NX2 GUI/CLI User Guide

BACS4-SWUM100-R

5300 California Avenue • Irvine, CA 92617 • Phone: 949-926-5000 • Fax: 949-926-5203

August 09, 2012

Revision History

Revision	*Date*	*Change Description*
BACS4-SWUM100-R	08/09/12	Initial release

Broadcom Corporation
5300 California Avenue
Irvine, CA 92617

Table of Contents

List of Figures

List of Tables

About This Document

Purpose and Audience

This document is designed for users who will be configuring and managing Broadcom® Converged Network Adapters using the BACS4 GUI and CLI. Users who want to list and view the legacy Broadcom network adapters will find this guide useful. This guide also can be used by anyone who wants to be familiar with the BACS4 GUI design in general and learn about the features of CNA.

Acronyms and Abbreviations

In most cases, acronyms and abbreviations are defined on first use.

For a comprehensive list of acronyms and other terms used in Broadcom documents, go to: http://www.broadcom.com/press/glossary.php.

Document Conventions

The following conventions may be used in this document:

Convention	***Description***
Bold	User input and actions: for example, type **exit**, click **OK,** press **Alt+C**
`Monospace`	Code: `#include <iostream>` HTML: `<td rowspan = 3>` Command line commands and parameters: `wl [-l] <command>`
< >	Placeholders for *required* elements: enter your <username> or `wl <command>`
[ ]	Indicates *optional* command-line parameters: `wl [-l]` Indicates bit and byte ranges (inclusive): [0:3] or [7:0]

References

The references in this section may be used in conjunction with this document.

Note: Broadcom provides customer access to technical documentation and software through its Customer Support Portal (CSP) and Downloads and Support site (see Technical Support).

For Broadcom documents, replace the “xx” in the document number with the largest number available in the repository to ensure that you have the most current version of the document.

Document (or Item) Name	*Number*	*Source*
Other Items		
[1] Securing a Remote WMI Connection	–	http://msdn.microsoft.com/en-us/library/aa393266%28v=vs.85%29.aspx

Technical Support

Broadcom provides customer access to a wide range of information, including technical documentation, schematic diagrams, product bill of materials, PCB layout information, and software updates through its customer support portal (https://support.broadcom.com). For a CSP account, contact your Sales or Engineering support representative.

In addition, Broadcom provides other product support through its Downloads and Support site (http://www.broadcom.com/support/).

Introduction

The BACS4 is a primary Broadcom Management Application designed to configure the NX2 family of adapters, also known as the Converge Network Adapter (CNA). It can also be used to list and view information about legacy network adapters. The BACS4 design is based on the reliable and time-tested BACS3 management application, which is currently the main application used to manage a wide range of Broadcom adapters. This ensures familiarity with the existing user interface and thus a shorter learning curve for the user.

BACS4 GUI/CLI Design Features

This section focuses on the BACS4 architecture and components. This will make the user familiar with various components of the GUI/CLI, but will also form a basis for the remaining contents of the user guide.

Architecture

There are two main components of the BACS4 GUI/CLI – providers and GUI/CLI client. The provider is a software component named either CIM providers (for Windows hosts) and CMPI providers (for Linux hosts) that are developed and provided by Broadcom. The windows hosts have a WMI server component that is provided by and running in the operating system. The similar component for Linux is Pegasus. The CIM/CMPI provider component communicates with various drivers using the BMAPI software component. The providers are installed on the host which needs to be managed using the BACS4 client – or Managed host. The second component, the BACS4 client, is a graphical user interface which can be installed on any computer running Windows XP or higher. The GUI/CLI client connects to the CIM/CMPI providers running on the managed host to view and manage the Converged Network Adapter installed in it. The minimum requirements are listed for both managed host and client system in this guide. The GUI/CLI client can be installed and used on the same host on which CIM/CMPI providers are installed.

The Converged Network Adapters are made up of various distinct components and can be described as manageable elements. These manageable elements are organized in an object-oriented, hierarchical manner in the BACS4 GUI. Each object has an associated description that explains what properties/data that object exposes, what properties/data are and are not configurable, what actions can and cannot be performed on the object itself, and what relationships exist between the objects.

Architectural Diagram

Windows System

The following block diagram shows the relationship between the Ethernet controller and driver. A host may have multiple chips, each chip may have multiple physical ports, and each physical port may have multiple functions. Each function may contain NDIS only, VBD and NDIS, iSCSI, or FCoE.

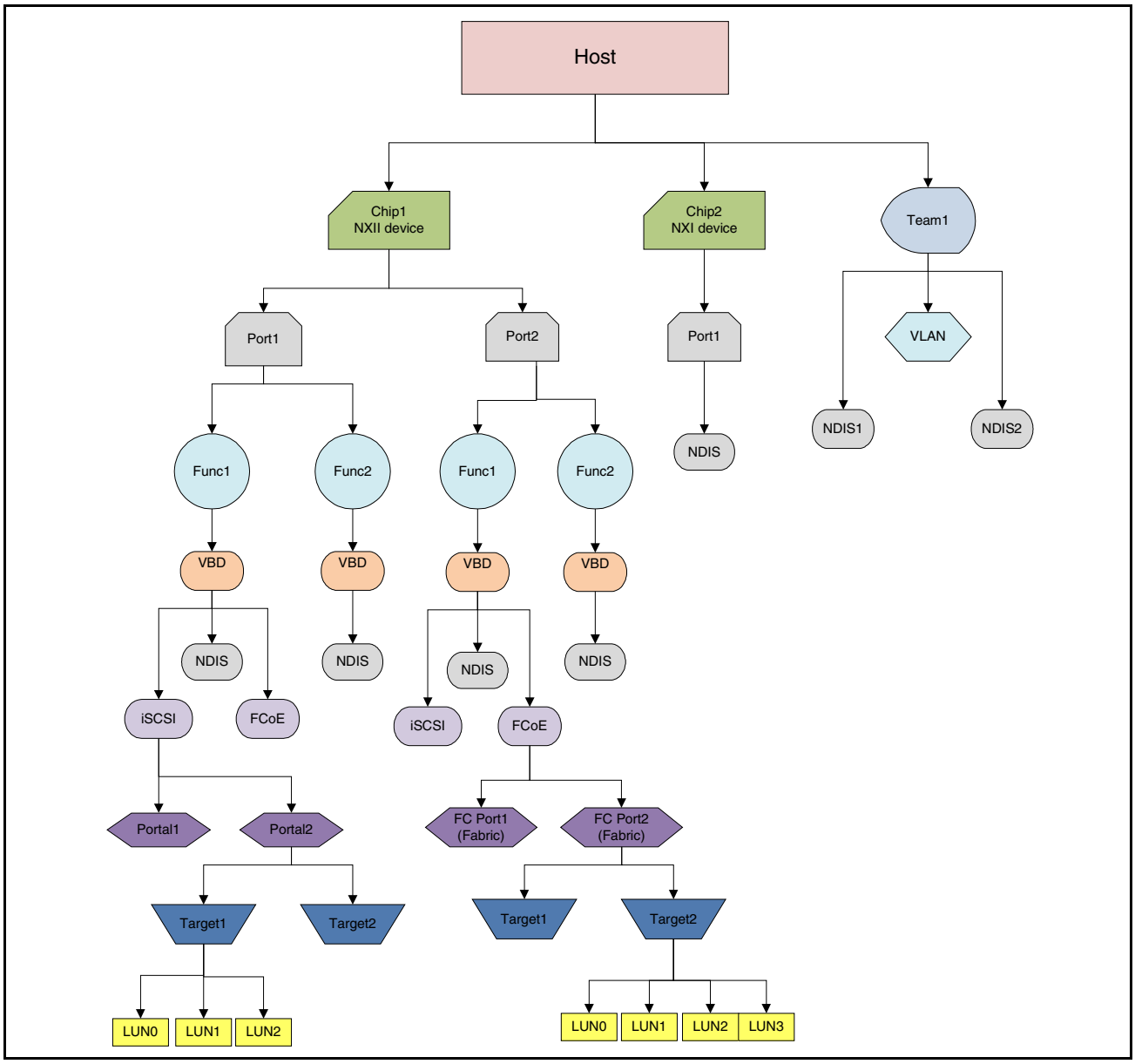


Figure 1: BACS4 Architecture (Windows)

Linux System

The following block diagram shows the relationship between the Ethernet controller and driver. A host may have multiple chips, each chip may have multiple physical ports, and each physical port may have multiple functions. Each function may contain an L2 device only, an L2 device, iSCSI, or FCoE.

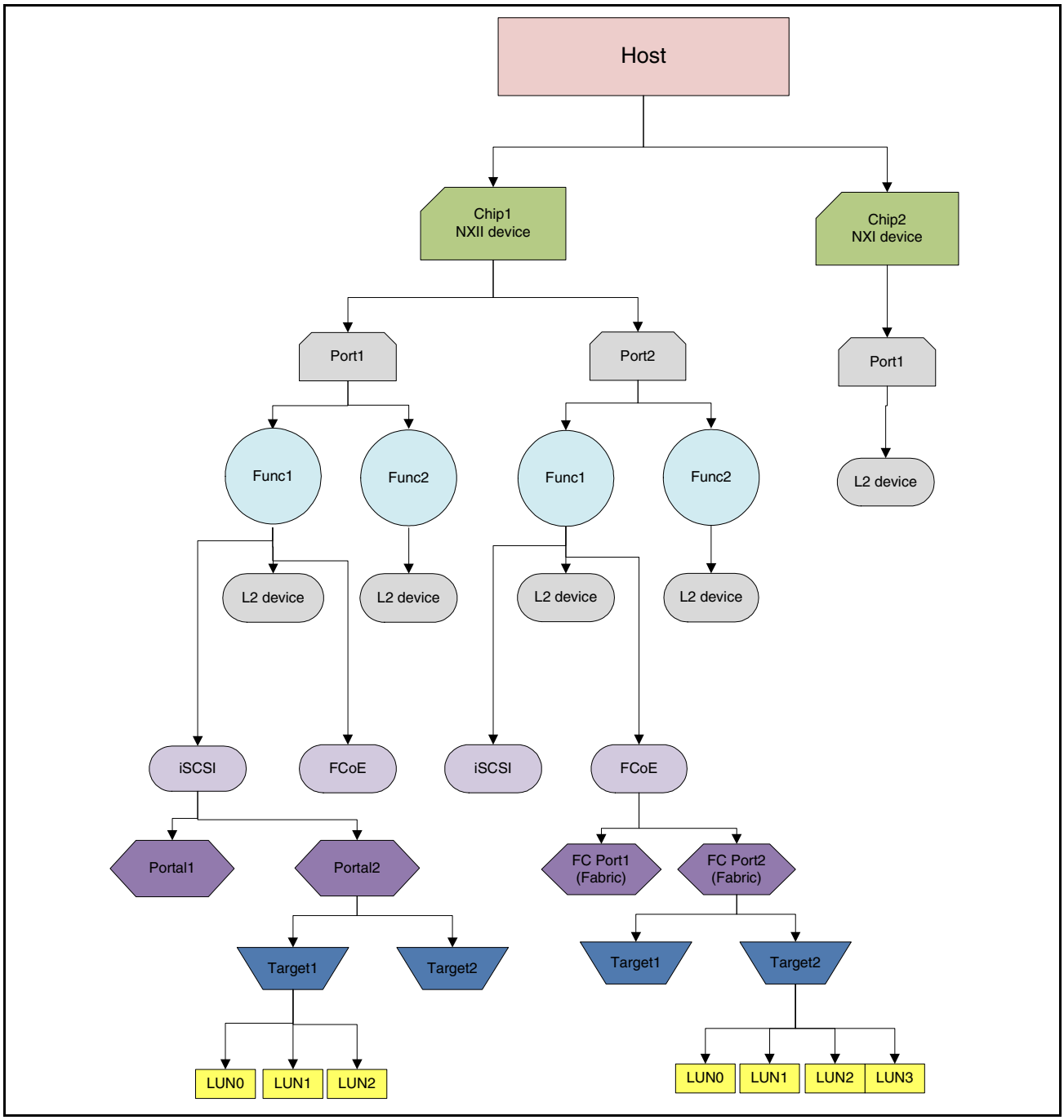


Figure 2: BACS4 Architecture (Linux)

Installation and Configuration

The installation of the BACS4 Management Application is performed using the BACS4 installer package. The following explains the requirements and installation procedure for the Windows and Linux operating systems.

Introduction

The installer package for Windows operating system is based on the Microsoft MSI installation technology. The managed host can be either Windows or Linux.

