

Advanced Control Suite

Gigabit Ethernet Network Adapters

AT-2916SX

AT-2931SX

AT-2972SX

AT-2972SX/2

AT-2972T/2

User's Guide

Copyright © 2007 Allied Telesis, Inc.

All rights reserved. No part of this publication may be reproduced without prior written permission from Allied Telesis, Inc.

Microsoft and Internet Explorer are registered trademarks of Microsoft Corporation. Netscape Navigator is a registered trademark of Netscape Communications Corporation. All other product names, company names, logos or other designations mentioned herein are trademarks or registered trademarks of their respective owners.

Allied Telesis, Inc. reserves the right to make changes in specifications and other information contained in this document without prior written notice. The information provided herein is subject to change without notice. In no event shall Allied Telesis, Inc. be liable for any incidental, special, indirect, or consequential damages whatsoever, including but not limited to lost profits, arising out of or related to this manual or the information contained herein, even if Allied Telesis, Inc. has been advised of, known, or should have known, the possibility of such damages.

Contents

Preface	7
Where to Find Web-based Guides	8
Contacting Allied Telesis	9
Online Support	9
Email and Telephone Support	9
Returning Products	9
Sales or Corporate Information	9
Management Software Updates	9
Chapter 1: Advanced Server Program Overview	11
Broadcom Advanced Server Program (BASP) Overview	12
Broadcom Advanced Control Suite 2 (BACS 2) Features	13
BASP for Windows 2000, Windows 2003, and Windows XP	14
Failover and Load Balance	14
Virtual LAN (VLANs)	14
Chapter 2: Broadcom Advanced Control Suite 2 (BACS 2) Applications	15
Overview	16
Information Provided by the BACS 2 Applications	17
BACS 2 Features	17
Installing the BACS 2 Application	19
Installing Using the GUI	19
Using Silent Installation	19
Managing the BACS Application	21
Initializing the BACS 2 Application	21
Updating the BACS Application	21
Removing the BACS Application	21
Configuring the BACS 2 Application	23
Vital Sign Tab	23
Resources Tab	25
Hardware Tab	26
Advanced Tab	27
Network Test Tab	31
Diagnostics Tab	31
Cable Analysis Tab	33
Statistics Tab	34
General Statistics	35
IEEE 802.3 Statistics	36
Custom Statistics	36
BASP Statistics Tab	37
Configuring Teaming	39
Creating a Team Using the Wizard	40
Creating a Team Using the Expert Mode	50
Modifying a Team	54
Viewing the Team Properties and Statistics	59
Chapter 3: Installing BACS on Windows 2000, Windows 2003, and Windows XP Systems	61
Installing the BASP	62
Uninstalling the BASP	63

Chapter 4: Key Protocols and Interfaces	65
Adapter Teaming	66
Smart Load Balancing (SLB)™	66
Link Aggregation (802.3ad)	66
Generic Link Aggregation (Trunking).....	66
Smart Load Balance Auto-Failback Disable	67
Failover Teaming	68
VLANs Overview.....	69
VLANs Support.....	71
Adaptive Interrupt Frequency	71
Dual DMA Channels	71
32-bit or 64-bit PCI Bus Master	72
ASIC with Embedded RISC Processor.....	72
Chapter 5: Troubleshooting	73
Verifying the Correct Drivers are Loaded.....	74
Windows	74
Software Problems and Solutions.....	75
Windows 2000	75
Broadcom Advanced Server Program (BASP).....	76

Figures

Figure 1. Advanced Control Suite 2 Menu.....	16
Figure 2. Vital Sign Tab	23
Figure 3. Resources Tab	25
Figure 4. Hardware Tab.....	26
Figure 5. Advanced Tab	27
Figure 6. Network Test Tab	31
Figure 7. Diagnostics Tab.....	32
Figure 8. Cable Analysis Tab.....	33
Figure 9. Statistics Tab	35
Figure 10. BASP Statistics Tab	38
Figure 11. New Team Configuration Window.....	39
Figure 12. Broadcom Teaming Wizard Welcome Page.....	41
Figure 13. Team Name Page	41
Figure 14. Team Type Page	42
Figure 15. Assigning Team Members Page	43
Figure 16. Team Member Selection	44
Figure 17. Team Standby Member Page.....	44
Figure 18. Standby Member Selection	45
Figure 19. Configuring LiveLink Page.....	46
Figure 20. Configure VLAN Support Page.....	46
Figure 21. VLAN Naming Page	47
Figure 22. VLAN Tagging Page.....	48
Figure 23. Additional VLANs Page	49
Figure 24. Final Teaming Wizard Page	49
Figure 25. Commit Changes Warning Message.....	50
Figure 26. Team Properties Tab.....	50
Figure 27. Broadcom Teaming Wizard Welcome Page.....	51
Figure 28. New Team Configuration.....	51
Figure 29. New Team Configuration Menu.....	52
Figure 30. Team Properties Tab.....	54
Figure 31. Add VLAN Dialog Box	56
Figure 32. VLAN Name Selected.....	57
Figure 33. Save As Dialog Box.....	58
Figure 34. Open Dialog Box	58
Figure 35. Example of Servers Supporting Multiple VLANs with Tagging.....	69
Figure 36. Vital Sign Tab for Troubleshooting	74

Preface

This guide contains instructions on how to install and configure the Advanced Control Suite software for the AT-29xxSX Gigabit Ethernet network adapters on Windows 2000, Windows 2003, and Windows XP platforms. For information about how to install the adapters as well as procedures to install and configure the related software, see the *Gigabit Ethernet Network Adapters Installation Guide* (part number 613-000049).

The Preface contains the following sections:

- “Where to Find Web-based Guides” on page 8
- “Contacting Allied Telesis” on page 9

Where to Find Web-based Guides

The installation and user guides for all Allied Telesis products are available in portable document format (PDF) on our web site at **www.alliedtelesis.com**. You can view the documents online or download them onto a local workstation or server.

Contacting Allied Telesis

This section provides Allied Telesis contact information for technical support as well as sales and corporate information.

Online Support

You can request technical support online by accessing the Allied Telesis Knowledge Base: <http://kb.alliedtelesis.com>. You can use the Knowledge Base to submit questions to our technical support staff and review answers to previously asked questions.

Email and Telephone Support

For Technical Support via email or telephone, refer to the Support & Services section of the Allied Telesis web site: www.alliedtelesis.com.

Returning Products

Products for return or repair must first be assigned a return materials authorization (RMA) number. A product sent to Allied Telesis without an RMA number will be returned to the sender at the sender's expense.

To obtain an RMA number, contact Allied Telesis Technical Support through our web site: www.alliedtelesis.com.

Sales or Corporate Information

You can contact Allied Telesis for sales or corporate information through our web site: www.alliedtelesis.com. To find the contact information for your country, select Contact Us -> Worldwide Contacts.

Management Software Updates

New releases of management software for our managed products are available from either of the following Internet sites:

- Allied Telesis web site: www.alliedtelesis.com
- Allied Telesis FTP server: <ftp://ftp.alliedtelesis.com>

If you prefer to download new software from the Allied Telesis FTP server from your workstation's command prompt, you will need FTP client software and you must log in to the server. Enter "anonymous" for the user name and your email address for the password.

Chapter 1

Advanced Server Program Overview

This chapter provides an introduction to the Allied Telesis Advanced Server Program and contains following sections:

- ❑ “Broadcom Advanced Server Program (BASP) Overview” on page 12
- ❑ “Broadcom Advanced Control Suite 2 (BACS 2) Features” on page 13
- ❑ “BASP for Windows 2000, Windows 2003, and Windows XP” on page 14

Broadcom Advanced Server Program (BASP) Overview

BASP is an intermediate software driver for Windows 2000, Windows 2003, and Windows XP that provides load-balancing, fault-tolerance, and VLAN features.

The BASP features are provided by creating teams (virtual adapters) that consist of multiple NIC interfaces. A team can consist of one to eight NIC interfaces. You can designate each interface as a primary or standby* interface. 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. VLANs can be added to a team to allow multiple VLANs with different VLAN IDs. A virtual adapter is created for each VLAN added. Load-balancing and fault-tolerance features work with any third party's NIC adapters, but are only supported with the Allied Telesyn Gigabit Ethernet adapters. VLANs only work with the Allied Telesyn Gigabit Ethernet adapters.

Note

*You can use Standby only in Smart Load-Balance mode (see Limitations below).

Smart Load-balance (SLB) mode 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. In comparison, IPX traffic is load-balanced in the outbound direction only. Other protocol packets are sent and received through one primary NIC only. Fault-tolerance for non-IP traffic is only supported using the Allied Telesyn Gigabit Ethernet adapters. The Generic Trunking mode 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). This mode is protocol-independent and all traffic should be load-balanced and fault-tolerant.

Note

Allied Telesis recommends that you disable the spanning tree protocol at the switch when you use BASP. This setting minimizes the downtime due to spanning tree loop determination when failing over.

Note

The Broadcom Advanced Server Program (BASP) requires that at least one adapter in the team be an Allied Telesyn Gigabit Ethernet adapters.

Broadcom Advanced Control Suite 2 (BACS 2) Features

The Broadcom Advanced Control Suite 2 (BACS 2) is a graphical user interface with the following functions. (See Chapter 2, "Broadcom Advanced Control Suite 2 (BACS 2) Applications" on page 15 for additional information.)

- ❑ Vital Sign – The Vital Sign screen allows you to view vital adapter information, network status, and network connectivity. Active Adapters are listed.
- ❑ Resources – Shows the system resources of the selected device.
- ❑ Hardware – Shows the hardware information (the ASIC version and the firmware version) for the selected device.
- ❑ Network Test – The Network Test screen allows you to verify IP network connectivity. This test verifies if the NDIS driver is installed correctly. Also, it tests connectivity to a gateway or other specified IP address on the same subnet.
- ❑ Diagnostics – The Diagnostics screen allows you to view information about adapters. This function is used to test the network interface card.
- ❑ Configuration – Sets configuration options (NIC Battery Saving Mode, for example).
- ❑ Statistics – The Statistics screen allows you to view traffic statistics for the Allied Telesyn Gigabit Ethernet adapters as well as adapters from other vendors. Statistical values and coverage is more comprehensive for the Allied Telesyn Gigabit Ethernet adapters.
- ❑ Load Balance/Virtual LAN – The Load Balance/Virtual LANs screen allows you to configure advanced features. You can configure any available adapter as part of a team.

BASP for Windows 2000, Windows 2003, and Windows XP

The following options are supported under Windows 2000, Windows 2003, and Windows XP. For additional information, see Chapter 3, “Installing BACS on Windows 2000, Windows 2003, and Windows XP Systems” on page 61.

Failover and Load Balance

- Adapter teaming for failover
- Smart Load Balance™
- Smart Load Balance (auto-failback disable)
- Generic Link Aggregation (GEC/FEC, Open trunk)
- Link aggregation (IEEE 802.3ad)

Virtual LAN (VLANs)

- Up to 64 VLANs (63 tagged and 1 untagged) per adapter using IEEE 802.1Q-1988 tagging. VLANs are supported only on the Allied Telesyn Gigabit Ethernet adapters.

Chapter 2

Broadcom Advanced Control Suite 2 (BACS 2) Applications

This chapter describes the Broadcom Advanced Control Suite 2 (BACS 2) applications and contains the following sections:

- “Overview” on page 16
- “Installing the BACS 2 Application” on page 19
- “Managing the BACS Application” on page 21
- “Configuring the BACS 2 Application” on page 23
- “Configuring Teaming” on page 39

Note

There are two BACS 2 versions. One is a 32-bit version located in /BACS/IA32 for standard (32-bit) Windows 2000/2003/XP operating systems. The other is a 64-bit version located in /BACS/x64 for Windows 2003 and Windows XP 64-bit operating systems.

Overview

The Broadcom Advanced Control Suite 2 (BACS 2) application is an integrated application (with a graphical user interface) that provides useful information about each network adapter that is installed in your computer. The BACS application also enables you to perform detailed tests, diagnostics, and analyses on each adapter, as well as view traffic statistics and set configuration options for each adapter, as shown in Figure 1. The BACS application is designed to run on the Windows 2000, Windows 2003, and Windows XP operating systems.

The Broadcom Advanced Server Program (BASP) application, which runs within BACS, is used to configure load balancing, fault tolerance, and virtual local area networks (VLANs). This application is available only on computers that use more than one network adapter.

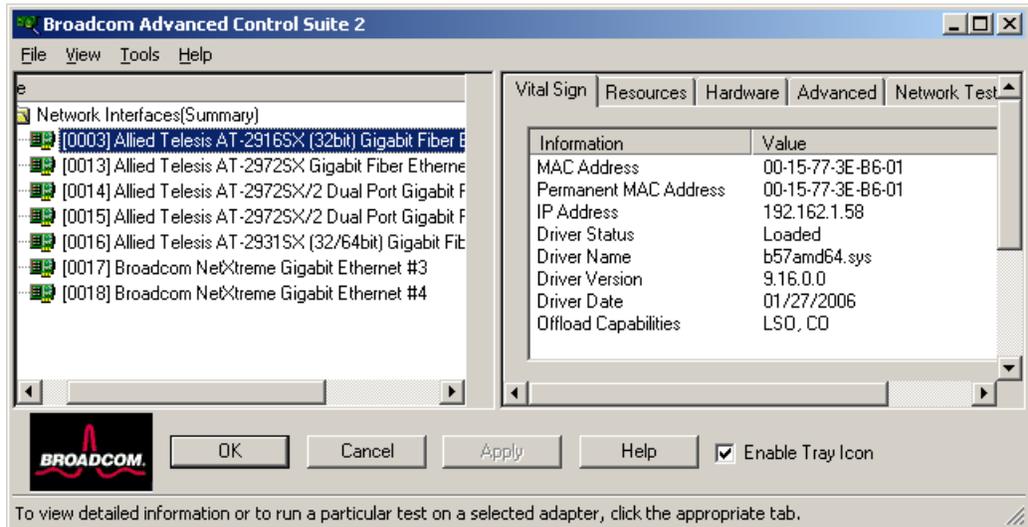


Figure 1. Advanced Control Suite 2 Menu

Information Provided by the BACS 2 Applications

The Broadcom Advanced Control Suite 2 lists all of the network adapters in your computer and provides the following information, if available, about each device, as shown in Table 1.

