pack after you have successfully installed the operating system on the system.

Installing NetWare Server 5.1/6.0 Driver Software

 NOTE: The following instructions are for installing Novell NetWare Server 5.1 or 6.0 driver software. For instructions on installing Novell NetWare Server 6.5 driver software, see Installing NetWare Server 6.5 Driver Software.

Verify that the system has the latest support pack available installed. See Table 1 for information on obtaining the latest support pack for your version. You may want to create an archive disk (see Creating a Driver Disk) by copying all the files from the CDROM\NetWare\Driver directory onto a floppy disk. If you elect to use the CD directly, ensure that the CDROM.NLM file is loaded and that you know the NetWare volume name for the CD.

1. From the NetWare Server console, type **LOAD NWCONFIG**, and then press ENTER.
2. From the **Configuration Options** menu, select **Driver options**, and then press ENTER.
3. Select **Configure network drivers**, and then press ENTER.
4. Select **Select an additional driver**, and then press ENTER.
5. Insert the installation CD or the archive disk, and then select **Install an unlisted driver** by pressing INSERT.

6. If you inserted the archive disk, press ENTER. If you have the installation CD mounted as a NetWare volume, press F3 and type *Volume Name: NetWare\Driver* as the source path, where *Volume Name* is the name of the NetWare volume for the installation CD, and *NetWare\Driver* is the directory containing the specific files on the installation CD needed for this installation.
7. Press ENTER to select the highlighted driver.
8. Select **Yes**, and then press ENTER.
9. Select **Yes**, and then press ENTER to copy the .ldi file. This is the installation script for the driver.
10. Select **Save parameters and load driver** to continue.
11. Select **Exit** to return to the NetWare Server console prompt.

 **NOTE:** If you are performing an initial installation of NetWare 5.1/6.0 and have more than two network adapters installed, the install program allows you to allocate the actual number of packet receive buffers needed by the adapter. During installation, the RxBuffers value is set to 32, the minimum number of buffers the driver requires for each adapter. Although this setting affects adapter performance, it allows the installation of the operating system and up to 8 adapters during initial installation process. After you complete the installation, increase the number of buffers allocated to the driver, as described in Viewing or Modifying Adapter Properties.

12. After NetWare 5.1/6.0 has been successfully installed, set the minimum packet Receive Buffers property in the Startup.ncf file to 1500 for each adapter in the system. Set the maximum packet receive buffers to three times the minimum packet receive buffers. Typically, 4 MB of RAM are required per 1000 receive buffers. For more information, see Viewing or Modifying Adapter Properties.
13. In the Autoexec.ncf file, delete the packet Receive Buffers property (RxBuffers = 32) in the load statement for this adapter. Deleting the Receive Buffers phrase from the load statement resets the Receive Buffers property to the default value of 200.

 **NOTE:** The system must be restarted for the new configuration to take effect.

Example: The default maximum number of receive buffers for the system is 500, and the default minimum is 128. Edit the Startup.ncf file to have the following entries. The actual number of receive buffers is a function of the number of ports in the system. The following is an example for a system with 8 ports installed:

```
set maximum packet receive buffers = 36000
set minimum packet receive buffers = 12000
```

Installing NetWare Server 6.5 Driver Software

 **NOTE:** The following instructions are for installing the NetWare Server 6.5 driver software. For instructions on installing NetWare Server 5.1 or 6.0 driver software, see *Installing NetWare Server 5.1/6.0 Driver Software*.

You may want to create an archive disk (see *Creating a Driver Disk*) by copying all the files from the CDROM\NetWare\Driver directory onto a disk. If you elect to use the CD directly, ensure that the CDROM.NLM file is loaded and that you know the NetWare volume name for the CD.

1. From the NetWare Server console, type **HDETECT**, and then press ENTER.
2. From **Options**, press ENTER to accept **Platform Support Module** and **Hot-Plug Support Module** and continue detecting devices.
3. From **Options**, scroll down to select **Modify**, and then press ENTER to change focus to detected devices.
4. Scroll down to **Network boards** and press ENTER.
5. From **Additional Driver Options**, scroll down to **Modify**, and then press ENTER.
6. Insert the CD or archive floppy disk you created, and then select the **Add** option by pressing INSERT.
7. Select the **Install an unlisted driver** option, by pressing INSERT.
8. If you inserted the archive floppy disk, press ENTER. If you have the CD mounted as a NetWare volume, press F3 and type *Volume Name: NetWare\Driver* as the source path, where *Volume Name* is the name of the NetWare volume for the CD, and *NetWare\Driver* is the directory of the specific files on the CD needed for this installation.
9. Use the DOWN ARROW or TAB to switch back to **Additional Driver Options**.
10. Choose **Return to driver summary**, and then press ENTER.
11. Choose **Continue** in **Options**.
12. Choose **Continue** from **Protocol Options** unless you want to configure and bind protocols before continuing. The installation is now complete.

Viewing or Modifying Adapter Properties

When an adapter configuration is saved, the NetWare installation program adds load and bind statements to the Autoexec.ncf file. By accessing this file, you can view and modify properties or add properties for each network adapter.

 **NOTE:** The Novell monitor program and the **config** command are also useful for viewing driver configuration properties. For information on how to use these programs, see the *Utilities Reference* in your Novell NetWare online documentation.

The properties that can be defined in the load statements are described below:

Configuration Properties for the B57.lan driver

TxDescriptors=

Initializes Descriptor resources on the adapter for transmits.

Min = 100

Max = 512

Default = 120

RxBuffers=

This is to pre-allocate receive ECBs & Receive adapter resources. This setting may be affected by the NetWare Server maximum/minimum packet receive buffer settings.

Min = 32

Max = 1000

Default = 200

Speed=

This keyword forces the line speed of the adapter. When this keyword is used, the switch to which the adapter cable is connected must be forced. Otherwise, the adapter and switch may run at different duplex modes. It is important to have the switch and adapter set properly. The best way to ensure good connectivity is to not set the speed keyword and allow for automatic link setup (auto-negotiation).

AUTO

10FD

10HD

100FD

100HD

The default setting is AUTO. Note that 1000 Mbit/s speed is auto-detected and cannot be forced. Forced 1000 Mbit/s speed is not needed for copper links. Auto-negotiation is the proper supported configuration under the IEEE specification.

Link=

This keyword is set to AUTO to allow the adapter to auto-negotiate with a switch using the speed keyword as an advertised speed upper limit. It is best to allow for auto-negotiation of the adapter and switch by not setting this keyword or the Speed keyword.

AUTO

FORCE

The default is AUTO. When set to FORCE, auto-negotiation is disabled and the link speed is forced to a specific value.

RxTicks=

Enables the use of batching receives within a specific time period.

Min = 0 (disabled)

Max = 5000000 (5 seconds)

Units are in microseconds and the default value is 300.

TxTicks=

Enables the use of a transmit tick threshold interrupt within a specific time period.

Min = 0 (disabled)

Max = 5000000 (5 seconds)

Units are in microseconds. The default value is 200.

TxPacketsPer=

Enables allowing an interrupt to occur after a specific amount of packets is transmitted.

Min = 0 (disabled)

Max = 100

The default value is 20.

RxPacketsPer=

Enables allowing an interrupt to occur after a specific amount of packets is received.

Min = 0 (disabled)

Max = 100

The default value is 75.

Checksum=

Enables or disables the transmit and receive checksum offload feature. Checksum offload support is only for TCP/IP packets; therefore, the default setting for checksum offload is OFF.

OFF

ON

TX

RX

TxFLOW=

This keyword allows enabling/disabling of transmit flow control.

ON

OFF (default)

RxFLOW=

This keyword allows enabling/disabling of receive flow control.

ON

OFF (default)

PDriver=

Enables the driver to operate in persistent driver mode. Use only if the adapter is placed in a hot-plug slot and only if you must swap with an adapter that is exactly the same.

OFF (default)

ON

NODE=

Allows an input Ethernet node address to replace the adapter factory-programmed Ethernet node address until a subsequent reboot.

NODE=*nnnnnnnnnnnn*

FRAME=

Specifies the frame type. The default value is ETHERNET_802.2.

ETHERNET_II

ETHERNET_802.3

ETHERNET_802.2

ETHERNET_SNAP

SLOT=

Used to set a system-wide unique hardware instance number (HIN) that may be the physical slot number on a slot-based bus such as PCI.

SLOT=*n*

Jumbo=

Enables jumbo frame support. When enabled, jumbo packets of up to 9000 bytes are supported.

Jumbo=1536–9100

The default setting is no jumbo packets.

**Notes:**

- Jumbo frames are supported only on NetWare 6.0 and later. Also, the first frame loaded must be ETHERNET_II.
- Jumbo frame support must have the following text in the Startup.ncf file: Set maximum physical receive packet size = 18000

P3=

This keyword is used when running Perform3.exe tests and may be used to increase performance on networks running with many IPX clients.

P3=1 when running the Perform3 test back to back to a single client

P3=2 when running the Perform3 test with many clients

The default setting is P3=0.

Spuriousfix=

When this keyword is set to 1 (Spurious Fix is ON), the spurious interrupts count that is sometimes displayed on the NetWare console may be reduced. Setting this keyword to 0 (Spurious Fix is OFF) may enhance performance.

Spuriousfix=0 (Spurious Fix is OFF)

Spuriousfix=1 = (Spurious Fix is ON) (default)

Poll=

Disables the interrupt driven mode. When set to Poll=1, the driver does not use interrupts, but is polled by the NetWare operating system. This is a common feature supported in NetWare. The poll mode may increase driver performance in some environments.

0 = OFF (default)

1 = ON

Wirespeed=

Provides adapter link and data integrity even if the adapter is attached to a questionable cable and/or switch. For example, an adapter that is trying to connect at 1000 Mbit/s on a Category 3 cable ordinarily would not link. With Wirespeed= set to 1, the link is made at 100 Mbit/s.

0 = OFF

1 = ON (default)

Model=

Allows the addition of a subsystem ID of a specific adapter so that the driver loads only on the first adapter found with a matching subsystem ID. For example, Model=0x14E4. The default value is 0

Fiber=

The driver has support for the 1000FD fiber adapter. The fiber auto-negotiates link with a fiber switch even though it only supports 1000FD. In some cases, the user may want to force the adapter to 1000FD.

AUTO (default)

FORCE

 **NOTE:** If you modify any of the adapter properties, you must reboot the system before the changes take effect. If you make changes and do not reboot, you may experience problems.

A valid Autoexec.ncf file is shown below. One set of **load** and **bind** commands (in **bold**) is added for each frame type the adapter is configured to support.

```

SET Daylight Savings Time Offset = 1:00:00
SET Start Of Daylight Savings Time = (MARCH SUNDAY LAST 2:00:00 AM)
SET End Of Daylight Savings Time = (OCTOBER SUNDAY LAST 2:00:00 AM)
SET Time Zone = TPST8TPDT
# Note: The Time zone information mentioned above
# should always precede the SERVER name.
# WARNING!!
FILE SERVER NAME DL760
# WARNING!!
# If you change the name of this server, you must update
# the server name in all the licenses that are assigned
# to it using iManager.
SERVERID 487B10D
LOAD ODINEB.NLM
LOAD IPXRTR
LOAD IPXRTRNM
LOAD TCPIP
LOAD B57 SLOT=2 FRAME=Ethernet_802.2 NAME=B57_1_E82
BIND IPX B57_1_E82 NET=FAFD3D25
LOAD B57 SLOT=2 FRAME=Ethernet_802.3 NAME=B57_1_E83
BIND IPX B57_1_E83 NET=5A2D8D6D
LOAD B57 SLOT=2 FRAME=Ethernet_SNAP NAME=B57_1_ESP
BIND IPX B57_1_ESP NET=477A35BD
LOAD B57 SLOT=2 FRAME=Ethernet_II NAME=B57_1_EII
BIND IPX B57_1_EII NET=C3C8F2E4
BIND IP B57_1_EII ADDR=172.16.1.1 MASK=ff.ff.ff.0
mount all
SEARCH ADD SYS:\JAVA\BIN
SEARCH ADD SYS:\JAVA\NWGFX

```

Removing Drivers from Autoexec.ncf

To remove the drivers from the Autoexec.ncf file, locate the **load** and **bind** command lines associated with the Broadcom driver and remark them out by inserting the # symbol at the beginning of each command line, or by deleting the statement.

Example:

```
# LOAD B57 SLOT=2 FRAME=Ethernet_802.2 NAME=B57_1_E82
# BIND IPX B57_1_E82 NET=FAFD3D25
# LOAD B57 SLOT=2 FRAME=Ethernet_802.3 NAME=B57_1_E83
# BIND IPX B57_1_E83 NET=5A2D8D6D
# LOAD B57 SLOT=2 FRAME=Ethernet_SNAP NAME=B57_1_ESP
# BIND IPX B57_1_ESP NET=477A35BD

# LOAD B57 SLOT=2 FRAME=Ethernet_II NAME=B57_1_EII
# BIND IPX B57_1_EII NET=C3C8F2E4
# BIND IP B57_1_EII ADDR=172.16.1.1 MASK=ff.ff.ff.0
```

 **NOTE:** If you modify the Autoexec.ncf file, you must reboot the server before the changes take effect.

3.6.2 Broadcom Advanced Server Program Driver Software (NetWare)

BASP Overview

BASP.LAN is Broadcom's virtual Ethernet driver for NetWare 5.1 and 6.x that provides load balancing, fault-tolerance, and VLAN features. These features are provided by creating teams (virtual adapters) that consist of multiple NIC interfaces. A team can consist of one to six (eight on some systems) NIC interfaces and each interface can be designated primary or standby*. All primary interfaces in a team will participate in Load-balancing operations by sending and receiving a portion of the total traffic**. Standby interfaces will take over in the event that all primary interfaces have lost their links. VLANs can be added to a team to allow multiple VLANs with different VLAN IDs to share the virtual adapter.

Load-balancing and fault-tolerance features work with any third-party NIC adapters. VLANs only work with Broadcom or Alteon NIC adapters.

*Standby can only be used in Smart Load-Balance mode (See below).

**In IEEE 802.3ad mode, the number of NIC interfaces aggregated is automatically determined through LACP (see below).

Balance Modes and Limitations

Smart Load-balance (SLB) is a protocol-specific scheme and the level of support for IP, IPX, and other protocols are listed below.

Protocol	Load Balancing Support	Fault Tolerance Support
IP	Yes	Yes
IPX	Yes*	Yes**
Other protocols	No	Yes**

*Only outbound load-balancing for IPX (on NetWare only).

**Only for Broadcom NICs. Alteon's driver ALT.LAN must be version 2.05b or newer released by Broadcom.

SLB works with all Ethernet switches without configuring the switch ports to any special trunking mode. Only IP traffic is load-balanced in both inbound and outbound directions. IPX traffic will be load-balanced in outbound direction only. Other protocol packets will be sent and received through one primary NIC only. Fault-tolerance for non-IP traffic is only supported using Broadcom or Alteon NICs.

The Generic Trunking mode requires the Ethernet switch to support some form of port trunking mode (Cisco's Gigabit EtherChannel or other switch vendor's link aggregation mode). Trunking mode must be statically configured on the switch ports that are connected to the team. This mode is protocol-independent and all traffic should be load-balanced and fault-tolerant.

The IEEE 802.3ad mode requires the Ethernet switch to support IEEE 802.3ad with LACP (Link Aggregation Control Protocol). LACP will try to configure the maximum number of NICs in the team that are compatible for link aggregation. If LACP determines that some NICs are not able to aggregate (because of some restrictive limitations or configurations on the switch), the remaining NICs that cannot aggregate will be idle. If LACP is completely disabled on the switch, then only one of the NICs in the team will be used. Some switches require the LACP ports to be in full-duplex mode for them to work. LACP can be configured active or passive on the team and most switches allow active or passive selections on a per port basis. At least one side of each connection must be active otherwise the connection will never be selected for

aggregation. This mode is also protocol-independent and all traffic should be load-balanced and fault-tolerant.

NESL Compliance

For optimum fault tolerance and recovery operations, the `BASP.LAN` driver relies on the adapter drivers to generate NetWare Event Service Layer (NESL) events during link changes and other failure events. NESL is an optional feature in the ODI driver specification, and not all drivers support it. For NESL events to propagate properly to the `BASP.LAN` driver, the `ODINEB.NLM` driver must be loaded before the NESL-compliant ODI drivers are loaded.

Do the following to check if an adapter driver supports NESL events: Load the `BASP.LAN` driver and create a team by binding the adapter to the virtual slot (see the following instructions and examples). In the Virtual Adapter X Team Members console, the link status of all bound adapters is shown. Disconnect or connect the adapter cable. If the adapter driver supports NESL events, the link status should change immediately.

Loading Broadcom Advanced Server Program

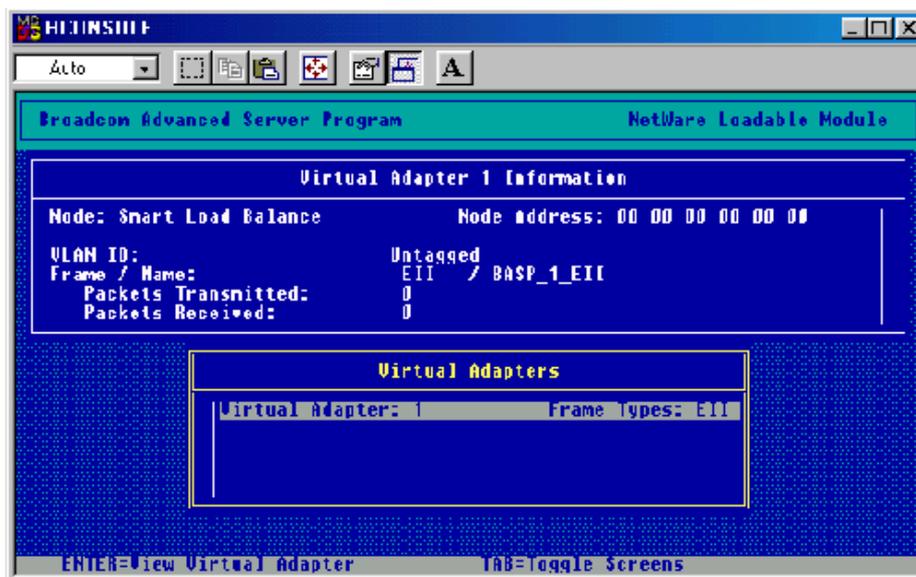
1. Load the `BASP.LAN` driver just as you would a standard LAN driver with all necessary frame types for the team. The `BASP.LAN` driver requires a special `VSLOT` parameter to specify the virtual slot. The virtual slot can be viewed as team numbers 1 through 4, which supports up to eight adapters and up to four teams.

NOTES:

- Be sure to load `BASP.LAN` before loading your standard LAN driver.
- The `BASP` configuration procedure also applies when you are adding an adapter by hot plugging.

Example:

```
LOAD BASP.LAN FRAME=ETHERNET_II NAME=BASP_1_EII VSLOT=1
```



2. Load the network drivers for the adapters that are to be on the team. The frame types loaded should be the same for all adapters on the team and the same as those loaded for BASP.LAN in step 1. Do not bind protocols directly to these adapters. Be sure to load ODINEB.NLM (supplied by Novell) before all network drivers are loaded.

Example:

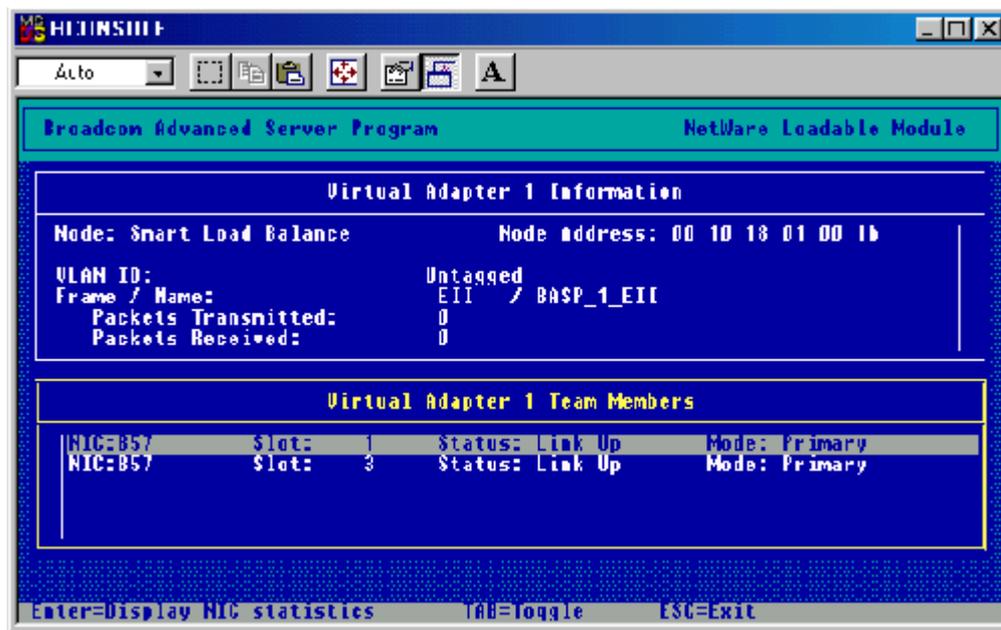
```
LOAD ODINEB.NLM
LOAD B57.LAN FRAME=ETHERNET_II NAME=B57_1_EII SLOT=1
LOAD B57.LAN FRAME=ETHERNET_II NAME=B57_2_EII SLOT=2
```

After BASP.LAN is successfully loaded, a new screen similar to the one above appears. This screen displays all virtual adapter settings and statistics. Press ALT+ESC to switch back to the console and continue with step 3.

1. Bind BASP.LAN to the adapters on the team by using a custom **BASP BIND** command at the console.

Example:

```
BASP BIND BASP_1_EII B57_1_EII
BASP BIND BASP_1_EII B57_2_EII
```

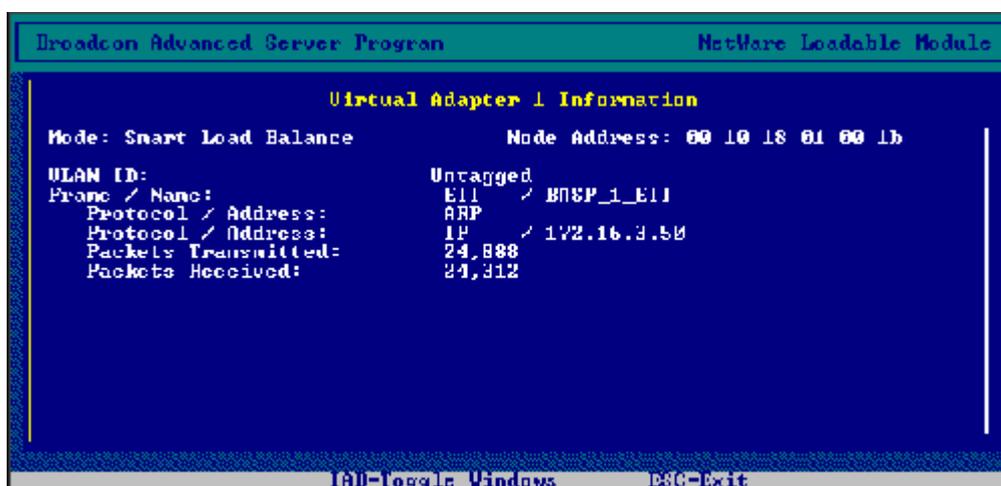


NOTE: If there are multiple frame types loaded on the virtual and the physical adapters, it is necessary to bind only one frame type on the virtual adapter to the same frame type on the physical adapter. The other frame types are automatically bound.

2. Bind protocols to BASP.LAN.

Example:

```
BIND IP BASP_1_EII ADDR=x.x.x.x MASK=x.x.x.x
```



 NOTE: The recommended sequence is to load BASP.LAN before the network drivers as outlined above. This allows BASP.LAN to determine the initial link state of the bound adapters without delay.

Unloading BASP

To unload Broadcom Advanced Server Program, unload the adapter driver and the BASP drivers.

For the adapter driver, at the Command Line Interface (CLI):

```
UNLOAD B57
```

The response is:

```
Module B57.LAN unloaded
```

For the BASP driver, at the Command Line Interface (CLI):

```
UNLOAD BASP
```

The response is:

```
Module BASP.LAN unloaded
```

 NOTE: BASP can not be unloaded if one or more adapters are bound to BASP.