The Broadcom Windows CIM Provider supports WS-MAN (Web Service Management), WMI (Windows Management Interface) protocol to connect to the server from the client. The Broadcom Linux CIM provider supports the WS-MAN protocol and the CimXML protocol to connect to the server from the client.

Hardware Requirements

This section lists the minimum hardware requirement for hosts.

- One or more of the following Broadcom adapters:
  - Broadcom 578xx series Converged Network Adapters
  - Broadcom 57712 series converged Network adapters
  - Broadcom legacy 5709/57711 series Network adapters
- Single or multiprocessor system:
  - Pentium III with 450 MHz or greater for Windows XP Professional, Windows Vista, Windows 2000, Windows 2003, Windows 2008 server 2008 or Windows 2008 R2 to install the GUI client software component.
  - Pentium III with 450 MHz or greater for Windows XP Professional, Windows Vista, Windows 2000, Windows 2003, Windows 2008 Server, Windows 2008 R2 Server, Linux Red Hat 6 64-bit version and 32-bit version, SLES 11 64-bit version to install the providers.
- 128 MB of Physical RAM to run the BACS4 GUI Management Application; 256 MB is recommended. Running with less memory will severely affect the performance
- Video card capable of handling 256K colors and screen resolution of 800 x 600 pixel required; 16K colors and 1024 x 768 pixels is recommended.
- About 200 MB of disk space.

Software Requirement

There is no software requirement for the Windows Operating System except SNMP service, if you intend to use the SNMP management. All required software components are included in the BACS4 GUI installer package and are installed as part of the installation.

The Linux Operating System requires specific software components. The details about installing them are covered in “Installation and Configuration” on page 18.

Windows

Windows Package Contents

The following components are used and installed with this installer package.

Table 1: Windows Package Contents

Component	*Location*
Bmapi.dll	BMAPI share library
BrcmUtils.dll	BRCM_CIM provider library
BmapiObjServices.dll	BRCM_CIM provider library
BnxCmpiProvider.dll	BRCM_CIM provider library
libeasy32.dll	OpenSSL library
tcl83.dll	TCL library
tcldde83.dll	TCL library
tclpip83.dll	TCL library
tclreg83.dll	TCL library
BnxAdapter.mof	MOF file
BnxCDM.mof	MOF file
BnxCmpiProvier.mof	MOF file
BnxCmpiProvierReg.mof	MOF file
CIM_Core.mof	MOF file
CIM_Device.mof	MOF file
CIM_Interop.mof	MOF file
CIM_Network.mof	MOF file
CIM_Physical.mof	MOF file
CIM_System.mof	MOF file
CIM_System_Device.mof	MOF file

Windows Operating System Support

This section defines various supported operating system versions.

Table 2: Windows OS Versions

Item	*Operating System*	*Type*	*Hardware Platform*
1	Windows Server 2003	32-bit	Intel x86, Intel 64, AMD 64
2	Windows Server 2008	32-bit, 64-bit	Intel x86, Intel 64, AMD 64
3	Windows Server 2008 R2	64-bit	Intel 64, AMD 64
4	Windows Vista	32-bit, 64-bit	Intel 64, AMD 64
5	Windows XP Professional	32-bit, 64-bit	Intel 64, AMD 64

Linux

Linux Package Contents

Table 3: Linux Package Contents

Component	*Location*
libbmapi.so.{version}	BMAPI share library
libBrcmUtils.so	BRCM_CIM provider library
libBmapiObjServices.so	BRCM_CIM provider library
libBnxCmpiProvider.so	BRCM_CIM provider library
BnxAdapter.mof	MOF file
BnxCDM.mof	MOF file
BnxCmpiProvier.mof	MOF file
BnxCmpiProvierReg.mof	MOF file
CIM_Core.mof	MOF file
CIM_Device.mof M	MOF file
CIM_Interop.mof	MOF file
CIM_Network.mof	MOF file
CIM_Physical.mof	MOF file
CIM_System.mof	MOF file
readme.txt	Readme file
release.txt	Release information

Linux Operating System Support

This section defines various supported operating system versions.

Table 4: Linux Operating System Versions

Item	*Operating System*	*Type*	*Hardware Platform*
1	Red Hat Enterprise 5	32-bit, 64-bit	Intel x86, Intel 64, AMD 64
2	Red Hat Enterprise 6	32-bit, 64-bit	Intel x86, Intel 64, AMD 64
3	SuSE Enterprise (SLES) 10	32-bit, 64-bit	Intel x86, Intel 64, AMD 64
4	SuSE Enterprise (SLES) 11	32-bit, 64-bit	Intel x86, Intel 64, AMD 64

Communication Protocols

Broadcom provides various options for communication protocol between server and client system. This can help a company select the best option depending on the prevailing standard practice in their company. The available options are listed in Table 5.

Table 5: Communication Protocols

	WINDOWS (Server)	***LINUX (Server)***
WINDOWS (Client)	WMI[a] WS-MAN[b] (WinRM)	CimXML (Open Pegasus) WS-MAN (Open Pegasus)
LINUX (Client)	WS-MAN (WinRM)	CimXML (Open Pegasus) WS-MAN (Open Pegasus)

a. Windows Management Instrumentation
b. Web Service Management

If there are a mix of Windows and Linux clients accessing Windows and Linux servers in your network, then WS-MAN is the obvious choice. If Linux is the only operating system installed on the servers, then CimXML is an option. In the case of only Windows servers and clients, WMI is a possible option. WMI is very simple to configure, but is supported only on Windows operating system.

Depending on the communication protocol you wish to use, the installation components and procedures are different. The following is a step summary. The detailed steps for server and clients are listed under each operating system section.

WS-MAN

If you are planning to use WS-MAN protocol to connect to server from client, use the following procedure.

Windows Server

On Windows servers, the WinRM service is required to be configured using the following steps.

1. Install the WinRM software component on the server. See "Install the WinRM Software Component on the Server" on page 24.
2. Perform basic configuration on the server. See "Perform Basic Configuration." on page 24.
3. Perform user configuration on the server. See "Perform the User Configuration" on page 25.
4. Perform HTTP configuration on the server. See "Perform HTTP Configuration (If Using HTTP)" on page 25.
5. Perform HTTPS configuration on server. See "Perform HTTPS Configuration (If Using HTTPS)" on page 26.
   a. Generate a self-signed certificate for Windows server.
   b. Install the self-signed certificate on the Windows server.
6. Configure and test WinRM listener on the server. See "Configure WinRM HTTPS/SSL" on page 29.
7. Perform additional configuration, if required, like Firewall configuration on the server. See "Additional Configuration" on page 30.
8. Install the BACS management application. See "Install BACS management application." on page 31.

Windows Client

On the Windows client, perform the following configuration steps.

1. Perform HTTP configuration on the client (if you plan to use HTTP with WS-MAN). See “Perform HTTP Configuration (If Using HTTP)” on page 32.
2. Perform HTTPS configuration on the client (if you plan to use HTTPS with WS-MAN). See “Perform HTTPS Configuration (If Using HTTPS)” on page 33.
3. Configure the WinRM listener on the client. See “Configure WinRM HTTPS/SSL.” on page 33.
4. Install the BACS client application on the client systems (Windows or Linux). See “Install BACS management application.” on page 31.

Linux Server

On the Linux server, install OpenPegasus using the following steps. There are two options available with respect to OpenPegasus – install from Inbox RPM or install from source. Inbox OpenPegasus is only available on the Red Hat operating system. For SLES11, the only available option is to use the source RPM. The WS-MAN is not supported with the Inbox RPM. If you plan to use WS-MAN, you must install OpenPegasus from the source.

1. Install OpenPegasus on the server from the Inbox RPM “Install OpenPegasus from Inbox RPM (Red Hat only).” on page 34
2. Install OpenPegasus on the server from the source RPM. See “Install OpenPegasus from Source (Red Hat and SuSE)” on page 34.
3. Start the CIM server on the server. See “Start CIM Server on the Server.” on page 36.
4. Configure OpenPegasus on the server. See “Configure OpenPegasus on Server” on page 36.
5. Install the Broadcom CIM provider. See “Install the Broadcom CIM Provider” on page 37.
6. Perform additional configuration, if required (for example, firewall configuration). See “Linux Firewall Configuration” on page 38.
7. Install the BACS client application on the client systems (Windows or Linux). See “Install BACS management application.” on page 31.

Linux Client

For HTTP, no special configuration is required on the Linux client system. Only the BACS management application is required to be installed. Perform the following configuration steps.

1. Perform HTTPS configuration on the client (if you plan to use HTTPS with WS-MAN). See “Configure HTTPS on Linux Client” on page 39.
2. Install the BACS client application on the client system. See “Install the BACS Management Application” on page 39.
3. Uninstall the BACS client application from the client system. See “Uninstall the BACS Management Application” on page 39.

CimXML

CimXML is not supported on the Windows operating system. The installation steps for the Linux server are similar to WS-MAN.

Linux Server

On the Linux server, install OpenPegasus using the following steps. There are two options available with respect to OpenPegasus – install Inbox RPM or install OpenPegasus from source. The Inbox OpenPegasus is only available on Red Hat operating system. For SLES11, the only available option is to use the source RPM. The WS-MAN is not supported with the Inbox RPM. If you plan to use WS-MAN then you must install OpenPegasus from source.

1. Install OpenPegasus on server from Inbox RPM. See "Install OpenPegasus from Inbox RPM (Red Hat only)." on page 34.
2. Install OpenPegasus on server from source RPM. See "Install OpenPegasus from Source (Red Hat and SuSE)" on page 34.
3. Start CIM server on the server. See "Start CIM Server on the Server." on page 36.
4. Configure OpenPegasus on server. See "Configure OpenPegasus on Server" on page 36.
5. Install Broadcom CIM provider. See "Install the Broadcom CIM Provider" on page 37.
6. Perform additional configuration, if required, like Firewall configuration. See "Linux Firewall Configuration" on page 38.
7. Install BACS client application on client systems (Windows or Linux). See "Install BACS management application." on page 31.

Linux Client

1. Install BACS client application on client system. See "Install the BACS Management Application" on page 39.
2. Uninstall BACS client application from client system. See "Uninstall the BACS Management Application" on page 39.

WMI

The WMI protocol is only supported on the Windows operating system. If servers and clients both are running Windows, then WMI can be used.

Windows Server

1. Set Namespace Security using WMI control. See "Setting up Namespace Security Using WMI Control" on page 40.
2. Grant DCOM remote launch and activate permission for a user/group. See "Grant DCOM Remote Launch and Activate Permission" on page 40.
3. Perform special configuration, if necessary. See "Special Configuration for WMI on Different Systems" on page 43.

Windows Client

No special configuration is required on windows client system except installing the BACS management application. See “Install BACS management application.” on page 31.

Installation Steps

WS-MAN - Windows Server

Install the WinRM Software Component on the Server

Windows 7 and Windows Server 2008 R2

WinRM 2.0 is preinstalled on Windows 7 and Windows 2008 R2.

Windows XP, Windows Server 2003, Windows 2003 and Windows 2008

Install the Windows Management Framework Core that includes WinRM 2.0 and Windows Powershell 2.0 from the following link:

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

Note: For Windows 2003 R2, follow the procedure in “Windows 2003 R2”.

Windows 2003 R2

The Hardware Management (including WA-Management) feature is not installed by default. It can be installed from the Management and Monitoring Tools section of the Add/Remove Windows Components Wizard by following the steps below.

1. In Control Panel, select **Add or Remove Programs**.
2. Select **Add/Remove Windows Configuration**.
3. Select **Management and Monitoring Tools** and click the **Details** button to open the **Management and Monitoring Tools** windows.
4. Select the **Hardware Management** option.
5. Click **OK** to select the Hardware Management Component.
6. Click **Next** to install Hardware Management (including WinRM).

Perform Basic Configuration.

The Windows firewall must be enabled for WinRM to work properly. For detailed information about firewall configuration, see “Additional Configuration” on page 30. Once the firewall is configured, open a command prompt and run the following command.

```
winrm quickconfig
```

This command enables the remote management on the Windows server.

You can also get the configuration information for the service Client by running the following command:
```
winrm get winrm/config
```

Perform the User Configuration

To connect to WinRM, the account must be a member of the local administrators group on the local or remote computer. The output of above command is as follows:
```
RootSDDL = O:NSG:BAD:P(A;;GA;;;BA)S:P(AU;FA;GA;;;WD)(AU;SA;GWGX;;;WD)
```

BA stands for BUILTIN\Administrators.