Table 1. BACS Application Information

Driver Status	Driver Version	Frames Rx OK
MAC Address	Driver Date	Team Name
Link Status	Firmware Version	Team Type
IP Address	ASIC Version	VLAN Name
Memory Address	Bus Type	VLAN ID
Physical Address	Bus No.	BASP Tx Packet
Speed	Device No.	BASP Tx Packet Discarded
Duplex	Function No.	BASP Tx Packet Queried
Slot No.	Interrupt Request	BASP Rx Packet
Driver Name	Frames Tx OK	BASP Rx Packet Discarded

BACS 2 Features

The following features are accessible from the BACS 2 application:

- ❑ “Vital Sign Tab” on page 23. Provides at-a-glance status reports on all of the LAN devices in your computer.
- ❑ “Resources Tab” on page 25. Displays the system resources of the selected device.
- ❑ “Hardware Tab” on page 26. Displays the hardware information (the ASIC version and the firmware version) for the selected device.
- ❑ “Advanced Tab” on page 27. Allows you to change the advanced properties.
- ❑ “Network Test Tab” on page 31. Confirms network connectivity to a remote station. The network test sends ICMP packets to remote systems and waits for a response. If a gateway is configured, the test automatically sends packets to that system. If a gateway is not configured or if the gateway is unreachable, the test prompts you for a destination IP address.
- ❑ “Diagnostics Tab” on page 31. Performs comprehensive diagnostics on Broadcom network adapters.
- ❑ “Statistics Tab” on page 34. Provides detailed performance statistics on each selected device.

- ❑ “BASP Statistics Tab” on page 37. Configures the load balance and failover by grouping multiple network adapters.

Installing the BACS 2 Application

You can install the BACS 2 software through the GUI or by using the silent install option. See the following procedures:

- “Installing Using the GUI,” next
- “Using Silent Installation” on page 19

Note

Before installing the BACS 2 software on a computer running Windows 2000 Advanced Server with Terminal Services, type **change user /install** from the DOS command prompt.

Installing Using the GUI

To install the BACS 2 application using the GUI (graphical user interface), perform the following procedure.

Note

Before you begin the installation, close all applications, windows, and dialog boxes

1. Double-click **setup.exe** in the appropriate directory (IA32 or x64).
2. Click **Next** in **Broadcom Management Programs Setup**.
3. Read the license agreement and click **I accept**.
4. In **Select Components**, click the component you want to install:
 - Control Suite**. Installs the Broadcom Advanced Server Control Suite.
 - BASP**. Installs the Broadcom Advanced Server Program.
5. Follow the on-screen instructions.

You can start the Control Suite from the Control Panel by double-clicking **Broadcom Control Suite 2**. Or, click **Start**, point to **Programs**, point to **Broadcom**, and then click the **Broadcom Advanced Control Suite 2**.

Using Silent Installation

The recommended installation procedure is to copy the installation files to your hard disk before you run the silent install because the **setup /s** command automatically generates a Setup.log file in the directory where it is run.

Note

Before you begin the installation, close all applications, windows, and dialog boxes.

1. Type **setup /s** and press **ENTER**.

Managing the BACS Application

This section contains the following procedures for managing the BACS application:

- “Initializing the BACS 2 Application,” next
- “Updating the BACS Application” on page 21
- “Removing the BACS Application” on page 21

Initializing the BACS 2 Application

To initialize the BACS 2 application on your computer, perform the following procedure.

1. In the Control Panel, double-click **Broadcom Control Suite 2**.

Or, click **Start**, point to **Programs**, point to **Broadcom**, and then click **Broadcom Advanced Control Suite 2**.

Note

You must install the Allied Telesis adapters before you initialize the BACS application.

Updating the BACS Application

To update the BACS application on your computer, perform the following procedure.

Note

Before you begin the update, close all applications, windows, and dialog boxes.

1. Double-click **Setup.exe**.
2. Click **Next** in **Broadcom Management Programs Setup**.
3. Read the license agreement and click **I accept**.
4. In **Select Components**, click the component you want to install:
 - **Control Suite**. Installs the Broadcom Advanced Server Control Suite.
 - **BASP**. Installs the Broadcom Advanced Server Program.
5. Follow the on-screen instructions.

Removing the BACS Application

To remove the BACS application from your computer, perform the following procedure.

1. In the Control Panel, double-click **Add/Remove Programs**.

2. Click **Broadcom Management Programs** and click **Change/Remove** (Windows 2003, Windows XP) or **Add/Remove** (Windows 2000).
3. Click **Next**.
4. In **InstallShield Wizard**, click **Remove**, and then click **Next**.
5. Click **OK** to remove the application and all of its components.
6. Click **OK**.
7. Restart your computer.

Configuring the BACS 2 Application

Start the BACS application and then click the tab on **Broadcom Advanced Control Suite 2** that provides the information of interest or access to the tests, diagnostics, analyses, and configuration functions you want to perform. Or, on the **Tools** menu, click **Create a Team** to start the BASP application. Select from the following tabs:

- “Vital Sign Tab” on page 23
- “Resources Tab” on page 25
- “Hardware Tab” on page 26
- “Advanced Tab” on page 27
- “Network Test Tab” on page 31
- “Diagnostics Tab” on page 31
- “Statistics Tab” on page 34
- “BASP Statistics Tab” on page 37

Vital Sign Tab

The Vital Sign tab contains information about the adapter and other network adapters that are installed, the link status of the network, and network connectivity. To view this information for any installed network adapter, click the name of the device, as shown in Figure 2 on page 23.

Note

Information about network adapters made by other vendors is less comprehensive than the information provided about the Allied Telesis AT-29xxSX series Gigabit Ethernet adapters or other Broadcom-based adapters.

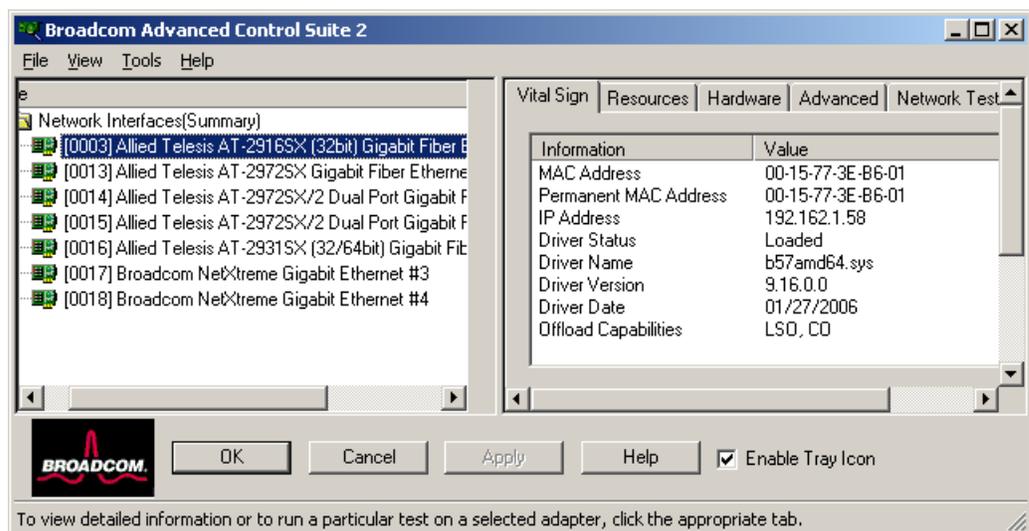


Figure 2. Vital Sign Tab

The Vital Sign tab contains the following fields:

- ❑ **MAC Address.** This address can either be the permanent MAC address or an address assigned by the Locally Administered Address in the Advanced properties tab.
- ❑ **Permanent MAC Address.** This is a physical MAC (media access control) address that is assigned to the device by the manufacturer. The physical address cannot be all 0s.
- ❑ **IP Address.** The network address that is associated with the device. If the IP address is all 0's, the associated driver has not been bound with the Internet Protocol (IP).
- ❑ **Driver Status.** Information about the status of the driver that is associated with the selected controller.
 - **Driver Loaded.** Normal operating mode. The driver that is associated with the device has been loaded by Windows and is functioning.
 - **Driver Not Loaded.** The driver that is associated with the device has not been loaded by Windows.
 - **Information Not Available.** The value is not obtainable from the driver that is associated with the device.
- ❑ **Driver Name/Version/Date.** The file name, version, and creation date of the software driver that is associated with the device.
- ❑ **Offload Capabilities.** The options are:
 - **LSO (Large Send Offload).** The network adapter performs TCP segmentation.
 - **CO (Checksum Offload).** The adapter computes the TCP/IP checksum.
- ❑ **BASP State.** Information about the status of the BASP application. This information is displayed only when there is a team. See “Configuring Teaming” on page 39
- ❑ **Network Status:** The following network status information is provided:
 - **Link Status.** The indicator is green if a link is established. A red indicator means that a link is not established.
 - **Speed.** The link speed of the device.
 - **Duplex.** The duplex mode in which the device is operating.

Resources Tab This section describes the Resources tab, as shown in Figure 3.

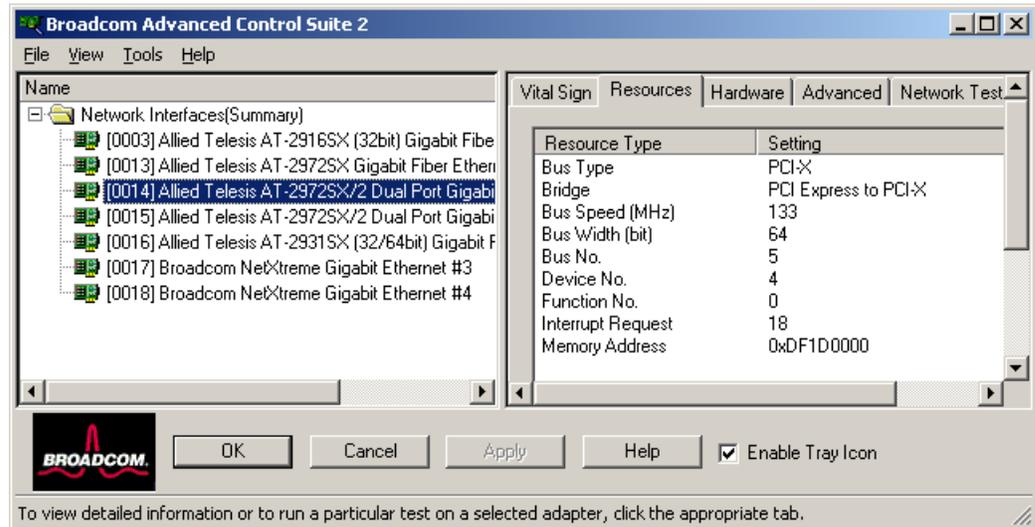


Figure 3. Resources Tab

The Resources tab contains the following fields:

- ❑ **Bus Type.** For PCI devices, indicates the PCI bus type (PCI or PCI-X).
- ❑ **Bridge.** For PCI-E devices, indicates the bridge type.
- ❑ **Slot No.** Indicates the PCI slot number of the installed adapter.
- ❑ **Bus Speed (MHz).** Indicates the PCI bus speed (33, 66, 100, or 133 MHz).
- ❑ **Bus Width (bit).** Indicates the PCI bus data width of either 32 or 64 bits.
- ❑ **Bus No.** Indicates the PCI bus number and the device number for the device.

Example: [0] 14 indicates that the controller resides in PCI bus 0, device 14.

- ❑ **Device No.** The number assigned to the device 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 device. Valid numbers range from 2 to 25.
- ❑ **Memory Address.** The memory mapped address that is assigned to the device. This value can never be 0.

Hardware Tab This section provides a description of the Hardware tab, as shown in Figure 4.

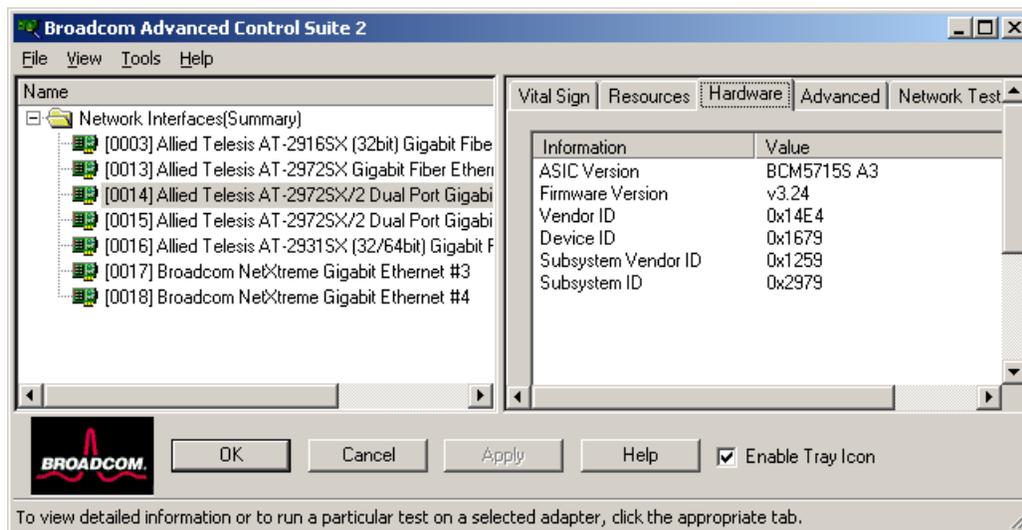


Figure 4. Hardware Tab

The Hardware tab contains the following fields:

- ASIC Version.** The chip version of the adapter. This information is not available for devices made by other vendors.
- Firmware Version.** The firmware version of the adapter. This information is not available for devices made by other vendors.
- Vendor ID.** A unique vendor ID that is registered by the PCI-SIG organization.
- Device ID.** A unique device ID that is registered by Broadcom.
- Subsystem Vendor ID.** A unique vendor ID that is registered by the PCI-SIG organization.
- Subsystem ID.** A unique ID registered by Allied Telesis, Inc.