Configuring Teaming

 NOTES:

- Spanning Tree Protocol should be disabled on all switch ports to which teamed adapters are connected.
- If remote management (IPMI) is enabled on a device, the IPMI service could be disrupted when the device is added to a team other than an SLB team.

Balance Mode Selection

Use MODE=SLB for a Smart Load-Balancing type of team, MODE=TRUNK for a Generic Trunking type of team, or MODE=802.3AD for an 802.3ad type of team. The default selection is SLB.

Example:

```
LOAD BASP.LAN FRAME=ETHERNET_II NAME=BASP_1_EII VSLOT=1 MODE=TRUNK
```

NOTES:

- For an SLB type of team, IPX traffic is load-balanced only on the send side, but not on the receive side.
- For optimum fault tolerance and recovery operations, the BASP.LAN driver relies on the adapter drivers to generate NESL (NetWare Event Service Layer) events during link changes and other failure events. NESL is an optional feature in the ODI driver specification and not all drivers support it. For NESL events to propagate properly to BASP.LAN, ODINEB.NLM must be loaded before the NESL compliant ODI drivers are loaded.

Do the following to check if an adapter driver supports NESL events: Load the BASP.LAN driver and create a team by binding the adapter to the virtual slot. Disconnect or connect the adapter cable. The link status of each bound adapter is shown on the Virtual Adapter X Team Members screen of the BASP.LAN menu interface. If the adapter driver supports NESL events, the displayed link status shown on the screen should change immediately.

In IEEE 802.3ad mode, an untagged Ethernet II frame type must be loaded before LACP frames can be transmitted and received. LACP defaults to active for all adapters in the team. Use the parameter LACP=PASSIVE to change LACP to passive mode for all adapters in the team. Note that at least one side (system or switch) must be in LACP active mode for it to work.

Example:

```
LOAD BASP.LAN FRAME=ETHERNET_II NAME=BASP_1_EII VSLOT=1 MODE=802.3AD
LACP=PASSIVE
```

Loading Frame Types

After one or more adapters are bound to a virtual adapter, additional frame types can only be loaded in the virtual adapter if the corresponding frame types are also loaded in the bound

adapters. For example, ETHERNET_802.2 can be loaded in BASP VSLOT 1 if ETHERNET_802.2 is loaded for the B57 driver in SLOT 1 and 2 in the example below. Similarly, a virtual adapter can only be bound to a physical adapter if the physical adapter has all the frame types loaded in the virtual adapter.

Example:

```
LOAD ODINEB.NLM
LOAD BASP.LAN FRAME=ETHERNET_802.2 NAME=BASP_1_E82 VSLOT=1
LOAD B57.LAN FRAME=ETHERNET_802.2 NAME=B57_1_E82 SLOT=1
LOAD B57.LAN FRAME=ETHERNET_802.2 NAME=B57_2_E82 SLOT=2
```

Hot Standby

For a Smart Load Balancing™ (SLB) type of team, only one adapter can be designated as a hot standby member. Use the keyword **standby** in the BASP **bind** command to bind an adapter as a hot standby member.

Example:

```
BASP BIND BASP_1_EII B57_1_EII
BASP BIND BASP_1_EII B57_2_EII STANDBY
```

In the above example, B57_1_EII and B57_2_EII are bound as primary and hot standby members, respectively. Note that a standby member can be used only on a Smart Load Balancing type of team.

 **NOTE:** No traffic is passed to the standby member until the primary member fails

Configuring VLANs

 **NOTES:**

- VLANs are not supported on non-Broadcom adapters. VLANs are supported on the Alteon adapters if the ALT.LAN driver provided by Broadcom is used. If a non-Broadcom adapter is a member of a failover team, VLANs are not supported for that team.
- To avoid failover problems when using BASP, make sure that the spanning tree is disabled on the switch to which the network adapter is connected.

To add VLANs to a team, do the following:

1. Load the BASP.LAN driver with the all necessary frame types and specify the VLAN ID for each frame type. You can specify a maximum of 64 VLAN IDs and each VLAN ID can be loaded up to four times with four different frame types.

Example: **(VLAN ID 2 for Ethernet II)**

```
LOAD BASP.LAN FRAME=ETHERNET_II NAME=BASP_1_V2_EII VSLOT=1 VLAN=2
```

 **NOTE:** When adding 64 VLANs, the 64th VLAN must have a VLAN ID of 0 (63 VLANs are tagged and 1 VLAN is untagged)

2. Load the network drivers for the adapters on the team with all the frame types specified in step 1. Note that the one or more VLAN IDs specified in step 1 do not have to be specified when loading the network drivers. Each frame type loaded in step 1 needs to be loaded only once for each network driver, even if it is loaded multiple times with different VLAN IDs in step 1. Only Broadcom and Alteon NIC adapters can be used. The ALT.LAN driver must be version 2.05b or later (released by Broadcom) and must include the keyword FORVLANS.

Example: **(Broadcom adapters)**

```
LOAD ODINEB.NLM
LOAD B57.LAN FRAME=ETHERNET_II NAME=B57_1_EII SLOT=1
LOAD B57.LAN FRAME=ETHERNET_II NAME=B57_2_EII SLOT=2
```

Example: **(Alteon adapters)**

```
LOAD ODINEB.NLM
LOAD ALT.LAN FRAME=ETHERNET_II NAME=ALT_1_EII SLOT=1 FORVLANS
LOAD ALT.LAN FRAME=ETHERNET_II NAME=ALT_2_EII SLOT=2 FORVLANS
```

3. Bind BASP.LAN to the NIC adapters in the team for each protocol.

Example:

```
BASP BIND BASP_1_V2_EII B57_1_EII
BASP BIND BASP_1_V2_EII B57_2_EII
```

If there are multiple VLANs (each with one or more frame types) loaded on the virtual adapter, it is only necessary to bind one frame type on one VLAN on the

virtual adapter to the same frame type on the physical adapter. The other VLANs are automatically bound.

4. Bind protocols to BASP.LAN.

Example:

```
BIND IP BASP_1_V2_EII ADDR=x.x.x.x MASK=x.x.x.x
```

This example creates a team with two adapters using VLAN ID 2. Outbound packets are tagged with VLAN ID 2, and only similarly-tagged packets can be received by the adapters on the team. Additional VLANs with different VLAN IDs can be created on the same team. The maximum number of VLANs per virtual slot is 64. The valid range of values for VLAN IDs is from 1 to 4094. VLAN=0 indicates the VLAN is untagged and is the default. Use decimal numbers to specify the VLAN ID.

The following are examples of multiple VLAN configurations:

```
LOAD BASP FRAME=ETHERNET_II NAME=BASP_1_V100_EII VSLOT=1 VLAN=100
LOAD BASP FRAME=ETHERNET_II NAME=BASP_1_V200_EII VSLOT=1 VLAN=200
LOAD BASP FRAME=ETHERNET_II NAME=BASP_1_V300_EII VSLOT=1 VLAN=300
LOAD ODINEB.NLM
LOAD B57 FRAME=ETHERNET_II NAME=B57_1_EII SLOT=1
LOAD B57 FRAME=ETHERNET_II NAME=B57_2_EII SLOT=2
BASP BIND BASP_1_V100_EII B57_1_EII
BASP BIND BASP_1_V100_EII B57_2_EII
BIND IP BASP_1_V100_EII ADDR=172.16.210.1 MASK=255.255.0.0
BIND IP BASP_1_V200_EII ADDR=172.17.210.1 MASK=255.255.0.0
BIND IP BASP_1_V300_EII ADDR=172.18.210.1 MASK=255.255.0.0
```

NOTES:

- When `BASP BIND BASP_1_V100_EII B57_1_EII` is executed, the adapter `B57_1_EII` is bound to all three VLANs.
- If you are unable to log on to the system after configuring BASP, add the following command lines before loading BASP:

```
UNLOAD SLPTCP
LOAD SLPTCP
```

Jumbo Frames

Jumbo Frames are supported in all load balancing types of teams. The maximum frame size is automatically set to the smallest maximum frame size of all adapters in the team. Use appropriate keywords to enable Jumbo Frames when loading the adapter drivers.

Example:

```
startup.ncf
SET MAXIMUM PHYSICAL RECEIVE PACKET SIZE=18000
autoexec.ncf
LOAD BASP.LAN FRAME=ETHERNET_II NAME=BASP_1_EII VSLOT=1
LOAD B57.LAN FRAME=ETHERNET_II NAME=B57_1_EII SLOT=1 JUMBO=9000
LOAD B57.LAN FRAME=ETHERNET_II NAME=B57_2_EII SLOT=2 JUMBO=9000
BASP BIND BASP_1_EII B57_1_EII
BASP BIND BASP_1_EII B57_2_EII
```

Additional Command Line Keywords

CHECKSUM = ON

Enables BASP.LAN to offload TCP/UDP and IP checksums to the bound adapters (if supported by the operating system). This setting improves performance if some or all adapters in the team support hardware checksums. Be sure to load the adapter drivers with hardware checksums enabled.

Example:

A team of two BCM5700 NICs with hardware checksums enabled.

```
LOAD BASP.LAN FRAME=ETHERNET_II NAME=BASP_1_EII CHECKSUM=ON VSLOT=1
LOAD ODINEB.NLM
LOAD B57.LAN FRAME=ETHERNET_II NAME=B57_1_EII CHECKSUM=ON SLOT=1
LOAD B57.LAN FRAME=ETHERNET_II NAME=B57_2_EII CHECKSUM=ON SLOT=2
BASP BIND BASP_1_EII B57_1_EII
BASP BIND BASP_1_EII B57_2_EII
```

NOSCREEN

Disables the menu-driven screen when BASP.LAN is loaded for the first time.

Example:

```
LOAD BASP.LAN FRAME=ETHERNET_II NAME=BASP_1_EII VSLOT=1 NOSCREEN
```

GVRP

Enables GVRP (GARP VLAN Registration Protocol) for the VLAN that is loaded. An untagged IEEE 802.2 frame type must be loaded in the virtual adapter and all bound physical adapters for GVRP to take effect. This is necessary because GVRP uses untagged 802.2 frames to advertise VLAN memberships. Use VLAN=0 FRAME=ETHERNET_802.2 in the load command to specify untagged IEEE 802.2 frame type.

Example:

```
LOAD BASP.LAN FRAME=ETHERNET_II NAME=BASP_1_V2_EII VSLOT=1 VLAN=2 GVRP
LOAD BASP.LAN FRAME=ETHERNET_802.2 NAME=BASP_1_E82 VSLOT=1 VLAN=0
```

Editing the Autoexec.ncf File

When an adapter configuration is saved, the NetWare install program adds load and bind statements to the Autoexec.ncf file. By accessing this file, you can verify the parameters configured for each adapter, add or delete parameters, or modify parameters.

A valid autoexec.ncf file is shown below with various VLAN and teaming examples.

Example:

```
# Team of 2 NIC adapters with frame type Ethernet_II and one VLAN, number
2
```

```
# Load BASP.LAN with the frame types and VLAN ID(s) specified.
```

```
LOAD ODINEB.NLM
```

```
LOAD BASP.LAN FRAME=ETHERNET_II NAME=BASP_1_V2_EII VSLOT=1 VLAN=2
```

```
# Load the network drivers for the NIC adapters in the team with the same
# frames types.
```

```
LOAD B57.LAN FRAME=ETHERNET_II NAME=B57_1_EII SLOT=1
```

```
LOAD B57.LAN FRAME=ETHERNET_II NAME=B57_2_EII SLOT=2
```

```
# Bind BASP.LAN to the NIC adapters in the team for each protocol.
```

```
BASP BIND BASP_1_V2_EII B57_1_EII
```

```
BASP BIND BASP_1_V2_EII B57_2_EII
```

```
#Bind protocols to BASP.LAN.
```

```
BIND IP BASP_1_V2_EII ADDR=192.168.2.200 MASK=255.255.255.0
```

Example:

```
# Team of 2 NIC adapters with frame type Ethernet_II and three VLANs,  
number 2,3,4
```

```
#Load BASP.LAN with the frame types and VLAN ID(s) specified.
```

```
LOAD ODINEB.NLM
```

```
LOAD BASP.LAN FRAME=ETHERNET_II NAME=BASP_1_V2_EII VSLOT=1 VLAN=2
```

```
LOAD BASP.LAN FRAME=ETHERNET_II NAME=BASP_1_V3_EII VSLOT=1 VLAN=3
```

```
LOAD BASP.LAN FRAME=ETHERNET_II NAME=BASP_1_V4_EII VSLOT=1 VLAN=4
```

```
# Load the network drivers for the NIC adapters in the team with the same  
# frame types and VLANs specified.
```

```
LOAD B57.LAN FRAME=ETHERNET_II NAME=B57_1_EII SLOT=1
```

```
LOAD B57.LAN FRAME=ETHERNET_II NAME=B57_2_EII SLOT=2
```

```
# Bind BASP.LAN to the NIC adapters in the team for each protocol
```

```
# NOTE: BASP BIND is only used for the first VLAN all other VLANs are  
automatically
```

```
# bound to the virtual adapter (VSLOT=1).
```

```
BASP BIND BASP_1_V2_EII B57_1_EII
```

```
BASP BIND BASP_1_V2_EII B57_2_EII
```

```
# Bind protocols to BASP.LAN.
```

```

BIND IP BASP_1_V2_EII ADDR=192.168.2.200 MASK=255.255.255.0
BIND IP BASP_1_V3_EII ADDR=192.168.3.200 MASK=255.255.255.0
BIND IP BASP_1_V4_EII ADDR=192.168.4.200 MASK=255.255.255.0

```

```
mount all
```

 **NOTE:** If you modify any adapter parameters, you must reboot the system before the changes take effect. If you make changes and do not reboot, you may experience configuration problems.

Example of Multiple SLB TEAMS with Multiple Frame Types

```

LOAD BASP.LAN FRAME=ETHERNET_II NAME=BASP_1_EII VSLOT=1
LOAD BASP.LAN FRAME=ETHERNET_802.2 NAME=BASP_1_E82 VSLOT=1
LOAD BASP.LAN FRAME=ETHERNET_II NAME=BASP_2_EII VSLOT=2
LOAD BASP.LAN FRAME=ETHERNET_802.3 NAME=BASP_2_E83 VSLOT=2
LOAD B57.LAN FRAME=ETHERNET_II NAME=B57_1_EII SLOT=1
LOAD B57.LAN FRAME=ETHERNET_802.2 NAME=B57_1_E82 SLOT=1
LOAD B57.LAN FRAME=ETHERNET_II NAME=B57_2_EII SLOT=2
LOAD B57.LAN FRAME=ETHERNET_802.2 NAME=B57_2_E82 SLOT=2
LOAD B57.LAN FRAME=ETHERNET_II NAME=B57_3_EII SLOT=3
LOAD B57.LAN FRAME=ETHERNET_802.3 NAME=B57_3_E83 SLOT=3
LOAD B57.LAN FRAME=ETHERNET_II NAME=B57_4_EII SLOT=4
LOAD B57.LAN FRAME=ETHERNET_802.3 NAME=B57_4_E83 SLOT=4
BASP BIND BASP_1_EII B57_1_EII
BASP BIND BASP_1_EII B57_2_EII
BASP BIND BASP_2_EII B57_3_EII
BASP BIND BASP_2_EII B57_4_EII
BIND IP BASP_1_EII ADDR=172.16.1.100 MASK=255.255.0.0
BIND IPX BASP_1_E82 NET=ABAB
BIND IP BASP_2_EII ADDR=172.18.1.100 MASK=255.255.0.0
BIND IPX BASP_2_E83 NET=BEEF

```

 **NOTE:** When B57_1_EII is bound to BASP_1_EII, B57_1_E82 is also bound to BASP_1_E82. IPX load balance works only with an all-Broadcom adapter or an all-Alteon adapter configuration. Values for VLSOT range from 1 to 4 (only four teams can be configured).

Example of VLAN with BASP

```

LOAD ODINEB.NLM
LOAD BASP.LAN FRAME=ETHERNET_II NAME=BASP_1_V100_EII VSLOT=1 VLAN=100
LOAD BASP.LAN FRAME=ETHERNET_II NAME=BASP_1_V200_EII VSLOT=1 VLAN=200
LOAD BASP.LAN FRAME=ETHERNET_II NAME=BASP_1_V300_EII VSLOT=1 VLAN=300
LOAD B57.LAN FRAME=ETHERNET_II NAME=B57_1_EII SLOT=1
LOAD B57.LAN FRAME=ETHERNET_II NAME=B57_2_EII SLOT=2
BASP BIND BASP_1_V100_EII B57_1_EII
BASP BIND BASP_1_V100_EII B57_2_EII
BIND IP BASP_1_V100_EII ADDR=172.16.210.1 MASK=255.255.0.0
BIND IP BASP_1_V200_EII ADDR=172.17.220.1 MASK=255.255.0.0
BIND IP BASP_1_V200_EII ADDR=172.18.230.1 MASK=255.255.0.0

```

 **NOTE:** When B57_1_V100_EII is bound to B57_1_EII, B57_1_EII is also bound to the other VLANs on the same VSLOT. VLAN refers to the VLAN ID, and valid value for VLAN ID ranges from 1 to 4094.

Example of TRUNKING with BASP

```

LOAD ODINEB.NLM
LOAD BASP.LAN FRAME=ETHERNET_II NAME=BASP_1_EII VSLOT=1 MODE=TRUNK
LOAD B57.LAN FRAME=ETHERNET_II NAME=B57_1_EII SLOT=1
LOAD B57.LAN FRAME=ETHERNET_II NAME=B57_2_EII SLOT=2
BASP BIND BASP_1_EII B57_1_EII
BASP BIND BASP_1_EII B57_2_EII
BIND IP BASP_1_EII ADDR=172.16.210.1 MASK=255.255.0.0

```

 **NOTE:** Switch ports must be configured for trunking (for example: FEC or GEC for Cisco switches)

Example of GVRP with BASP

```

LOAD ODINEB.NLM
LOAD BASP.LAN FRAME=ETHERNET_II NAME=BASP_1_EII VSLOT=1 VLAN=100 GVRP
LOAD BASP.LAN FRAME=ETHERNET_802.2 NAME=BASP_1_E82 VSLOT=1
LOAD B57.LAN FRAME=ETHERNET_II NAME=B57_1_EII SLOT=1
LOAD B57.LAN FRAME=ETHERNET_802.2 NAME=B57_1_E82 SLOT=1
LOAD B57.LAN FRAME=ETHERNET_II NAME=B57_2_EII SLOT=2
LOAD B57.LAN FRAME=ETHERNET_802.2 NAME=B57_2_E82 SLOT=2
BASP BIND BASP_1_EII B57_1_EII

```

```
BASP BIND BASP_1_EII B57_2_EII BIND IP BASP_1_EII ADDR=172.16.210.1
MASK=255.255.0.0
```

NOTES:

- In this example, VLAN 100 is advertised to the switch using GVRP.
- The untagged 802.2 frame must be loaded to allow sending and receiving GVRP frames. Switch ports must be configured with GVRP enabled.

Using INETCFG

When INETCFG is used to set up teaming, the physical adapters being added to the team must not have any protocols bound to them before they are added to the team. To ensure the proper operation of the team, the physical adapters in a team should have only the BASP protocol bound to them.

Load inetcfg.nlm. When you are prompted, accept the configuration. On the

Internetworking Configuration console:

1. Select **Board**, and then press ENTER.
2. Press INSERT.
3. Select a physical device driver, such as B57.
4. Press ENTER, and then type a name, such as B57_1.
5. Press ESC, and then select **Yes** to save the configuration. Repeat steps 2 through 5 to configure another adapter. Name subsequent adapters B57_2, B57_3, and so on.
6. Press INSERT.
7. Select a virtual device driver, such as BASP.
8. Press ENTER, and then type a name, such as BASP_1. In this console, **virtual slot number**, **Balance Mode**, and **VLAN ID** can be selected.

NOTES:

- The first virtual adapter (TEAM) should have a virtual slot of 1.
 - VLAN 0 (zero) is a default, and this VLAN is untagged.
9. Press ESC, and then select **Yes** to save the configuration.
 10. Scroll down to **Protocols**, and then press ENTER to select.
 11. Scroll down to **User-specified Protocol**, and then press ENTER to select.

12. Press INSERT.
13. Type the name for the protocol, such as `BASP1` for TEAM 1, `BASP2` for TEAM 2, `BASP3` for TEAM 3, or `BASP4` for TEAM 4.
14. Press ESC to return to the **Internetworking Configuration** console.
15. Select **Bindings**.
16. Press INSERT to configure the protocol.
17. Select **TCP/IP**, then press ENTER.
18. Select **A Network Interface**, then press ENTER.
19. Select a virtual adapter (`BASP`, for example).
20. Define the IP address.
21. Press ESC, and then select **Yes** to save.

Repeat steps 16 through 21 to configure IPX and multiple frame types.

 **NOTE:** The physical adapters must be configured with the same frame types as the virtual team

1. Press INSERT to bind the physical adapter to a virtual team.
2. Select **User-specified Protocol**.
3. Select **A Network Interface**, and then press ENTER.
4. Select a physical adapter (`B57`, for example).
5. Type `BASP1` for Protocol.
6. Select a frame type, type any special parameters (refer to `B57.LAN readme.txt` for parameters), press ESC, then select **Yes** to save.

 **NOTES:**

- Use names such as `BASP1` for TEAM 1, `BASP2` for TEAM 2, `BASP3` for TEAM 3 and `BASP4` for TEAM 4.
- When you modify a team, you may need to reboot after reinitialization for the changes to take effect.

Repeat steps 22 through 27 to configure an additional physical driver and to configure additional frame types. The configuration can be viewed in the **View Configuration - All INETCFG Commands** console.

3.6.3 SNMP Agent

This SNMP agent is designed to support the configuration information pertaining to the Broadcom BASP driver for NetWare.

Installation

When the BASP.LDI driver is installed using **nwconfig** or **nwinstall**, the driver automatically copies the BASP.LAN, bmapl.nlm, and bsnmp.nlm files to the system.

After you configure and run the BASP and bind the BASP to network adapters, load the Broadcom SNMP Instrumentation Agent (BSNMP) as follows:

From the NetWare Server console command line interface, type:

```
load bmapl.nlm
load bsnmp.nlm
```

SNMP Objects

BASP SNMP objects are provided in the BASP-Config.MIB file, which is on your installation CD. The **snmpget** and **snmpgetnext** commands can be used to receive the BASP SNMP objects such as:

```
snmpget localhost public BASP-Config-MIB::btTeamNumber
snmpgetnext localhost public BASP-Config-MIB::btTeamNumber
```

 **NOTE:** Only BASP configuration information is available through SNMP in NetWare. Statistical events are only available for the base adapters

Files

- BASP.LAN
- bmapl.nlm
- bsnmp.nlm
- BASP-CONFIG.MIB

3.7 Windows Driver Software

3.7.1 Installing the Driver Software

 **NOTE:** If your adapter was installed at the factory, the driver software has been installed for you.

When Windows first starts after a hardware device (such as a D-Link NetXtreme Gigabit Ethernet adapter) has been installed, or after the existing device driver has been removed, the operating system automatically detects the hardware and prompts you to install the driver software for that device.

Both a graphical interactive installation mode (see Using the Installer) and a command-line silent mode for unattended installation (see Using Silent Installation) are available.

 **NOTES:**

- Before installing the driver software, verify that the Windows operating system has been upgraded to the latest version with the latest service pack applied.
- A network device driver must be installed before the D-Link NetXtreme Gigabit Ethernet adapter can be used with your Windows operating system. Drivers are located on the installation CD.

Using the Installer

1. **To install the D-Link NetXtreme drivers**When **Found New Hardware Wizard** opens, click **Cancel**.
2. Insert the installation CD into the CD-ROM or DVD drive.
3. On the installation CD, open the folder for your operating system, open the DrvInst folder, and then double-click Setup.exe file to open the InstallShield Wizard.
4. Click **Next** to continue.
5. After you review the license agreement, click **I accept the terms in the license agreement**, and then click **Next** to continue.
6. Select how you want to install the NetXtreme drivers and then click **Next**.
7. Click **Install**.
8. Click **Finish** to close the wizard.
9. The installer will determine if a system restart is necessary. Follow the on-screen instructions.

Using Silent Installation

NOTES:

- All commands are case sensitive.
- User must "Run as Administrator" for Vista when using "msiexec" for "silent" install/uninstall(s).
- For more detailed instructions and information about unattended installs, refer to the Silent.txt file in the DrvInst folder.