To add another user group to WinRM allowed connect list, the RootSDDL needs to be modified to include the new user group. The SSDL ID for the group you want to add is required. For example, the following command adds the new user group with SDDL id S-1-5-21-1866529496-2433358402-1775838904-1021.
```
winrm set winrm/config/Service @{RootSDDL="O:NSG:BAD:P(A;GA;;;BA)(A;;GA;;;
S-1-5-21-1866529496-2433358402-1775838904-1021)S:P(AU;FA;GA;;
WD)(AU;SA;GWGX;;;WD)"}
```

Perform HTTP Configuration (If Using HTTP)

The default HTTP port is 5985 for WinRM 2.0.

1. Run **gpedit.msc** (Local Group Policy Editor) from **Start/Run**.
2. Under Computer Configuration/Administrative Templates/Windows Components, select **Windows Remote Management (WinRM).**
3. Under **Windows Remote Management (WinRM)**, select **WinRm Client**.
4. Double click **Trusted Hosts** under **WinRM Client**.
5. For **TrustedHostsList**, enter the host names of the clients.
6. If all clients are trusted, enter *only and click **OK**.
7. Select **WinRM Service**.
8. Enable **Allow Basic Authentication**, then click **OK**.
9. Enable **Allow unencrypted traffic**, then click **OK**.
10. Close **gpedit.msc.**
11. From the command prompt run the following command to configure WinRM with default settings:
    ```
    winrm qc or winrm quickconfig
    ```
12. Enter **y** when the tool displays Make these changes[y/n]?
13. Check if a HTTP listener is created by the following command:
    ```
    winrm  enumerate winrm/confg/listener
     or
    winrm e winrm/config/Listener
    ```
14. Run the following command from the command prompt to test locally.
    ```
    winrm id
    ```

Perform HTTPS Configuration (If Using HTTPS)

This step consists of two distinct processes — generating self-signed certificate if certificate does not exists and importing it on a windows server. A self-signed certificate has to be configured on the Windows Server to connect over HTTPS/SSL from BACS running on Windows or Linux Client, if the security certificate does not exist for the server. The Windows and Linux client should also be configured with the self-signed certificate. See "Perform HTTPS Configuration (If Using HTTPS)" on page 33 to configure Windows and "Configure HTTPS on Linux Client" on page 39 to configure the Linux client.

Note: The self-signed certificate can be created on any Windows or Linux server. The server does not require BACS installed. The self-signed certificate generated on any Windows/Linux server then should be copied on a local drive of client.

1. Run **gpedit.msc** (Local Group Policy Editor) from **Start/Run**.
2. Under Computer Configuration/Administrative Templates/Windows Components, select **Windows Remote Management (WinRM).**
3. Under **Windows Remote Management (WinRM)**, select **WinRm Client**.
4. Double Click **Trusted Hosts** under **WinRM Client**.
5. In the dialog, for **TrustedHostsList**, enter the hostnames of the clients.
6. If all clients are trusted then enter "*" only.
7. Now select **WinRM Service**.
8. Enable **Allow Basic Authentication**.

Generating a Self-Signed Certificate for Windows/Linux Server

Openssl is used to create a self-signed certificate. Openssl on Linux or Windows can be used to generate the self-signed certificate.

1. Generate a Private key
   ```
   openssl genrsa –des3 –out server.key 1024
   ```

Note: It will ask for a pass phrase. Remember this pass phrase

2. Generate a CSR (Certificate Signing Request).

   During the generation of the CSR, it will prompt for several pieces of information. One of the prompts will be for "Common Name". It is important that this field is filled with the Windows Server HostName or IP Address.

   The command to generate the CSR is as follows:
   ```
   openssl req –new –key server.key –out server.csr
   ```
   The following information will be asked:

   Country Name (2 letter code) []:US

   State or Province Name (full name) []: California

Locality Name (e.g., city) []: Irvine

Organization Name (e.g., company) []: Broadcom Corporation

Organizational Unit Name (e.g., section) []: Engineering

Common Name (e.g., YOUR name) []: Enter Host name or IP address of the Windows Server Email Address []:

3. Enter the following 'extra' attributes to be sent with your certificate request

   A challenge password []:linux1

   An optional company name []:

Note: Enter a parameter value for all parameters in bold.

4. Remove Pass phrase from Key.
5. Run the following commands:
   ```
   cp server.key server.key.org
   openssl rsa -in server.key.org -out server.key
   ```
6. Generate a Self-Signed Certificate.
7. To generate a self-signed certificate which is good for 365 days, issue the following command:
   ```
   openssl x509 -req -days 365 -in server.csr -signkey server.key -out server.crt
   ```
   The output will be as shown below:
   ```
   Signature ok
   subject=/C=US/ST=California/L=Irvine/O=Broadcom Corporation/OU=Engineering/CN=MGMTAPP-   LAB3/
   emailAddress= Getting Private key
   ```
8. Verify the generated Self-Signed Certificate.
   ```
   openssl verify server.crt
   ```
   The output will be as shown below:
   ```
   server.crt:/C=US/ST=California/L=Irvine/O=Broadcom Corporation/OU=Engineering/CN=MGMTAPP-
   LAB3/emailAddress= error 18 at 0 depth lookup:self signed certificate
   OK
   ```
   Ignore error message **error 18 at 0 depth lookup:self signed certificate.** This error indicates that this is a self-signed certificate.
9. Convert the certificate from “crt” to “pkcs12” format.

   For Windows Server, the certificate should be in pkcs12 format. The command to convert is as follows:
   ```
   openssl pkcs12 -export -in server.crt -inkey server.key -out hostname.pfx
   ```
   It will ask for the following:

   Enter Export Password:

   Verifying - Enter Export Password:
10. Enter the password and note this password. This will be required while importing the certificate on Windows Server and Client.
11. Finally, make a copy of server.crt and place the certificate file on the server where BACS will be installed so that it can be imported. If you plan to use Windows/Linux client to connect to the server running BACS then the certificate also needs to be transferred (copy and paste the certificate file) on the client system.

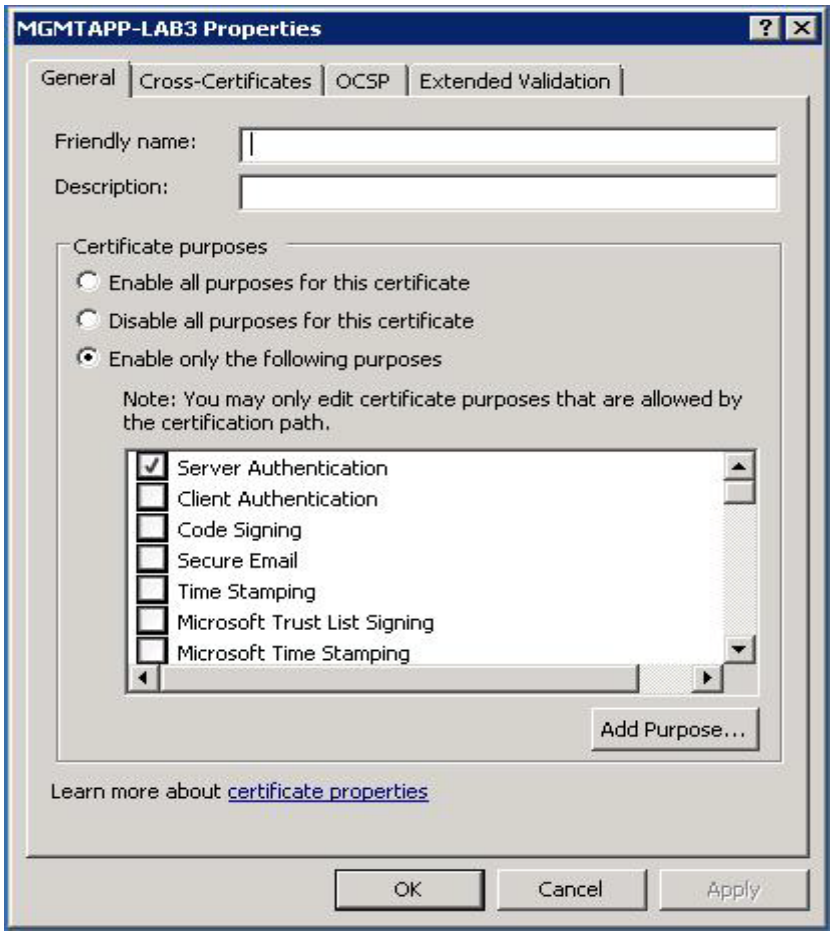
In Linux, the certificate should be with extension ".pem". The extension ".crt" and ".pem" are same, so there is no need to use openssl command to convert from .crt to .pem. You can just make a copy.

Install the Self-Signed Certificate on Windows Server

Transfer the **hostname.pfx** generated earlier on the Windows Server before you start installing the certificate.

1. Click **Start/Run**… and type in **MMC** and click **OK**.
2. From **File Menu,** select **Add/Remove Snap-in…**
3. Select Certificates and click **Add**.
4. Select **Computer Account**.
5. Click **Next** button
6. Click **Finish** button
7. Click **OK** Button
8. Expand **Certificates (Local Computer)**.
9. Expand **Personal** and right-click **Certificates**.
10. Select **All Tasks** and then **Import….**
11. Specify the file location to import the certificate. Browse and select **hostname.pfx**
12. At the prompt for the password for the private key, enter the same password you created in Step 9 of "Generating a Self-Signed Certificate for Windows/Linux Server" on page 26**.**
13. Follow the instructions, select the defaults and continue.

    The certificate will be shown as installed on the right side. The name will be the CN that you selected while creating a self-signed certificate.
14. Right-click the certificate and select **Properties**. A dialog box will appear as follows:



15. Ensure that only **Server Authentication** is enabled as shown in the above dialog box.

16. Expand **Trusted Root Certification Authorities**.

17. Expand **Certificates**.

18. Repeat Step 11 through Step 16.

Note: See "Import the Self-Signed Certificate on Linux Client." on page 39 to import the self-signed certificate on the client.

Configure WinRM HTTPS/SSL

1. Create WinRM Listener.

a. From **MMC**, select the self-signed certificate from the **Personal store**.

b. For example if the certificate is created with host name, the host name will appear.

c. Double click it to open it.

d. Select the **Details** tab.

e. Scroll down to the **Thumbprint** field and select it.

f. Select and copy the **Thumbprint** in the **Details** window so you can insert it in the next step.

g. Return to the command prompt.

h. Run the following command:

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

Note: If the certificate is generated using Host Name, provide Host Name or else provide IP Address if it generated by IP Address.

The above command creates a listener on the HTTPS port (5986) using any/all network address of the server, and my SelfSSL generated certificate.

i. Use **winrm create** to modify/set https listener as WinRM listeners can be configured on any user defined port.

j. From the command prompt, run the following command to verify the listeners that have been configured:

```
winrm e winrm/config/listener
```

2. Test HTTPS/SSL connection on the Server

a. From the command prompt on the server, run the following command:

```
winrs -r:https://yourserver -u:username -p:password hostname
```

b. If everything was setup correctly, the output of the command will print the server host name.

c. To check WinRM Service Configuration, run the following command

```
winrm get winrm/config/service
```

Additional Configuration

Modify the Firewall rules (if necessary) as follows:

Windows Server 2008 R2

1. Open **Windows Firewall with Advanced Security** from the Administrative Tools menu.

2. Right-click the **Inbound Rules** and select **New Rule** – the new rule wizard opens.

3. Click the **Port** radio button.

4. On the **Protocol and Ports** screen, select **TCP**, enter the specific port (e.g., 5985 [for HTTP] or 5986 [HTTPS]), then click **Next**.

5. On the **Action** screen, select **Allow the connection**, then click **Next**.

6. For Profile, select all three if your server is in a workgroup, then click **Next**.

7. Give the rule a name and click **Finish**.

You should be able to see the new rule and it should be enabled (green check box).

Windows XP

1. Go to **Control Panel**, then double click **Windows Firewall**.

2. Click the **Exception** tab.

3. Click **Add Port…** button.
4. Enter a meaningful Name (e.g., “WinRM rule” and port number, e.g., 5985 [for HTTP] or 5986 [HTTPS]).
5. Click the **OK** button.