Advanced Tab

This section describes the Advanced tab, as shown in Figure 5

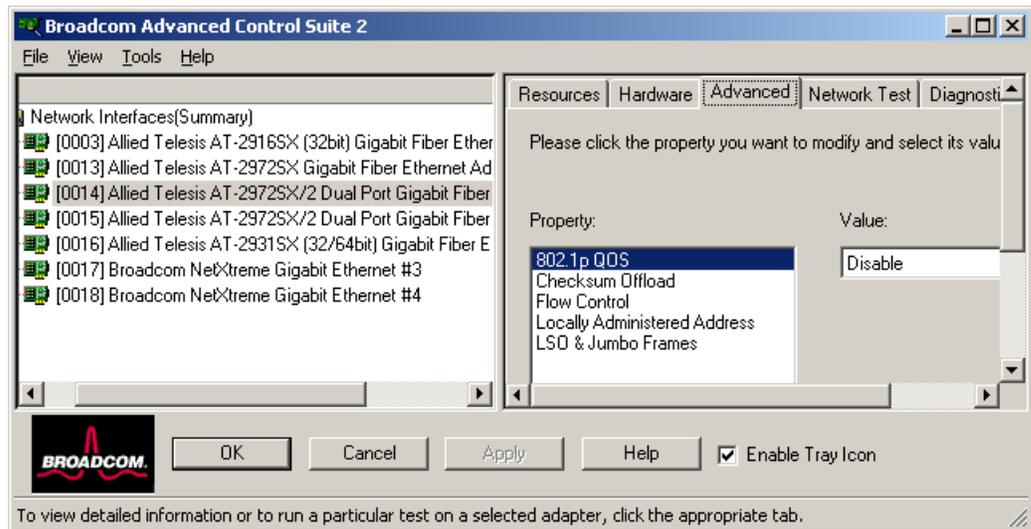


Figure 5. Advanced Tab

The Advanced tab contains the following fields:

- ❑ **802.1p QoS.** The 802.1p QoS property enables quality of service, which is an Institute of Electrical and Electronics Engineering (IEEE) specification that treats different types of network traffic differently to ensure required levels of reliability and latency according to the type of traffic. This property is disabled by default. Unless the network infrastructure supports QoS, do not enable QoS. Otherwise, problems may occur.
- ❑ **Checksum Offload.** Normally the Checksum Offload 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 TCP/IP Checksum. Enables receive TCP, IP, and UDP checksum offloading.
 - Tx TCP/IP Checksum. Enables transmit TCP, IP, and UDP checksum offloading.
 - TX/Rx TCP/IP Checksum (default). Enables transmit and receive TCP, IP, and UDP checksum offloading.
 - None. Disables checksum offloading.
- ❑ **Ethernet@Wirespeed™.** The Ethernet@Wirespeed property enables a Gigabit Ethernet adapter to establish a link at a lower speed when only 2 pairs of wires are available in the cabling plant. By default, this

property is set to Enable. To disable Ethernet@Wirespeed, change the setting to Disable.

Note

This parameter is available only for copper devices and is not displayed for the AT-29xx Series Gigabit Ethernet adapters.

- Disable. Disables Ethernet@Wirespeed.
 - Enable (default). Enables Ethernet@Wirespeed
- **Flow Control.** The Flow Control property enables or disables the receipt or transmission of PAUSE frames. PAUSE frames enable 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.
- **LSO & Jumbo Frames.** The Jumbo property allows 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. If Jumbo frames is not one of the properties listed for a selected adapter, the feature is not supported. BCM5721- and BCM5751-based adapters do not support Jumbo frames.

Frame size is set at 1500 bytes by default when you select 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 LSO property, the TCP segmentation can be done by the network adapter.

- Both Disabled. LSO and Jumbo frames are both disabled.
- LSO Enabled, Jumbo Off (default). LSO is enabled and Jumbo

frames is disabled.

- LSO Off, Jumbo 3000. The Jumbo frame size allowed is 3000 bytes and LSO is off.
 - LSO Off, Jumbo 4500. The Jumbo frame size allowed is 4500 bytes and LSO is off.
 - LSO Off, Jumbo 6000. The Jumbo frame size allowed is 6000 bytes and LSO is off.
 - LSO Off, Jumbo 7500. The Jumbo frame size allowed is 7500 bytes and LSO is off.
 - LSO Off, Jumbo 9000. The Jumbo frame size allowed is 9000 bytes and LSO is 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 0000 0000 0001 to FFFF FFFF FFFD.

* Do not use a multicast address (least significant bit of the high byte = 1).

* Do not use all 0s or all F's.

- **Speed & Duplex.** The Speed & Duplex property sets the connection speed and mode to that of the network. Note that Full-Duplex mode allows the adapter to transmit and receive network data simultaneously.

Note

This parameter is available only for copper devices and is not displayed for the AT-29xxSX Series adapters.

- 10 Mb Full. Sets the speed at 10 Mbit/s and the mode to Full-Duplex.
- 10 Mb Half. Sets the speed at 10 Mbit/s and the mode to Half-

Duplex.

10 Mb Half and 100 Mb Half settings force the network adapter to connect to the network in Half-Duplex mode. The network adapter may not function if the network is not configured to operate at the same mode.

- 100 Mb Full. Sets the speed at 100 Mbit/s and the mode to Full-Duplex.
- 100 Mb Half. Sets the speed at 100 Mbit/s and the mode to Half-Duplex.

10 Mb Full and 100 Mb Full settings force the network adapter to connect to the network in Full-Duplex mode. The network adapter may not function if the network is not configured to operate at the same mode.

- Auto (default). Sets the speed and mode for optimum network connection (recommended). This setting allows the network adapter to dynamically detect the line speed of the network. Whenever the network capability changes, the network adapter automatically adjusts to the new line speed and duplex mode. A speed of 1 Gbit/s is enabled by selecting Auto, when that speed is supported.

- **Wake Up Capabilities.** The Wake Up Capabilities property enables the network adapter to wake up from a low-power mode when it receives a network wake-up frame. Two types of wake-up frames are possible: Magic Packet and Wake Up Frame.

Note

This parameter is available only for copper devices and is not displayed for the AT-29xxSX Series adapters.

- Both (default). Selects both Magic Packet and Wake Up Frame as wake-up frames.
- Magic Packet. Selects Magic Packet as the wake-up frame.
- None. Selects no wake-up frame.
- Wake Up Frame. Selects Wake Up Frame as the wake-up frame and allows the network adapter to wake the system when an event such as a ping or an Address Resolution Protocol (ARP) request is received.

- **WOL Speed.** The WOL Speed property sets the speed at which the network adapter connects to the network while the network adapter is

in Wake on LAN mode. By default, the WOL Speed property is set to Auto.

Note

This parameter is available only for copper devices and is not displayed for the AT-29xxSX Series adapters.

- 10 Mb. Sets the speed to 10 Mbit/s. This is the network speed when the system is in a standby mode awaiting a wake-up frame.
- 100 Mb. Sets the speed to 100 Mbit/s.
- Auto (default). Sets the speed for optimum network connection.

Network Test Tab

In the Network Test tab, you can 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, as shown in Figure 6.

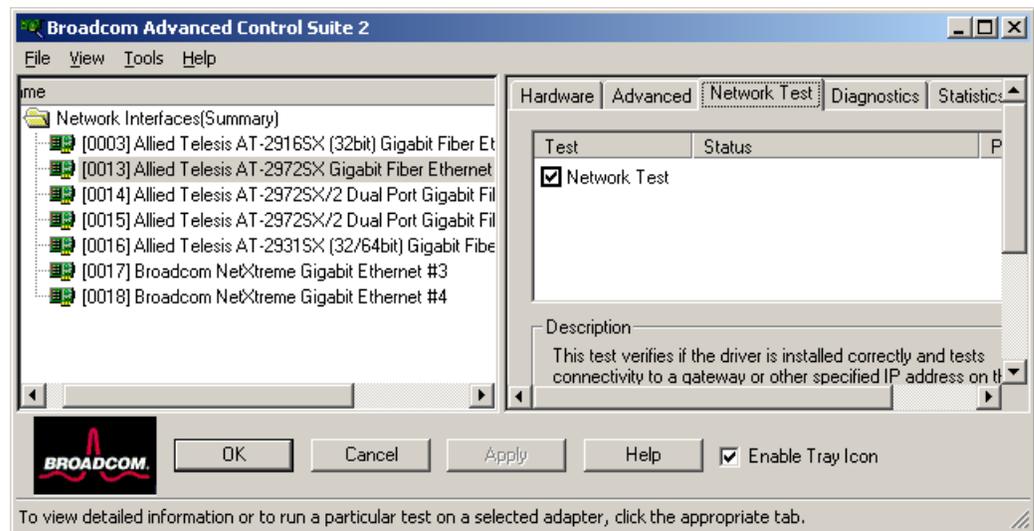


Figure 6. Network Test Tab

Diagnostics Tab

On the Diagnostics tab you can perform diagnostic tests on Allied Telesis network adapters. You use this function to test the physical components of the adapter, as shown in Figure 7 on page 32.

Note

The network connection is temporarily lost when the diagnostic tests are running.

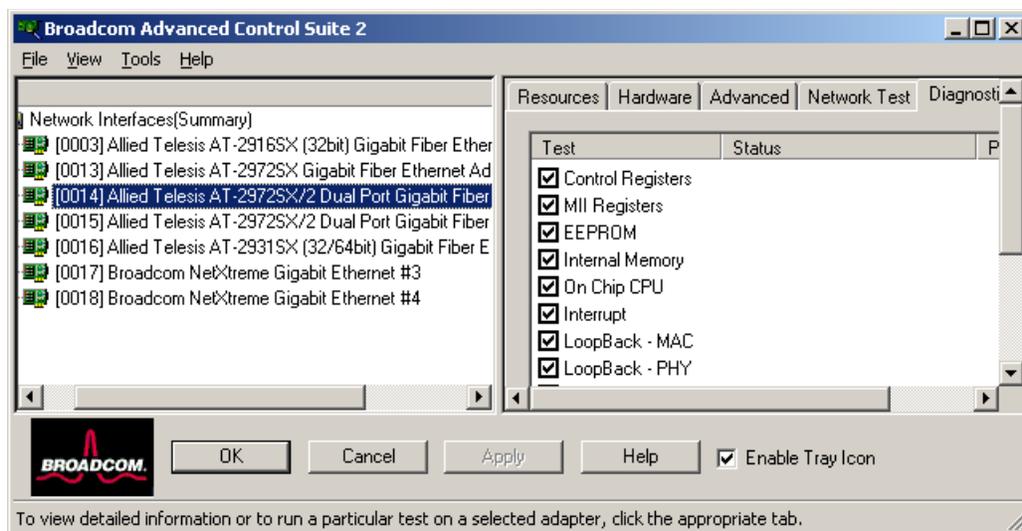


Figure 7. Diagnostics Tab

The Diagnostics tab contains the following fields:

- Control Registers.** This test verifies the read and write capabilities of the network controller registers by writing various values to the registers and verifying the results. The device driver uses these registers to perform network functions such as sending and receiving information. If the test fails, the device may not work properly.
- MII Registers.** This test verifies the read and write capabilities of the registers of the physical layer (PHY). This field is not displayed for fiber adapters.
- 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 device 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 device cannot function without its internal memory.
- On-Chip CPU.** This test verifies the operation of the internal CPUs in the device.

- ❑ **Interrupt.** This test verifies that the NDIS driver is able to receive interrupts from the device.
- ❑ **Loopback MAC.** This test verifies that the Network Device Driver Interface Specification (NDIS) driver is able to send packets to and receive packets from the network microcontroller.
- ❑ **Loopback PHY.** This test verifies that NDIS is able to send packets to and receive packets through the network microcontroller and the integrated PHY chip.
- ❑ **Test LED.** This test causes all of the LEDs to blink 5 times for the purpose of identifying the device.

Cable Analysis Tab

On the Cable Analysis tab, as shown in Figure 8, you can monitor the condition of each wire pair in an Ethernet Category 5 cable connection with an Ethernet network. The analysis measures the cable quality and compares it against the IEEE 802.3ab specification for compliance.

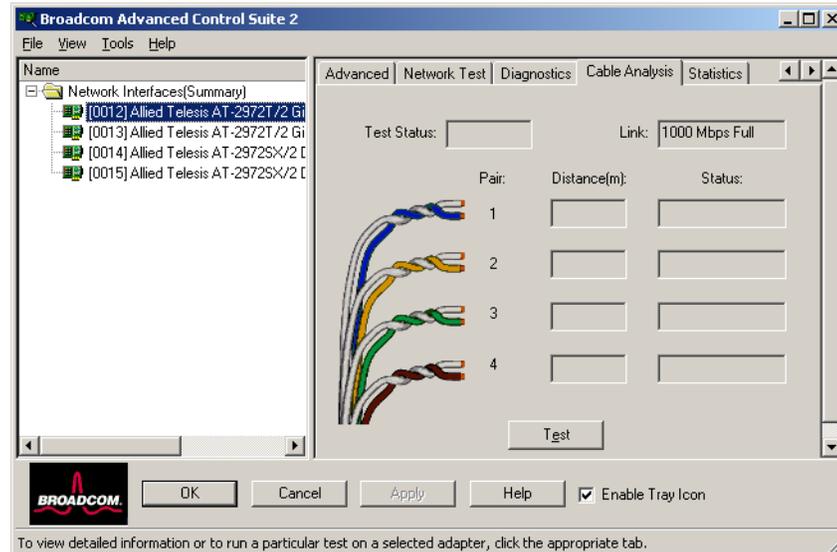


Figure 8. Cable Analysis Tab

Note

You must have administrator privileges to run the cable diagnosis test.