To perform a silent install from within the installer source folder

Type the following:

```
setup /s /v/qn
```

-or-

```
msiexec /i "BDrvInst.msi" /qn
```

To perform a silent upgrade from within the installer source folder

Type the following:

```
setup /s /v/qn
```

To perform a silent uninstall from within the installer source folder

Type the following:

```
msiexec /x "BDrvInst.msi" /qn
```

To perform a silent uninstall from any folder

Type the following:

```
msiexec /x "{B7F54262-AB66-44B3-88BF-9FC69941B643}" /qn
```

To perform a silent reinstall of the same installer

Type the following:

```
setup /s /v"/qn REINSTALL=ALL"
```

To perform a GUI reinstall of the same installer

Type the following:

```
setup /V"REINSTALL=ALL"
```

Using the Found New Hardware Wizard

These instructions apply to Windows Server 2003.

1. When **Found New Hardware Wizard** opens, click **No, not this time**, and then click **Next**.
2. Click **Install from a list or specific location (Advanced)**, and then click **Next**.
3. Click **Include this location in the search**, browse to the folder on the installation CD where the drivers are located, and then click **Next**.
4. Click **Finish** to close the wizard.

3.7.2 Updating the Driver Software

To update the driver software

1. Start Windows and log on. You must have administrative privileges to update the driver software.
2. In Control Panel, click **System** to view **System Properties**.
3. Click the **Hardware** tab, and then click **Device Manager**.
4. Right-click the name of the D-Link NetXtreme 5718 Gigabit Ethernet Controller and click **Update Driver**.
5. Follow the on-screen instructions provided by the **Hardware Update Wizard**.
6. Click **Include this location in the search**, browse to the folder on the installation CD where the drivers are located, and then click **Next**.
7. Click **Finish** to close the wizard.

3.7.3 Viewing or Changing the Properties of the Controller

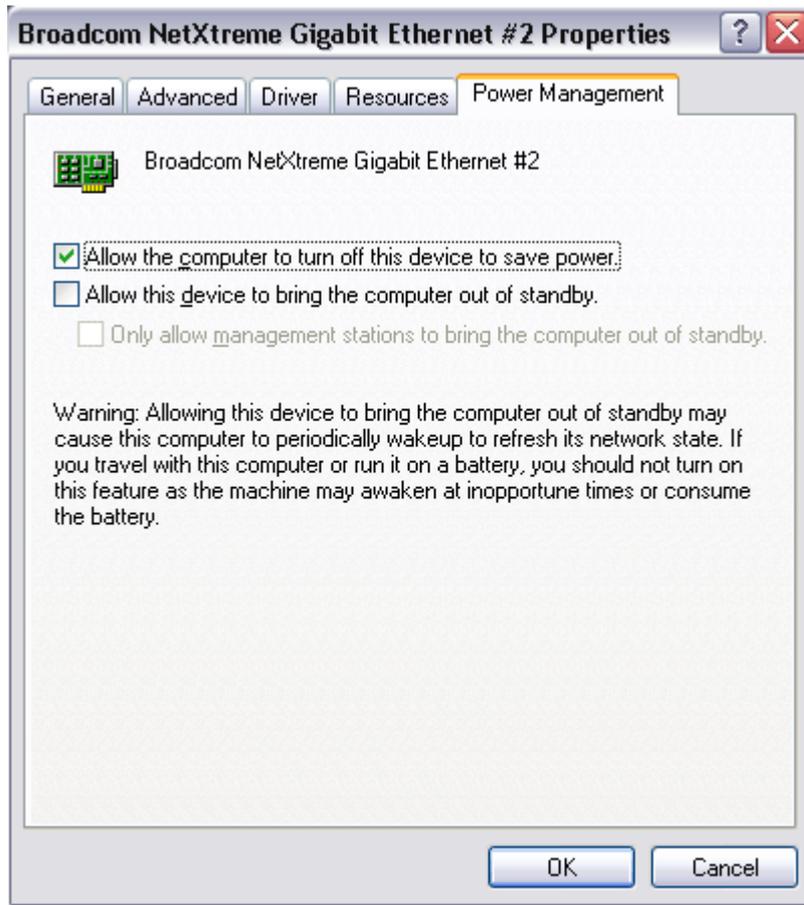
To view or change the properties of the D-Link NetXtreme 5718 Gigabit Ethernet Controller

1. Right-click the **Control Suite** icon in the taskbar notification area, and then click **Launch BACS**.
2. Click the **Advanced** tab.
3. See Setting Adapter Properties for a detailed description of the available properties as well as for instructions for viewing and changing the value of a particular property.

 NOTE: You can also open Broadcom Advanced Control Suite in Control Panel.

3.7.4 Setting Power Management Options

You can set Power Management options to allow the operating system to turn off the adapter to save power. If the device is busy doing something (servicing a call, for example) however, the operating system will not shut down the device. The operating system attempts to shut down every possible device only when the system attempts to go into hibernation. To have the adapter stay on at all times, do not select the **Allow the computer to turn off the device to save power** check box.



NOTES:

- The Power Management tab is available only for systems that support power management.

⚠ CAUTION! Do not select the **Allow the computer to turn off the device to save power** check box for any adapter that is a member of a team.

3.7.5 Removing the Device Drivers

1. Open **Add or Remove Programs** in **Control Panel**.
2. Click **D-Link NetXtreme Ethernet Controller**, and then click **Remove**.
3. Click **Yes** to remove the drivers and management applications.
4. Restart your system.

 NOTE: You can also remove the device drivers by running the InstallShield installer again and clicking **Remove**.

Chapter 4: Installing Management Applications

4.1 Installing Broadcom Advanced Control Suite and Related Management Applications

The Broadcom Advanced Control Suite (BACS) software and related management applications can be installed from the installation CD or by using the silent install option.

The following are installed when running the installer:

- **Control Suite.** Broadcom Advanced Control Suite (BACS).
- **BASP.** Installs Broadcom Advanced Server Program.
- **SNMP.** Installs the Simple Network Management Protocol subagent.

NOTES:

- Ensure that the Broadcom network adapter(s) is physically installed in the system before installing BACS.
- Before you begin the installation, close all applications, windows, or dialog boxes.

4.1.1 Using the Installer

To install the management applications

1. Insert the installation CD into the CD or DVD drive.
2. On the installation CD, open the MgmtApps folder, select IA32 or x64, and then double-click **Setup.exe** to open the InstallShield Wizard.
3. Click **Next** to continue.
4. After you review the license agreement, click **I accept the terms in the license agreement** and then click **Next** to continue.

5. Select the features you want installed. If you receive a warning regarding .NET Framework 2.0, then press OK to continue installing BACS and manually install .NET Framework 2.0 when installation completes, or Cancel to quit.
6. Click **Next**.
7. Click **Install**.
8. Click **Finish** to close the wizard.

4.1.2 Using Silent Installation

NOTES:

- All commands are case sensitive.
- User must "Run as Administrator" for Vista when using "msiexec" for "silent" install/uninstall(s).
- For detailed instructions and information about unattended installs, refer to the Silent.txt file in the MgmtApps folder.

To perform a silent install (or upgrade) from within the installer source folder

Type the following:

```
setup /s /v/qn
```

If performing a silent upgrade, your system may reboot automatically. To suppress the reboot, type the following:

```
setup /s /v"/qn REBOOT=ReallySuppress"
```

To perform a silent install and create a log file

Type the following:

```
setup /s /v"/qn /L f:\ia32\1testlog.txt"
```

The 1testlog.txt log file will be created at f:\ia32.

To perform a silent uninstall from any folder on the hard drive

```
msiexec /x "{26E1BFB0-E87E-4696-9F89-B467F01F81E5}" /qn
```

 NOTES:

- The hexadecimal number above may differ from your current installer. Check the Key name corresponding with the Broadcom Advanced Control Suite (BACS) application in HKLM\Software\Microsoft\Windows\CurrentVersion\Uninstall for the correct hexadecimal number.
- After performing a silent uninstall, it is necessary to reboot the system before reinstalling this installer. If a reboot is not performed, BASP will not install correctly.

To perform a silent install by feature on IA32 platforms

Use ADDSOURCE to include any of the features listed below.

 NOTE: CHM32 or CHM64 installs the BACS help file and must be included when installing the BACS feature.

```
setup /s /v"/qn ADDSOURCE=BACSi32,CHM32,BASPi32,SNMPi32,CIMi32"
```

To perform a silent install by feature on AMD64/EM64T platforms

Type the following:

```
setup /s /v"/qn ADDSOURCE=BACSa64,CHMa64,BASPa64,SNMPa64"
```

To perform a silent install from within a batch file

To perform a silent install from within a batch file and wait for the install to complete before continuing with the next command line, type the following:

```
start /wait setup /s /w /v/qn
```

4.2 Modifying Management Applications

To modify the management applications

1. In Control Panel, double-click **Add or Remove Programs**.
2. Click **Broadcom Management Programs** and then click **Change**.
3. Click **Next** to continue.

4. Click **Modify** to change program features.
5. Click **Next** to continue.
6. Click on an icon to change how a feature is installed.
7. Click **Next**.
8. Click **Install**.
9. Click **Finish** to close the wizard.
10. Reboot your system to complete the modification of the management applications.

4.3 Repairing Management Applications

To repair or reinstall the management applications

1. In Control Panel, double-click **Add or Remove Programs**.
2. Click **Broadcom Management Programs**, and then click **Change**.
3. Click **Next** to continue.
4. Click **Repair** to repair errors in installed applications.
5. Click **Next** to continue.
6. Click **Install**.
7. Click **Finish** to close the wizard.

4.4 Removing Management Applications

To remove all management applications

1. In Control panel, double-click Add or Remove Programs.
2. Click **Broadcom Management Programs**, and then click **Remove**.
3. Reboot your system to complete the removal of management applications.

Chapter 5: Using Broadcom Advanced Control Suite 4

5.1 Broadcom Advanced Control Suite

Overview

Broadcom Advanced Control Suite (BACS) is an integrated utility that provides useful information about each network adapter that is installed in your system. BACS also enables you to perform detailed tests, diagnostics, and analyses on each adapter, as well as to view and modify property values and view traffic statistics for each adapter.

Broadcom Advanced Server Program (BASP), which runs within Broadcom Advanced Control Suite, is used to configure teams for load balancing, fault tolerance, and virtual local area networks (VLANs). BASP functionality is available only on systems that use at least one Broadcom network adapter.

NOTES:

- This chapter introduces all functions of Broadcom Control Suite 4 designed for NetXtreme 57xx family. However, function supports depend on the chip chosen. Please refer to adapter's specification for detail.

5.2 Starting Broadcom Advanced Control Suite

In Control Panel, click **Broadcom Control Suite 4**, or click the BACS icon in the taskbar located at the bottom of the Windows desktop.

5.3 Using Broadcom Advanced Control Suite

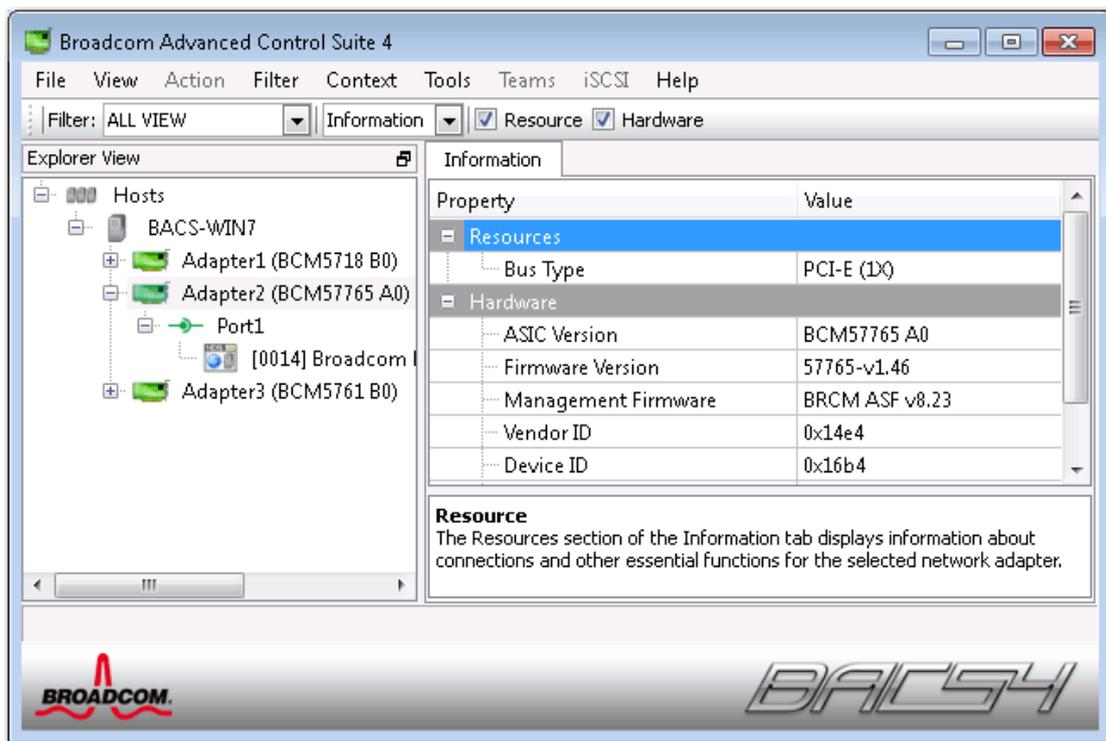
Start BACS. Click the tab that provides the information of interest or from which to perform a desired test, diagnostic, analysis, or set adapter properties. To create a team, see Configuring Teaming.

5.3.1 BACS Interface

The BACS interface is comprised of the following regions:

- Explorer View pane
- Context View selector
- Context View pane
- Menu bar
- Description pane

By default, the Explorer View pane is docked and pinned on the left side of the main window, the Context View pane on the right, the Context View selector below the menu bar, and the Description pane below the Context View pane. Drag the splitter between any two panes to vary the size of the panes.



Explorer View Pane

You can dock and pin the Explorer View pane on the left side, right side, top, or bottom of the main window.

The Explorer View pane lists the objects that can be viewed, analyzed, tested, or configured by BACS. When an item is selected in the Explorer View pane, the tabs showing the information and options that are available for the item appear in the Context View pane.

The organization of this panel is designed to present the manageable objects in the same hierarchical manner as drivers and its subcomponents. This simplifies the management of various elements of the network interface controller (NIC). The top level of the hierarchy is the Host container, which lists all hosts managed by BACS. Below the hosts are the installed network adapters, with the manageable elements, such as physical port, VBD, and NDIS below the adapters.

The icon next to each device in the Explorer View pane shows its status. An icon next to a device name that appears normal means the device is connected and working.

- **X.** A red "X" that appears on the device's icon indicates the device is currently not connected to the network.
- **Greyed out.** A device icon that appears greyed out indicates the device is currently disabled.

Context View Selector

The Context View selector appears below the menu bar and includes the filter and tab categories. Although you can expand and collapse the categories that appear on tabs in the Context View pane, you can alternatively display a category by selecting the box next to the category name.

Filter View

In a multiple-host environment using several network adapters, there can be a large number of manageable elements per adapter that can be difficult and cumbersome to view, configure, and manage all elements. Use the filter to select a particular device function. Possible filter views include:

- All
- Team view
- NDIS view
- iSCSI view
- FCoE view

- iSCSI Target view
- FCoE Target view

Context View Pane

The Context View pane displays all the parameters that you can view for the object selected in the Explorer View pane. The parameters are grouped by tabs and categories, depending on the parameter type. The available tabs are Information, Configuration, Diagnostics, and Statistics. Because the BACS interface is context-sensitive, only the parameters that apply to the selected object can be viewed or configured in the Context View pane.

Menu Bar

The following appear on the menu bar, but because the menu items are context-sensitive, not all items will be available at all times:

File menu

- Team Save As: saves the current team configurations to a file
- Team Restore: restores any saved team configuration from a file

Action menu

- Remove Host: removes the selected host
- Refresh Host: refreshes the information for the selected host

View menu

- Explorer View: displays/hides the Explorer View pane
- Tool Bar: displays/hides the tool bar
- Status Bar: displays/hides the status bar
- Broadcom Logo: displays/hides the Broadcom Logo on BACS to optimize the maximum viewable space

Tools menu

- Options: used for configuring BACS preferences

Teams

- **Create Teams:** creates new teams with either the Teaming Wizard or in Advanced mode
- **Manage Teams:** manages existing teams with either the Teaming Wizard or in Advanced mode

Description Pane

The Description pane provides information, configuration instructions, and options for the selected parameter in the Context View pane.

5.3.2 Configuring Preferences

To enable or disable the BACS tray icon

BACS places an icon in the Windows taskbar when the program is installed. Use the Options window to turn this icon on or off.

1. From the **Tools** menu, select **Options**.
2. Select or clear **Enable BACSTray** (the option is enabled by default).
3. Click **OK**.

Setting the teaming mode

1. From the **Tools** menu, select **Options**.
2. Select **Expert Mode** if you do not need the assistance of the teaming wizard to create teams; otherwise, select **Wizard Mode**.
3. Click **OK**.

Setting the Explorer View refresh time

1. From the **Tools** menu, select **Options**.
2. Select **Auto** to set the Explorer View refresh time to 5 seconds. Otherwise, select **Custom** and select a time, in seconds.
3. Click **OK**.

5.3.3 Connecting to a Host

You can add one or more Windows or Linux hosts to manage from BACS.

To add a local host

1. From the **Action** menu, click **Add Host**.
2. For both Windows and Linux hosts, do not change the default settings. The **User name** and **Password** are not required while connecting to the local host.
3. Select **Persist** if you want BACS to save the information for this host.
4. Click **Ok**. BACS can now be used to view information and manage the host.

To add a remote host

1. From the **Action** menu, click **Add Host**.
2. Type the remote host's name or IP address in the **Host** box.
3. Select the protocol from the **Protocol** list. The protocol options for Windows are **WMI**, **WinRM**, or **Try All**. The protocol options for Linux are **CimXML**, **WinRM**, or **Try All**. The **Try All** option forces the GUI client to try all options.
4. Select the **HTTP** scheme, or the **HTTPS** scheme for added security.
5. Type the **Port Number** value you used to configure the host, if it is different than the default value of **5985**.
6. Type the **User name** and **Password**.
7. Select **Persist** if you want BACS to save the information for this host. The host will appear in the Explorer Pane whenever you reopen BACS, and you will not need to enter the host IP address or host name when connecting to the host. For security reasons, you must enter the **User name** and **Password** every time.
8. Click **OK**.

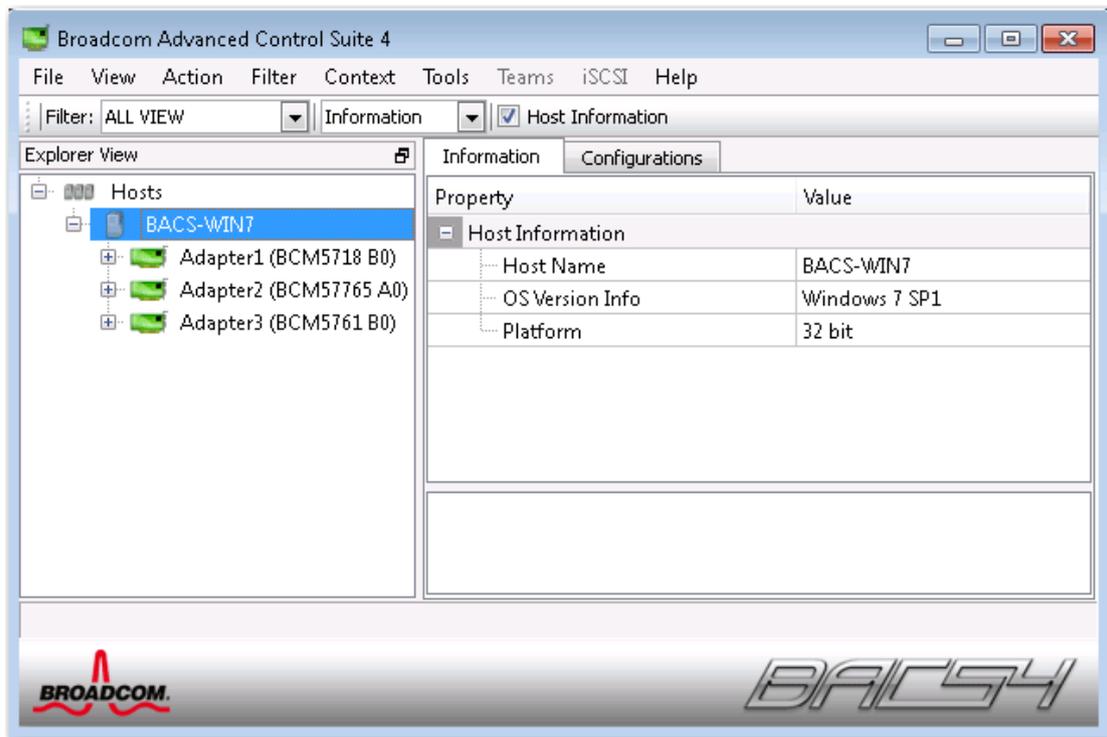
5.3.4 Managing the Host

At the host level, you can view host information and configure parameters from the following tabs:

- Information
- Configuration

To view host information

Select the host in the **Explorer View** pane, and then select the **Information** tab to view host-level information.



Information Tab: Host Information

Host Name

Displays the name of the host.

OS Version Info

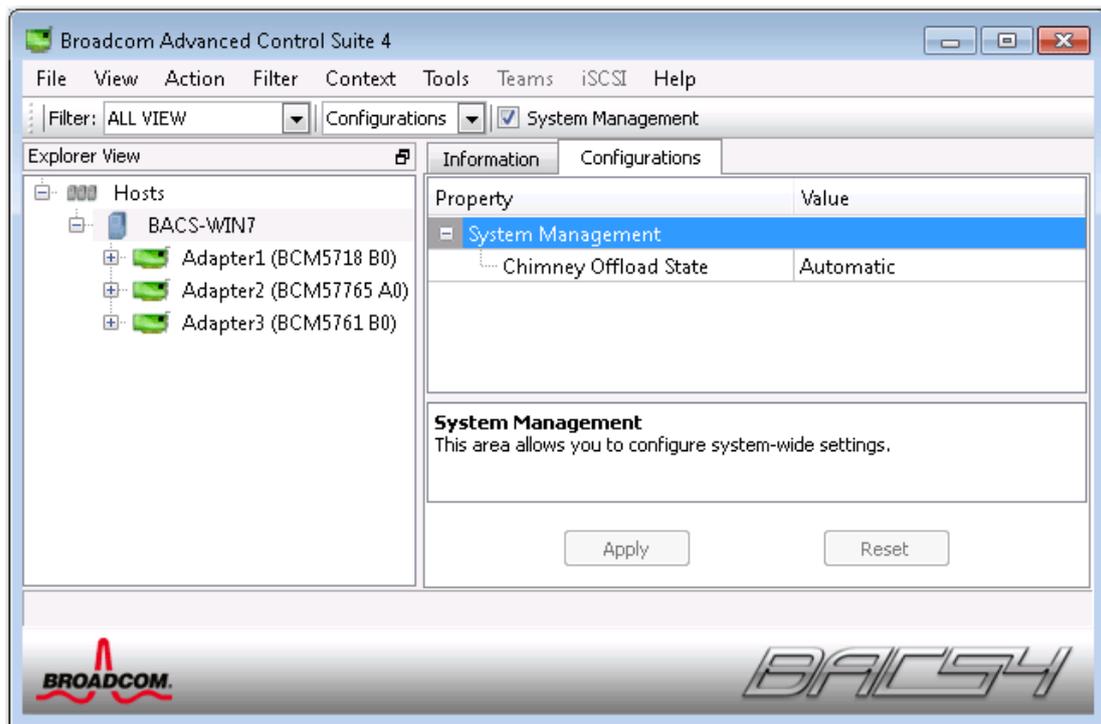
Displays the operating system, including the version.

Platform

Displays the hardware architecture platform (for example, 32-bit or 64-bit)

To configure the host

Select the host in the **Explorer View** pane, and then select the **Configuration** tab to configure host-level parameters.



Configuration Tab: System Management

Chimney Offload State

Enable or disable chimney offload at the host level, rather than at the device level, and then click **Apply**.