Useful WinRM Commands

winrm quickconfig or winrm qc

Configures WinRM with the default settings.

```
winrm enumerate winrm/config/Listener or  winrm e winrm/config/Listener
```

This command helps to check which service listener are enabled and listening on which port and IP Address.

```
winrm get winrm/config/Service
```

Checks the WinRM Service Configuration.

```
winrm delete winrm/config/Listener?Address=*+Transport=HTTPS
```

Deletes a Listener. In this case, deletes a HTTPS listener.

```
winrm set winrm/config/service @{CertificateThumbprint="=49598a83f844c5eee3ed379a391d41270da0b20b"}
```

Useful WinRM Links

The following are useful WinRM links:

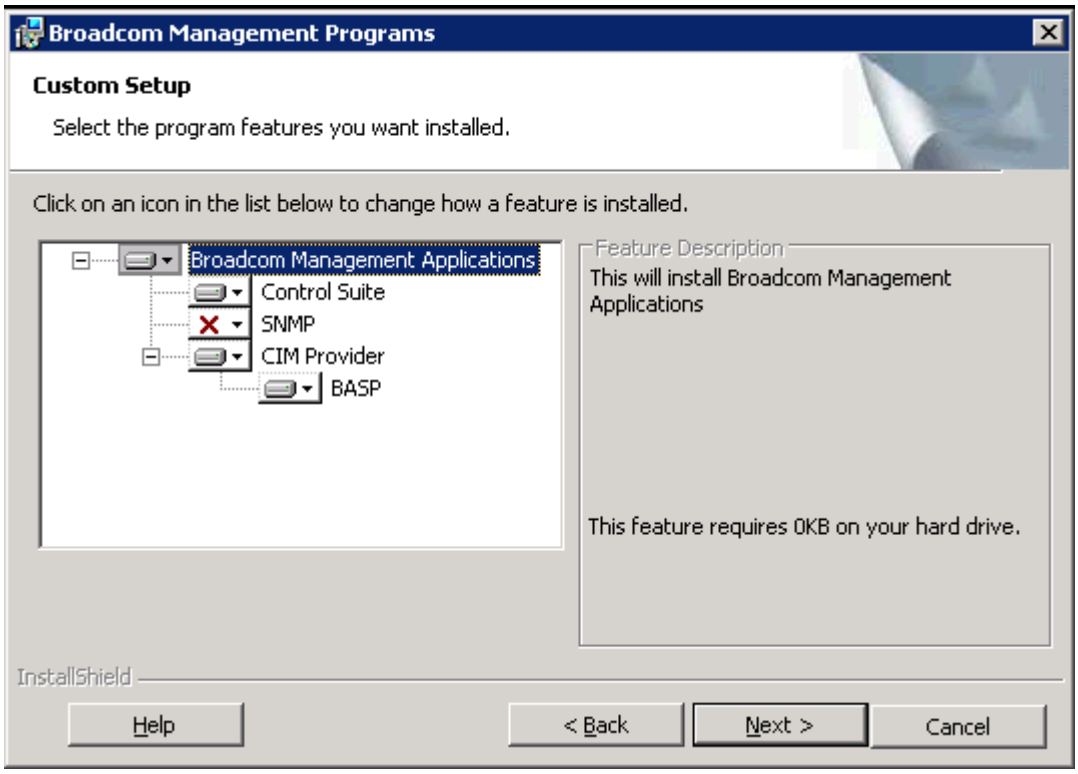
- http://msdn.microsoft.com/en-us/library/aa384372%28v=vs.85%29.aspx
- http://support.microsoft.com/kb/968929
- http://blogs.technet.com/b/jonjor/archive/2009/01/09/winrm-windows-remote-management-troubleshooting.aspx
- http://support.microsoft.com/kb/2019527
- http://technet.microsoft.com/en-us/library/cc782312%28WS.10%29.aspx
- http://msdn.microsoft.com/en-us/library/aa384295%28v=VS.85%29.aspx

Install BACS management application.

To install the BACS4 GUI/CLI Management Application, follow these steps:

1. Download Broadcom BACS4 installer package on the local drive and extract the files.
2. Open the appropriate folder, depending on the hardware platform.
3. Double click **Setup.exe** to start the installation.
4. Click **Next**.
5. Accept the license agreement and click **Next**.
6. Select the components you would like to install.
   - Control Suite: This is a graphical user Interface – or GUI component. Select this option if you want to install GUI and CLI Client on the host. Both GUI and CLI clients are installed.

- SNMP: This feature will install the SNMP subagent allowing SNMP manager to monitor the Broadcom Network Adapters.
- CIM Provider: This component presents the network adapter information to WMI based management applications. Select this component on a host that has a Broadcom adapter installed and that you want to manage using GUI client.
- BASP: This is a Broadcom intermediate NDIS driver to configure VLAN, Team, Load Balancing etc.



7. Click **Next**.
8. Click **Next** and then **Install**.
9. If Windows security dialogue box is displayed, select “Install this driver software anyway” to proceed with the installation.
10. Click **OK**.
11. Click **Finish**.
12. After successful installation, you can start the GUI from Windows Start menu.

WS-MAN - Windows Client

Perform HTTP Configuration (If Using HTTP)

1. Run **gpedit.msc** (Local Group Policy Editor) from **Start/Run**.
2. Under Computer Configuration/Administrative Templates/Windows Components, select **Windows Remote Management (WinRM)**.

3. Under **Windows Remote Management (WinRM)**, select **WinRm Client**.
4. Double click **Trusted Hosts** under **WinRM Client**.
5. In the dialog, for **TrustedHostsList**, enter the hostnames of the clients.
6. If all clients are trusted, then enter "*" only.
7. Select **WinRM Service**.
8. Enable **Allow Basic Authentication**.
9. Run the following command from the command prompt to test the connection:
   `winrm id -remote:<remote machine Hostname or IP Address>`

Perform HTTPS Configuration (If Using HTTPS)

After generating the self-signed certificate a mentioned in "Generating a Self-Signed Certificate for Windows/ Linux Server" on page 26, the certificate now can be imported on the client to facilitate connection between server and client. Ensure that all steps mentioned in "Generating a Self-Signed Certificate for Windows/Linux Server" on page 26are completed (including copy of **hostname.pfx** at the location from where client can access it**)** before you proceed with the steps below.

1. Click **Start/Run…** and type **MMC.** Click **OK**.
2. Click **File** Menu and the select **Add/Remove Snap-in…**
3. Select Certificates and click **Add**.
4. Select **Computer Account.**
5. Click the **Next** button.
6. Click the **Finish** button.
7. Click the **OK** button.
8. Right-click **Trusted Root Certification Authorities.**
9. Select **All Tasks**.
10. Select **Import…**
11. Follow the instructions and provide location of the exported file saved as .pfx and **Continue**.

Configure WinRM HTTPS/SSL.

Test the WinRM HTTPS/SSL connection from client using the following steps.

1. Run winrm from a client to retrieve information from the server using WinRM HTTPS connection.
2. To retrieve the server operating system information, issue the following command.
   ```
   winrm e wmi/root/cimv2/Win32_OperatingSystem
   -r:https://yourservername -u:username -p:password -skipCAcheck
   ```
3. To retrieve the server WinRM identity information, issue the following command.
   ```
   winrm id -r:https://yourservername -u:username -p:password
   -skipCAcheck
   ```
4. To enumerate windows services on the server, issue the following command.
   ```
   winrm e wmicimv2/Win32_service -r:https://yourservername
   ```

```
-u:username -p:password -skipCAcheck
```

It is important to use –skipCAcheck switch in the WinRM command line testing as the certificate is self-generated and not imported on the client, otherwise, you will get the following error: WSManFault.

Note: Next section will explain how to export and import the self-signed certificate.

WS-MAN & CimXML - Linux server

There are two options available with respect to OpenPegasus – install from Inbox RPM or install from source. The Inbox OpenPegasus is only available on Red Hat operating system. For SLES11, the only available option is to use the source RPM. The WS-MAN is not supported with the Inbox RPM. If you plan to use WS-MAN, you must install OpenPegasus from source.

Install OpenPegasus from Inbox RPM (Red Hat only).

On Red Hat an inbox OpenPegasus rpm is available as `tog-pegasus-<version>.<arch>.rpm`.

1. Install tog-pegasus with the following command.
   `rpm -ivh tog-openpegasus-<version>.<arch>.rpm`
2. Start Pegasus with the following command.
   `/etc/init.d/tog-pegasus start`

Note: On SuSE Linux, inbox OpenPegasus RPM is not available. The OpenPegasus needs to be installed form source. See below for the procedure.

Note that inbox Pegasus does not have HTTP protocol enabled by default. After Inbox OpenPegasus is installed successfully, if no further configuration is required then go to “Install the Broadcom CIM Provider” on page 37. To enable HTTP, see “Uninstall the BACS Management Application” on page 39

Install OpenPegasus from Source (Red Hat and SuSE)

The OpenPegasus source can be downloaded from www.openpegasus.org.

Note: If not installed already, download and install openssl and libopenssl-devel rpm. This step is optional and required only if you are planning to use HTTPS to connect Client to the Managed Host.

Set the Environment Variable.

Set the environment variables for building OpenPegasus as follows.

Table 6: OpenPegasus Environment Variables

Environment Variable	*Description*
PEGASUS_ROOT	The location of the Pegasus source tree.

Table 6: OpenPegasus Environment Variables (Cont.)

Environment Variable	*Description*
PEGASUS_HOME	The location for the built executable, repository. e.g. $PEGASUS_HOME/bin, PEGASUS_HOME/lib, $PEGAUS_HOME/repository, and $PEGASUS_HOME/mof subdirectories.
PATH	$PATH:$PEGASUS_HOME/bin
PEGASUS_ENABLE_CMPI_PROVIDER_MANAGER	True
PEGASUS_CIM_SCHEMA	“CIM222”
PEGASUS_PLATFORM	For Linux 32 bit systems: “LINUX_IX86_GNU” For Linux 64 bit systems: “LINUX_X86_64_GNU”
PEGASUS_HAS_SSL	Optional. Set to “true” for HTTPS support.
PEGASUS_ENABLE_PROTOCOL_WSMAN	Optional. Set to “true” for WSMAN protocol support.

Additional Settings

$PEGASUS_HOME needs to be set up in the shell environment, and $PEGASUS_HOME/bin needs to be appended to the $PATH environment.

Examples:

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

For SSL Support, add the following environment variable:

```
export PEGASUS_HAS_SSL=true
```

For WS-MAN Support, add the following environment variable:

```
export PEGASUS_ENABLE_PROTOCOL_WSMAN=true
```

CimXML or WSMAN in Openpegasus uses the same ports for HTTP or HTTPs. The default port numbers for HTTP and HTTPS are 5989 and 5989 respectively.

Note: You can add these exports at the end of the .bash_profile. This file is located in the /root directory.

- The environment variables will be set when a user logs in using putty.
- On Linux system itself, for each terminal if the environment variables are not set run the following command:
  `source /root/.bash_profile`
- When you logout and login, the environment variables will be set.

Build and Install OpenPegasus.

From $PEGASUS_ROOT (the location of the Pegasus source root directory), run the following:

```
make clean
make
make repository
```

Note: Whenever OpenPegasus is build from source, all configurations will be reset to default. If you are rebuilding OpenPegasus, you must redo the configuration as described in "Configure OpenPegasus on Server" on page 36.

Start CIM Server on the Server.

1. Start cimserver with the command **cimserver**.

   You can stop cimserver with command **cimserver –s**.

2. To check if OpenPegasus has been installed properly, issue the following command.

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

Note: For OpenPegasus compiled from source, it is necessary to have PEGASUS_HOME defined when you start cimserver. Otherwise cimserver will not load the repository properly. Consider setting PEGASUS_HOME in the ".bash_profile" file.

Configure OpenPegasus on Server

Configuration is done using the cimconfig command:

Table 7: cimconfig Command

cimconfig Command	*Description*
cimconfig -l	List all valid property names.
cimconfig -l -c	List all valid property names and its value.
cimconfig -g <property name>	Query a particular property.
cimconfig -s <property name>=<value> -p	Set a particular property
cimconfig --help	Find out more about the command.

cimserver needs to be started before running cimconfig, and restarted for configuration changes to take effect.

Enable Authentication

The following OpenPegasus properties have to be set as mentioned else the Broadcom CIM Provider will not work properly. Ensure the following are set before launching BACS and connecting to the provider.

1. If cimserver is not started, start cimserver.
2. `cimconfig -s enableAuthentication=true -p`
3. `cimconfig -s enableNamespaceAuthorization=false -p`
4. `cimconfig -s httpAuthType=Basic -p`
5. `cimconfig -s passwordFilePath=cimserver.passwd -p`

6. `cimconfig -s forceProviderProcesses=false -p`
7. If you want root user to connect remotely:
   `cimconfig -s enableRemotePrivilegedUserAccess=true -p`
8. User Configuration with privilege.