The network connection is temporarily lost during the analysis.

To run a cable analysis, perform the following procedure:

1. Connect the cable to a port on a switch where the port is set to “auto” and the speed and duplex are also set to “auto.”

2. Click the Allied Telesis Gigabit Ethernet adapter listed in the Name pane.
3. Click **Test**.

The Test Status displays one of two options: Complete or Failed. The test results are one of the following:

- Good. Good cable/PCB signal paths, but no Gigabit link.
- Crossed. Pin short or crosstalk along two or more cable/PCB signal paths.
- Open. One or both pins are open for a twisted pair.
- Short. Two pins from the same twisted pair are shorted together.
- Noise. Persistent noise present (most likely caused by Forced 10/100).
- GB Link. A Gigabit link is up and running.
- N/A. Algorithm failed to reach a conclusion.

Note

Valid cable lengths are displayed for all test results except for Noise.

There are several factors that could affect the test results:

- Link partner. Various switch and hub manufacturers implement different PHYs. Some PHYs are not IEEE compliant.
- Cable quality. Category 3, 4, 5, and 8 may affect the test results.
- Electrical interference. The testing environment may affect the test results.

Statistics Tab

On the Statistics tab, shown in Figure 9, you can view traffic statistics for both Allied Telesis network devices and network devices made by other vendors. Statistical information and coverage are more comprehensive for the Allied Telesis adapters.

Note

If an adapter is disabled, team statistics are not displayed.

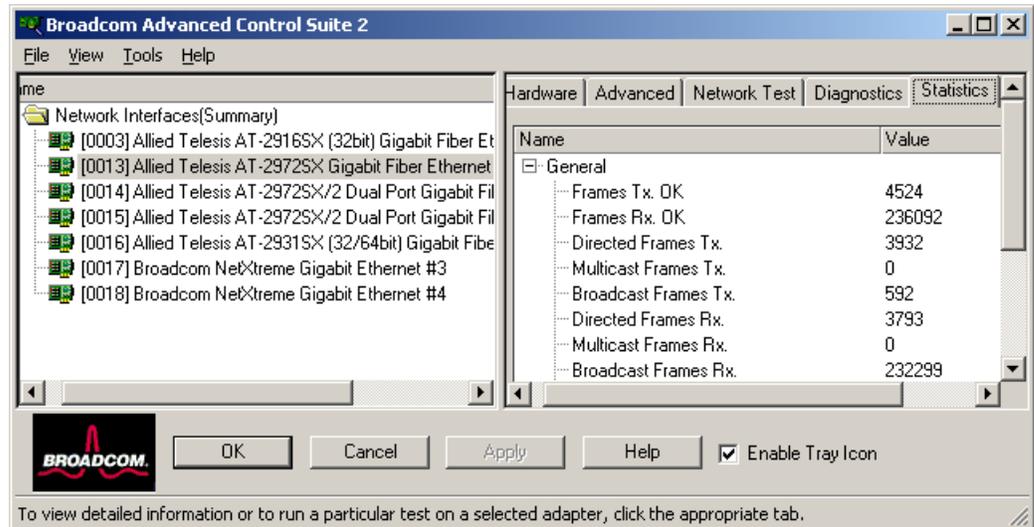


Figure 9. Statistics Tab

General Statistics

Definitions of the general statistics parameters are provided below.

- Frames Tx OK.** A count of frames that are successfully transmitted. This counter is incremented when the transmit status is reported as **Transmit OK**.
- Frames Rx OK.** A count of frames that are successfully received (**Receive OK**). This does not include frames received with frame-too-long, frame check sequence (FCS), length or alignment errors, or frames lost due to internal MAC sublayer errors. This counter is incremented when the receive status is reported as **Receive OK**.
- Directed Frames Tx.** A count of directed data frames that are successfully transmitted.
- Multicast Frames Tx.** A count of frames that are successfully transmitted (as indicated by the status value **Transmit OK**) to a group destination address other than a broadcast address.
- Broadcast Frames Tx.** A count of frames that were successfully transmitted (as indicated by the transmit status **Transmit OK**) to the broadcast address. Frames transmitted to multicast addresses are not broadcast frames and, therefore, are excluded.
- Directed Frames Rx.** A count of directed data frames that are successfully received.
- Multicast Frames Rx.** A count of frames that are successfully received and are directed to an active nonbroadcast group address.

This does not include frames received with frame-too-long, FCS, length errors, alignment errors, or frames lost due to internal MAC sublayer errors. This counter is incremented as indicated by the **Receive OK** status.

- ❑ **Broadcast Frames Rx.** A count of frames that are successfully received and are directed to a broadcast group address. This count does not include frames received with frame-too-long, FCS, length errors, alignment errors, or frames lost due to internal MAC sublayer errors. This counter is incremented as indicated by the **Receive OK** status.

IEEE 802.3 Statistics

Definitions of the IEEE 802.3 statistics parameters are provided below.

- ❑ **Frames Rx with Alignment Error.** A count of frames that are not an integral number of octets in length and do not pass the FCS check. This counter is incremented when the receive status is reported as **Alignment Error**.
- ❑ **Frames Tx with one Collision.** A count of frames that are involved in a single collision and are subsequently transmitted successfully. This counter is incremented when the result of a transmission is reported as **Transmit OK** and the attempt value is 2.
- ❑ **Frames Tx with more than one Collision.** A count of frames that are involved in more than one collision and are subsequently transmitted successfully. This counter is incremented when the transmit status is reported as **Transmit OK**, and the value of the attempts variable is greater than 2 and less or equal to the attempt limit.
- ❑ **Frames Tx after Deferral.** A count of frames whose transmission was delayed on the first attempt because the medium was busy. The frames involved in any collision are not counted.

Custom Statistics

Definitions of the custom statistics parameters are provided below.

Note

Custom statistics are available only for an enabled adapter.

- ❑ **Number of Interrupts generated by this adapter.** The number of interrupts generated by the device.
- ❑ **Number of Interrupts avoided by this adapter.** The number of interrupts avoided by the device.
- ❑ **Tx Max Coalesce Frames Threshold hit.** The number of times the *Send Max Coalesce Frames Threshold* was hit.

- ❑ **Rx Max Coalesce Frames Threshold hit.** The number of times the *Receive Max Coalesce Frames Threshold* was hit.
- ❑ **DMA write Queue was full.** The number of times the *DMA write queue* was full.
- ❑ **DMA write High Priority Queue was full.** The number of times the *DMA write high priority queue* was full.
- ❑ **DMA Read Queue was full.** The number of times the *DMA read queue* was full.
- ❑ **DMA Read High Priority Queue was full.** The number of times the *DMA read high priority queue* was full.
- ❑ **Send Data Completion FTQ was full.** The number of times the *send data completion FTQ (flow through queue)* was full.
- ❑ **NIC ran out of the Recv Buffer.** The number of times the network adapter ran out of the Recv Buffer descriptors.
- ❑ **Frames size less than 64-byte with bad FCS.** The number of frames with a size less than 64 bytes with bad FCS.
- ❑ **MAC Rx w/ Pause Command and Length = 0.** MAC control frames with the **pause** command and a length equal to 0.
- ❑ **MAC Rx w/ Pause Command and Length greater than 0.** MAC control frames with the **pause** command and a length greater than 0.
- ❑ **MAC Rx w/ no Pause Command.** MAC control frames with no **pause** command.
- ❑ **MAC Sent X-on.** MAC Transmit with X-on was on.
- ❑ **MAC Sent X-off.** MAC Transmit with X-on was off.

BASP Statistics Tab

On the BASP Statistics tab you can view performance information about the network adapters that are on a team. To view this information for any team member adapter, click the name of the device. To view the BASP statistics for the team as a whole, click the name of the team, as shown in Figure 10.

Note

To see the BASP Statistics tab, you must have a team.

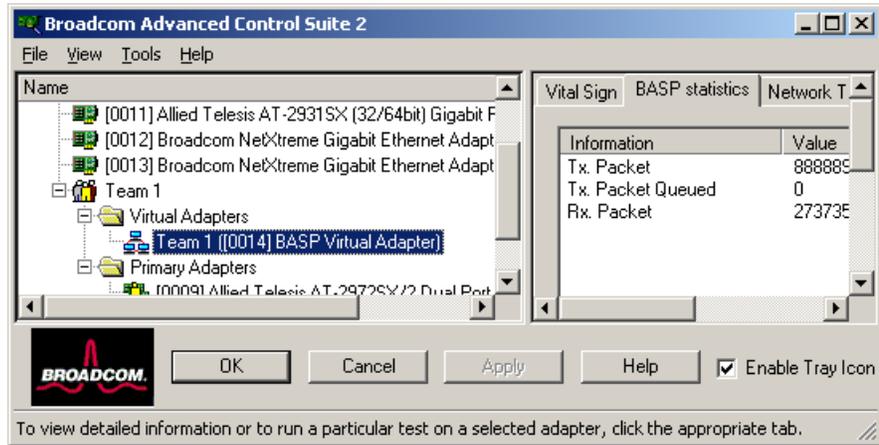


Figure 10. BASP Statistics Tab

The BASP Statistics tab contains the following fields:

Tx. Packet.

The number of packets transmitted.

Tx. Packet Queued

The number of packets in the queue to be transmitted.

Rx. Packet

The number of packets received.

Configuring Teaming

The teaming function allows you to group available network devices together to function as a team. Teaming is a method of creating a virtual LAN (a group of multiple devices that function as a single device). The benefit of this approach is that it enables load balancing and failover. You use BASP to set up teaming. For more information about BASP, see “Overview” on page 16.

Note

BASP is available only on computers that use at least one Allied Telesis Gigabit Ethernet adapter or other Broadcom NetXtreme devices.

An example of teaming is shown in Figure 11. This example shows several network adapters in the **Available Adapters** list. When these adapters are moved to the **Load Balance Members** list, they function as a single adapter—that is, each member shares the traffic burden.

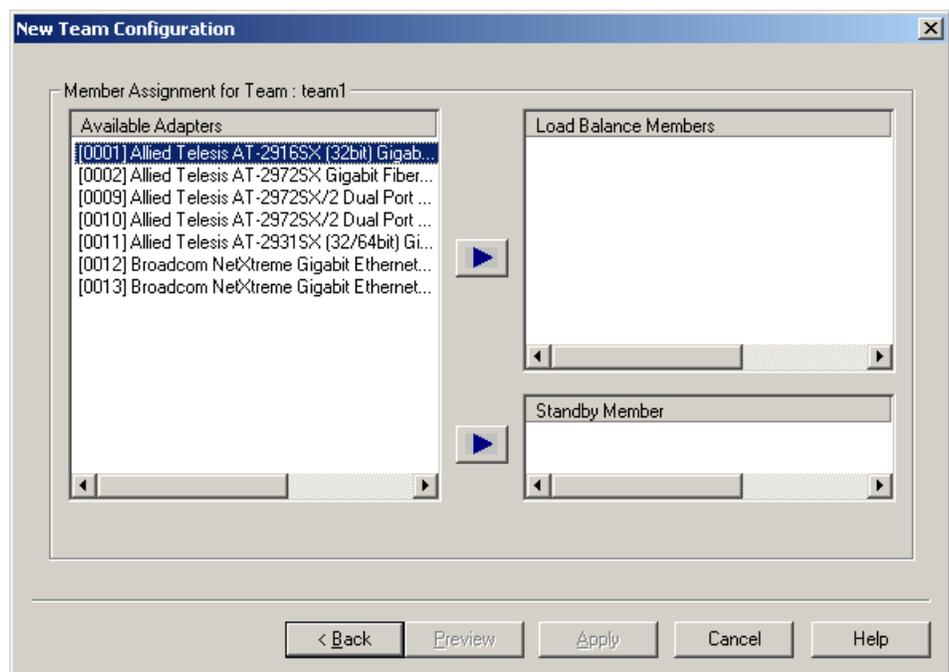


Figure 11. New Team Configuration Window

There are four types of load balance teams:

- ❑ **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 the traffic.

- **Link Aggregation.** 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 team's 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.** This type of team is very similar to the Link Aggregation type in that all of the adapters in the team need to be configured to receive packets for the same MAC address. However, 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. Generic 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 on line, the team continues using the standby member instead of switching 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 when the adapter is removed or installed via the Device Manager or a Hot-Plug PCI application.

Creating a Team Using the Wizard

To create a team using the wizard, perform the following procedure.

1. From the **Tools** menu, click **Create a Team**.

The Welcome page of the Broadcom Teaming Wizard is shown in Figure 12.

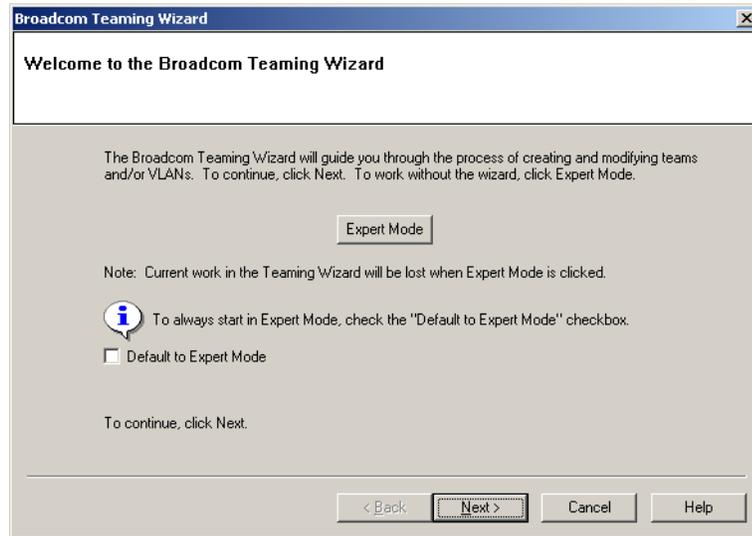


Figure 12. Broadcom Teaming Wizard Welcome Page

2. Click **Next**.

The Team Name page asks for a name for the team, as shown in Figure 13.