5.3.5 Managing the Network Adapter

The installed network adapters appear one level below the host in the hierarchical tree in the Explorer View pane. At the adapter level, you can view information and configure parameters from the following tabs:

- Information
- Configuration

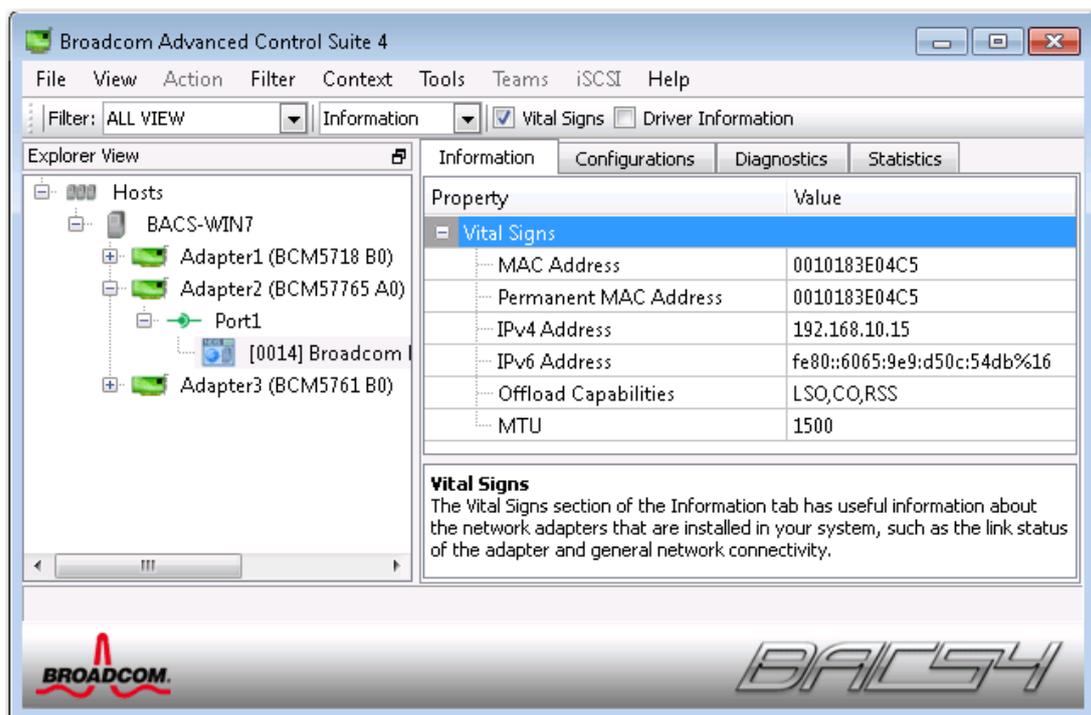
Viewing Adapter Information

The **Vital Signs** section of the **Information** tab has useful information about the network adapters that are installed in your system, such as the link status of the adapter and general network connectivity.

Select the network adapter in the **Explorer View** pane, and then select the **Information** tab to view adapter-level information.

NOTES:

- Information about Broadcom network adapters may be more comprehensive than information about network adapters made by others.
- Some information may not be available for all Broadcom network adapters.



MAC Address

A physical MAC (media access control) address that is assigned to the adapter by the manufacturer. The physical address is never all 0s.

Permanent MAC Address

The unique hardware address assigned to the network adapter.

IP Address

The network address associated with the adapter. If the IP address is all 0s, the associated driver has not been bound with Internet Protocol (IP).

Link Status

The status of the network link.

- **Up.** A link is established.
- **Down.** A link is not established.

Duplex

The adapter is operating in the indicated duplex mode.

Speed (in Mbps)

The link speed of the adapter, in megabits per second.

Offload Capabilities

The offload capabilities supported by the adapter.

This information is only available for D-Link NetXtreme adapters.

- **LSO.** Large Send Offload (LSO) prevents an upper level protocol such as TCP from breaking a large data packet into a series of smaller packets with headers appended to them.
- **CO.** Checksum Offload (CO) allows the TCP/IP/UDP checksums for send and receive traffic to be calculated by the adapter hardware rather than by the host CPU.

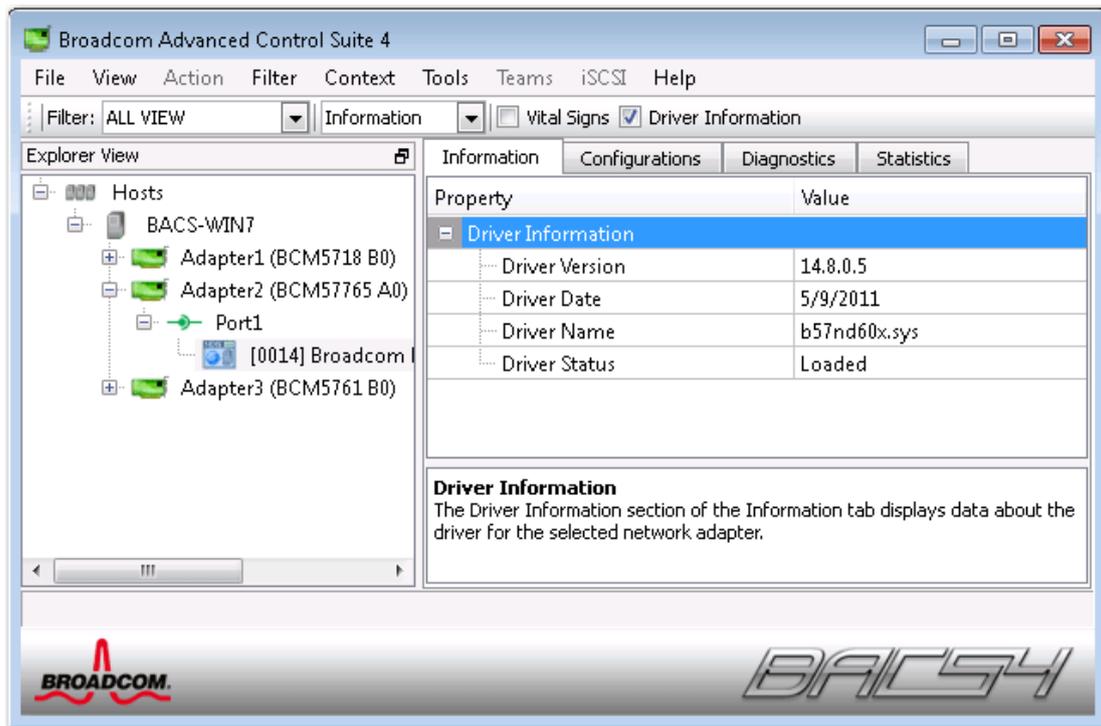
LiveLink IP Address

The network address of the LiveLink enabled adapter.

Viewing Driver Information

The **Driver Information** section of the **Information** tab displays data about the driver for the selected network adapter.

To view Driver Information for any installed network adapter, click the name of the adapter listed in the Explorer View pane, then click the **Information** tab.



Driver Status

The status of the adapter driver.

- **Loaded.** Normal operating mode. The adapter driver has been loaded by Windows and is functioning.
- **Not Loaded.** The driver associated with the adapter has not been loaded by Windows.
- **Information Not Available.** The value is not obtainable from the driver that is associated with the adapter.

Driver Name

The file name of the adapter driver.

Driver Version

The current version of the adapter driver.

Driver Date

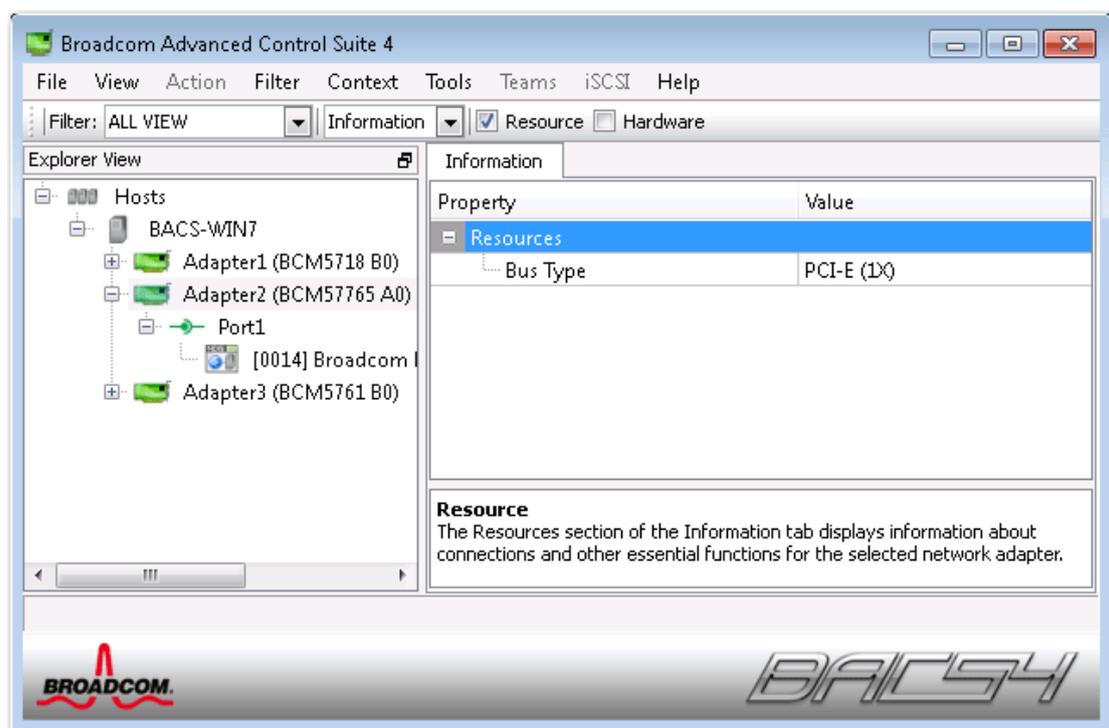
The creation date of the adapter driver.

Viewing Resource Information

The **Resources** section of the **Information** tab displays information about connections and other essential functions for the selected network adapter.

To view Resources for any installed network adapter, click the name of the adapter listed in the Explorer View pane, then click the **Information** tab.

 **Note:** Some information may not be available for all Broadcom network adapters.



Bus Type

The type of input/output (I/O) interconnect used by the adapter.

Slot No

The slot number on the system board occupied by the adapter. This item is not available for PCI Express type adapters.

Bus Speed (MHz)

The bus clock signal frequency used by the adapter. This item is not available for PCI Express type adapters.

Bus Width (bit)

The number of bits that the bus can transfer at a single time to and from the adapter. This item is not available for PCI Express type adapters.

Bus No

Indicates the number of the bus where the adapter is installed.

Device No

The number assigned to the adapter by the operating system.

Function No

The port number of the adapter. For a single-port adapter, the function number is 0. For a two-port adapter, the function number for the first port is 0, and the function number for the second port is 1.

Interrupt Request

The interrupt line number that is associated with the adapter. Valid numbers range from 2 to 25.

Memory Address

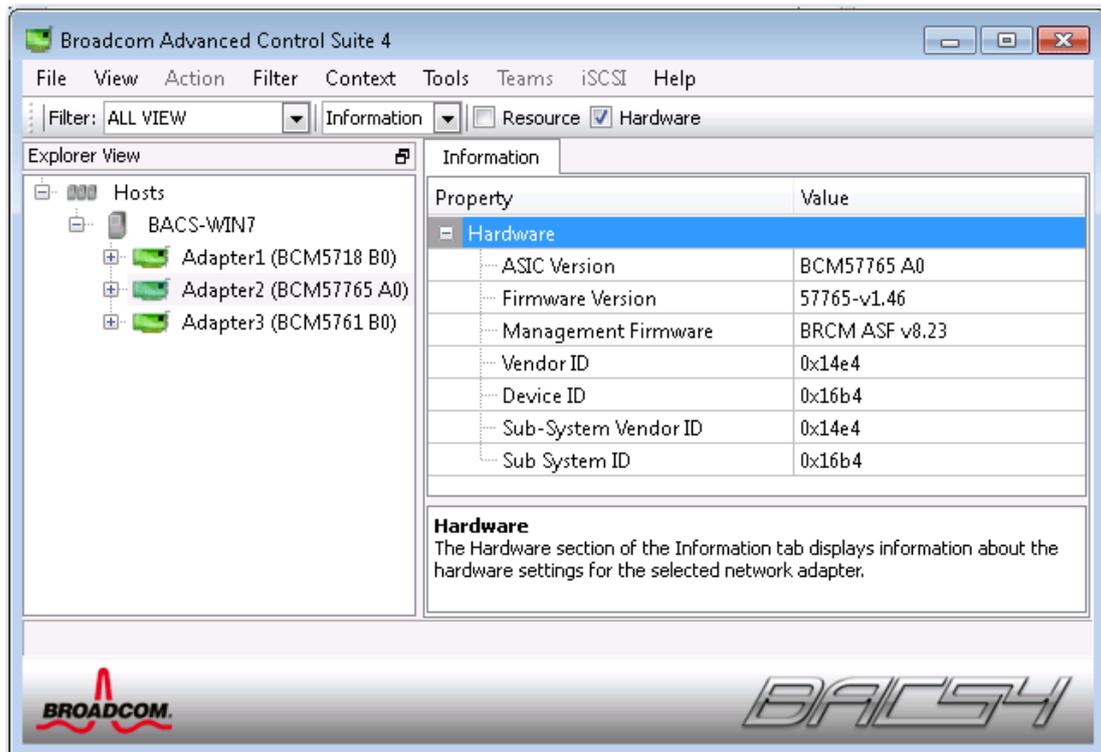
The memory mapped address that is assigned to the adapter. This value can never be 0.

Viewing Hardware Information

The Hardware section of the **Information tab** displays information about the hardware settings for the selected network adapter.

To view Hardware for any installed network adapter, click the name of the adapter listed in the Explorer View pane, then click the Information tab.

 Note: Some information may not be available for all Broadcom network adapters.



ASIC Version

The chip version of the Broadcom adapter (this information is not available for adapters made by others).

Firmware Version

The firmware version of the Broadcom adapter (this information is not available for adapters made by others). This information is only available for D-Link NetXtreme adapters.

Vendor ID

The vendor ID.

Device ID

The adapter ID.

Subsystem Vendor ID

The subsystem vendor ID.

Subsystem ID

The subsystem ID.

Testing the Network

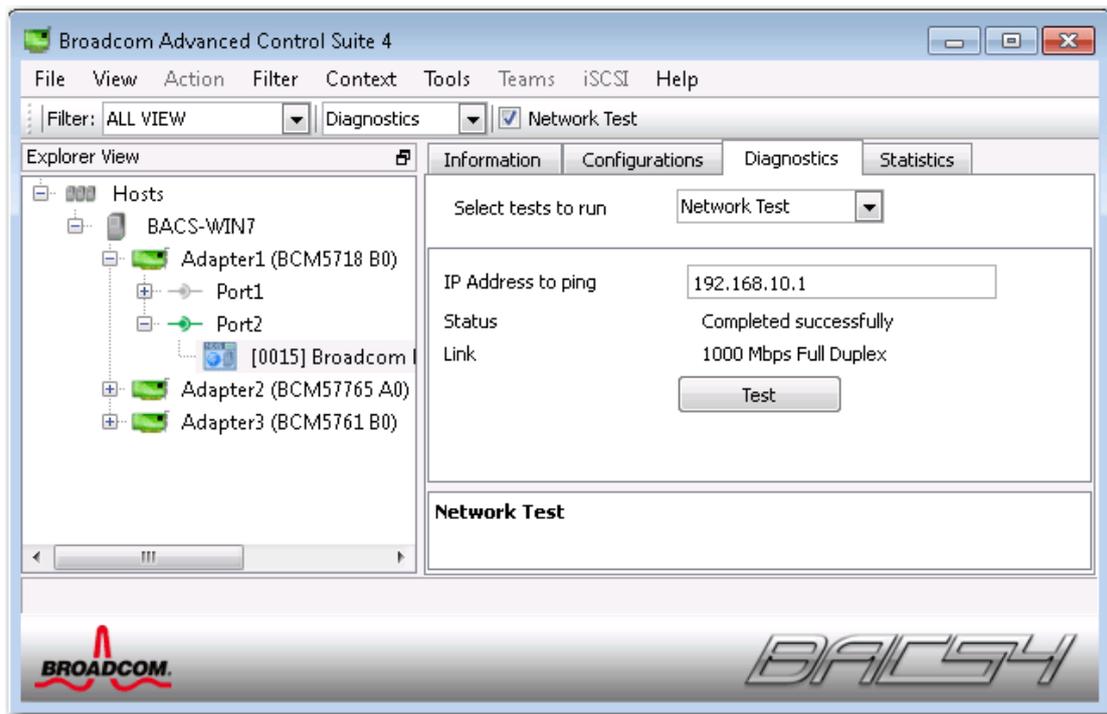
The **Network Test** option on the **Diagnostics** tab lets you verify IP network connectivity. This test verifies if the driver is installed correctly and tests connectivity to a gateway or other specified IP address on the same subnet. The network test uses TCP/IP to send ICMP packets to remote systems, then waits for a response.

 **Note:** The network test option is not available on adapters that are grouped into a team (see Configuring Teaming).

To run the network test

1. Click the name of the adapter to test in the Explorer View pane.
2. From the **Select a test to run** list, select **Network Test**. If the **Network Test** option is not available, then from the **Context View** tab on the right side of the window, select **Diagnostics** and then select **Network Test**.
3. To change the destination IP address, select **IP address to ping**. In the Network Test window, enter a Destination IP address, then click **OK**.
4. Click **Test**.

The results of the network test are displayed in the **Status** field.



Running Diagnostic Tests

The **Diagnostic Tests** option on the **Diagnostics** tab lets you check the state of the physical components on a Broadcom network adapter. You can trigger the tests manually, or choose to have BACS 4 continuously perform them. If the test are performed continuously, then the number of passes and fails in the **Result** field for each test increments every time the tests are performed. For example, if a test is performed four times and there are no fails, the value in the **Result** field for that test is 4/0. However, if there were 3 passes and 1 fail, the value in the **Result** field is 3/1.

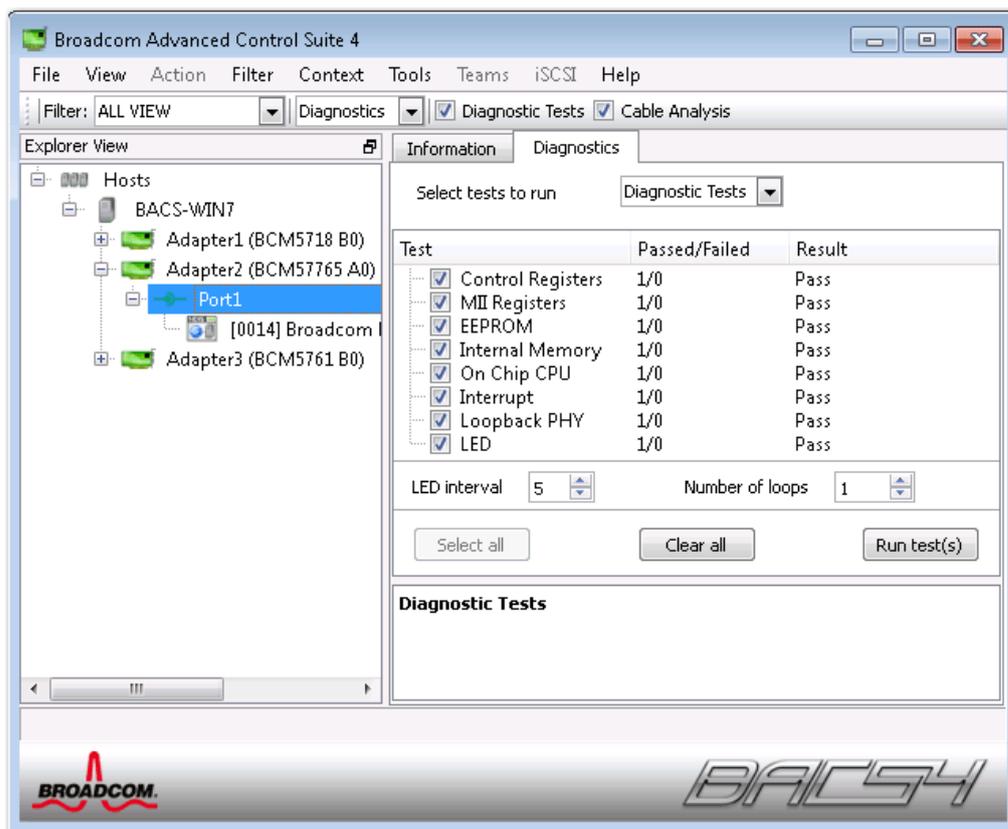
NOTES:

- You must have administrator privileges to run diagnostic tests.
- The network connection is temporarily lost while these tests are running.
- Some tests are not supported on all Broadcom adapters.

To run the diagnostic tests once

1. Click the name of the adapter to test in the Explorer View pane and select the Diagnostics tab.
2. From the **Select a test to run** list, select **Diagnostic Tests**.

3. Select the diagnostic tests you want to run. Click **Select All** to select all tests or **Clear All** to clear all test selections.
4. Select the number of times to run the tests from **Number of loops**.
5. Click **Run test(s)**.
6. In the error message window that warns of the network connection being temporarily interrupted, click **Yes**. The results are displayed in the **Result** field for each test.



NOTES:

- DGE-560SX supports fiber interface and so the information of MII Registers, LoopBack MAC, and LoopBack PHY are not available.

The list of available properti

Control Registers

This test verifies the read and write capabilities of the network adapter registers by writing various values to the registers and verifying the results. The adapter driver uses these

registers to perform network functions such as sending and receiving information. A test failure indicates that the adapter may not be working properly.

MII Registers

This test verifies the read and write capabilities of the registers of the physical layer (PHY). The physical layer is used to control the electrical signals on the wire and to configure network speeds such as 1000 Mbit/s.

EEPROM

This test verifies the content of the electrically erasable programmable read-only memory (EEPROM) by reading a portion of the EEPROM and computing the checksum. The test fails if the computed checksum is different from the checksum stored in the EEPROM. An EEPROM image upgrade does not require a code change for this test.

Internal Memory

This test verifies that the internal memory of the adapter is functioning properly. The test writes patterned values to the memory and reads back the results. The test fails if an erroneous value is read back. The adapter cannot function if its internal memory is not functioning properly.

On-Chip CPU

This test verifies the operation of the internal CPUs in the adapter.

Interrupt

This test verifies that the Network Device Driver Interface Specification (NDIS) driver is able to receive interrupts from the adapter.

LoopBack MAC

This test verifies that the NDIS driver is able to send packets to and receive packets from the adapter.

LoopBack PHY

This test verifies that the NDIS driver is able to send packets to and receive packets from the adapter.

Test LED

This test causes all of the port LEDs to blink 5 times for the purpose of identifying the adapter.

Setting Adapter Properties

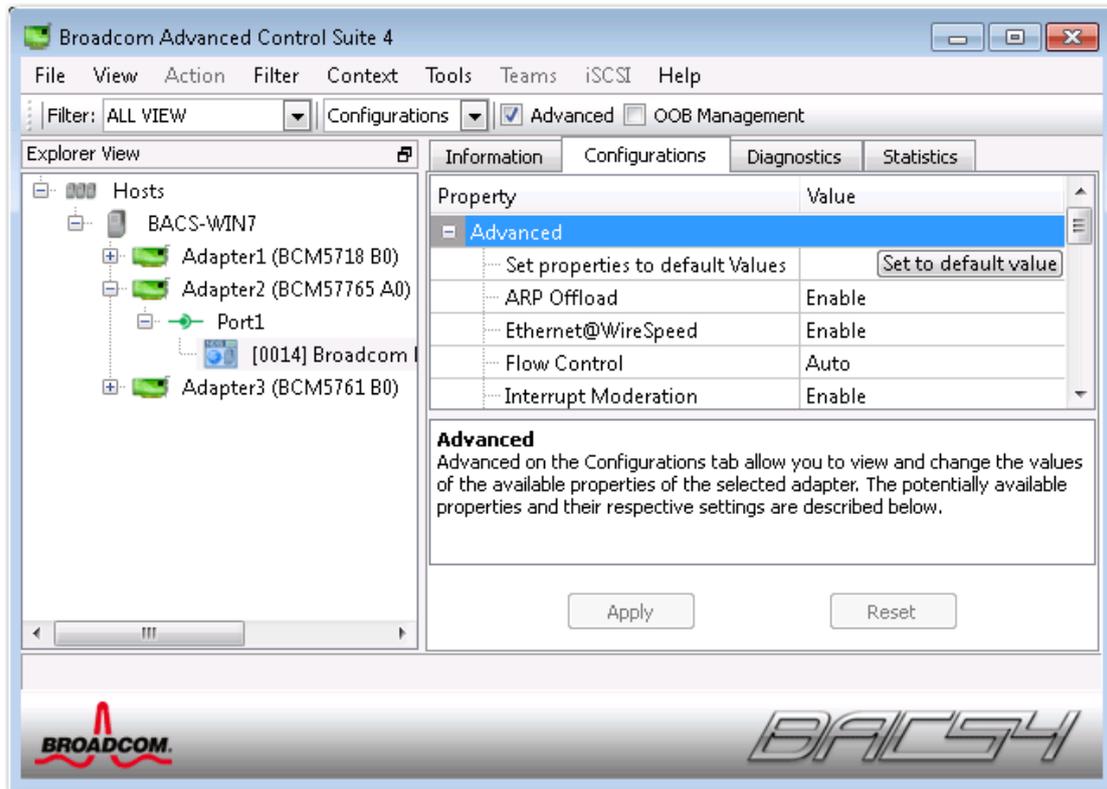
Advanced on the **Configurations** tab allow you to view and change the values of the available properties of the selected adapter. The potentially available properties and their respective settings are described below.