   The Linux system users are used for OpenPegasus authentication. The systems users have to be added to OpenPegasus using cimuser to connect via BACS:
   `cimuser -a -u <username> -w <password>`

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

Enable HTTP

1. If cimserver is not started, start cimserver.
2. Set up HTTP port with the following command: (Optional)
   `cimconfig -s httpPort=5988 -p`

   This property is not available for inbox OpenPegasus.
3. Enable HTTP connection with the following command:
   `cimconfig -s enableHttpConnection=true -p`
4. Stop and restart cimserver with `cimserver –s` and `cimserver` for the new configuration to take effect.

Enable HTTPS

1. If cimserver is not started, start cimserver.
2. Set up HTTPS port with the following command: (Optional)
   `cimconfig -s httpsPort=5989 -p`

   This property is not available for inbox OpenPegasus.
3. Enable HTTPS connection with the following command:
   `cimconfig -s enableHttpsConnection=true -p`
4. Stop and restart cimserver with ***cimserver -s*** and ***cimserver*** for the new configuration to take effect.

Install the Broadcom CIM Provider

Ensure that OpenPegasus is installed properly before installing CMPI Provider.

Install

Issue the following command to install the Broadcom CMPI Provider.

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

Uninstall

Issue the following command to uninstall the Broadcom CMPI Provider.

```
% rpm -e BRCM_CMPIProvider
```

Linux Firewall Configuration

To open the appropriate ports in the Firewall follow below procedure.

RedHat

1. Click **System** menu and then select **Administration** and then select **Firewall**.
2. Select **Other Ports**.
3. In the **Port and Protocol Dialog** box, check **User Defined**.
4. In the **Port/Port Range** filed, add the port number.
5. In the **Protocol** filed add the protocol as **TCP** or **UDP** etc.
6. Click **Apply** for the firewall rules to take effect.

   Example:

   - For CimXML over HTTP, the port number is 5988 and protocol is TCP
   - For CimXML over HTTPs, the port number is 5989 and protocol is TCP

SuSE

1. Click **Compute** menu and then **YaST.**
2. Select **Security & Users** on the left pane.
3. On the Right Pan, double click **Firewall**.
4. In the displayed Dialog box, select **Custom Rules** on the left Pane.
5. On the Right Pane click **Add**, a dialog box appears and then fill in the following:

   Source Network: 0/0 (means all)

   Protocol: TCP (or the appropriate protocol)

   Destination Port: <Port Number> or <Range of Port Numbers

   Source Port: Leave it blank.
6. After finishing the configuration, click **Next** and then click **Finish** for the firewall rules to take effect.

   Example: For CimXML, do the following:

```
Source Network: 0/0 (means all)
Protocol: TCP
Destination Port: 5988:5989
Source Port: Leave it blank.
```

WS-MAN and CimXML — Linux Client

No special software components are required on the Linux client system to use the HTTP except installing BACS management application.

Configure HTTPS on Linux Client

Import the Self-Signed Certificate on Linux Client.

On Linux distributions, note the following certificate directory.

- For all SuSE version the certificate directory is /etc/ssl/certs.
- For RedHat the certificate directory can be different for each version. For some versions, it is /etc/ssl/certs or /etc/pki/tls/certs. For other versions, find out the certificate directory.

Copy hostname.pem that is created in "Generating a Self-Signed Certificate for Windows/Linux Server" on page 26 into the certificate directory of the Linux client. For example, if the certificate directory is /etc/ssl/certs, copy hostname.pem to /etc/ssl/certs.

1. Change directory to /etc/ssl/certs.
2. Create a Hash value by running the following command.
   ```
   openssl x509 -noout -hash -in hostname.pem
   ```
   Output will print a value such as below.

   100940db
3. Create a symbolic link to the hash value by running the following command:-
   ```
   ln -s hostname.pem 100940db.0
   ```

Test HTTPS/SSL connection from Linux client.

Test if the certificate is installed correctly on Linux by running the following command:-

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

If this fails then the certificate is not installed correctly and it provides appropriate message to take corrective action.

Install the BACS Management Application

1. Download the latest BACS management application RPM package.
2. Install the RPM package as:
   ```
   rpm -i BACS-{version}.{arch}.rpm
   ```

Uninstall the BACS Management Application

To uninstall BACS management application issue the following command.

```
rpm –e BACS
```

The following two steps are to be performed only for configuring WMI on the windows server.

WMI – Windows

Setting up Namespace Security Using WMI Control

The WMI Control provides one way to manage namespace security. You can start the WMI Control from the command prompt using this command:

```
wmimgmt
```

On Windows 9x or Windows NT4 computers that have WMI installed, type this command instead:

```
wbemcntl.exe
```

Alternatively, you can access the WMI Control and the Security tab by doing the following:

1. Right-click My Computer and click **Manage**.
2. Double-click **Services and Applications** and then double-click **WMI Control**.
3. Right-click **WMI Control** and then click **Properties**.
4. In the **WMI Control Properties** dialog box click the **Security** tab.

   A folder named **Root** with a plus sign **(+)** next to it should now be visible. Expand this tree as necessary to locate the namespace for which you want to set permissions.
5. Click the **Security** button. A list of users and their permissions appears. If the user is on that list, modify the permissions as appropriate. If the user is not on the list, click the **Add** button, and add the user from the location (local machine, domain, etc.) where the account resides.

Note the following:

- In order to view and set namespace security, the user must have Read Security and Edit Security permissions. Administrators have these permissions by default, and can assign the permissions to other user accounts as required.
- If this user needs to access the namespace remotely, you must select the Remote Enable permission.
- By default, user permissions set on a namespace apply only to that namespace. If you want the user to have access to that namespace and all subnamespaces in the tree below it, or in subnamespaces only, click the Advanced button. Click Edit and specify the scope of access in the resulting dialog box.

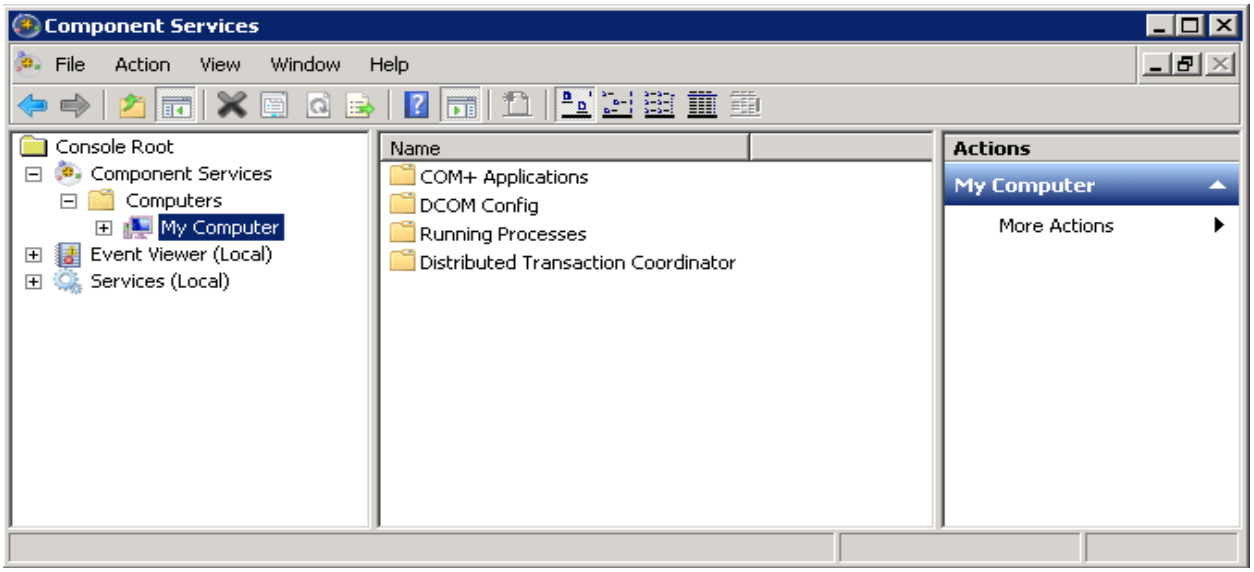
Grant DCOM Remote Launch and Activate Permission

In the Windows domain environment, the Domain Administrator account has necessary privilege to access the WMI component for the BACS management and therefore no special configuration needs to be done. However, in large enterprise, user who is accessing the local / remote host using the BACS4 client GUI may not always have the domain administrator account privilege. It is necessary to configure WMI security access on the remote host to allow user to connect to it using BACS4 client GUI.

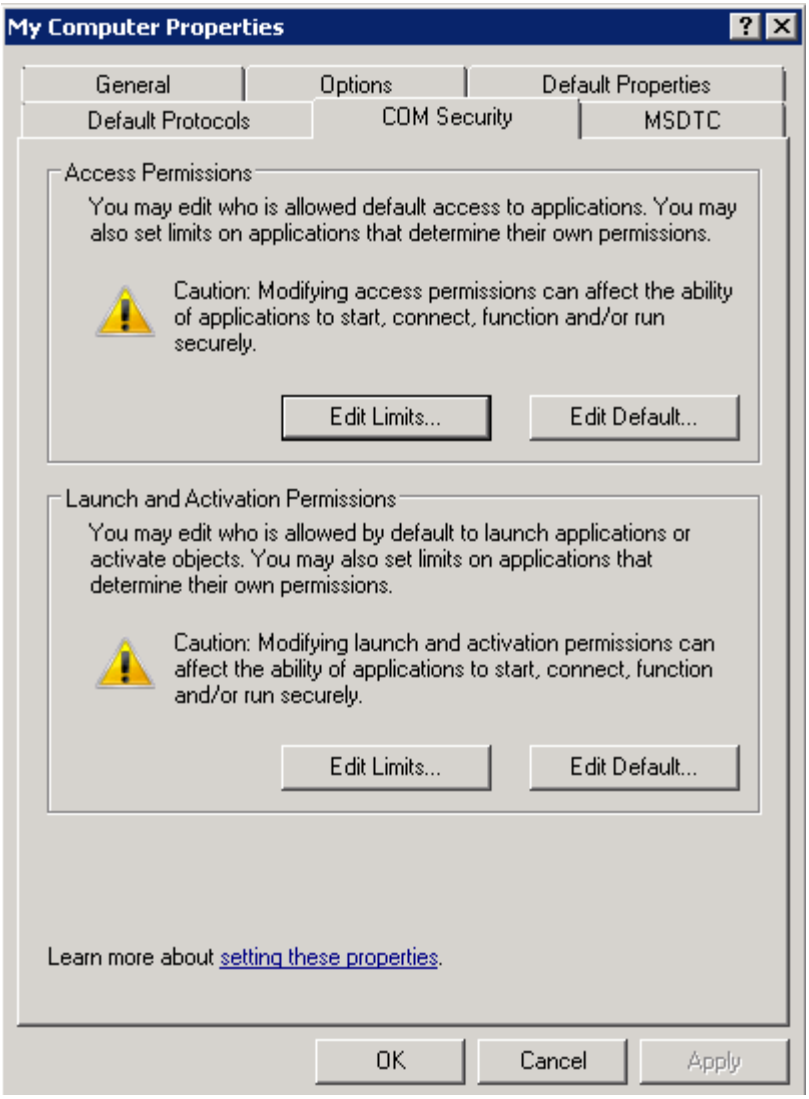
This can be easily done using the following procedure. Contact your Network Administrator to configure security for WMI access, if you do not have enough privilege for the configuration.