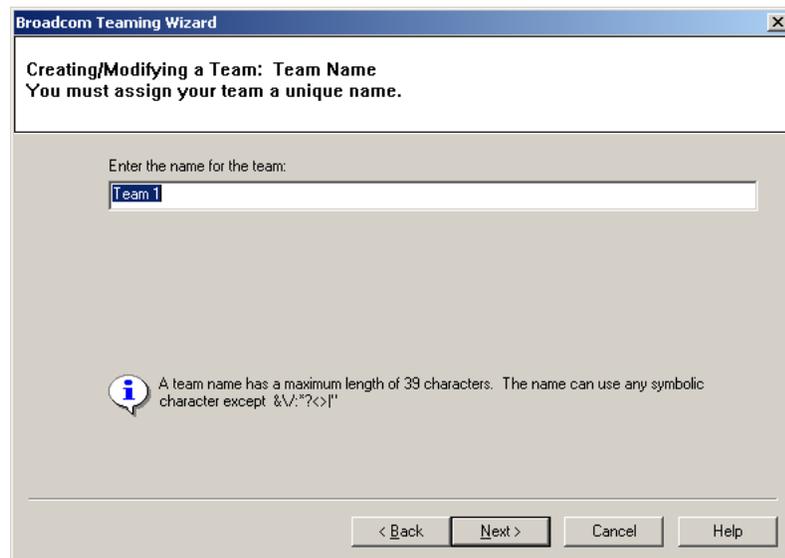


Figure 13. Team Name Page

Note

The number of characters that can be used in a team name is a minimum of 1 and a maximum of 39.

Note

A team name cannot begin with spaces or contain the character "&".

Note

Team names must be unique. If you attempt to use a team name more than once, an error message appears indicating that the name already exists.

Note

The maximum number of members in a team is 8.

Note

When team configuration has been correctly performed, a Virtual Team adapter driver is created for each configured team.

3. Type a name for the team and click **Next**.

The Team Type page, shown in Figure 14, asks you to choose what type of team you want to create.

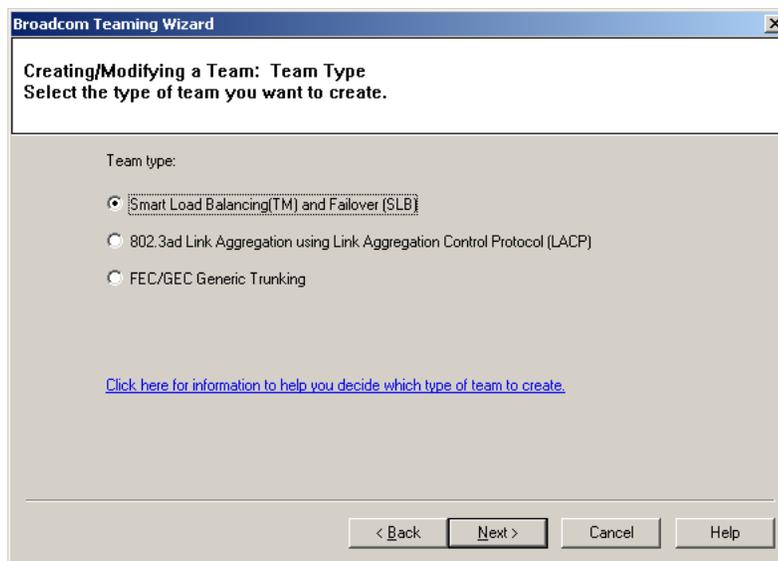


Figure 14. Team Type Page

The options are:

- ❑ **Smart Load Balancing 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 the traffic.
 - ❑ **802.3ad Link Aggregation using Link Aggregation Control Protocol (LACP).** 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 team's 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.
 - ❑ **FEC/GEC Generic Trunking.** This type of team is very similar to the Link Aggregation type in that all of the adapters in the team need to be configured to receive packets for the same MAC address. However, 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. Generic trunking supports load balancing and failover for both outbound and inbound traffic.
4. Select the team type you want to use and click **Next**.

The Assigning Team Members page asks you to specify which adapters you want to include in the team, as shown in Figure 15.

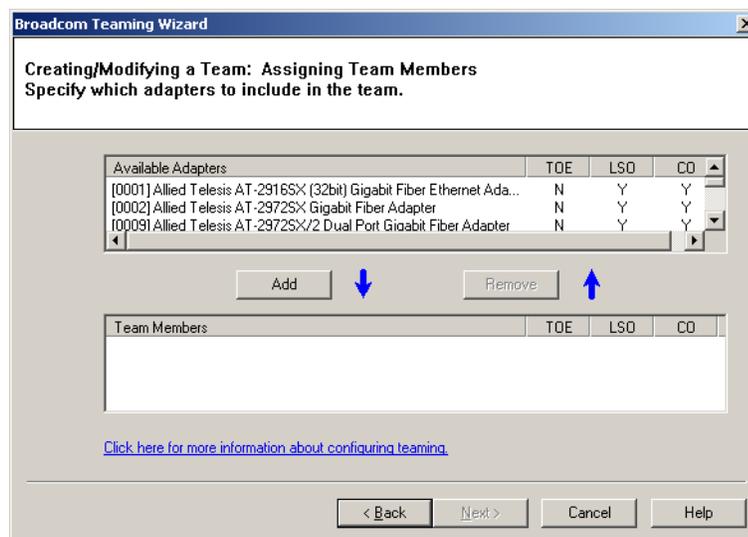


Figure 15. Assigning Team Members Page

5. Add or remove team members from the Available Adapters list to the Team members list, as shown in Figure 16, until you have all the members of the team identified.



Figure 16. Team Member Selection

6. Click **Next**.

The Designating a Standby Member page asks if you want to identify a standby member of the team, as shown in Figure 17.

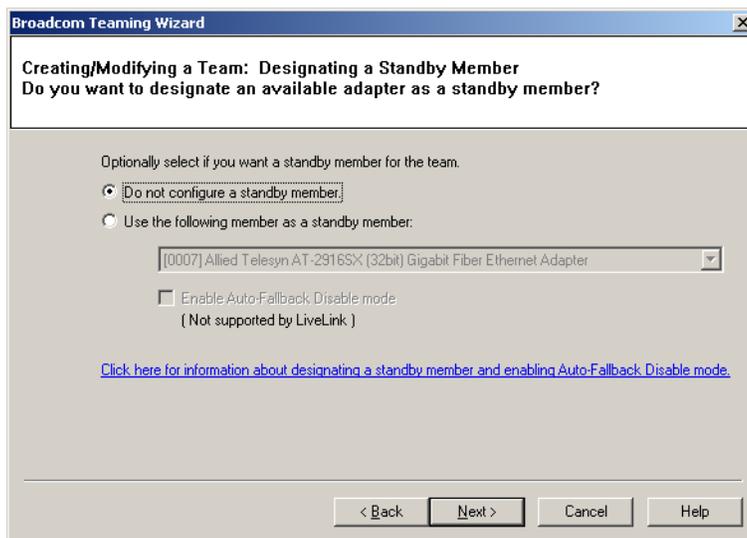


Figure 17. Team Standby Member Page

The options are:

- Do not configure a standby member
- Use the following member as a standby member

- ❑ **Enable Auto-Fallback Disable Mode.** When this option is enabled, 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 the traffic.
7. If you want a standby member, click **Use the following member as a standby member** and select one from the list, as shown in Figure 18.

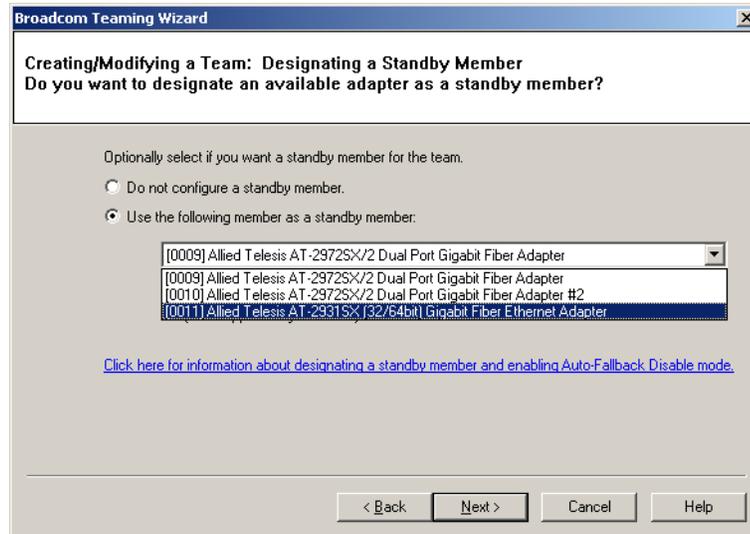


Figure 18. Standby Member Selection

8. Click **Next**.

The Configuring LiveLink page asks if you want to configure LiveLink, as shown in Figure 19.

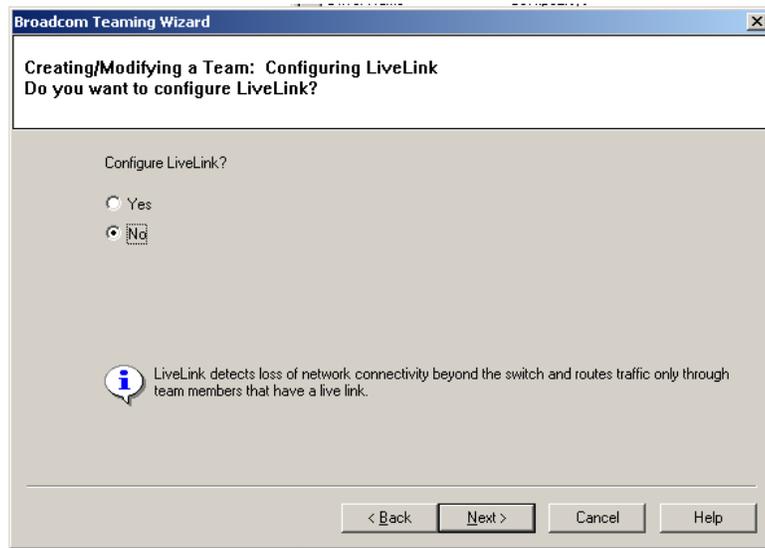


Figure 19. Configuring LiveLink Page

The options are:

- Yes.** When you select this option, another page opens where you configure this feature.
- No.** This option does not allow you to configure LiveLink. This is the default and the setting that Allied Telesis recommends.

9. Click **Next**.

The Configure VLAN Support page, as shown in Figure 20, allows you to create a VLAN.

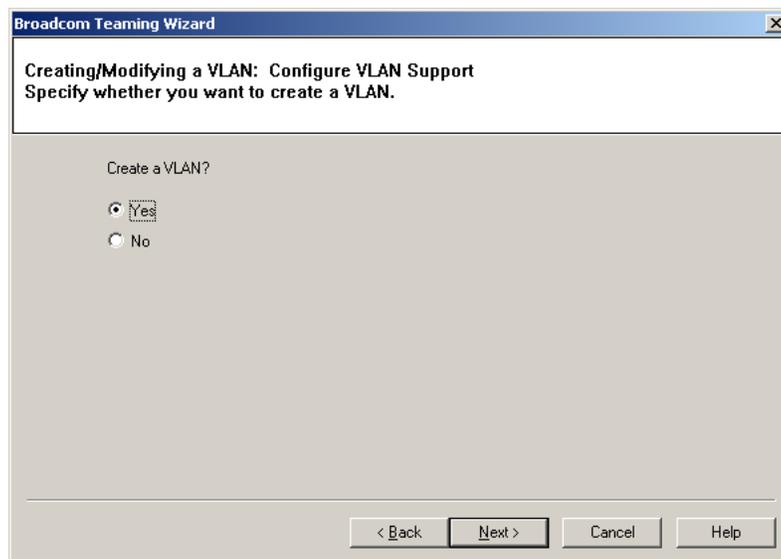


Figure 20. Configure VLAN Support Page

The options are:

- Yes.** Allows you to configure a VLAN. Proceed to step 10.
- No.** Skips the VLAN creation process. Proceed to step 13.

10. Click **Next**.

The VLAN Naming page, as shown in Figure 21, asks for a name for the VLAN.

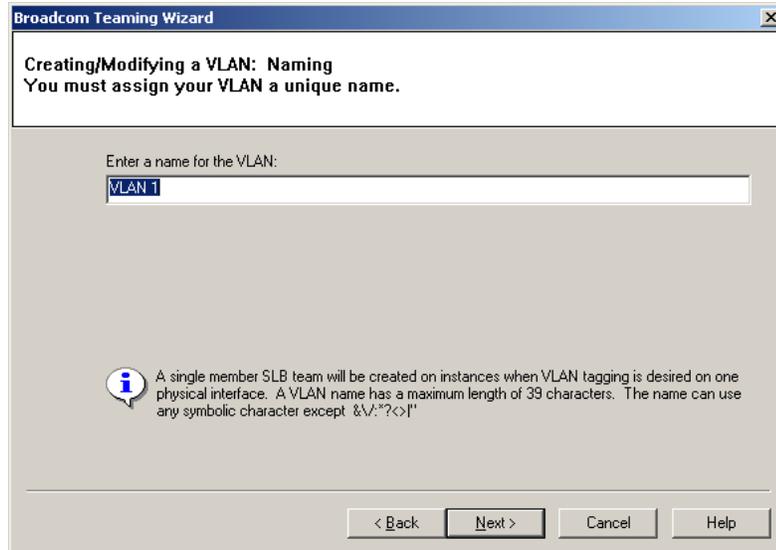


Figure 21. VLAN Naming Page

11. Enter a name for the VLAN and click **Next**.

The VLAN Tagging page, as shown in Figure 22, asks you to specify the VLAN type.