NOTES:

- You must have administrator privileges to change the values for a property.
- The list of available properties for your particular adapter may be different.
- Some properties may not be available for all Broadcom network adapters.

To set adapter properties

1. Click the name of the adapter in the Explorer View pane, and click the **Configurations** tab.
2. From the **Advanced** section, select the property you want to set.
3. To change the value of a property, select an item from the property's list or type a new value, as appropriate (selection options are different for different properties).
4. Click **Apply** to confirm the changes to all properties. Click **Reset** to return the properties to their original values.



802.1p QOS

Enables *quality of service*, which is an Institute of Electrical and Electronics Engineering (IEEE) specification that treats different types of network traffic diversely to ensure required levels or reliability and latency according to the type of traffic. This property is disabled by default. Unless the network infrastructure supports QoS, do not enable this property. Otherwise, problems may occur.

Ethernet@Wirespeed

Enables a Gigabit Ethernet adapter to establish a link at a lower speed when only two pairs of wires are available in the cabling plant. The default setting for this property is Enabled.

Flow Control

Enables or disables the receipt or transmission of PAUSE frames. PAUSE frames allow the network adapter and a switch to control the transmit rate. The side that is receiving the PAUSE frame momentarily stops transmitting.

- **Auto** (default). PAUSE frame receipt and transmission are optimized.
- **Disable**. PAUSE frame receipt and transmission are disabled.

- **Rx PAUSE.** PAUSE frame receipt is enabled.
- **Rx/Tx PAUSE.** PAUSE frame receipt and transmission are enabled.
- **Tx PAUSE.** PAUSE frame transmission is enabled.

IPv4 Checksum Offload

Normally, the checksum function is computed by the protocol stack. When you select one of the Checksum Offload property values (other than None), the checksum can be computed by the network adapter.

- **Rx Enabled.** Enables receive TCP/IP/UDP checksum offload.
- **Tx Enabled.** Enables transmit TCP/IP/UDP checksum offload.
- **Tx/Rx Enabled** (default). Enables transmit and receive TCP/IP/UDP checksum offload.
- **None.** Disables checksum offload.

IPv4 Large Send Offload

Normally, the TCP segmentation is done by the protocol stack. When you enable the Large Send Offload property, the TCP segmentation can be done by the network adapter. The default setting for this property is Enabled.

Jumbo MTU

Enables the network adapter to transmit and receive oversized Ethernet frames that are greater than 1514 bytes, but less than or equal to 9000 bytes in length (9600 bytes for network adapters that operate at 10 Gbps). This property requires the presence of a switch that is able to process jumbo frames.

Frame size is set at 1500 bytes by default. To increase the size of the received frames, raise the byte quantity in 500-byte increments.

LSO & Jumbo Frames

Enables the network adapter to transmit and receive oversized Ethernet frames that are greater than 1514 bytes, but less than 9000 bytes in length. This property requires the presence of a switch that is able to process Jumbo frames.

Frame size is set at 1500 bytes by default by selecting the **LSO Enabled, Jumbo Off** option.

 Note: Jumbo Frames and Large Send Offload (LSO) are mutually-exclusive properties.

Normally, the TCP segmentation is done by the protocol stack. When you enable the Large Send Offload (LSO) property, the TCP segmentation can be done by the network adapter.

- **Both Disabled.** LSO & Jumbo frames are both disabled.
- **LSO Enabled, Jumbo Off** (default). LSO enabled and jumbo frames disabled.
- **LSO Off, Jumbo 3000.** Frame size of 3000 bytes and LSO off.
- **LSO Off, Jumbo 4500.** Frame size of 4500 bytes and LSO off.
- **LSO Off, Jumbo 6000.** Frame size of 6000 bytes and LSO off.
- **LSO Off, Jumbo 7500.** Frame size of 7500 bytes and LSO off.
- **LSO Off, Jumbo 9000.** Frame size of 9000 bytes and LSO off.

Locally Administered Address

The Locally Administered Address is a user-defined MAC address that is used in place of the MAC address originally assigned to the network adapter. Every adapter in the network must have its own unique MAC address. This locally administered address consists of a 12-digit hexadecimal number.

- **Value.** Assigns a unique node address for the adapter.
- **Not Present** (default). Uses the factory-assigned node address on the adapter.

The appropriate assigned ranges and exceptions for the locally administered address include the following:

- The range is 00:00:00:00:00:01 to FF:FF:FF:FF:FF:FD.
- Do not use a multicast address (least significant bit of the high byte = 1).
- Do not use all 0s or all Fs.

Receive Side Scaling

Allows configuring network load balancing across multiple CPUs. The default setting for this property is Enabled.

Large Send Offload (IPv4)

Normally the TCP segmentation is done by the protocol stack. When you enable the Large Send Offload property, the TCP segmentation can be done by the network adapter.

TCP/UDP Checksum Offload (IPv4)

Allows configuring checksum offload for the IPv4 protocol.

- **Disable.** Disables checksum offload.
- **Rx Enabled.** Enables receive TCP/IP/UDP checksum offload.
- **Tx Enabled.** Enables transmit TCP/IP/UDP checksum offload.
- **TX & Rx Enabled (default).** Enables transmit and receive TCP/IP/UDP checksum offload.

Priority & VLAN

Allows enabling both the prioritization of network traffic and VLAN tagging. VLAN tagging only occurs when the VLAN ID setting is configured with a value other than 0 (zero).

- **Priority & VLAN Enabled (default).** Allows for packet prioritization and VLAN tagging.
- **Priority & VLAN Disabled.** Prevents packet prioritization and VLAN tagging.
- **Priority Enabled.** Allows packet prioritization only.
- **VLAN Enabled.** Allows VLAN tagging only.

 **Note:** If an intermediate driver is managing the network adapter for VLAN tagging, the **Priority & VLAN Disabled** and **Priority Enabled** settings should not be used. Use the **Priority & VLAN Enabled** setting and change the **VLAN ID** to 0 (zero).

VLAN ID

Enables VLAN tagging and configures the VLAN ID when **Priority & VLAN Enabled** is selected as the **Priority & VLAN** setting. The range for the VLAN ID is 1 to 4094 and must match the VLAN tag value on the connected switch. A value of 0 (default) in this field disables VLAN tagging.

Risk Assessment of VLAN Tagging through the NDIS Miniport Driver

Broadcom's NDIS 6.0 miniport driver provides the means to allow a system containing a Broadcom adapter to connect to a tagged VLAN. On Windows XP systems, this support was only provided through the use of an intermediate driver (e.g., Broadcom Advanced Server Program - BASP). Unlike BASP, however, the NDIS 6 driver's support for VLAN participation is only for a single VLAN ID.

Also unlike BASP, the NDIS 6.0 driver only provides VLAN tagging of the outbound packet, but does not provide filtering of incoming packets based on VLAN ID membership. This is the default behavior of all miniport drivers. While the lack of filtering packets based on VLAN membership may present a security issue, the following provides a risk assessment based on this driver limitation for an IPv4 network:

A properly configured network that has multiple VLANs should maintain separate IP segments for each VLAN. This is necessary since outbound traffic relies on the routing table to identify which adapter (virtual or physical) to pass traffic through and does not determine which adapter based on VLAN membership.

Since support for VLAN tagging on Broadcom's NDIS 6.0 driver is limited to transmit (Tx) traffic only, there is a risk of inbound traffic (Rx) from a different VLAN being passed up to the operating system. However, based on the premise of a properly configured network above, the IP segmentation and/or the switch VLAN configuration may provide additional filtration to limit the risk.

In a back-to-back connection scenario, two computers on the same IP segment may be able to communicate regardless of their VLAN configuration since no filtration of VLAN membership is occurring. However, this scenario assumes that the security may already be breached since this connection type is not typical in a VLAN environment.

If the risk above is not desirable and filtering of VLAN ID membership is required, then support through an intermediate driver would be necessary.

5.4 Configuring Teaming

The teaming function allows you to group any available network adapters together to function as a team. Teaming is a method of creating a virtual NIC (a group of multiple adapters that functions as a single adapter). The benefit of this approach is that it enables load balancing and failover. Teaming is done through the Broadcom Advanced Server Program (BASP) software.

Teaming can be accomplished by either of the following methods:

- Using the Broadcom Teaming Wizard
- Using Expert Mode

 NOTES:

- For further information regarding teaming protocols, see "Teaming" in your Broadcom network adapter user guide.
- If you do not enable LiveLink™ when configuring teams, disabling Spanning Tree Protocol (STP) at the switch is recommended. This minimizes the downtime due to spanning tree loop determination when failing over. LiveLink mitigates such issues.
- BASP is available only if a system has one or more Broadcom network adapters installed.
- The Large Send Offload (LSO) and Checksum Offload properties are enabled for a team only when all of the members support and are configured for the feature.
- You must have administrator privileges to create or modify a team.
- The load balance algorithm in a team environment in which members are connected at different speeds favors members connected with a Gigabit Ethernet link over members connected at lower speed links (100 Mbps or 10 Mbps) until a threshold is met. This is normal behavior.

Team Types

You can create four types of load balance teams:

- Smart Load Balance and Failover
- Link Aggregation (802.3ad)
- Generic Trunking (FEC/GEC)/802.3ad-Draft Static
- SLB (Auto-Fallback Disable) – The Auto-Fallback Disable feature is configured for Smart Load Balance and Failover type teams in the Teaming Wizard.

Smart Load Balance and Failover

In this type of team, a standby member handles the traffic if all of the load balance members fail (a failover event). All load balance members have to fail before the standby member takes over. When one or more of the load balance members is restored (fallback), the restored team member(s) resumes the handling of the traffic. The LiveLink feature is supported for this type of team.

Link Aggregation (802.3ad)

In this type of team, you can dynamically configure the network adapters that have been selected to participate in a given team. If the link partner is not correctly configured for IEEE 802.3ad link configuration, errors are detected and noted. All adapters in the team are configured to receive packets for the same MAC address. The outbound load balancing scheme is determined by the BASP driver. The link partner of the team determines the load balancing scheme for inbound packets. In this mode, at least one of the link partners must be in active mode.

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

This type of team is very similar to the link aggregation type, in that all adapters in the team must be configured to receive packets for the same MAC address. This mode does not provide link aggregation control protocol (LACP) or marker protocol support. This mode supports a variety of environments where the link partners are statically configured to support a proprietary trunking mechanism. Trunking supports load balancing and failover for both outbound and inbound traffic.

SLB (Auto-Fallback Disable)

This team is identical to Smart Load Balance and Failover, with the following exception: when the standby member is active, if a primary member comes back online, the team continues using the standby member rather than switching back to the primary member. This type of team is supported only for situations in which the network cable is disconnected and reconnected to the network adapter. It is not supported for situations in which the adapter is removed/installed through Device Manager or Hot-Plug PCI. If any primary adapter assigned to a team is disabled, the team functions as a Smart Load Balancing and Failover type of team in which auto-fallback occurs. The LiveLink feature is supported for this type of team.

Standby Team Member and Auto-Fallback Disable

Mode

You can designate one team member in an SLB type of team to be the standby member. The standby member does not actively send and receive normal network traffic while other adapters on the team are active. If all of the active adapters on the team fail or are disconnected, the standby member takes over the handling of the network activities.

In Auto-Fallback Disable mode, if a load balance member returns on line, the team continues using the standby member rather than switching back to using the load balance member. Consequently, the adapter that was initially designated a load balance member remains in an inactive state and becomes the new standby member.

LiveLink

LiveLink is a feature of BASP that is available for the Smart Load Balancing (SLB) and SLB (Auto-Fallback Disable) type of teaming. The purpose of LiveLink is to detect link loss beyond the switch and to route traffic only through team members that have a live link.

5.4.1 Using the Broadcom Teaming Wizard

You can use the Broadcom Teaming Wizard to create a team, configure an existing team if a team has already been created, or create a VLAN.

1. Create or edit a team:

To create a new team, select **Create a Team** from the **Team** menu, or right-click one of the devices in the "Unassigned Adapters" section and select **Create a Team**. This option is not available if there are no devices listed in the "Unassigned Adapters" sections, which means all adapters are already assigned to teams.

To configure an existing team, right-click one of the teams in the list and select **Edit Team**. This option is only available if a team has already been created and is listed in the Team Management pane.

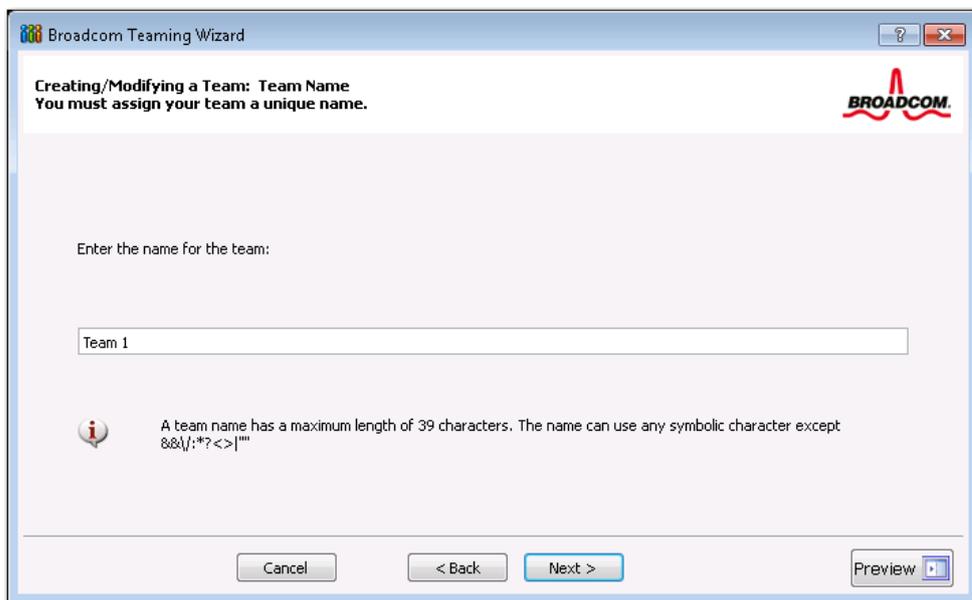
 **Note:** If you prefer to work without the wizard for now, click **Expert Mode**. If you want to always use Expert Mode to create a team, select **Default to Expert Mode on next start**. See Using Expert Mode.

2. To continue using the wizard, click **Next**.

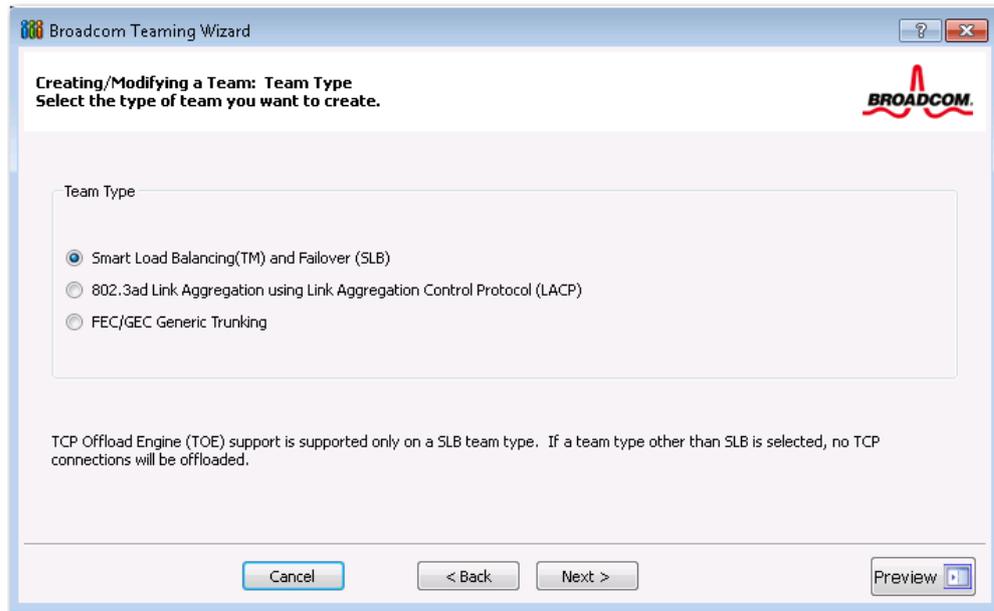


3. Type the team name and then click **Next**. If you want to review or change any of your settings, click **Back**. Click **Cancel** to discard your settings and exit the wizard.

 **Note:** The team name cannot exceed 39 characters, cannot begin with spaces, and cannot contain any of the following characters: & \ / : * ? < > |



4. Select the type of team you want to create. If the team type is an SLB type team, click **Next**. If the team type is not an SLB type team, then a dialog box appears. Verify that the network switch connected to the team members is configured correctly for the team type, click **OK**, and continue.

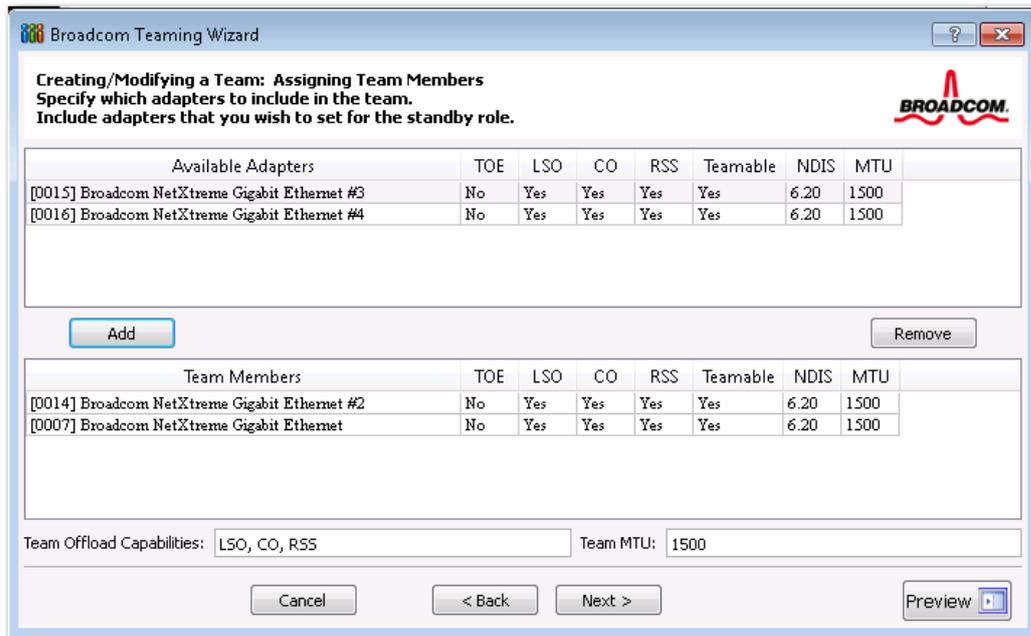


5. From the **Available Adapters** list, click the adapter you want to add to the team and then click **Add**. Remove team members from the **Team Members** list by clicking the adapter and then clicking **Remove**. Click **Next**.

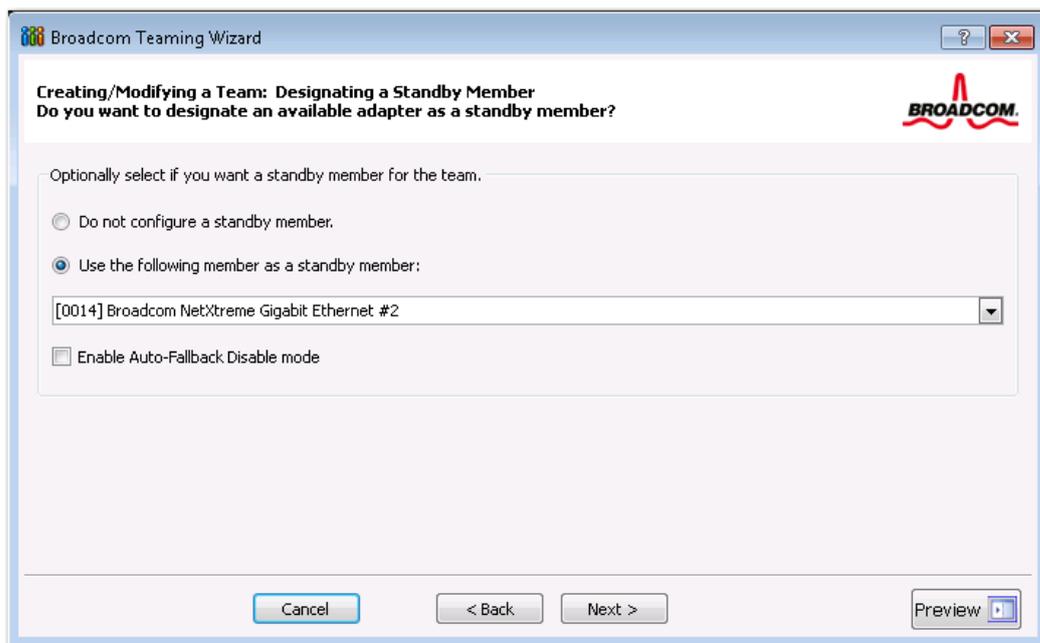
 **Note:** There must be at least one Broadcom network adapter assigned to the team.

The TCP Offload Engine (TOE), Large Send Offload (LSO) and Checksum Offload (CO) columns indicate if the TOE, LSO, and/or the CO properties are supported for the adapter. The TOE, LSO, and CO properties are enabled for a team only when all of the members support and are configured for the feature. If this is the case, then the team offload capabilities appear on the bottom of the screen.

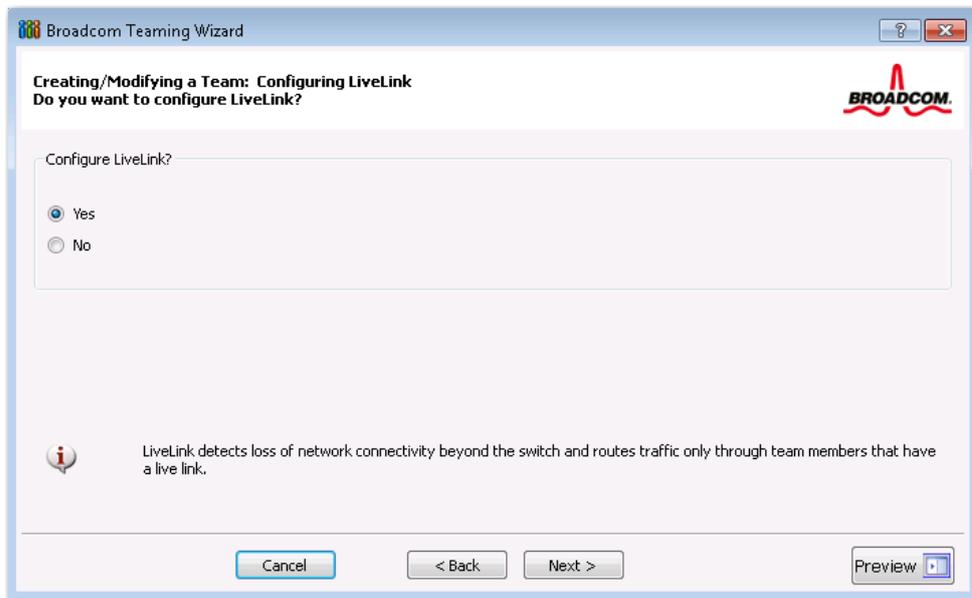
 **Note:** Adding a network adapter to a team where its driver is disabled may negatively affect the offloading capabilities of the team. This may have an impact on the team's performance. Therefore, it is recommended that only driver-enabled network adapters be added as members to a team.