1. Click **Start**, click **Run**, type **DCOMCNFG**, and then click **OK**.

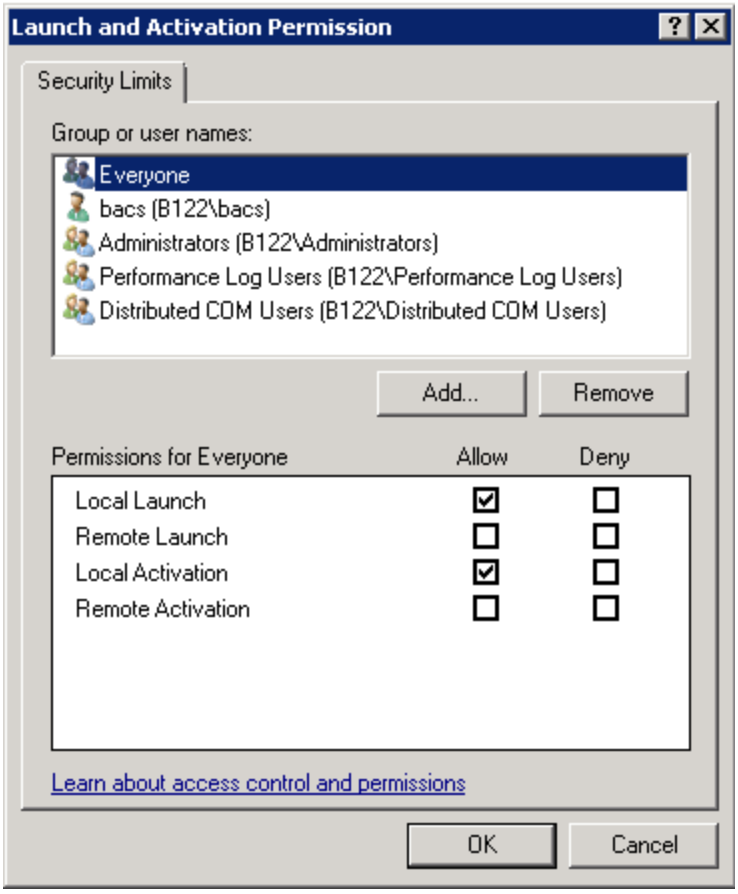
   The Component Services window, shown below, will be displayed.



2. In the **Component Services** dialog box, expand **Component Services**, expand **Computers**, and then right-click **My Computer** and click **Properties**.
3. In the **My Computer Properties** dialog box, click the **COM Security** tab.



4. Under **Launch and Activation Permissions**, click **Edit Limits**.



5. In the **Launch Permission** dialog box, follow these steps if your name or your group does not appear in the **Groups or user names list**:
   a. In the **Launch Permission** dialog box, click **Add**.
   b. In the **Select Users, Computers, or Groups** dialog box, add your name and the group in the **Enter the object names to select** box, and then click **OK**.
6. In the **Launch Permission** dialog box, select your user and group in the **Group or user names** box. In the **Allow** column under **Permissions for User**, select **Remote Launch** and select **Remote Activation**, and then click **OK**.

For more information, see *Securing a Remote WMI Connection* in the MSDN Library.

Special Configuration for WMI on Different Systems

- On a Windows XP Pro or Windows 2003 Server computer, make sure that remote logons are not being coerced to the GUEST account (e.g., ForceGuest, which is enabled by default on computers that are not attached to a domain). To do this, open the Local Security Policy editor (e.g., by typing 'secpol.msc' into the Run box, without quotes). Expand the Local Policies node and select Security Options. Now scroll down to the setting titled Network access: Sharing and security model for local accounts. If this is set to Guest only, change it to Classic and restart the computer.
- In Windows Vista and Windows 7, in order to let all users in administrator group to connect WMI name space, user might need to change LocalAccountTokenFilterPolicy as needed.

Getting Familiar

GUI

This section is divided in three sections to familiarize the user with the GUI manipulation, Layout Design and other features like Menu bar and Filters.

GUI Manipulation

BACS4 is developed based on existing BACS3 GUI design to maintain the same user experience and familiarity. Since BACS4 is developed using a different framework - a cross platform framework that work for both Windows and Linux, some existing GUI features may not be available depending on the new framework limitations.

The main windows of BACS4 should contain three panels, Object explorer, Context view and Context view selector.

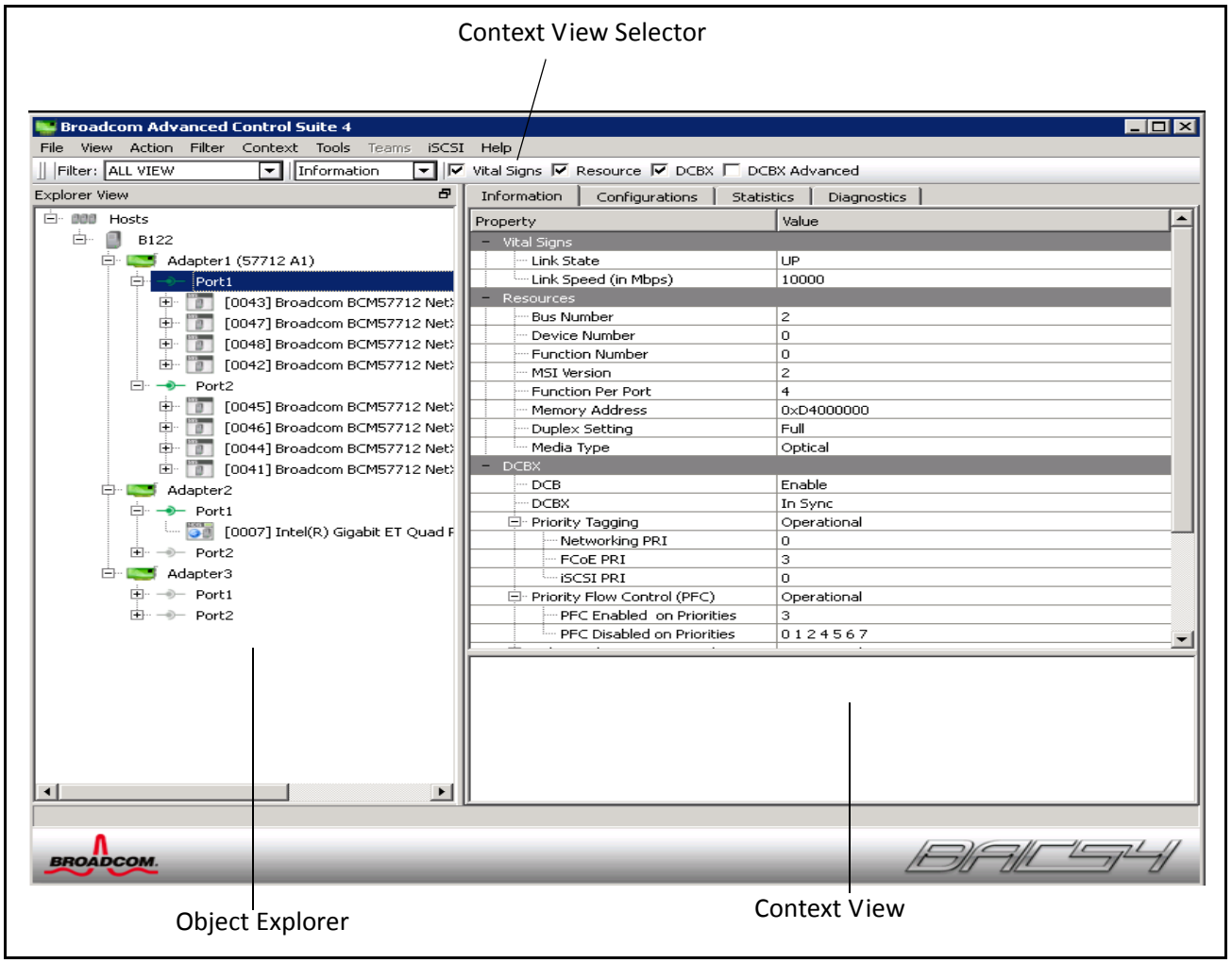


Figure 3: BACS4 Main Window

By default, Object explorer is docked to the left of main window and Context view selector is unpinned and rolled down to the bottom of the main window. See Figure 4.