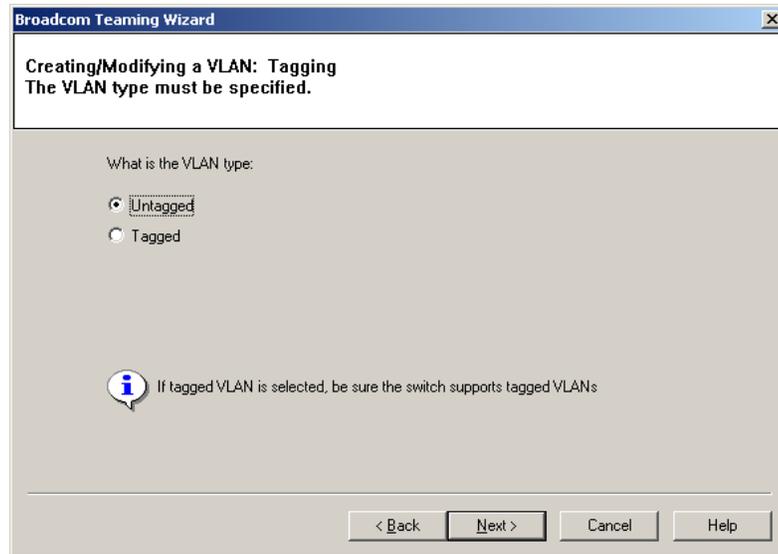


Figure 22. VLAN Tagging Page

The options are:

- Untagged.** This option does not insert a VLAN tag ID into the Ethernet packet, but relies on the switch configuration for VLAN membership.
- Tagged.** This option inserts the VLAN tag ID into the Ethernet packet to identify its VLAN ID or membership.

12. Select **Untagged** or **Tagged** and click Next.

The Additional VLANs page, as shown in Figure 23, asks if you want to create additional VLANs.

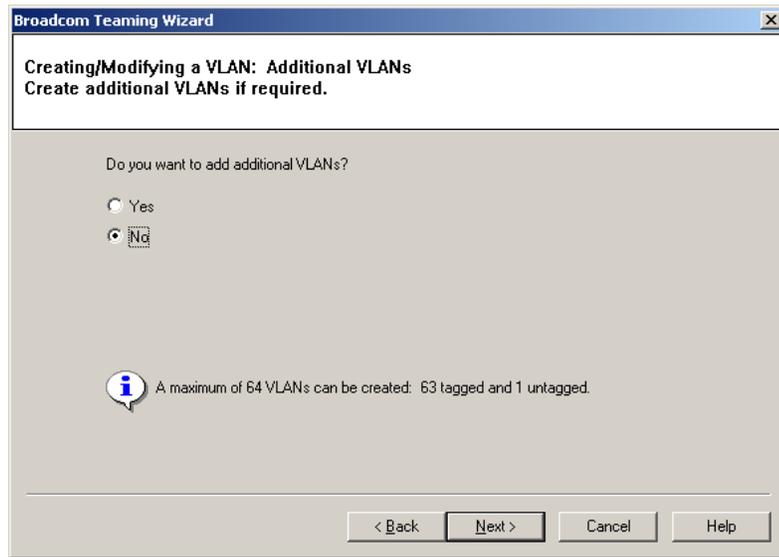


Figure 23. Additional VLANs Page

13. Click **Yes** if you want to create more VLANs and you will be repeating steps 11 and 12. or **No** if you do not want to create another VLAN.

When you click **No**, the final wizard page is displayed, as shown in Figure 24.

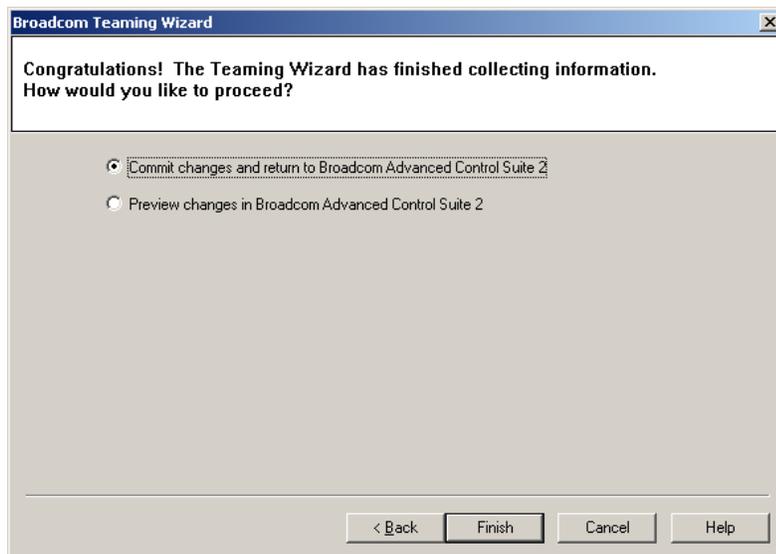


Figure 24. Final Teaming Wizard Page

14. Select one of the following:

- Commit changes and return to Broadcom Advanced Control**

Suite 2. A warning message is displayed, as shown in Figure 25.

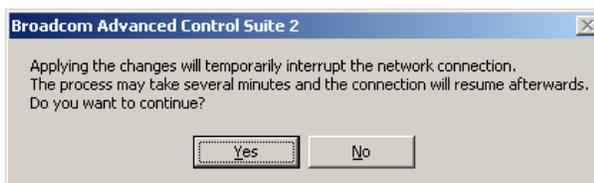


Figure 25. Commit Changes Warning Message

Click **Yes** to complete the process and return to the Broadcom Advanced Control Suite main window, or **No** to not save the changes.

- ❑ **Preview changes in Broadcom Advanced Control Suite 2.** This option shows the Team Properties tab where you can verify that the settings are correct for the named team, as shown in Figure 26.

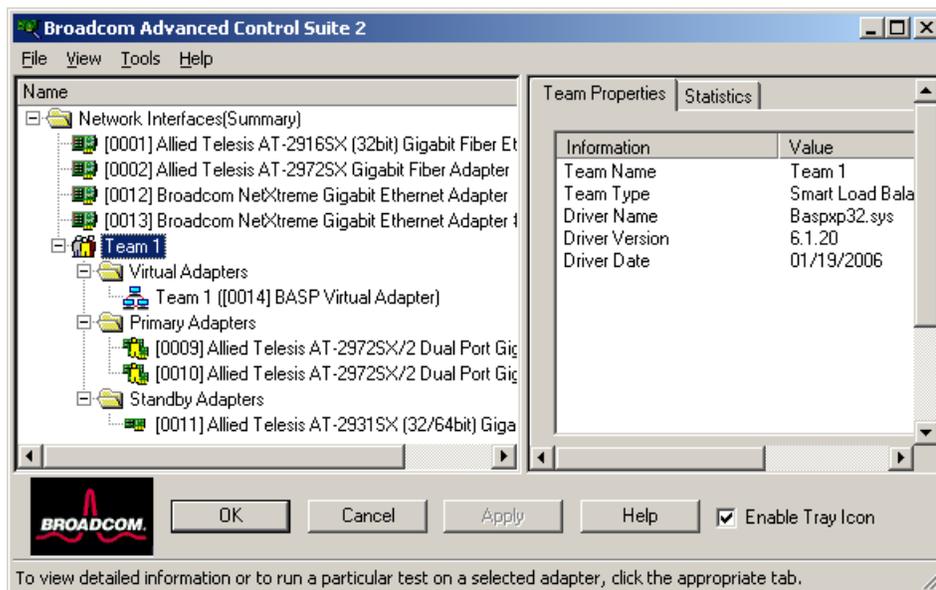


Figure 26. Team Properties Tab

Review your changes and click **Apply** to complete the process and return to the Broadcom Advanced Control Suite 2 main window.

Creating a Team Using the Expert Mode

To create a team, perform the following procedure.

1. From the **Tools** menu, click **Create a Team**.

The Welcome page of the Broadcom Teaming Wizard is shown in Figure 27.

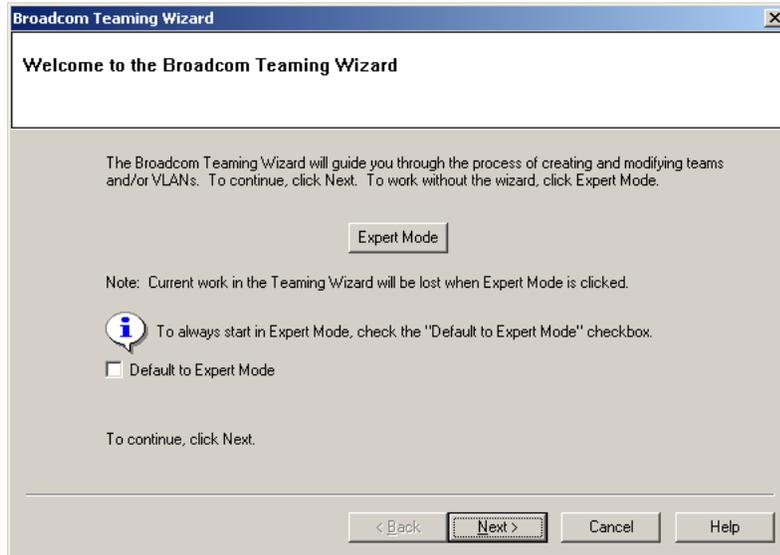


Figure 27. Broadcom Teaming Wizard Welcome Page

2. Click **Expert Mode**.

The New Team Configuration window opens, as shown in Figure 28.

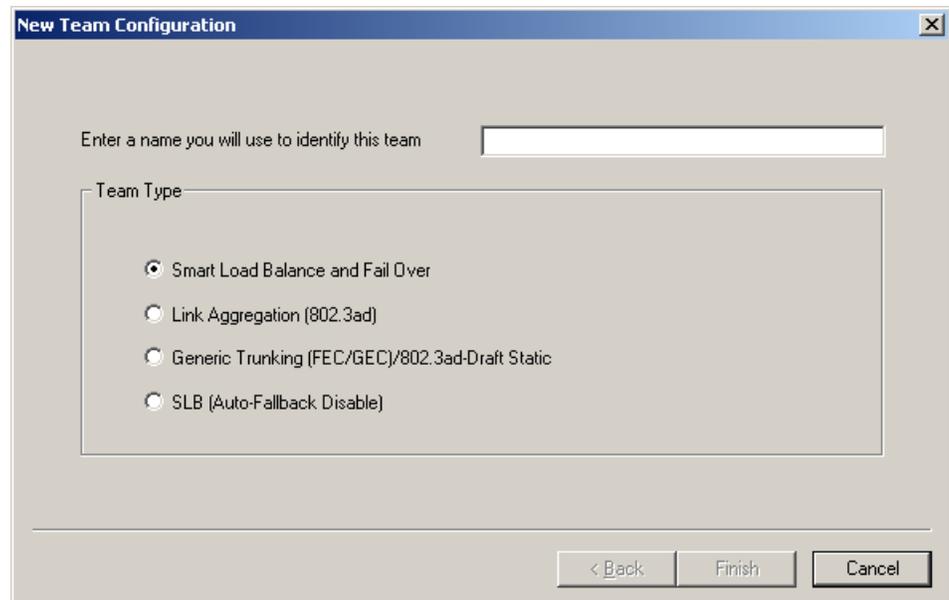


Figure 28. New Team Configuration

3. Type a team name in the **Enter a name you will use to identify this team** box.

Note

The number of characters that can be used in a team name is a minimum of 1 and a maximum of 39.

Note

A team name cannot begin with spaces or contain the character "&".

Note

Team names must be unique. If you attempt to use a team name more than once, an error message appears indicating that the name already exists.

Note

The maximum number of members in a team is 8.

Note

When team configuration has been correctly performed, a Virtual Team adapter driver is created for each configured team.

4. Click the type of team and click **Next**.

The New Team Configuration window opens, as shown in Figure 29.

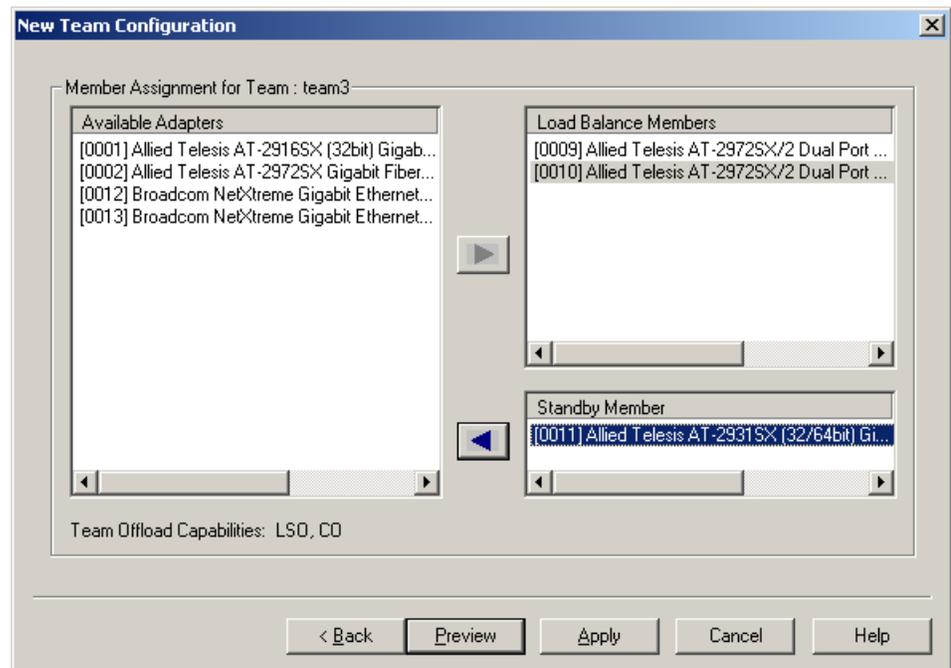


Figure 29. New Team Configuration Menu

5. Assign any available device or devices to the team by moving the device from the **Available Adapters** list to the **Load Balance Members** list.