- If you want to designate one of the adapters as a standby member (optional), select **Use the following member as a standby member**, then choose the standby member from the list of adapters.
- The Auto-Fallback Disable mode feature allows the team to continue using the standby member rather than switching back to the primary member if the primary member comes back online. To enable this feature, select **Enable Auto-Fallback Disable mode**. Click **Next**.



8. If you want to configure LiveLink, select **Yes**, otherwise select **No**, then click **Next**.



9. Select the probe interval (the number of seconds between each retransmission of a link packet to the probe target) and the maximum number of probe retries (the number of consecutively missed responses from a probe target before a failover is triggered).
10. Set the Probe VLAN ID to allow for connectivity with probe targets residing on a tagged VLAN. The number set must match the VLAN ID of the probe targets as well as the port(s) on the switch to which the team is connected.

 **Note:** Each LiveLink enabled team can only communicate with Probe Targets on a single VLAN. Also, VLAN ID 0 is equivalent to an untagged network. If the Probe VLAN ID is set to a value other than 0, then a VLAN must be created with an identical VLAN tag value (see Step 16.).

11. Click the probe target at the top of the list, click **Edit Target IP Address**, type the target IP address in the **IP Address** box for one or all probe targets, and then click **OK**. Click **Next**.

 **Note:** Only the first probe target is required. You can specify up to three additional probe targets to serve as backups by assigning IP addresses to the other probe targets.

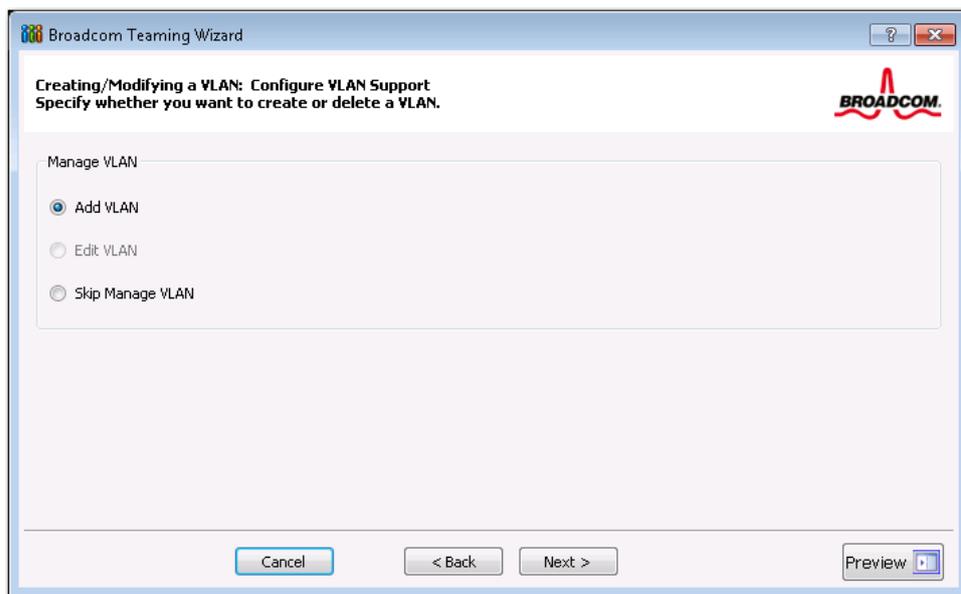
12. Select a listed team member, click **Edit Member IP Address**, and then type the member IP address in the IP Address box. Repeat for all listed team members and then click **OK**. Click **Next**.

 **Note:** All of the member IP addresses must be in the same subnet as the subnet of the probe targets.

13. If you want to create a VLAN on the team, select **Add VLAN**, or if you want to change the settings of an existing VLAN, select **Edit VLAN**, then click **Next**. If you do not want to create or edit a VLAN, select **Skip Manage VLAN**, then click **Next**, and continue with the wizard from the Finish screen (see Step 18. of this procedure).

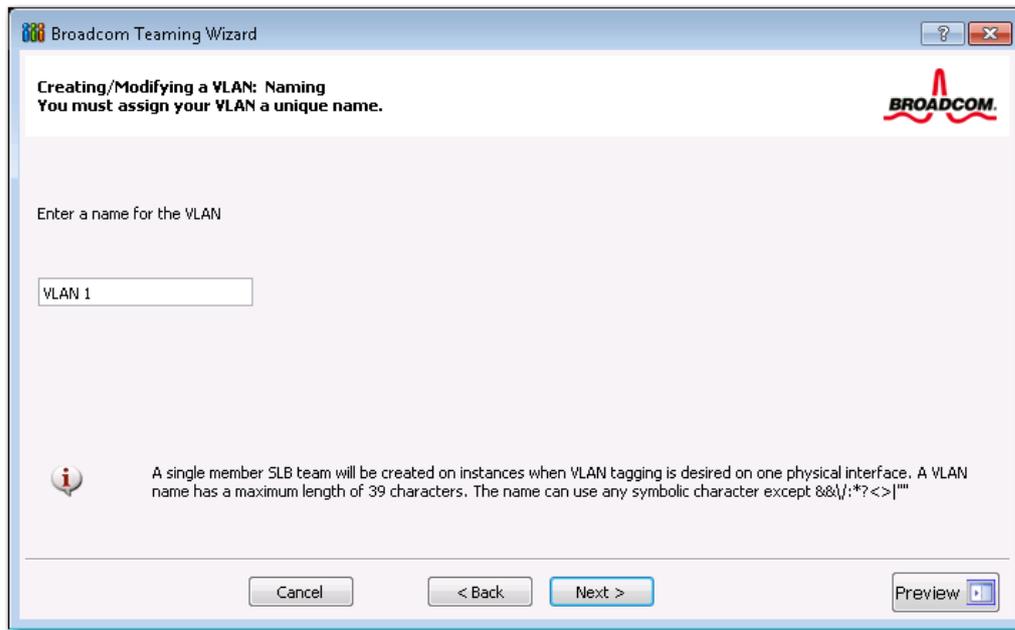
VLANs enable you to add multiple virtual adapters that are on different subnets. The benefit of this is that your system can have one network adapter that can belong to multiple subnets.

 **Note:** VLANs can only be created when all team members are Broadcom adapters.

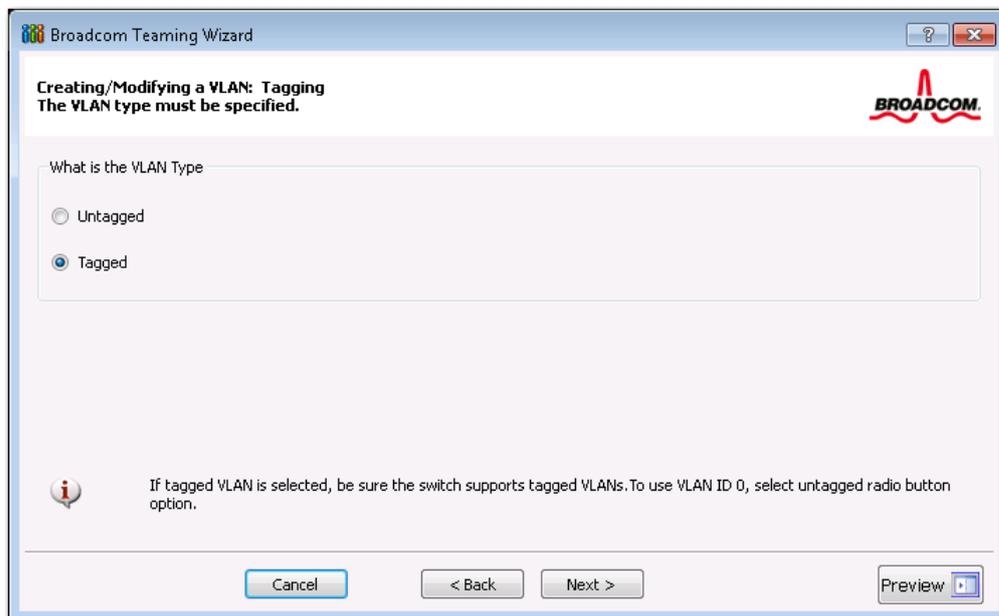


14. Type the VLAN name and then click **Next**.

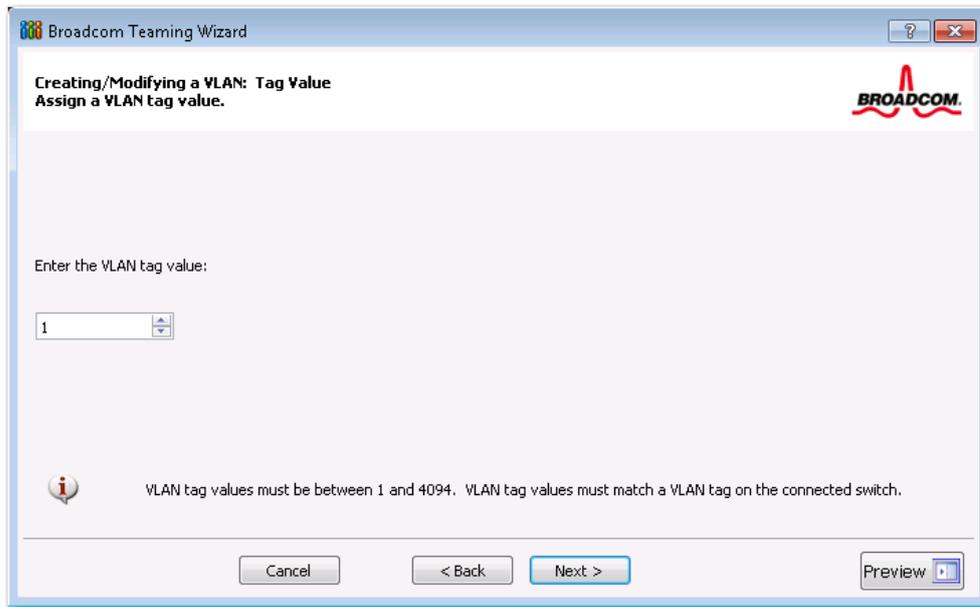
 **Note:** The team name cannot exceed 39 characters, cannot begin with spaces, and cannot contain any of the following characters: & \ / : * ? < > |



15. To tag the VLAN, select **Tagged** and then click **Next**. Otherwise, click **Untagged**, click **Next**, and continue with the wizard to add additional VLANs (see Step 17. of this procedure).

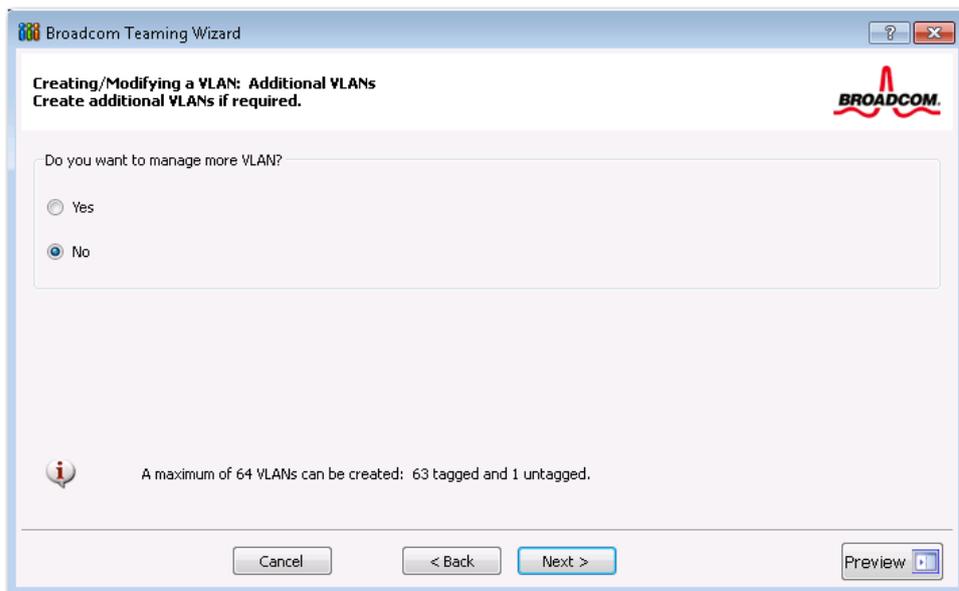


16. Type the VLAN tag value and then click **Next**. The value must be between 1 and 4094.

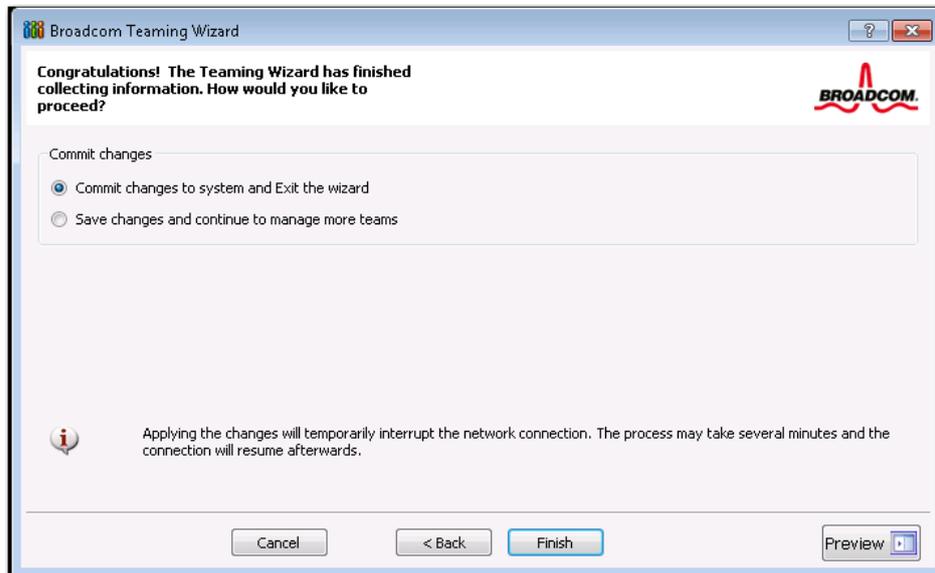


17. Select **Yes** to add or manage another VLAN and then click **Next**. Repeat until you do not want to add or manage any additional VLANs.

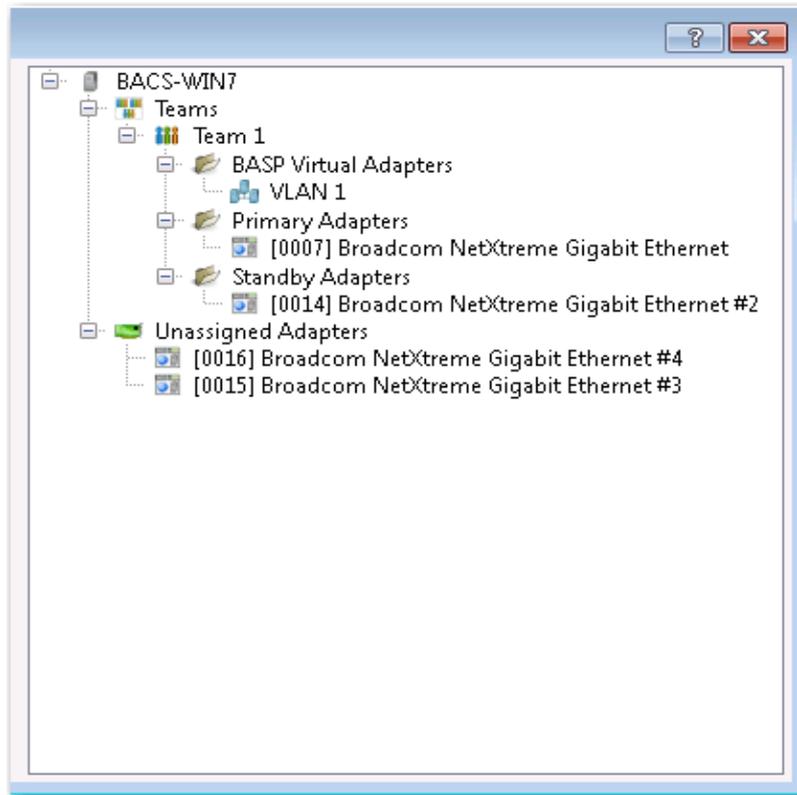
 **Note:** You can define up to 64 VLANs per team (63 VLANs that are tagged and 1 VLAN that is not tagged). Adding several VLANs may slow down the reaction time of the Windows interface due to memory and processor time usage for each VLAN. The degree to which Windows performance may suffer depends on system configuration.



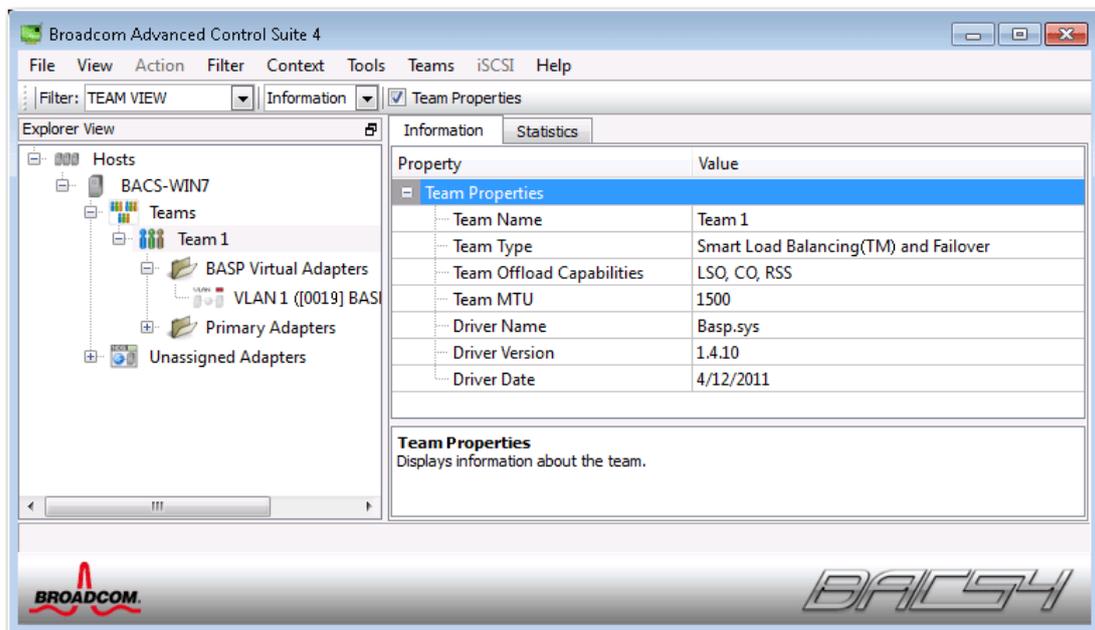
18. To apply and commit the changes to the team, select **Commit changes to system and Exit the wizard**. To apply your changes but continue using the wizard, select **Save changes and continue to manage more teams**. Click Finish.



 **Note:** At any point in the Broadcom Teaming Wizard procedure, click **Preview** to get a visual representation of what the team will look like before committing any changes.



19. Click the team name in the Team Management pane to view the team's properties in the **Information** tab, transfer and receive data in the **Statistics** tab.



5.4.2 Using Expert Mode

Use Expert Mode to create a team, modify a team, add a VLAN, and configure LiveLink for a Smart Load Balance and Failover and SLB (Auto-Fallback Disable) team. To create a team using the wizard, see Using the Broadcom Teaming Wizard.

To set the default Teaming Mode, select **Options** from the **Tools** menu, then select **Expert Mode** or **Wizard Mode** (the default is Wizard Mode).

Creating a Team

 Note: Enabling Dynamic Host Configuration Protocol (DHCP) is not recommended for members of an SLB type of team.

1. From the **Teams** menu, select **Create Team**, or right-click one of the devices in the "Unassigned Adapters" section and select **Create a Team**. This option is not available if there are no devices listed in the "Unassigned Adapters" sections, which means all adapters are already assigned to teams.
2. Click **Expert Mode**.

 Note: If you want to always use Expert Mode to create a team, click **Default to Expert Mode on next start**.

3. Click the **Create Team** tab.

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

Note: The **Create Team** tab appears only if there are teamable adapters available.

4. Click the **Team Name** field to enter a team name.
5. Click the **Team Type** field to select a team type.
6. Assign any available adapter or adapters to the team by selecting the adapter from the **Load Balance Members** list. There must be at least one adapter selected in the **Load Balance Members** list.
7. You can assign any other available adapter to be a standby member by selecting it from the **Standby Member** list.

Note: There must be at least one Broadcom network adapter assigned to the team.

The Large Send Offload (LSO), Checksum Offload (CO), and RSS indicate if the LSO, CO, and/or RSS properties are supported for the team. The LSO, CO, and RSS properties are enabled for a team only when all of the members support and are configured for the feature.

 **Note:** Adding a network adapter to a team where its driver is disabled may negatively affect the offloading capabilities of the team. This may have an impact on the team's performance. Therefore, it is recommended that only driver-enabled network adapters be added as members to a team.

8. Type the value for **Team MTU**.
9. Click **Create** to save the team information.
10. Repeat steps 4. through 9. to define additional teams. As teams are defined, they can be selected from the team list, but they have not yet been created. Click the **Preview** tab to view the team structure before applying the changes.
11. Click **Apply/Exit** to create all the teams you have defined and exit the Manage Teams window.
12. Click **Yes** when the message is displayed indicating that the network connection will be temporarily interrupted.

 **NOTES:**

- The team name cannot exceed 39 characters, cannot begin with spaces, and cannot contain any of the following characters: & \ / : * ? < > |
- Team names must be unique. If you attempt to use a team name more than once, an error message is displayed indicating that the name already exists.
- The maximum number of team members is 8.
- When team configuration has been correctly performed, a virtual team adapter driver is created for each configured team.
- If you disable a virtual team and later want to reen able it, you must first disable and reen able all team members before you reen able the virtual team.
- When you create Generic Trunking and Link Aggregation teams, you cannot designate a standby member. Standby members work only with Smart Load Balancing and Failover and SLB (Auto-Fallback Disable) types of teams.
- For an SLB (Auto-Fallback Disable) team, to restore traffic to the load balance members from the standby member, click the Fallback button on the Team Properties tab.
- When configuring an SLB team, although connecting team members to a hub is supported for testing, it is recommended to connect team members to a switch.

- Not all network adapters made by others are supported or fully certified for teaming.
13. Configure the team IP address.
 - a. From **Control Panel**, double-click **Network Connections**.
 - b. Right-click the name of the team to be configured, and then click **Properties**.
 - c. On the **General** tab, click **Internet Protocol (TCP/IP)**, and then click **Properties**.
 - d. Configure the IP address and any other necessary TCP/IP configuration for the team, and then click **OK** when finished.

Modifying a Team

After you have created a team, you can modify the team in the following ways:

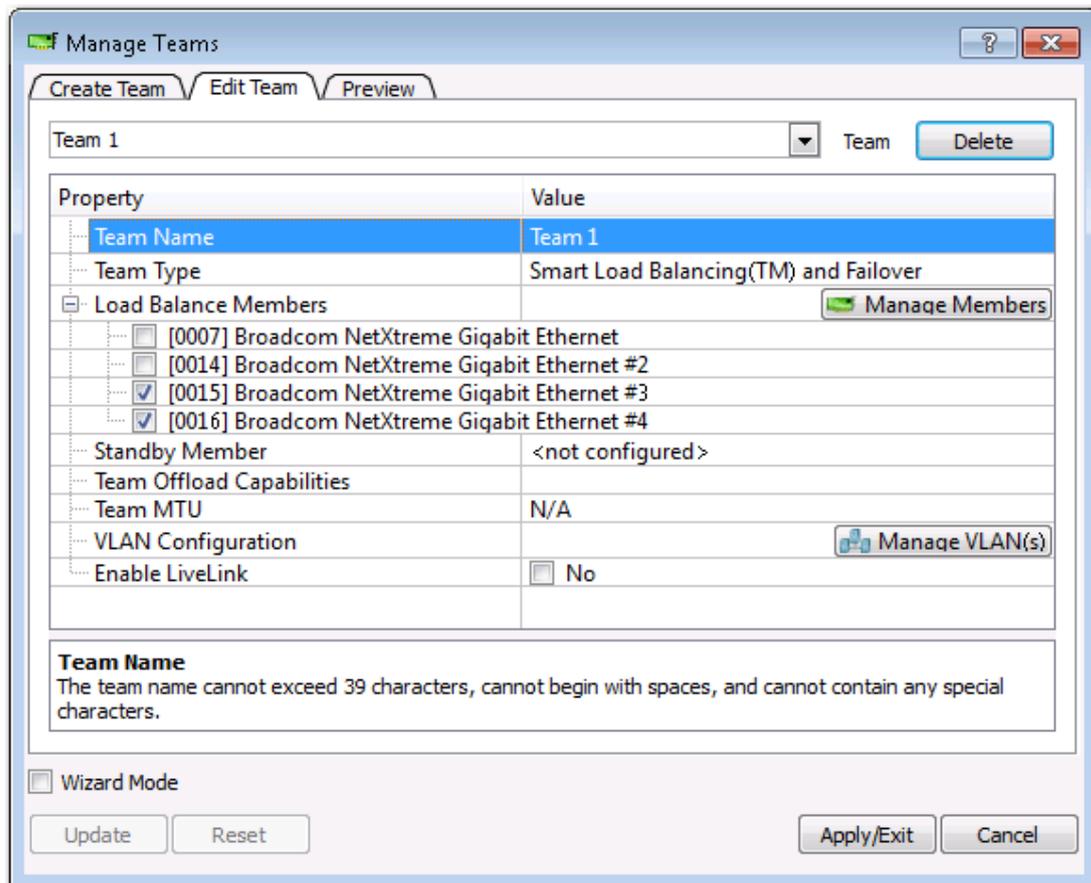
- Change the type of team
- Change the members assigned to the team
- Add a VLAN
- Modify a VLAN (using Expert Mode)
- Remove a team or a VLAN (using Expert Mode)

To modify a team

1. From the **Team** menu, click **Edit Team**, or right-click one of the teams in the list and select **Edit Team**. This option is only available if a team has already been created and is listed in the Team Management pane.
2. The wizard Welcome screen appears. Click **Next** to continue modifying a team using the wizard or click **Expert Mode** to work in Expert Mode.