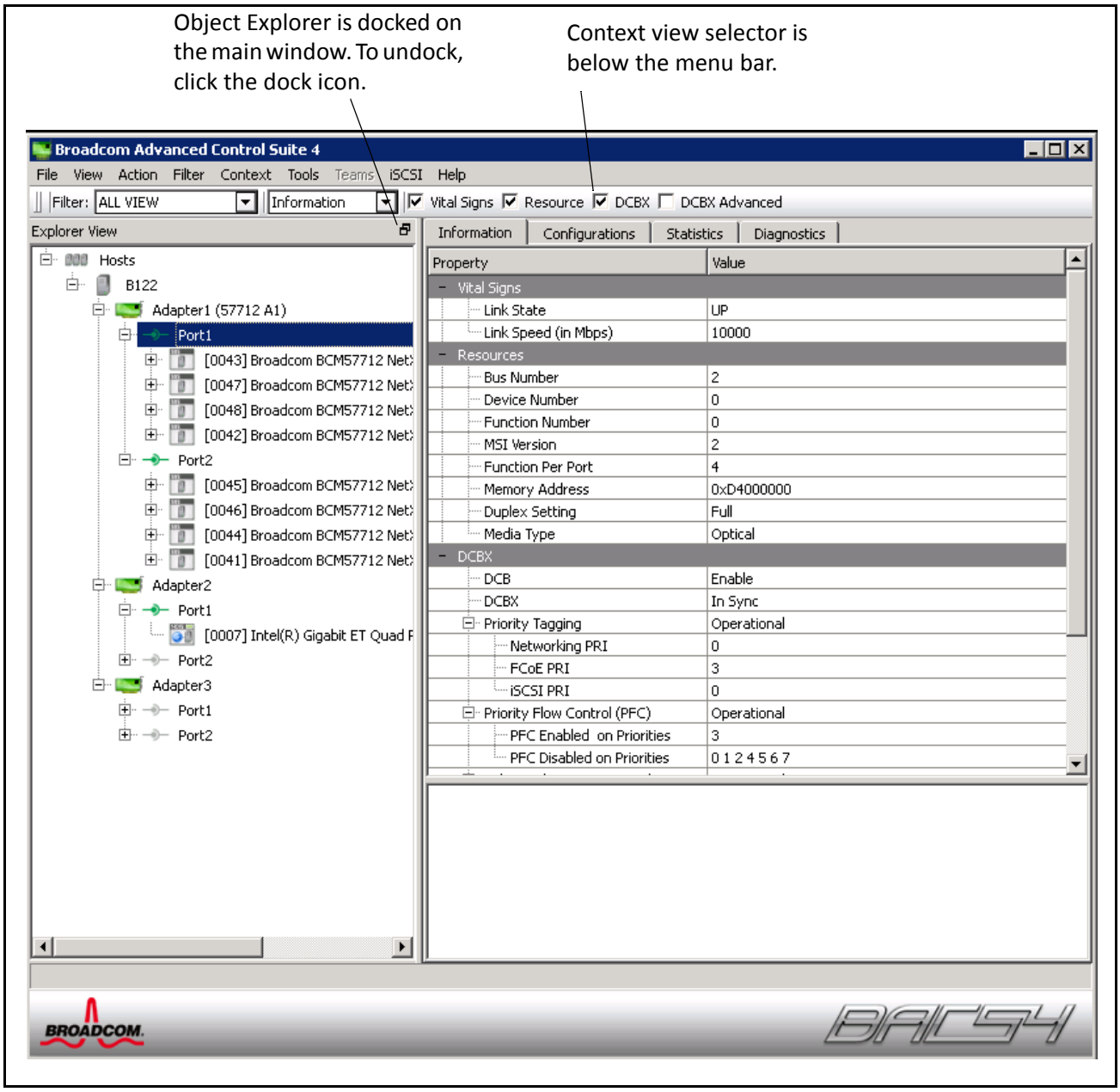


Figure 4: BACS4 Main Window Default Layout

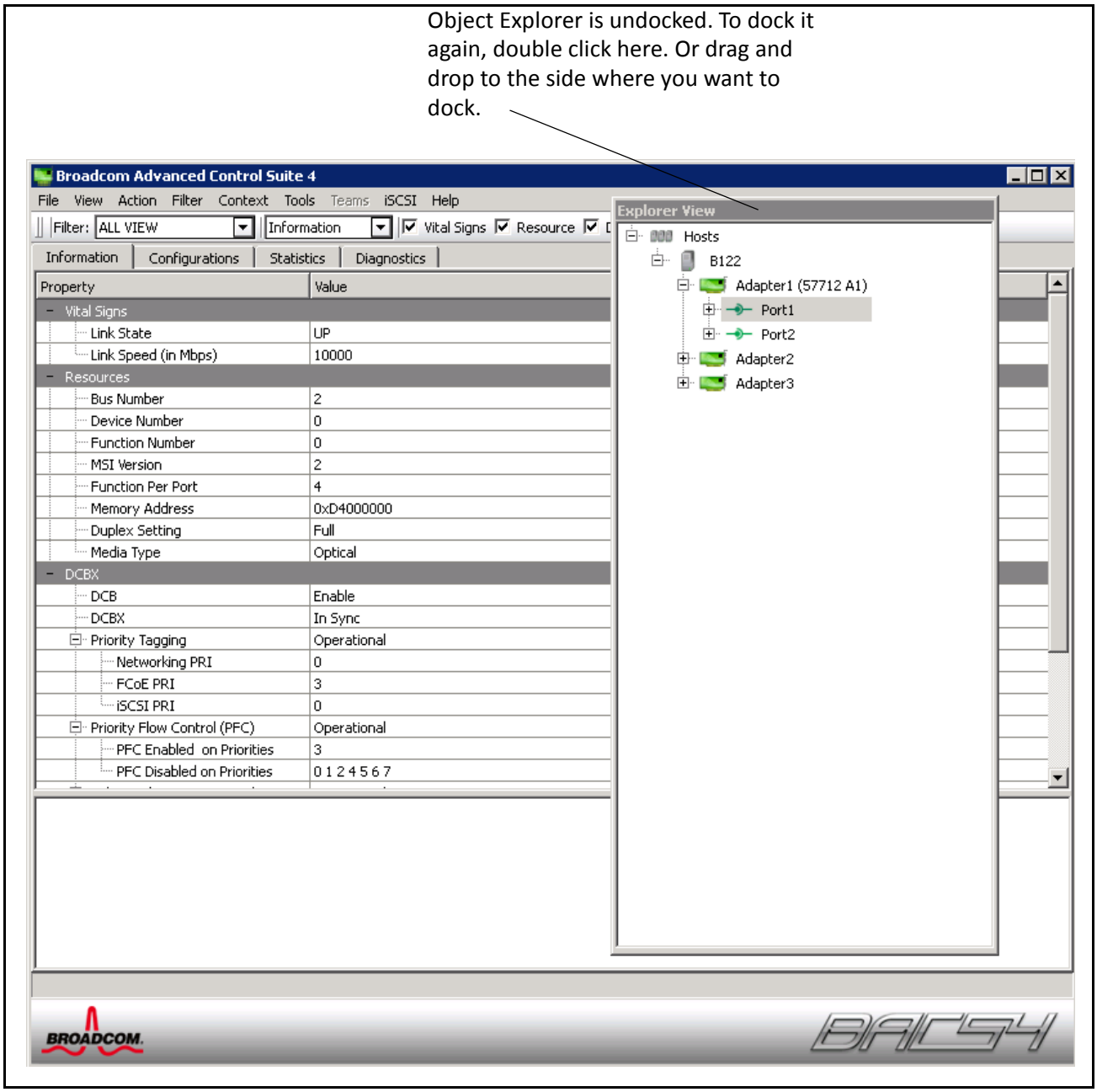


Figure 5: Docking & Undocking

To undock the Object Explorer, click the dock icon. Figure 5 above shows that the Object Explorer is undocked. To dock it again, click the undock icon.

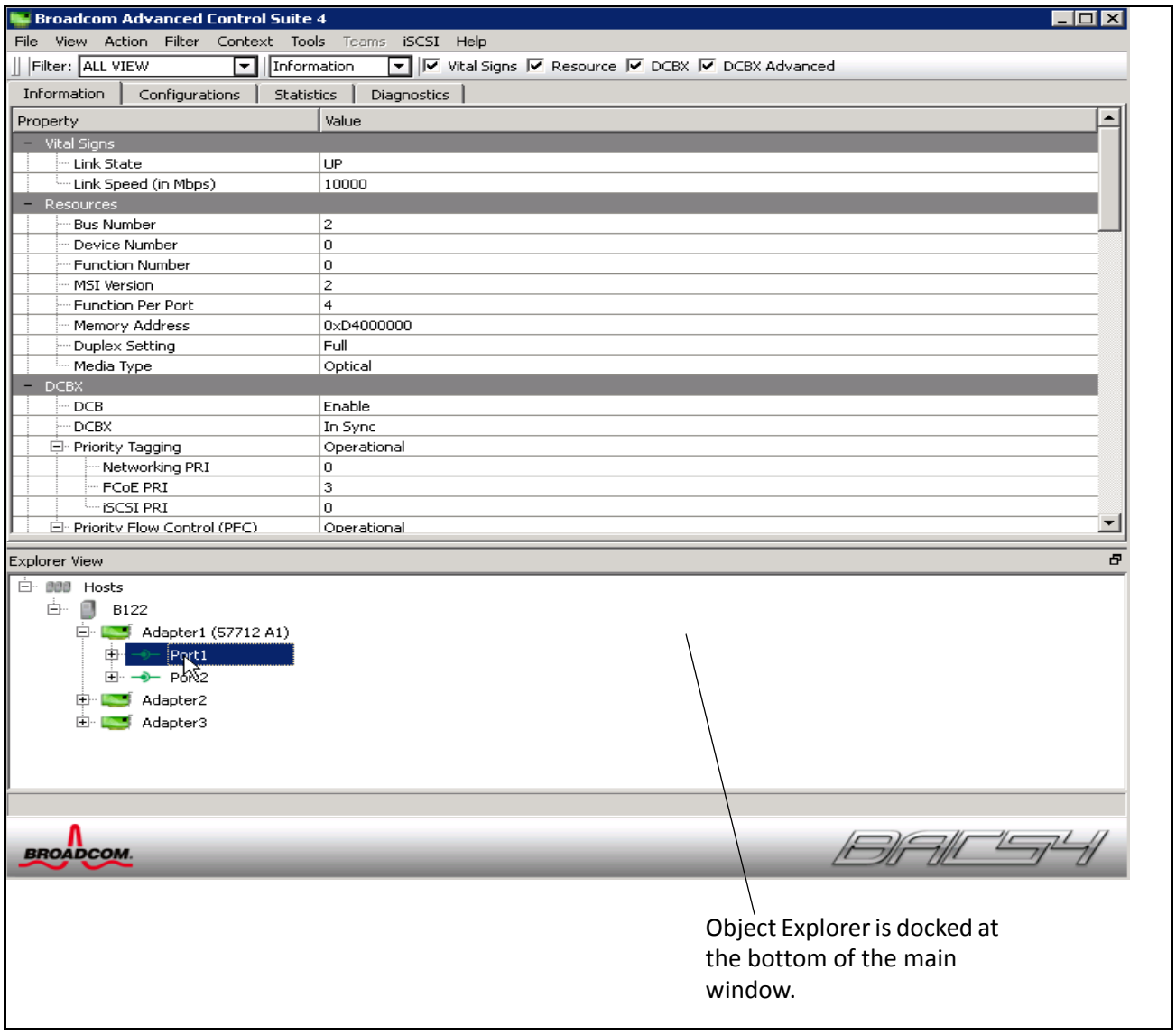


Figure 6: Docking at the Bottom

User can also dock the Object Explorer to top, bottom, left or right. Figure 6 shows that the Object Explorer is docked on the bottom of the main window.

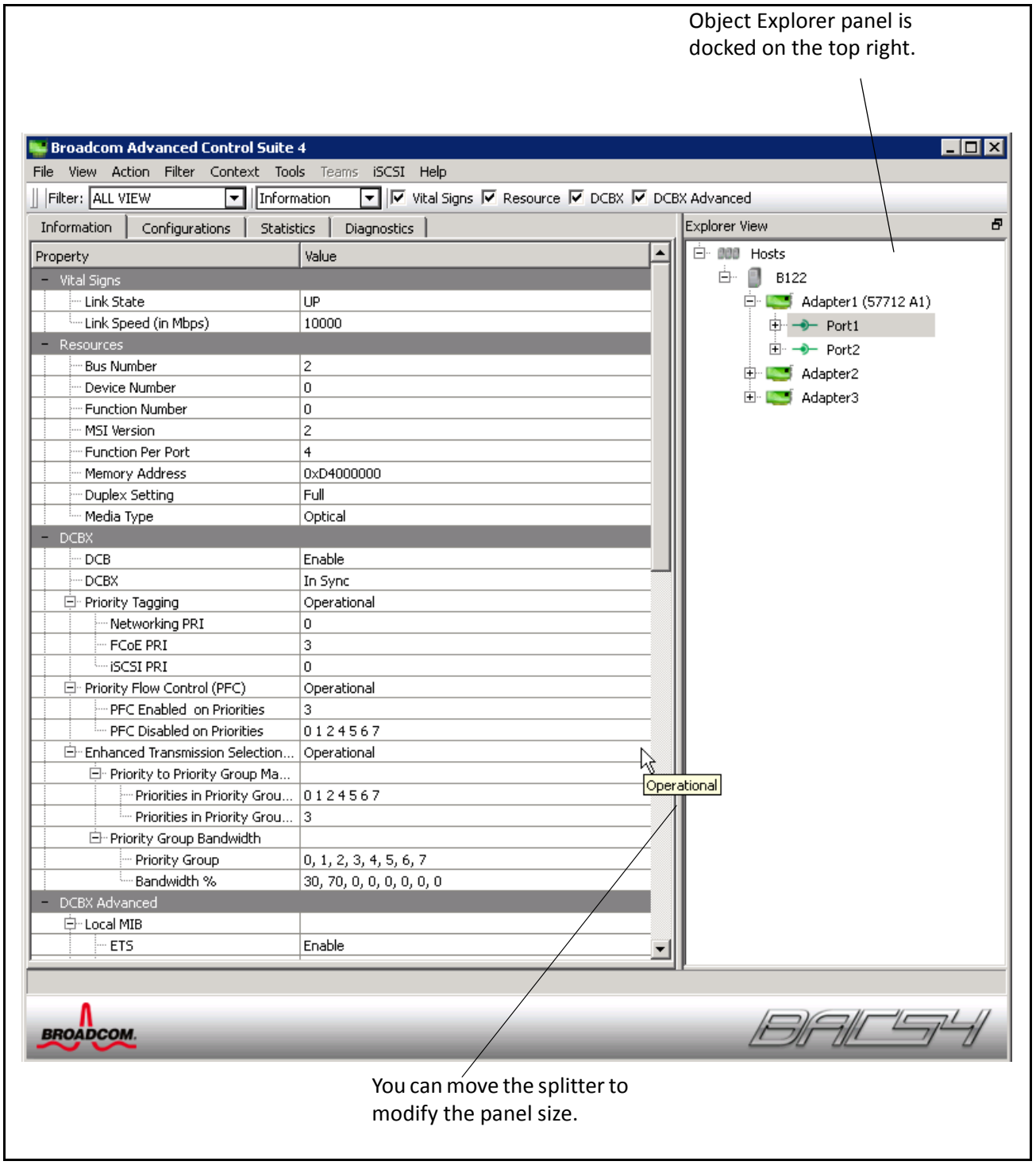


Figure 7: GUI Manipulation

At any time, user can click and drag the splitter between panels to adjust their size in order view more information on certain panel. See Figure 7.

User can also drag the Object Explorer outside the main window; they can float outside of the main window.

GUI Layout Design

The BACS4 GUI window has three main panels – Object Explorer, Context View and Context View Selector. This section will describe the details on these three panels.

Object Explorer

The object explorer will show all the objects that BACS4 will manage; it includes all the items shown on the architectural diagram. The user can browse to manageable objects.

The organization of this panel is designed to present the manageable objects in the same hierarchical manner as drivers and its subcomponents. This will greatly simplify the management of various manageable elements of the CNA adapter. At the top of the Device Tree is a container “Hosts” which lists all hosts that can be managed using the BACS4 Management Application. User can easily add the hosts using various methods which are explained later in this guide. For each host, the installed Converged Network Adapters are listed. Below adapter, all manageable elements for that adapter are listed in hierarchical manner such as Physical port, VBD, FCoE, NDIS, iSCSI etc. Clicking on any of this element will give user an option to view details of that element, configure the element, view statistics and perform diagnostic operation in adjacent Context View panel.

Sometimes it may be necessary to view only certain type of elements - all NDIS devices for all adapters in a host, for example. The filters help achieve this goal. The filters are explained late in this guide in detail.

Context View

The context view contains all the features belong to the selected object in the Object Explorer. Typically, it contains information, configuration, diagnostics and statistics tabs. In each tab, it contains several categories. For example, Information tab contains Vital Signs, Driver Information, Resource and Hardware categories.

In Figure 8 the right panel is the Context view with information page. When user selects a device on the object explorer, the information tab display read only information about the selected device. User can click the diagnostics tab to run diagnostic tests; click Configuration tab to configure the device or click the statistics tab to monitor the statistics of the device.