There must be at least one device in the **Load Balance Members** list.

Note

There must be at least one Allied Telesis Gigabit Ethernet adapter assigned to the team.

6. Click **Apply**.
7. Click **Yes** when you see the message indicating that the network connection will be temporarily interrupted.

Note

If you disable a virtual team and later want to reenable it, you must first disable and reenable all team members before you reenable the virtual team.

Note

When you create Generic Trunking and Link Aggregation teams, you cannot designate a Standby Member. Standby members work only with Smart Load Balance and Failover and SLB (Auto-Fallback Disable) types of teams.

Note

For an SLB (Auto-Fallback Disable) team, when you want to restore traffic to the load balance members from the standby member, click the **Fallback** button on the **Team Properties** tab.

Note

Not all network devices made by other vendors are supported or fully certified for teaming.

8. Configure the Team IP address if necessary by choosing **Start > Settings > the team name > Properties**.

If other network devices in your computer use TCP/IP bindings, the **TCP/IP Properties** windows is displayed.

9. Configure the IP address and any other necessary TCP/IP configuration for the team and 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
- Remove a team or a VLAN

To modify a team, perform the following procedure.

1. Select the team name.
2. From the **Tools** menu, click **Configure a Team**.

The Welcome page of the Broadcom Teaming Wizard is shown in Figure 12 on page 41.

3. Click **Next**.

The Team Name page asks for a name for the team, as shown in Figure 13 on page 41.

4. Type the name of the team you want to modify and click **Next**.

The Team Properties tab is displayed with the properties of the team you selected, as shown in Figure 30.

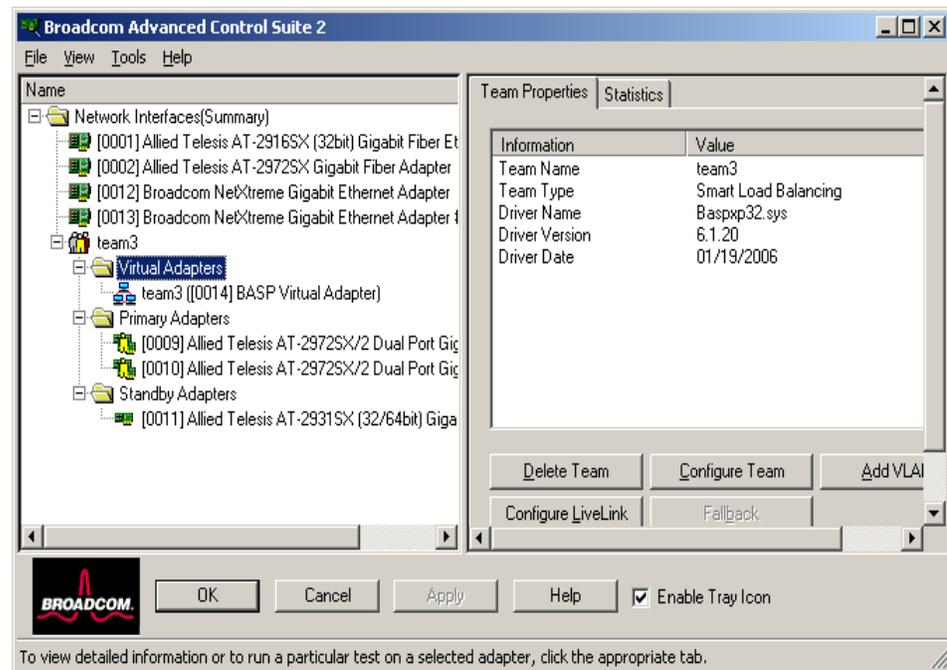


Figure 30. Team Properties Tab

5. In the list of adapters in the team shown on the left, right-click the name of the team you want to modify and click **Configure Team, Add VLAN, Configure LiveLink**, or **Fallback**.
6. When you are done with your changes, click **Apply**.
7. Click **Yes** when you see the message indicating that the network connection will be temporarily interrupted.

Adding a VLAN

You also can add VLANs to a team. The concept behind this is that you are adding multiple virtual adapters that are on different subnets. The benefit is that your server 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 tagged and 1 untagged). VLANs can only be created when all members are Allied Telesis adapters. If you try to create a VLAN with another type of adapter, an error message appears.

Note

Disabled adapters are not recognized and they prevent the creation of a VLAN. If you attempt to create a VLAN with a disabled adapter, an error message is displayed.

To configure a team with a VLAN, perform the following procedure.

Note

To maintain optimum adapter performance, your system must have 64 MB of system memory for each of the 8 VLANs created per adapter.

1. Select the team name.

The Team Properties tab opens as shown in Figure 26 on page 50.

2. In the list of adapters in the team shown on the left, right-click the name of the team you want to modify and click **Add VLAN**.

The Add VLAN dialog box opens, as shown in Figure 31

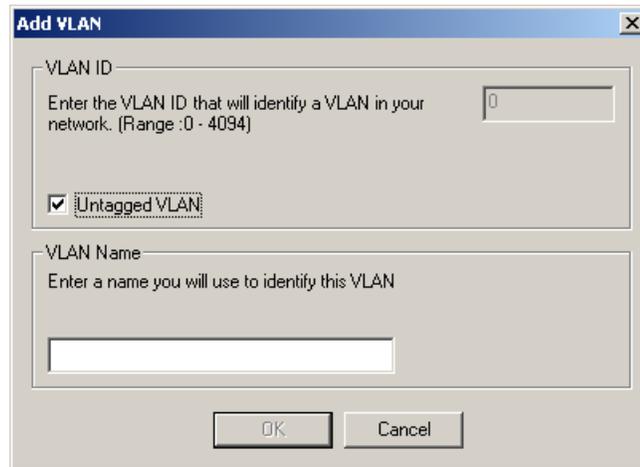


Figure 31. Add VLAN Dialog Box

3. Type the *VLAN ID* and *VLAN name*, then click **OK**.

The **Untagged VLAN** check box is exclusively used by the VLAN ID field. To use VLAN ID 0, simply click this check box. If you type a VLAN name or ID and the name already exists, an Input Error message appears.

4. When you are finished adding VLANs to this team, click **OK**.

A new virtual adapter is created for each VLAN.

5. Click **Apply**.
6. Click **Yes** when you see the message indicating that the network connection will be temporarily interrupted.

The available adapters are listed (these adapters are not currently members of any team).

Displaying VLAN Properties and Statistics and Running VLAN Tests

The procedures in this section describe how to display VLAN properties and statistics as well as how to run VLAN tests and delete a VLAN.

To display VLAN properties and statistics and to run VLAN tests, perform the following procedure.

1. In BACS2, click the VLAN name in the team's Virtual Adapters folder,

as shown in Figure 32.

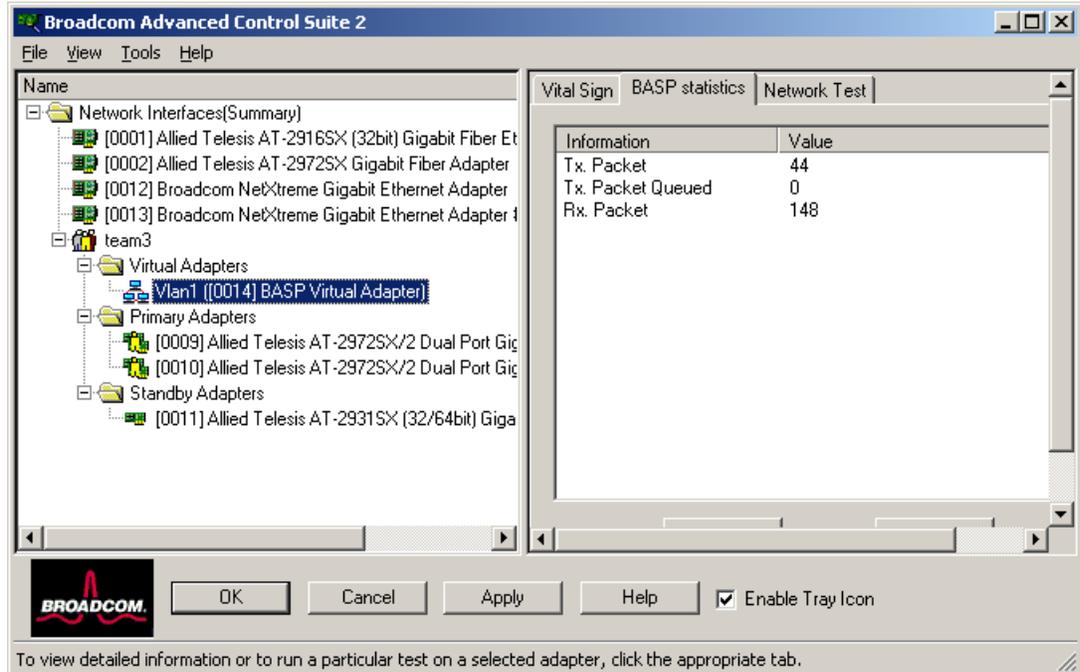


Figure 32. VLAN Name Selected

2. Click the **Vital Sign** tab to view the properties of the VLAN adapter.
3. Click the **BASP Statistics** tab to view the statistics for the VLAN adapter.
4. Click the **Network Test** tab to run a network test on the VLAN adapter.

To delete a VLAN, perform the following procedure.

1. In BACS2, select the VLAN name in the team's Virtual Adapters folder, as shown in Figure 32 on page 57.
2. Right-click the VLAN name and select click **Remove VLAN**.
3. Click **Apply**.
4. Click **Yes** when you see the message indicating that the network connection will be temporarily interrupted.

Note

When you delete a team, the VLANs configured for that team are also deleted.

Saving and Restoring a Configuration

The configuration file is a text file that can be viewed with any text editor. The file contains information about both the adapter and the team configuration. To save and restore a configuration file, see the following procedures.

To save a configuration, perform the following procedure.

1. From the **File** menu, click **Team Save As**.

The Save As dialog box is shown in Figure 32.

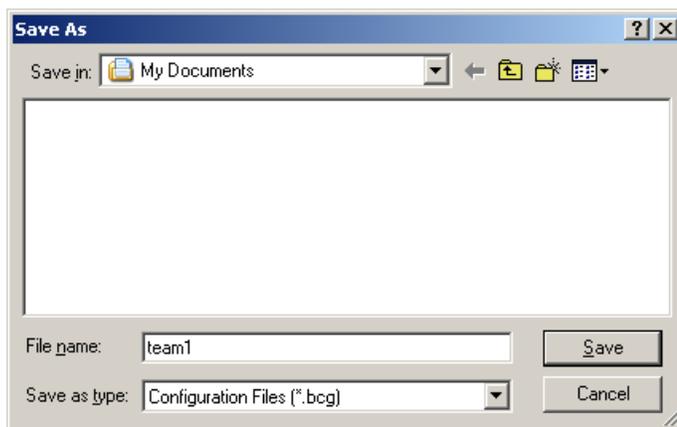


Figure 33. Save As Dialog Box

2. Type the path and file name of the new configuration file and click **Save** (a .bcg extension is added).

To restore a configuration, perform the following procedure.

1. From the **File** menu, click **Team Restore**.

The Open dialog box is shown in Figure 32.

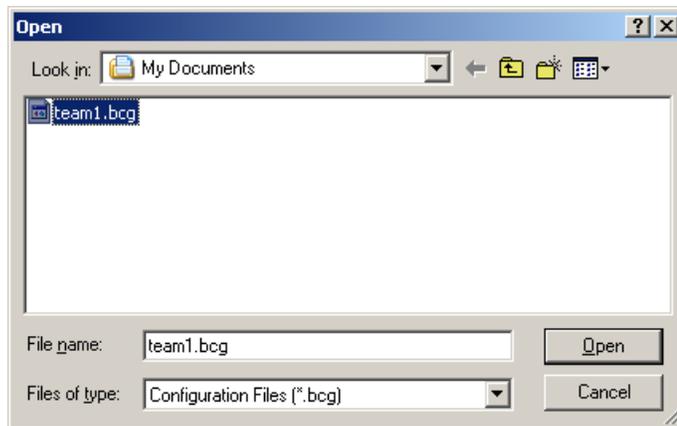


Figure 34. Open Dialog Box

2. Click the name of the file to be restored and click **Open**.

Note

You may need to navigate to the folder where the file is located.

If a configuration is already loaded, a message appears asking 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.

3. Click **Apply** to enable the Save Configuration feature.

Viewing the Team Properties and Statistics

To view the team properties and statistics, perform the following procedure.

1. Select the team name.

The Team Properties tab opens as shown in Figure 26 on page 50.

Chapter 3

Installing BACS on Windows 2000, Windows 2003, and Windows XP Systems

This chapter provides procedures for installing the BACS application and configuring teaming on Windows 2000, Windows 2003, and Windows XP systems. It contains the following sections:

- ❑ “Installing the BASP” on page 62
- ❑ “Uninstalling the BASP” on page 63

Installing the BASP

For BASP installation procedures, refer to Chapter 2, “Broadcom Advanced Control Suite 2 (BACS 2) Applications” on page 15.

Uninstalling the BASP

To uninstall the Broadcom Advanced Server Program Driver Properties (BASP), perform the following procedure:

1. Open the Control Panel
2. Double-click the **Add or Remove Programs** button.
3. Select Broadcom Management Programs and click **Change/Remove**.
4. Click **Next**.