 **Note:** The **Edit Team** tab in Expert Mode appears only if there are teams configured on the system.

3. Click the **Edit Team** tab.



4. Make the desired changes, and then click **Update**. The changes have not yet been applied; click the **Preview** tab to view the updated team structure before applying the changes.
5. Click **Apply/Exit** to apply the updates and exit the Manage Teams window.
6. Click **Yes** when the message is displayed indicating that the network connection will be temporarily interrupted.

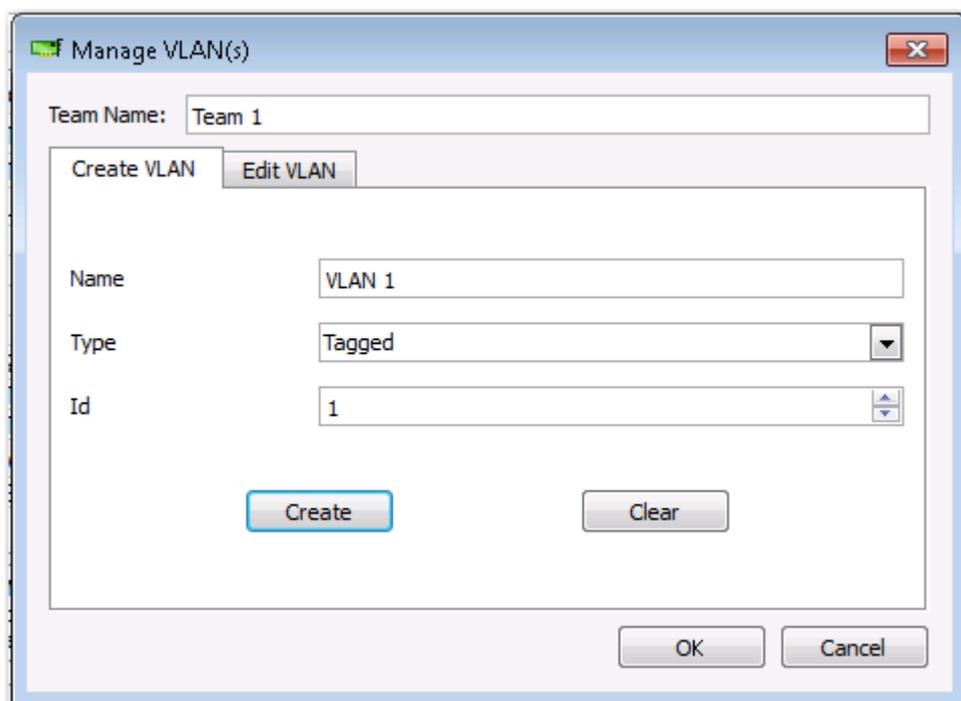
Adding a VLAN

You can add virtual LANs (VLANs) to a team. This enables you to add multiple virtual adapters that are on different subnets. The benefit of this is that your system can have one network adapter that can belong to multiple subnets. With a VLAN, you can couple the functionality of load balancing for the load balance members, and you can employ a failover adapter.

You can define up to 64 VLANs per team (63 VLANs that are tagged and 1 VLAN that is not tagged). VLANs can only be created when all teams members are Broadcom adapters. If you try to create a VLAN with a non-Broadcom adapter, an error message is displayed.

To configure a team with a VLAN

1. From the **Teams** menu, select **Add VLAN**.
2. The Welcome screen appears.
3. Click **Expert Mode**.
4. On the **Create Team** tab of the **Manage Teams** window, click **Manage VLAN(s)**.
5. Type the VLAN name, then select the type and ID.
6. Click **Create** to save the VLAN information. As VLANs are defined, they can be selected from the Team Name list, but they have not yet been created.
7. Continue this process until all VLANs are defined, then click **OK** to create them.



8. Click **Yes** when the message is displayed indicating that the network connection will be temporarily interrupted.

 **Note:** To maintain optimum adapter performance, your system should have 64 MB of system memory for each of the eight VLANs created per adapter.

Viewing VLAN Properties and Statistics and Running VLAN Tests**To view VLAN properties and statistics and to run VLAN tests**

1. Select one of the listed VLANs.
2. Click the **Information** tab to view the properties of the VLAN adapter.
3. Click the **Statistics** tab to view the statistics for the VLAN adapter.
4. Click the **Diagnostics** tab to run a network test on the VLAN adapter.

Deleting a VLAN

The procedure below applies when you are in Expert Mode.

To delete a VLAN

1. Select the VLAN to delete.
2. From the **Teams** menu, select **Remove VLAN**.
3. Click **Apply**.
4. Click **Yes** when the message is displayed indicating that the network connection will be temporarily interrupted.

 Note: If you delete a team, any VLANs configured for that team are also deleted.

Configuring LiveLink for a Smart Load Balancing and Failover and SLB (Auto-Fallback Disable) Team

LiveLink is a feature of BASP that is available for the Smart Load Balancing (SLB) and SLB (Auto-Fallback Disable) type of teaming. The purpose of LiveLink is to detect link loss beyond the switch and to route traffic only through team members that have a live link.

Read the following notes before you attempt to configure LiveLink.

NOTES:

- Before you begin configuring LiveLink™, review the description of LiveLink. Also verify that each probe target you plan to specify is available and working. If the IP address of the probe target changes for any reason, LiveLink must be reconfigured. If the MAC address of the probe target changes for any reason, you must restart the team (see "Troubleshooting").
- A probe target must be on the same subnet as the team, have a valid (not a broadcast, multicast, or unicast), statically-assigned IP address, and be highly available (always on).

- To ensure network connectivity to the probe target, ping the probe target from the team.
- You can specify up to four probe targets.
- The IP address assigned to either a probe target or team member cannot have a zero as the first or last octet.

To configure LiveLink

1. From the **Teams** menu, select **Edit Team**.
2. Click Expert Mode (to configure LiveLink using the Teaming Wizard, see Using the Broadcom Teaming Wizard).
3. In the Manage Members window, click the **Edit Team** tab.
4. Select **Enable LiveLink**. The LiveLink Configuration options appear below.
5. It is recommended to accept the default values for **Probe interval** (the number of seconds between each retransmission of a link packet to the probe target) and **Probe maximum retries** (the number of consecutively missed responses from a probe target before a failover is triggered). To specify different values, click the desired probe interval in the **Probe interval (seconds)** list and click the desired maximum number of probe retries in the **Probe maximum retries** list.
6. Set the **Probe VLAN ID** to correspond with the VLAN where the probe target(s) resides. This will apply the appropriate VLAN tag to the link packet based on the shared configuration of the attached switch port(s).

 Note: Each LiveLink enabled team can only communicate with Probe Targets on a single VLAN. Also, VLAN ID 0 is equivalent to an untagged network.

7. Select **Probe Target 1** and type the target IP address for one or all probe targets.

 Note: Only the first probe target is required. You can specify up to 3 additional probe targets to serve as backups by assigning IP addresses to the other probe targets.

8. Select one of the listed team members and type the member IP address.

 Note: All of the member IP addresses must be in the same subnet as the probe targets.

9. Click **Update**. Repeat these steps for each of the other listed team members.

10. Click **Apply/Exit**.

Saving and Restoring a Configuration

To save a configuration

1. From the **File** menu, select **Team Save As**.
2. Type *the path and file name of the new configuration file*, and then click **Save** (a .bcg extension is added).

The configuration file is a text file that can be viewed by any text editor. The file contains information about both the adapter and the team configuration.

To restore a configuration

1. From the **File** menu, select **Team Restore**.
2. Click the name of the file to be restored, and then click **Open**.

 Note: If necessary, go to the folder where the file is located.

3. Click **Apply**.
4. Click **Yes** when the message is displayed indicating that the network connection will be temporarily interrupted.
5. If a configuration is already loaded, a message is displayed that asks if you want to save your current configuration. Click **Yes** to save the current configuration. Otherwise, the configuration data that is currently loaded is lost.

 Note: The team may take a very long time to restore if the team is configured with many VLANs and a static IP address.

Viewing BASP Statistics

The Statistics section shows performance information about the network adapters that are on a team.

To view BASP Statistics information for any team member adapter or the team as a whole, click the name of the adapter or team listed in the Team Management pane, then click the **Statistics** tab.

Click **Refresh** to get the most recent values for each statistic. Click **Reset** to change all values to zero.

Tx. Packet

This is the number of packets transmitted.

Tx. Packet Discarded

This is the number of packets discarded.

Tx. Packet Queued

This is the number of packets queued.

Rx. Packet

This is the number of packets received.

Rx. Packet Discarded

This is the number of packets discarded.

Probes Retried

This is the number of consecutively missed responses from a probe target before a failover is triggered.

Chapter 6: User Diagnostics

6.1 Introduction

D-Link NetXtreme User Diagnostics is an MS-DOS based application that runs a series of diagnostic tests (see Table 1: "MS-DOS Command Prompt Mode Command Options") on the D-Link NetXtreme Gigabit Ethernet adapters in your system. D-Link NetXtreme User Diagnostics also allows you to update device firmware and to view and change settings for available adapter properties. D-Link NetXtreme User Diagnostics can be run in either of the following modes:

- MS-DOS Command Prompt mode
- Broadcom Command Line Interface (CLI) mode

In either mode, you can view the version of the adapter software and specify which adapter to test and which tests to perform. The MS-DOS Command Prompt mode is useful for viewing and changing the settings for available properties, updating and loading device firmware, viewing the version of and printing the error log (if any) to a file. The Broadcom CLI mode is useful for enabling/disabling available properties and enabling/disabling/selecting and setting the speed and duplex mode of available protocols.

To run D-Link NetXtreme User Diagnostics, create an MS-DOS 6.22 bootable disk containing the B57udiag.exe file. Next, start the system with the boot disk in drive A. See either Running in MS-DOS Command Prompt Mode or Running in Broadcom Command Line Interface Mode for further instructions.

6.2 System Requirements

Operating System: MS-DOS 6.22

Software: B57udiag.exe

6.3 Running D-Link NetXtreme User

Diagnostics

Running in MS-DOS Command Prompt Mode

At the MS-DOS prompt, type b57udiag using the command options as shown in Table 1.

 **NOTE:** In MS-DOS Command Prompt mode, you must include b57udiag at the beginning of the command string each time you type a command.

Table 1: MS-DOS Command Prompt Mode Command Options	
Command Options	Description
b57udiag	Performs all of the tests on all of the D-Link NetXtreme Gigabit Ethernet adapters in your system.
b57udiag -c <num>	Specifies the adapter to test, or the adapter on which to update the firmware or to view or change the settings for available properties.
b57udiag -cmd	Changes to the Broadcom CLI mode.
b57udiag -mba <value>	Enables/disables Multi-Boot Agent (MBA) protocol. 1 = Enable 0 = Disable
b57udiag -mbap <value>	Selects the specific MBA protocol. 0 = Preboot Execution Environment (PXE) 1 = Remote Program Load (RPL) 2 = Bootstrap Protocol (BOOTP)
b57udiag -mbas <value>	Selects the MBA speed and duplex mode. 0 = Auto 1 = 10 Mbps speed, half-duplex operation 2 = 10 Mbps speed, full-duplex operation 3 = 100 Mbps speed, half-duplex operation 4 = 100 Mbps speed, full-duplex operation 6 = 1000 Mbps speed, full-duplex (fiber)
b57udiag -firm <file>	Updates the EEPROM of the selected adapter based on the match between the existing image file name and the new image <file name>.

	<p>Examples:</p> <pre>b57udiag -firm ee5751c3.40a b57udiag -firm ee5721c3.40a</pre>
b57udiag -firmall <file>	Updates the EEPROM of all of the adapters based on the <file name> image match.
b57udiag -ver	Displays the version of the software/eeprom.bin file.
b57udiag -pxe <file>	<p>Loads the Preboot Execution Environment (PXE) firmware from a file.</p> <p>Example:</p> <pre>b57udiag -pxe b57mmba.nic</pre> <p>Note: This command should be used only for add-in adapters. For LOM adapters, the PXE firmware is loaded automatically during startup.</p>
b57udiag -elog <file>	Prints the error log to a file.
b57udiag -pipmi <file>	<p>Loads the Intelligent Platform Management Interface (IPMI) from a file.</p> <pre>b57udiag -pipmi pt5721c6.10 b57udiag -pipmi pt5704c2.36 b57udiag -pipmi pt5704s2.36</pre> <p>Use the file that is appropriate for the type of hardware interface (copper or fiber). For example, the pt5704c2.36 file should be used for copper, and the pt5704s2.36 file should be used for fiber.</p>
b57udiag -ipmi <value>	<p>Enables/disables IPMI.</p> <p>1 = Enable</p> <p>0 = Disable</p>
b57udiag -help	Displays this table of MS-DOS Command Prompt Mode Command Options.

Running in Broadcom Command Line Interface Mode

At the MS-DOS prompt, type `b57udiag -cmd`, and use the command options as shown in Table 2.

Table 2: Broadcom Command Line Interface (CLI) Mode Commands	
Command	Description

upgfrm	Updates the PXE or Boot Code from a file																																																	
dir	<p>Displays the file directory in NVRAM.</p> <p>Example:</p> <table border="1"> <thead> <tr> <th>Entry</th> <th>Type</th> <th>SRAM Addr</th> <th>EEP Offset</th> <th>Length</th> <th>Execute</th> <th>Version</th> </tr> </thead> <tbody> <tr> <td></td> <td>Boot Code</td> <td>08003000</td> <td>00000200</td> <td>000011B0</td> <td>CPUA(2)</td> <td>5721-v6.17</td> </tr> <tr> <td>0</td> <td>PXE</td> <td>00010000</td> <td>000013Bo</td> <td>0000C854</td> <td>NO</td> <td>7.0.1</td> </tr> <tr> <td>1</td> <td>AdvancedFw CFG</td> <td>00000000</td> <td>0001027C</td> <td>000001D4</td> <td>NO</td> <td>IPMIc V2.15</td> </tr> <tr> <td>2</td> <td>AdvancedFw CPUB</td> <td>C0034000</td> <td>00010450</td> <td>00002654</td> <td>NO</td> <td>IPMIc V2.15</td> </tr> <tr> <td>3</td> <td>AdvancedFw CPUA</td> <td>08000000</td> <td>00012AA4</td> <td>000035B4</td> <td>NO</td> <td>IPMIc V2.15</td> </tr> <tr> <td>4</td> <td>AdvancedFwINIT</td> <td>C0034000</td> <td>00016058</td> <td>00001A94</td> <td>CPUB</td> <td>IPMIc V2.15</td> </tr> </tbody> </table>	Entry	Type	SRAM Addr	EEP Offset	Length	Execute	Version		Boot Code	08003000	00000200	000011B0	CPUA(2)	5721-v6.17	0	PXE	00010000	000013Bo	0000C854	NO	7.0.1	1	AdvancedFw CFG	00000000	0001027C	000001D4	NO	IPMIc V2.15	2	AdvancedFw CPUB	C0034000	00010450	00002654	NO	IPMIc V2.15	3	AdvancedFw CPUA	08000000	00012AA4	000035B4	NO	IPMIc V2.15	4	AdvancedFwINIT	C0034000	00016058	00001A94	CPUB	IPMIc V2.15
Entry	Type	SRAM Addr	EEP Offset	Length	Execute	Version																																												
	Boot Code	08003000	00000200	000011B0	CPUA(2)	5721-v6.17																																												
0	PXE	00010000	000013Bo	0000C854	NO	7.0.1																																												
1	AdvancedFw CFG	00000000	0001027C	000001D4	NO	IPMIc V2.15																																												
2	AdvancedFw CPUB	C0034000	00010450	00002654	NO	IPMIc V2.15																																												
3	AdvancedFw CPUA	08000000	00012AA4	000035B4	NO	IPMIc V2.15																																												
4	AdvancedFwINIT	C0034000	00016058	00001A94	CPUB	IPMIc V2.15																																												
setpxe	<p>Enables/disables Preboot Exchange Environment (PXE) and sets PXE speed</p> <p>setpxe e = Enable PXE</p> <p>setpxe d = Disable PXE</p> <p>setpxe s 0 = Auto (Default)</p> <p>setpxe s 1 = 10 Mbps speed, half-duplex operation</p> <p>setpxe s 2 = 10 Mbps speed, full-duplex operation</p> <p>setpxe s 3 = 100 Mbps speed, half-duplex operation</p> <p>setpxe s 4 = 100 Mbps speed, full-duplex operation</p>																																																	
setasf	<p>Enables/disables Alert Standard Format (ASF)</p> <p>Do not use. Alert Standard Format (ASF) is not for system platforms.</p>																																																	
setmba	<p>Enables/disables Multi Boot Agent (MBA) and selects the MBA protocol</p> <p>setmba d = Disable MBA</p> <p>setmba e 0 = Enable Preboot Execution Environment (PXE) MBA (default)</p> <p>setmba e 1 = Enable Remote Program Load (RPL) MBA</p> <p>setmba e 2 = Enable Boot Protocol (BootP) MBA</p> <p>setmba s 0 = Auto speed and duplex (default)</p> <p>setmba s 1 = 10 Mbps speed, half-duplex operation</p> <p>setmba s 2 = 10 Mbps speed, full-duplex operation</p> <p>setmba s 3 = 100 Mbps speed, half-duplex operation</p> <p>setmba s 4 = 100 Mbps speed, full-duplex operation</p> <p>setmba s 6 = 1000 Mbps full-duplex (fiber)</p>																																																	
setipmi	<p>Enables/disables Intelligent Platform Management Interface (IPMI)</p> <p>setipmi e = Enable IPMI</p> <p>setipmi d = Disable IPMI</p>																																																	
nictest	<p>Runs the specified diagnostic tests</p> <p>Specify which individual test(s) within a group or which group(s) of tests to run by</p>																																																	

	including the test designation or group designation in the command string, as shown in the examples below: <code>nicctest abcd</code> = Run all tests <code>nicctest b</code> = Run all tests in group B <code>nicctest a3b1</code> = Run tests A3 and B1 only <code>nicctest a124b2</code> = Run tests A1, A2, A4, and B2
exit	Changes from the Broadcom CLI mode to the MS-DOS command prompt mode
device	Selects the device (adapter) <code>device <n></code> = Device number in hexadecimal notation (default = 00000000) <code>device r</code> = Remove all current Broadcom adapters and rescan available adapters <code>device s</code> = Silent mode (adapters are not displayed)
version	Displays the version of the adapter software
help	Displays this list of commands
reset	Resets the D-Link NetXtreme Gigabit Ethernet chip <code>reset c</code> = Simulate a cold reset <code>reset w</code> = Wait for firmware signature <code>reset t</code> = Display the time from reset to firmware invert signature
cls	Clears the screen
asfprg	Loads Alert Standard Format (ASF) into NVRAM Do not use. Alert Standard Format (ASF) is not for system platforms.

 NOTE: The values for settings are in decimal notation unless otherwise indicated.

6.4 Diagnostic Test Descriptions

The diagnostic tests are divided into 4 groups: Register Tests (Group A), Memory Tests (Group B), Miscellaneous Tests (Group C), and Driver Associated Tests (Group D). The diagnostic tests are listed and described in Table 3.

Table 3: Diagnostic Tests		
Test		Description
Number	Name	
Group A: Register Tests		
A1	Indirect Register	This test uses an indirect addressing method to write an increment of data to the MAC hash register table and read back data for verification. The memory read/write is done 100 times while incrementing test data.
A2	Control	Each register specified in the configuration content defines the

	Register	<p>read-only bit and the read/write bits. The test writes 0s and 1s to the test bits to ensure the read-only bits are not changed, and that read/write bits are changed.</p> <p>This test attempts to read the register configuration file (Ctrlreg.txt) for the register definitions. If the file does not exist, a default register offset and mask bits are used.</p> <table> <tr> <td>Offset</td> <td>Read-Only Mask</td> <td>Read/Write Mask</td> </tr> <tr> <td>0x00000400</td> <td>0x00000000</td> <td>0x007FFF8C</td> </tr> <tr> <td>0x00000404</td> <td>0x03800107</td> <td>0x00000000</td> </tr> </table>	Offset	Read-Only Mask	Read/Write Mask	0x00000400	0x00000000	0x007FFF8C	0x00000404	0x03800107	0x00000000
Offset	Read-Only Mask	Read/Write Mask									
0x00000400	0x00000000	0x007FFF8C									
0x00000404	0x03800107	0x00000000									
A3	Interrupt	This test verifies the interrupt functionality. It enables an interrupt and waits 500 ms for the interrupt to occur and reports an error if it cannot generate the interrupt.									
A4	Built-In Self-Test	This is the hardware built-in self-test (BIST).									
A5	PCI Cfg Register	This test verifies the access integrity of the PCI configuration registers.									
Group B: Memory Tests											
B1	Scratch Pad	<p>This test tests the onboard scratchpad SRAM. The following tests are performed:</p> <p>Address Test. This test writes each address with a unique increment of data and reads back data to ensure data is correct. After filling the entire address with the unique data, the program reads back the data again to ensure that the data is still correct.</p> <p>Walking bit. For each address, data one is written and read back for testing. Then it shifts the data left one bit, so the data becomes two and repeats the same test. It repeats the test 32 times until the test bit is shifted out of the test address. The same test is repeated for entire test range.</p> <p>Pseudo-Random Data. A precalculated pseudo-random data set is used to write unique data to each test RAM. After passing the test, the program reads back the data one more time to ensure that the data is still correct.</p> <p>Data Read/Write Test: This test writes test data to the SRAM and reads it back to ensure that the data is correct. The test data used is 0x00000000, 0xFFFFFFFF, 0xAA55AA55, and 0x55AA55AA.</p> <p>Alternate Data Pattern Test. This test writes test data into the</p>									

		SRAM, writes complement test data to the next address, and reads back both to ensure the data is correct. After the test, the program reads back data one more time to ensure that the data is still correct. The test data used is 0x00000000, 0xFFFFFFFF, 0xAA55AA55, and 0x55AA55AA.
B2	BD SRAM	This test tests the Buffer Descriptor (BD) SRAM. This test performs in the same way as the Scratch Pad Test described in B1.
B3	DMA SRAM	This test tests the direct memory access (DMA) SRAM by performing the Scratch Pad Test described in test B1.
B4	MBUF SRAM	This test tests the memory access buffer (MBUF) SRAM by performing the Scratch Pad Test described in test B1.
B5	MBUF SRAM via DMA	<p>This test uses 8 data test patterns. A 0x1000-sized data buffer is used for this test. Before each pattern test, the buffer is initialized and filled with the test pattern. It then performs a 0x1000-sized transmit DMA from the host buffer to the adapter MBUF memory.</p> <p>The test verifies the data integrity in the adapter MBUF memory against the host memory and repeats the DMA for the entire MBUF buffer. Then, the test performs a receive DMA from the adapter to the host. The 0x1000-byte test buffer is cleared to 0 before each receive DMA. After the test verifies the integrity of the data, the test is repeated for the entire MBUF SRAM range. The 8 test patterns are described below.</p> <p>Test Pattern Description</p> <p>16 00s and 16 FF's Fills the entire host DMA buffer with 16 bytes of 00s and then 16 bytes of FF's.</p> <p>16 FF's and 16 00s Fills the entire host DMA buffer with 16 bytes of FF's and then 16 bytes of 00s.</p> <p>32 00s and 32 FF's Fills the entire host DMA buffer with 32 bytes of 00s and then 32 bytes of FF's.</p> <p>32 FF's and 32 00s Fills the entire host DMA buffer with 32 bytes of FF's and then 32 bytes of 00s.</p> <p>00000000 Fills the entire host DMA buffer with all 00s.</p> <p>FFFFFFFF Fills the entire host DMA buffer with all FF's.</p>