The InstallShield Wizard screen appears.

5. Click the **Modify** radio button and click **Next**.
6. The Select Components screen opens.

Four install/uninstall selections are available from this screen.

7. Deselect the **BASP** checkbox, then click **Next**.
8. A question box appears indicating that removing BASP will uninstall your configured adapter team/VLAN. Click **Yes** to continue.
9. When complete, an information screen notifies you that the files were successfully uninstalled.
10. Click **OK** to complete the uninstall.

Chapter 4

Key Protocols and Interfaces

This chapter describes the key protocols and interfaces. It contains the following sections:

- ❑ “Adapter Teaming” on page 66
- ❑ “Failover Teaming” on page 68
- ❑ “VLANs Overview” on page 69

Adapter Teaming

Teaming provides traffic load balancing and redundant adapter operation in the event that a network connection fails. When multiple Allied Telesis adapters are installed in the same server, they can be grouped into teams. Each team can be configured on the server with up to 8 ports. If traffic is not identified on any of the adapter team members connections due to failure of the adapter, cable, switch port, or switch (where the teamed adapters are attached to separate switches), the load distribution is reevaluated and reassigned among the remaining team members. In the event that all of the primary adapters are down, the hot standby adapter becomes active. Existing sessions are maintained, causing no user impact.

BASP supports four schemes of load balancing: Smart Load Balancing, Link Aggregation (802.3ad), Generic Link Aggregation (Trunking), and Smart Load Balance Auto-Failback Disable. These schemes are described in the following sections.

Smart Load Balancing (SLB)[™]

The implementation of load balancing is based on IP flow. This feature supports balancing IP traffic across multiple adapters (that is, team members) in a bi-directional manner. In this mode, all adapters in the team have separate MAC addresses. It provides automatic fault detection and dynamic failover to other team members or to a hot standby member. This is done independently of the layer 3 protocol (IP, IPX, or Net Beui). It works with existing layer 2 and 3 switches.

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 there are 4 adapters in the system, you can select between 2 and 4 adapters to participate in the 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's link partner determines the load-balancing scheme for inbound packets. In this mode, at least one of the link partners must be in the active mode.

Generic Link Aggregation (Trunking)

This mode is very similar to 802.3ad in that you need to configure all of the adapters in the team to receive packets for the same MAC address. However, generic link aggregation mode does not provide LACP or marker protocol support. This mode supports a variety of environments where the NICs' link partners are statically configured to support a proprietary trunking mechanism. For instance, this mode could be used to support Lucent's "OpenTrunk" or Cisco's Fast EtherChannel (FEC).

Basically, generic link aggregation mode is a "light" version of the 802.3ad link aggregation and is often referred to as 802.3ad static. This approach is much simpler because there is not a formalized link aggregation control protocol. As with the other modes, the creation of teams and the allocation of physical adapters to various teams is done statically via user configuration software.

Trunking supports load balancing and failover for both the outbound and inbound traffic.

**Smart Load
Balance Auto-
Failback Disable**

This team is almost identical to Smart Load Balance and Failover with one exception. If a primary member comes back on line when the standby member is active, the team continues using the standby member rather than switching to the primary member.

Failover Teaming

Failover Teaming provides a redundant adapter operation in the event that a network connection fails. When multiple Gigabit Ethernet Adapters are installed in the same server, they can be paired into teams. Each team must have at least one adapter, but can support up to eight adapters. The number of teams is limited by the number of adapters that are installed.

If the primary adapter in a team is disconnected because the adapter, cable, or switch port fails, the secondary team member becomes active. In this case, the secondary team member redirects both the inbound and outbound traffic originally assigned to the primary adapter. Sessions are maintained; consequently, there is no impact to the user.

Note

Allied Telesis recommends disabling STP when you use the teaming and fault tolerance features.

VLANs Overview

VLANs allow you to split your physical LAN into logical subparts, to create logical segmentation of workgroups, and to enforce security policies among 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 Allied Telesis Gigabit Ethernet adapter in your server, depending on the amount of available memory in your system.

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. The adapters support multiple VLANs on a per-port or per-team basis, allowing very flexible network configurations.

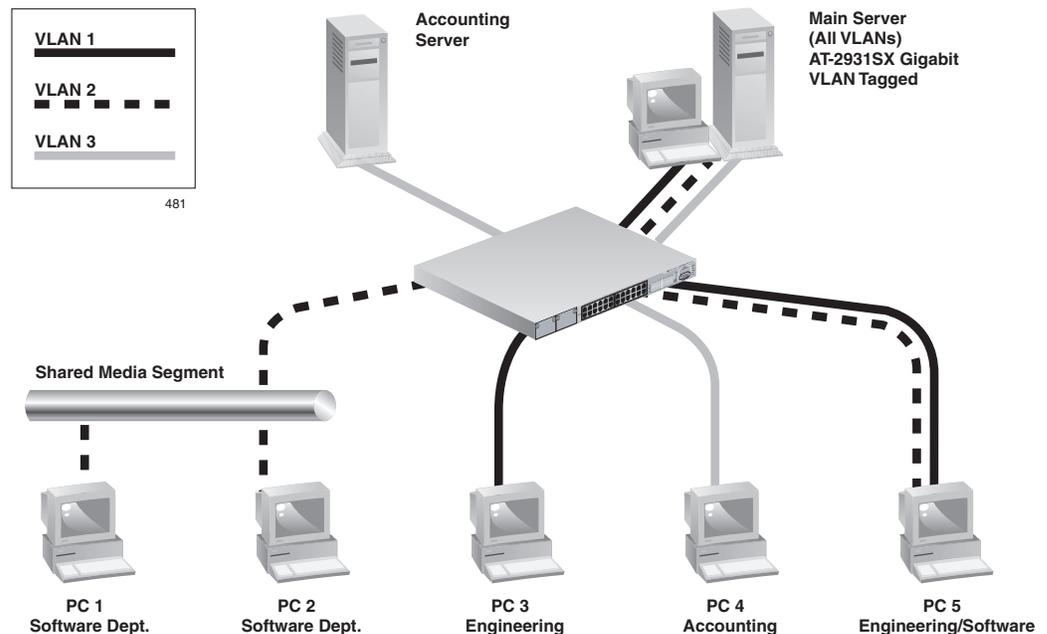


Figure 35. Example of Servers Supporting Multiple VLANs with Tagging

Figure 35 on page 69 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 2.

Table 2. 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 of the VLANs and IP subnets. The Main Server has an Allied Telesis 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 #2	Attached to a shared media hub that is then connected to the switch. PCs #1 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's switch port.
PC #4	A member of VLAN #3, PC #4 can only communicate with the servers. Tagging is not enabled on PC #4's switch port.

Table 2. Example VLAN Network Topology (Continued)

Component	Description
PC #5	A member of both VLANs #1 and #2, PC #5 has an Allied Telesis 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. It is also required on ports connected to tag-capable end-stations, such as servers or workstations with adapters.

VLANs Support

Virtual Local Area Networks (VLANs) are commonly used to split up groups of network users into manageable broadcast domains, to create logical segmentation of workgroups, and to enforce security policies among logical segments.

Each Team supports up to 64 VLANs. Note that only the Allied Telesis 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.

Note

Adapters that are members of a failover team can also be configured to support VLANs.

Adaptive Interrupt Frequency

Based on traffic conditions, the adapter driver intelligently adjusts host interrupt frequency 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 the host CPU cycles.

Dual DMA Channels

The PCI interface on the Gigabit Ethernet Adapter contains two independent DMA channels for simultaneous read and write operations.

**32-bit or 64-bit
PCI Bus Master**

Compliant with PCI Local Bus Rev 2.2, the PCI interface on the Gigabit Ethernet Adapter is compatible with both 32-bit and 64-bit PCI buses. As a bus master, the adapter requests access to the PCI bus, instead of waiting to be polled.

**ASIC with
Embedded RISC
Processor**

The core control for the Gigabit Ethernet Adapter resides in a tightly integrated, high-performance ASIC. The ASIC includes dual RISC processors. This provides the flexibility to add new features to the card and adapt it to future network requirements via a software download. This also enables the adapter drivers to exploit the built-in host offload functions on the adapter as host operating systems are enhanced to take advantage of these functions.

Chapter 5

Troubleshooting

This chapter describes troubleshooting procedures and contains the following sections:

- “Verifying the Correct Drivers are Loaded” on page 74
- “Software Problems and Solutions” on page 75

Verifying the Correct Drivers are Loaded

The following section describes how to check if the correct drivers are loaded for Windows.

Windows The Broadcom Advanced Control Suite, Vital Sign tab allows you to view vital adapter information, network status, and network connectivity. Active adapters are listed on the Vital Sign tab.

1. On the Vital Sign tab, select the adapter you want to test.
2. Press **Refresh** to display the driver status of the selected adapter.

Note

The information for other adapters is less comprehensive than the information listed for an Allied Telesis Gigabit Ethernet adapter.

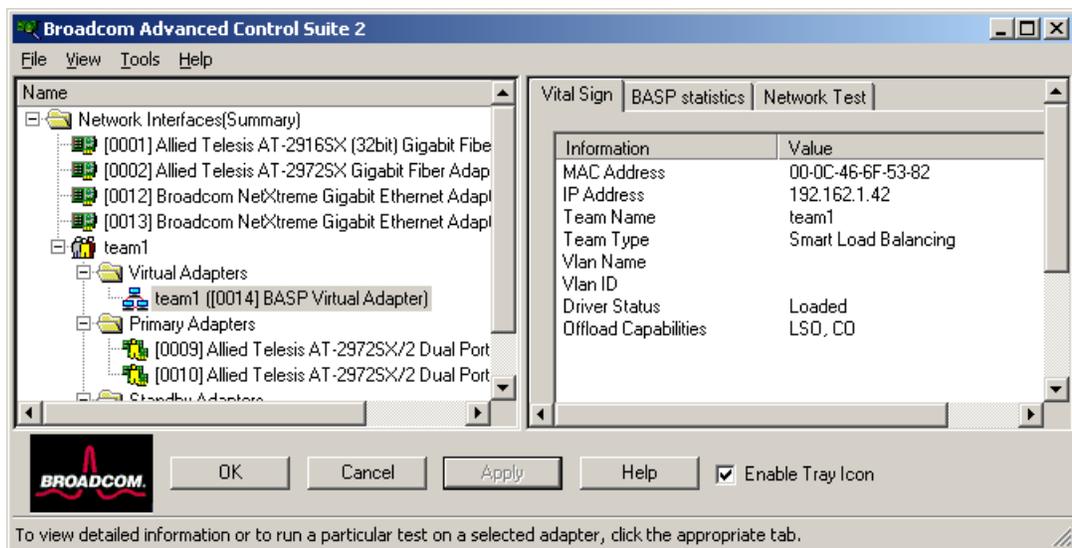


Figure 36. Vital Sign Tab for Troubleshooting

Software Problems and Solutions

This section describes common software problems and solutions and contains the following subsections:

- "Windows 2000," next
- "Broadcom Advanced Server Program (BASP)" on page 76

Windows 2000

This section lists known problems and solutions when using Windows 2000.

Problem: When uninstalling the BASP software, you are prompted to reboot early.

Solution: After configuring a BASP team, the Windows 2000 system may sometimes prompt you to reboot. This is because Plug and Play on W2k may fail to commit any change in the network protocol binding. You can choose not to reboot and continue configuring the intermediate driver without causing any side effects. When you have finished the configuration, you must reboot the system.

Problem: Cannot enable VLAN after it is disabled.

Solution: The BASP application creates additional network connections in the "Network Connection and Dial-up" Window. Similar to physical network connections, these virtual connections can be disabled via the context menu. However, if these virtual connections are re-enabled, the system reports a "connection failed!" error. This is a known problem with the Windows 2000 system. When this happens, rebooting the system reenables the virtual connection.

Problem: Able to configure Internet Connection Sharing (ICS) when there aren't any unassigned adapters.

Solution: Windows 2000 networking is shipped with the Internet Connection Sharing (ICS) application, which is designed to allow multiple computers to access the Internet via a Windows 2000 system. To configure the ICS application, you need to select a network connection as an "outside" connection and another network connection as an "inside" connection. However, the ICS application allows you to select any available network connection as an "outside" or "inside" connection, regardless of the BASP team configuration. Allied Telesis recommends that you do not select any network connection that is part of the BASP team to be "outside" or "inside."

Problem: Team configuration is not retained when you edit it.

Solution: In configuring BASP team configuration, the actual changes of the configuration are not committed until you click "OK" in the "Network Properties" window. If you do not click "OK" and, instead, return to the BASP team configuration window, all the previous uncommitted changes are lost. This requires you to reenter the configuration. As a workaround, always click "OK" in the "Network Properties" window after making changes.

Problem: IP address is configurable on a member of the team.

Solution: When a team is created, the TCP/IP properties for the adapters are unselected. You can select and configure the TCP/IP properties of the adapters and configure an IP address manually. This issue is a limitation of the Windows 2000 network installation paradigm where this invalid configuration is still allowed.

Problem: When creating 64 VLANs, all virtual adapters are displayed as disconnected or one of the 64 VLANs is displayed as disabled.

Solution: The maximum VLAN configurations are 63 tagged and one untagged VLAN ID 0. If 64 tagged VLANs are created, they are disconnected. A reboot is required and only the 63 tagged VLANs show links, while the 64th VLAN is disabled.

Broadcom Advanced Server Program (BASP)

This section lists known BASP problems and solutions that apply to all operating systems.

Problem: 802.3ad team member links disconnect and reconnect continuously.

Solution: This is a 3rd party issue. It is seen only when configuring an 802.3ad team with more than 2 members on the server and connecting an HP2524 switch, with LACP enabled as passive or active. The HP switch shows an LACP channel being brought up successfully with only 2 members. All other member's links disconnect and reconnect.

Note

This issue does not occur with a Cisco Catalyst 6500.