		AA55AA55 Fills the entire host DMA buffer with data 0xAA55AA55. 55AA55AA Fills the entire host DMA buffer with data 0x55AA55AA.																								
B7	CPU GPR	This test tests the CPU General Purpose registers and performs in the same way as the Scratch Pad Test (B1) over 3 different voltages (1.1V, 1.2V, and 1.3V).																								
Group C: Miscellaneous Tests																										
C1	NVRAM	Incremental test data is used in the electrically erasable programmable read-only memory (EEPROM) test. The test fills the test range with test data and reads the data back to verify the content. Afterwards, the test fills the test range with 0s to clear the memory.																								
C2	CPU	This test opens the Cpu.bin file. If the file exists and content is good, the test loads code to the RX CPU and TX CPU and verifies the CPU execution.																								
C3	DMA	This test tests both high-priority direct memory access (DMA) and low-priority DMA. The test moves data from the host memory to the adapter SRAM and verifies the data. The test then moves data back to the host memory to again verify the data.																								
C4	MII	<p>The medium independent interface (MII) test function is identical to that of the Control Register Test (A2). Each register specified in the configuration contents defines the read-only and read/write bits. The test writes 0s and 1s to the test bits to ensure that the read-only bit values are not changed and that the read/write bits are changed.</p> <p>The test attempts to read the register configuration file (Miireg.txt) for the register definitions. If the file does not exist, the following table is used:</p> <table border="1"> <thead> <tr> <th>Offset</th> <th>Read-Only Mask</th> <th>Read/Write Mask</th> </tr> </thead> <tbody> <tr> <td>0x00</td> <td>0x0000</td> <td>0x7180</td> </tr> <tr> <td>0x02</td> <td>0xFFFF</td> <td>0x0000</td> </tr> <tr> <td>0x03</td> <td>0xFFFF</td> <td>0x0000</td> </tr> <tr> <td>0x04</td> <td>0x0000</td> <td>0xFFFF</td> </tr> <tr> <td>0x05</td> <td>0xEFFF</td> <td>0x0000</td> </tr> <tr> <td>0x06</td> <td>0x0001</td> <td>0x0000</td> </tr> <tr> <td>0x07</td> <td>0x0800</td> <td>0xB7FF</td> </tr> </tbody> </table>	Offset	Read-Only Mask	Read/Write Mask	0x00	0x0000	0x7180	0x02	0xFFFF	0x0000	0x03	0xFFFF	0x0000	0x04	0x0000	0xFFFF	0x05	0xEFFF	0x0000	0x06	0x0001	0x0000	0x07	0x0800	0xB7FF
Offset	Read-Only Mask	Read/Write Mask																								
0x00	0x0000	0x7180																								
0x02	0xFFFF	0x0000																								
0x03	0xFFFF	0x0000																								
0x04	0x0000	0xFFFF																								
0x05	0xEFFF	0x0000																								
0x06	0x0001	0x0000																								
0x07	0x0800	0xB7FF																								

		0x08 0xFFFF 0x0000 0x09 0x0000 0xFF00 0x0A 0x7C00 0x0000 0x10 0x0000 0xFFBF 0x11 0x7C00 0x0000 0x19 0x7C00 0x0000 0x1E 0x0000 0xFFFF 0x1F 0x0000 0xFFFF
C5	VPD	The VPD test first saves the contents of the vital product data (VPD) memory before performing the test. The test then writes 1 of the 5 test data patterns (0xFF, 0xAA, 0x55, increment data, or decrement data) into VPD memory. By default, an incremental data pattern is used. The test writes and reads back the data for the entire test range, and then restores the original contents of the VPD memory.
C6	ASF Hardware	<p>Reset Test. This test sets the reset bit and polls for self-clearing bits. This test verifies the reset value of the registers.</p> <p>Event Mapping Test. This test sets the SMB_ATTN bit. By changing ASF_ATTN_LOC bits, the test verifies the mapping bits in TX_CPU or RX_CPU event bits.</p> <p>Counter Test</p> <ul style="list-style-type: none"> • Clears WG_TO, HB_TO, PA_TO, PL_TO, RT_TO bits (by setting the bits) and ensures that the bits clear. • Clears the timestamp counter. Writes a 1 to each of the PL, PA, HB, WG, RT counters. Sets the TSC_EN bit. • Polls each PA_TO bit and counts up to 50. Checks if the PL_TO bit is set at the end of the count to 50. Continues to count up to 200. Checks if all other TO bits are set and verifies if the timestamp counter is incremented.
C7	Expansion ROM	This test tests the ability to enable, disable, and access the expansion read-only memory (ROM) on the adapter.
C8	CPU Fetch	This test tests the PCU instruction fetch logic 100 times.
Group D: Driver Associated Tests		

D1	MAC Loopback	This test is an internal loopback data transmit/receive test. It initializes the medium access control (MAC) into an internal loopback mode and transmits 100 packets. The data should be routed back to the receive channel and received by the receive routine, which verifies the integrity of data. A 100-Mbit/s data rate is used for this test unless Gigabit Ethernet is enabled.
D2	PHY Loopback	This test is same as the MAC loopback test (D1), except that the data is routed back via a physical layer device (PHY). A 100-Mbit/s data rate is used for this test unless Gigabit Ethernet is enabled.
D5	MII Miscellaneous	This test tests the autopolling and PHY interrupt capabilities. These are functions of the PHY.
D6	MSI	This test tests the message signal interrupt (MSI) capability of the adapter. Refer to PCI Specification, version 2.3, for the MSI definition.

6.5 Diagnostic Test Messages

```

/* 0 */      "PASS",
/* 1 */      "Got 0x%08X @ 0x%08X. Expected 0x%08X",
/* 2 */      "Cannot perform task while chip is running",
/* 3 */      "Invalid NIC device",
/* 4 */      "Read-only bit %s got changed after writing zero
at offset 0x%X",
/* 5 */      "Read-only bit %s got changed after writing one
at offset 0x%X",
/* 6 */      "Read/Write bit %s did not get cleared after writing zero
at offset 0x%X",
/* 7 */      "Read/Write bit %s did not get set after writing one
at offset 0x%X",
/* 8 */      "BIST failed",
/* 9 */      "Could not generate interrupt",
/* 10 */     "Aborted by user",
/* 11 */     "TX DMA:Got 0x%08X @ 0x%08X. Expected 0x%08X",
/* 12 */     "Rx DMA:Got 0x%08X @ 0x%08X. Expected 0x%08X",

```

```
/* 13 */      "TX DMA failed",
/* 14 */      "Rx DMA failed",
/* 15 */      "Data error, got 0x%08X at 0x%08X, expected 0x%08X",
/* 16 */      "Second read error, got 0x%08X at 0x%08X, expected
0x%08X",
/* 17 */      "Failed writing EEPROM at 0x%04X",
/* 18 */      "Failed reading EEPROM at 0x%04X",
/* 19 */      "EEPROM data error, got 0x08X at 0x04X, expected 0x%08X",
/* 20 */      "Cannot open file %s",
/* 21 */      "Invalid CPU image file %s",
/* 22 */      "Invalid CPU image size %d",
/* 23 */      "Cannot allocate memory",
/* 24 */      "Cannot reset CPU",
/* 25 */      "Cannot release CPU",
/* 26 */      "CPU test failed",
/* 27 */      "Invalid Test Address Range\nValid NIC address is
0x%08X-0x%08X and exclude 0x%08X-0x%08X",
/* 28 */      "DMA:Got 0x%08X @ 0x%08X. Expected 0x%08X",
/* 29 */      "Unsupported PhyId %04X:%04X",
/* 30 */      "Too many registers specified in the file, max is %d",
/* 31 */      "Cannot write to VPD memory",
/* 32 */      "VPD data error, got %08X @ 0x04X, expected %08X",
/* 33 */      "No good link! Check Loopback plug",
/* 34 */      "Cannot TX Packet!",
/* 35 */      "Requested to TX %d. Only %d is transmitted",
/* 36 */      "Expected %d packets. Only %d good packet(s) have been
received\n%d unknown packets have been received.\n%d bad packets
have been received.",
/* 37 */      "%c%d is an invalid Test",
/* 38 */      "EEPROM checksum error",
/* 39 */      "Error in reading WOL/PXE",
/* 40 */      "Error in writing WOL/PXE",
/* 41 */      "No external memory detected",
```

```
/* 42 */      "DMA buffer %04X is large, size must be less than %04X",
/* 43 */      "File size %d is too big, max is %d",
/* 44 */      "Invalid %s",
/* 45 */      "Failed writing 0x%x to 0x%x",
/* 46 */      "",
/* 47 */      "Ambiguous command",
/* 48 */      "Unknown command",
/* 49 */      "Invalid option",
/* 50 */      "Cannot perform task while chip is not running. (need
driver)",
/* 51 */      "Cannot open register define file or content is bad",
/* 52 */      "ASF Reset bit did not self-clear",
/* 53 */      "ATTN_LOC %d cannot be mapped to %cX CPU event bit %d",
/* 54 */      "%s Register is not cleared to zero after reset",
/* 55 */      "Cannot start poll_ASF Timer",
/* 56 */      "poll_ASF bit did not get reset after acknowledged",
/* 57 */      "Timestamp Counter is not counting",
/* 58 */      "%s Timer is not working",
/* 59 */      "Cannot clear bit %s in %cx CPU event register",
/* 60 */      "Invalid \"EEPROM_FILENAME\" file size, expected %d but
only can read %d bytes",
/* 61 */      "Invalid magic value in %s, expected %08x but found %08x",
/* 62 */      "Invalid manufacture revision, expected %c but found %c",
/* 63 */      "Invalid Boot Code revision, expected %d.%d but found
%d.%d",
/* 64 */      "Cannot write to EEPROM",
/* 65 */      "Cannot read from EEPROM",
/* 66 */      "Invalid Checksum",
/* 67 */      "Invalid Magic Value",
/* 68 */      "Invalid MAC address, expected
%02X-%02X-%02X-%02X-%02X-%02X",
/* 69 */      "Slot error, expected an UUT to be found at location
%02X:%02X:00",
```

```
/* 70 */      "Adjacent memory has been corrupted while testing block  
0x%08x-0x%08x\nGot 0x%08x @ address 0x%08x. Expected 0x%08x",  
/* 71 */      "The function is not Supported in this chip",  
/* 72 */      "Packets received with CRC error",  
/* 73 */      "MII error bits set: %04x",  
/* 74 */      "CPU does not initialize MAC address register correctly",  
/* 75 */      "Invalid firmware file format",  
/* 76 */      "Resetting TX CPU Failed",  
/* 77 */      "Resetting RX CPU Failed",  
/* 78 */      "Invalid MAC address",  
/* 79 */      "Mac address registers are not initialized correctly",  
/* 80 */      "EEPROM Bootstrap checksum error",
```

Chapter 7: Troubleshooting

 **NOTE:** For additional information, go to *Broadcom Ethernet NIC Frequently Asked Questions* at http://www.broadcom.com/support/ethernet_nic/faq_drivers.php

7.1 Hardware Diagnostics

Loopback diagnostic tests are available for testing the adapter hardware. These tests provide access to the adapter internal/external diagnostics, where packet information is transmitted across the physical link (for instructions and information on running tests in an MS-DOS environment, see User Diagnostics. For Windows environments, see Running Diagnostic Tests).

7.1.1 BACS Diagnostic Tests Failures

If any of the following tests fail while running the diagnostic tests from the Running Diagnostic Tests tab in BACS, this may indicate a hardware issue with the NIC or LOM that is installed in the system.

- Control Registers
- EEPROM
- Internal Memory
- On-Chip CPU
- Test LED

Below are troubleshooting steps that may help correct the failure.

1. Remove the failing device and reseal it in the slot, ensuring the card is firmly seated in the slot from front to back.
2. Rerun the test.
3. If the card still fails, replace it with a different card of the same model and run the test. If the test passes on the known good card, contact your hardware vendor for assistance on the failing device.
4. Power down the machine, remove AC power from the machine, and then reboot the system.
5. Remove and re-install the diagnostic software.
6. Contact your hardware vendor.

7.1.2 BACS Network Test Failures

Typically, the BACS Testing the Network failures are the result of a configuration problem on the network or with the IP addresses. Below are common steps when troubleshooting the network.

1. Verify that the cable is attached and you have proper link.
2. Verify that the drivers are loaded and enabled.
3. Replace the cable that is attached to the NIC/LOM.
4. Verify that the IP address is assigned correctly using the command "ipconfig" or by checking the OS IP assigning tool.
5. Verify that the IP address is correct for the network to which the adapter(s) is connected.

7.2 Troubleshooting Checklist

 **CAUTION! Before you open the case of your system, review Safety Precautions.**

The following checklist provides recommended actions to take to resolve problems installing the D-Link NetXtreme Gigabit Ethernet adapter or running it in your system.

- Inspect all cables and connections. Verify that the cable connections at the network adapter and the switch are attached properly.
- Check the adapter installation by reviewing Installing the Hardware. Verify that the adapter is properly seated in the slot. Check for specific hardware problems, such as obvious damage to board components or the PCI edge connector.
- Check the configuration settings and change them if they are in conflict with another device.
- Verify that your system is using the latest BIOS.
- Try inserting the adapter in another slot. If the new position works, the original slot in your system may be defective.
- Replace the failed adapter with one that is known to work properly. If the second adapter works in the slot where the first one failed, the original adapter is probably defective.
- Install the adapter in another functioning system and run the tests again. If the adapter passed the tests in the new system, the original system may be defective.
- Remove all other adapters from the system and run the tests again. If the adapter passes the tests, the other adapters may be causing contention.

7.3 Checking for Network Link and Activity

See Testing Network Connectivity or Viewing Adapter Information to check the state of the network link and activity as indicated by the port LEDs.

7.4 Checking if Current Drivers are Loaded

Windows

See Vital Signs in Viewing Adapter Information to view useful information about the adapter, its link status, and network connectivity.

NetWare

To verify that the driver is loaded properly, type

```
LOAD B57.LAN FRAME_ETHERNET_II NAME=B57_1_EII
```

This command automatically verifies if the link is active. If the link is active, the command returns Link is up.

From the command line, type `config` then press ENTER. The following status information is displayed:

```
D-Link NetXtreme Gigabit Ethernet Adapter
Version:
Hardware Setting:
Node Address:
Frame Type:
Board Name:
LAN Protocol: ARP (see note)
LAN Protocol: IP Addr: (see note)
```

 **NOTE:** The LAN protocol status is displayed after an IP address is assigned to the adapter.

Linux

To verify that the TG3 Linux driver is loaded properly, run:

```
lsmod | grep tg3
```

If the driver is loaded, a line similar to the one below is displayed, where *size* is the size of the driver in bytes, and *n* is the number of adapters configured.

Module	Size	Used by
TG3	<i>size</i>	<i>n</i>

7.5 Testing Network Connectivity

 **NOTE:** When using forced link speeds, verify that both the adapter and the switch are forced to the same speed, or that both sides are configured for auto-negotiation.

Windows

Use the ping command to determine if the network connection is working.

 **NOTE:** Network connectivity can also be tested using the Testing the Network feature in Broadcom Advanced Control Suite 2.

1. Click **Start**, and then click **Run**.
2. Type **cmd** in the **Open** box, and then click **OK**.
3. Type **ipconfig /all** to view the network connection to be tested.
4. Type **ping IP address**, and then press ENTER.

The ping statistics that are displayed indicate whether the network connection is working or not.

NetWare

Ping an IP host on the network to verify connection has been established:

From the command line, type **ping IP address**, and then press ENTER.

The ping statistics that are displayed indicate whether the network connection is working or not.

Linux

To verify that the Ethernet interface is up and running, run **ifconfig** to check the status of the Ethernet interface. It is possible to use **netstat -i** to check the statistics on the Ethernet interface. Go to Linux Driver Software for information on **ifconfig** and **netstat**.

Ping an IP host on the network to verify connection has been established:

From the command line, type **ping IP address**, and then press ENTER.

The ping statistics that are displayed indicate whether the network connection is working or not.

7.6 Software Problems and Solutions

7.6.1 How to Add a Third-Party OEM Network Adapter to a RIS Installation

Problem: An error is encountered when attempting to load the Broadcom device driver for a 32-bit version of Windows XP, or later operating system, using a Windows 2000 Remote Installation Server: *File b57w2k.sys caused an unexpected error (21) at line 3752 in d:\xpsp1\base\boot\setup\setup.c.*

Solution: A modification to the b57win32.inf file can be made to allow for the installation to complete successfully. This will be in conjunction with instructions from the Microsoft Knowledge Base Article 315279 that describe "How to Add Third-Party OEM Network Adapters to RIS Installations."

Requirement: The Windows 2000 Server must be running Service Pack 3 or later.

1. Obtain the latest driver for your Broadcom adapter. The driver files included for the Broadcom 57xx adapter are b57win32.inf, b57win32.cat, and b57xp32.sys.
2. Create a copy of the b57win32.inf and b57xp32.sys files and save them in a separate folder called RIS. This allows you to distinguish the duplicate files from the originals.
3. For the b57win32.inf file located in the RIS folder, make the following change using a text editor such as Notepad:
 - a. Locate **[Manufacturer]** within the file.
 - b. Review the line below which reads: **%BRCM% = Broadcom, NTx86.5.1, NTamd64.**

- c. Modify that line to read: **%BRCM% = Broadcom.NTx86.5.1, NTamd64.**
(The change replaces the comma and the space after "Broadcom" with a period.
 - d. Save the file.
 4. On the RIS server, copy the b57win32.inf and b57xp32.sys files from the RIS folder to the RemoteInstall\Setup\Language\Images\Dir_name\i386 folder. This allows Setup to use the driver during the text-mode portion of the installation.
 - a. At the same level as the i386 folder on the RIS image, create a \$oem\$ folder. Use the recommended structure: \ \$oem\$ \ \$1 \ Drivers \ Nic
 - b. Copy the original b57win32.inf, b57xp32.sys, and b57win32.cat driver files to this folder.
 - c. Make the following changes to the **.sif** file that is used for this image installation:

```
[Unattended]
OemPreinstall = yes
OemPnpDriversPath = \Drivers\Nic
```
 5. Stop and then restart the Remote Installation service on the RIS server by typing the following from a command prompt:

```
net stop binlsv
net start binlsv
```

7.6.2 RIPREP Utility Problem

Problem: The following message is received when attempting to deploy a RIPREP image through Remote Installation Services (RIS): *"The operating system image you selected does not contain the necessary drivers for your network adapter. Try selecting a different operating system image. If the problem persists, contact your administrator. Setup cannot continue. Press any key to exit."*

Solution: This problem is not isolated to the Broadcom adapter. However, based on several inquiries, we are publishing the following instructions based on other customers successfully working around this issue:

1. Place the Broadcom driver files in the original image folder (the image folder created when risetup.exe was executed for the first time).

Example: i:\RemoteInstall\Setup\English\Images\ (Original Image)

2. Place the Broadcom driver files in the i386 subfolder under the original image folder.

Example: i:\RemoteInstall\Setup\English\Images*(Original Image)*\i386

3. Place the Broadcom driver files for the network adapter in the RIPREP Image folder.

Example: i:\RemoteInstall\Setup\English\Images*(RIPREP Image)*

4. Place the Broadcom adapter drivers in the i386 subfolder where the RIPREP Image is located.

Example: i:\RemoteInstall\Setup\English\Images*(RIPREP Image)*\i386

The Microsoft Knowledge base articles listed below were used as a reference for the following instructions:

<http://support.microsoft.com/default.aspx?scid=kb;EN-US;254078>

<http://support.microsoft.com/default.aspx?scid=kb;EN-US;246184>

1. Create the following path and place all Broadcom driver files in ..*(RIPREP Image)*\%oem%\\$1\Drivers.
2. Edit the riprep.sif file located in ..*(RIPREP Image)*\i386\Template to include the following information under the [Unattend] section:

```
OemPreinstall = yes  
OemPnPDriversPath = "Drivers  
DriverSigningPolicy = Ignore
```

3. Create the following path and place all Broadcom driver files in ..*(Original Image)*\%oem%\\$1\Drivers.
4. Edit the ristndrd.sif file located in ..*(Original Image)*\i386 \templates to include the following information under the [Unattend] section:

```
OemPreinstall = yes  
OemPnPDriversPath = "Drivers  
DriverSigningPolicy = Ignore
```

5. Restart the Remote Installation service. This can be performed from a command line with the following commands:

```
net stop binlsv  
net start binlsv
```

7.6.3 Linux and ASFIPMon

Problem: I brought down the interface and now I cannot bring it back up. When I try, the following message appears, `SIOCSIFFLAGS: Resource temporarily unavailable.'

Solution: When ASFIPMon is running, it does a quick access to flash ROM every 30 seconds or so. If the interface is brought down while this is happening, you cannot bring the interface back up in the usual way. To bring up the interface, unload and then reload the driver module.

7.6.4 Broadcom Boot Agent

Problem: Unable to obtain network settings through DHCP using PXE.

Solution: For proper operation make sure that the Spanning Tree Protocol (STP) is disabled or that portfast mode (for Cisco) is enabled on the port to which the PXE client is connected. For instance, set `spantree portfast 4/12 enable`.

7.6.5 Broadcom Advanced Server Program (BASP)

Problem: The 802.3ad team member links disconnect and reconnect continuously (applies to all operating systems).

Solution: This is a third-party issue. It is seen only when configuring an 802.3ad team with more than 2 members on the system and connecting to an HP2524 switch, with LACP enabled as passive or active. The HP switch shows an LACP channel being brought up successfully with only 2 team members. All other team member links disconnect and reconnect. This does not occur with a Cisco Catalyst 6500.

Problem: A Generic Trunking (GEC/FEC) 802.3ad-Draft Static type of team may lose some network connectivity if the driver to a team member is disabled.

Solution: If a team member supports underlying management software (ASF/IPMI/UMP) or Wake-On-LAN, the link may be maintained on the switch for the adapter despite its driver being disabled. This may result in the switch continuing to pass traffic to the attached port rather than route the traffic to an active team member port. Disconnecting the disabled adapter from the switch will allow traffic to resume to the other active team members.

Problem: The teaming changes I made when I modified my team using INETCFG did not take effect.

Solution: When you modify a team using INETCFG, you may need to reboot after reinitialization for the changes to the team to take effect.

7.6.6 Miscellaneous

Problem: Although installed, the Broadcom Advanced Control Suite (BACS) application does not start.

Solution: .NET Framework 2.0 is required for BACS to operate. Install .NET Framework 2.0.

Problem: When the bus on the system is operating in PCI mode, the D-Link NetXtreme Gigabit Ethernet adapter performs at PCI mode if it is added after the system has booted.

Solution: When the system is booted up without any adapter, the bus operates at the lowest mode, which is PCI mode. Reboot the system after the adapter has been added.

Problem: The D-Link NetXtreme Gigabit Ethernet adapter may not perform at optimal level on some systems if it is added after the system has booted.

Solution: The system BIOS in some systems does not set the cache line size and the latency timer if the adapter is added after the system has booted. Reboot the system after the adapter has been added.

Problem: Large Send Offload (LSO) and Checksum Offload are not working on my team.

Solution: If one of the adapters on a team does not support LSO, LSO does not function for the team. Remove the adapter that does not support LSO from the team, or replace it with one that does. The same applies to Checksum Offload.

Problem: When using the TG3 driver and Red Hat 4 (with any release prior to release 6), after setting the speed and duplex with ethtool, autonegotiation is disabled and cannot be restored.

Solution: Unload or reload the TG3 driver, or upgrade to the latest version of ethtool.

Problem: A DCOM error message (event ID 10016) appears in the System Event Log during the installation of the Broadcom adapter drivers.

Solution: This is a Microsoft issue. For more information, see Microsoft knowledge base KB913119 at <http://support.microsoft.com/kb/913119>.