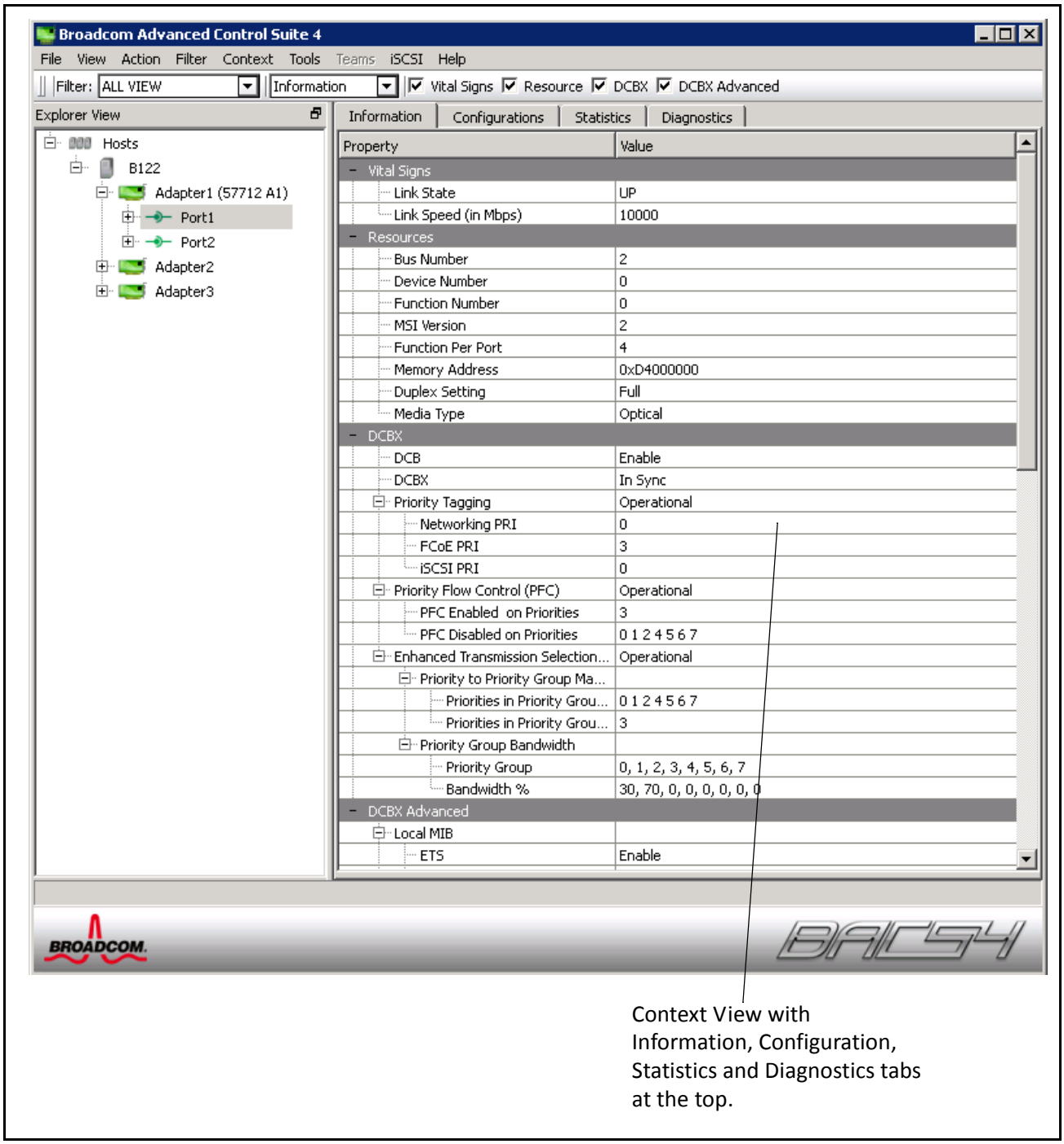


Figure 8: Context View

Context View Selector

The context view selector lets user to select which features should be displayed in the context view. The categories for each tab can be collapsed or expanded. Click the drop down menu below the menu bar (drop down menu shown below, in Figure 9) to select the tab.

To select a category to be displayed, check the corresponding check box. For example in Figure 9, all the categories in Information tab are selected, so they all show up in Context view.

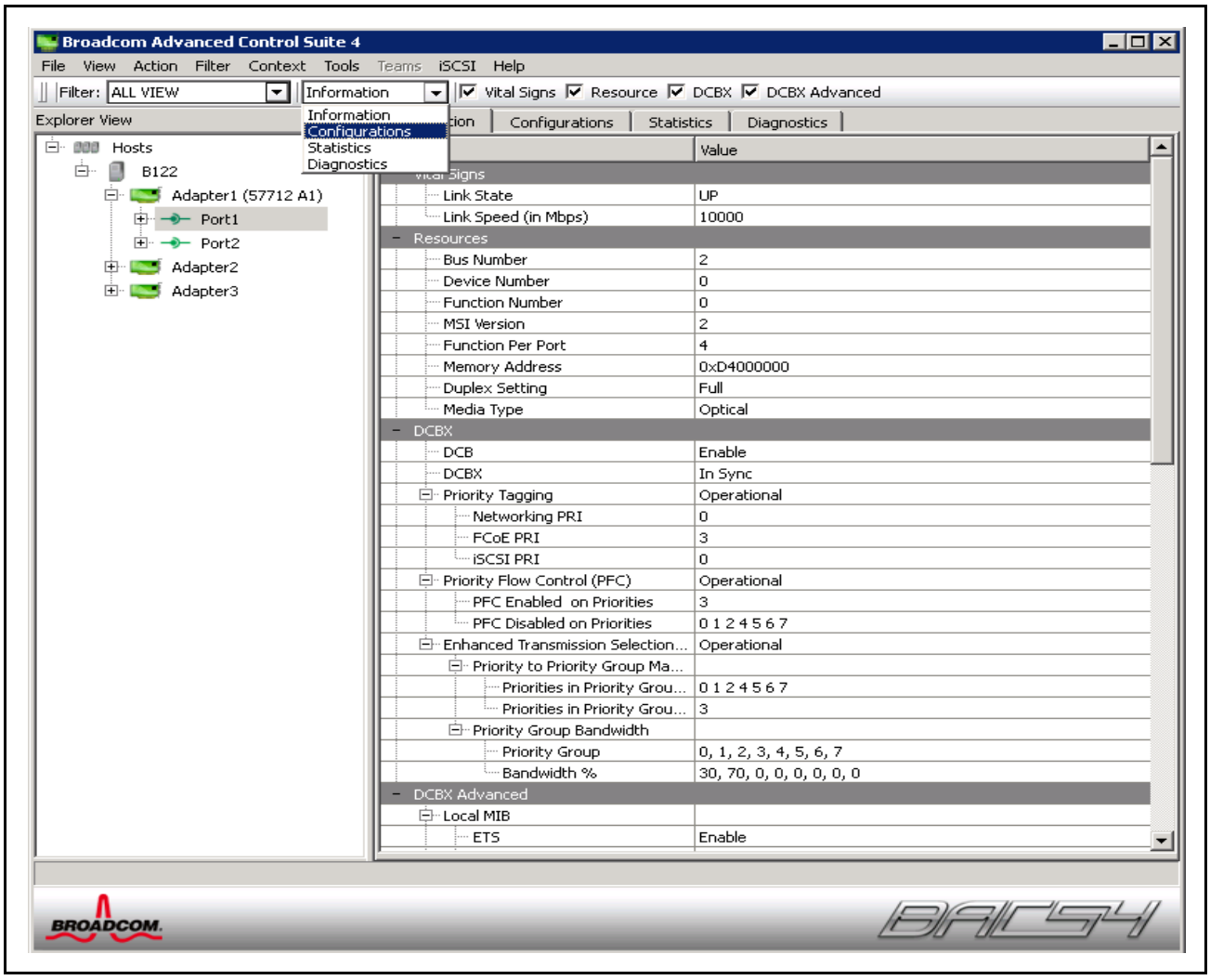


Figure 9: Context View Selector

If the user does not want to see certain category, uncheck the check box for that category. For example, deselecting the Vital Sign check box lists only the DCBX and Resource details in Context View panel.

Menu Bar

The menu items mostly behave the same as other applications menu. The File sub items handle two primary teaming operations: Team Save As and Team Restore. The Team Save will save the current team configurations to a file while Team Restore will restore any saved team configuration from a file. Further details of how teaming operations work will be discussed later in this guide.

The Action menu will allow user to add hosts or remove hosts in the BACS4 GUI. After adding a host, it can be managed using the BACS4 GUI.

Figure 10 below shows various Menu bar options available in BACS4 GUI Management Application.

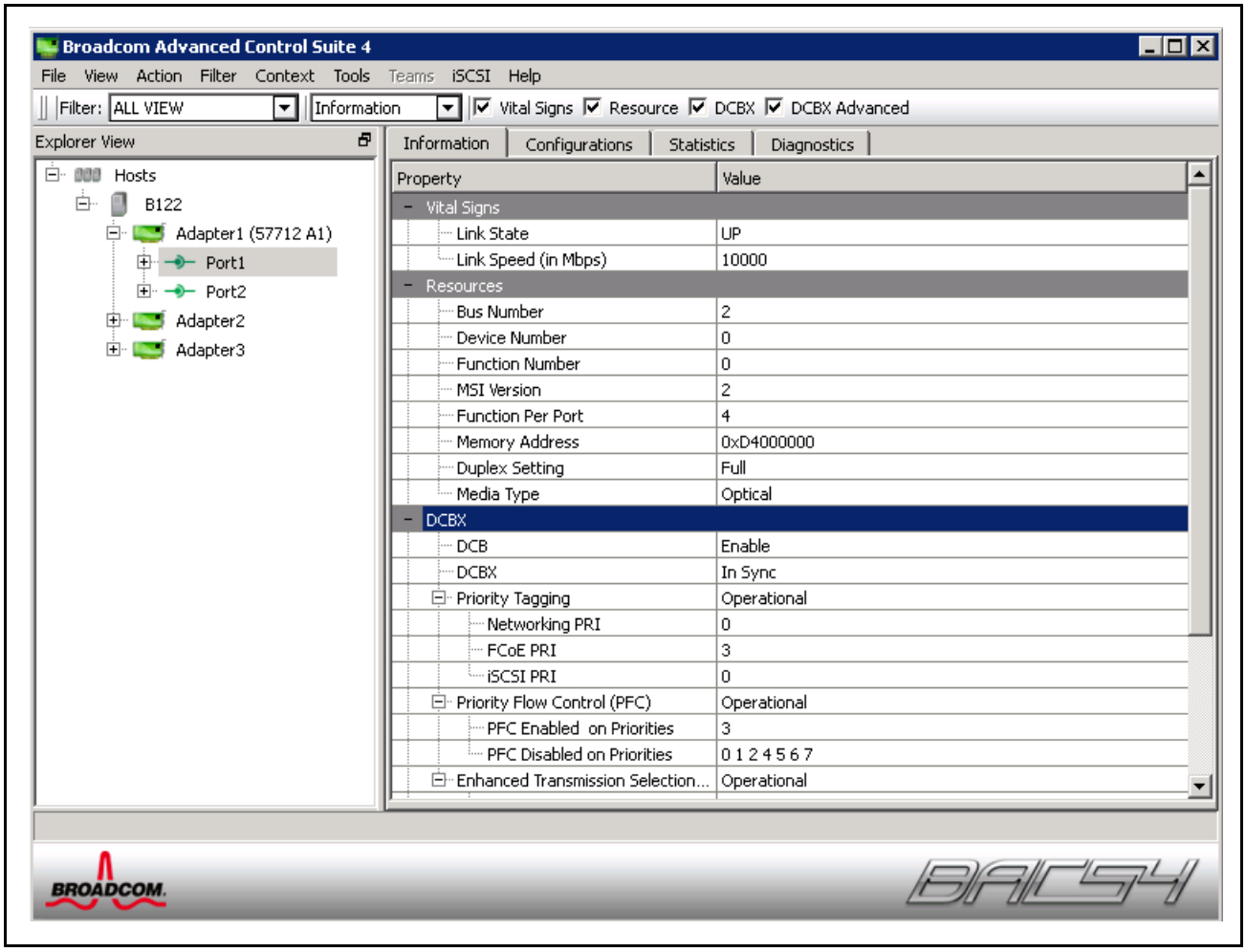


Figure 10: Menu Bar

The View menu item configures whether the Tool bar and Broadcom Logo should be displayed or now. For example, as displayed below in Figure 11, deselecting “Tool Bar” under View will remove the Tool Bar. Similarly, Broadcom logo can be removed to optimally utilize the maximize the space.

\

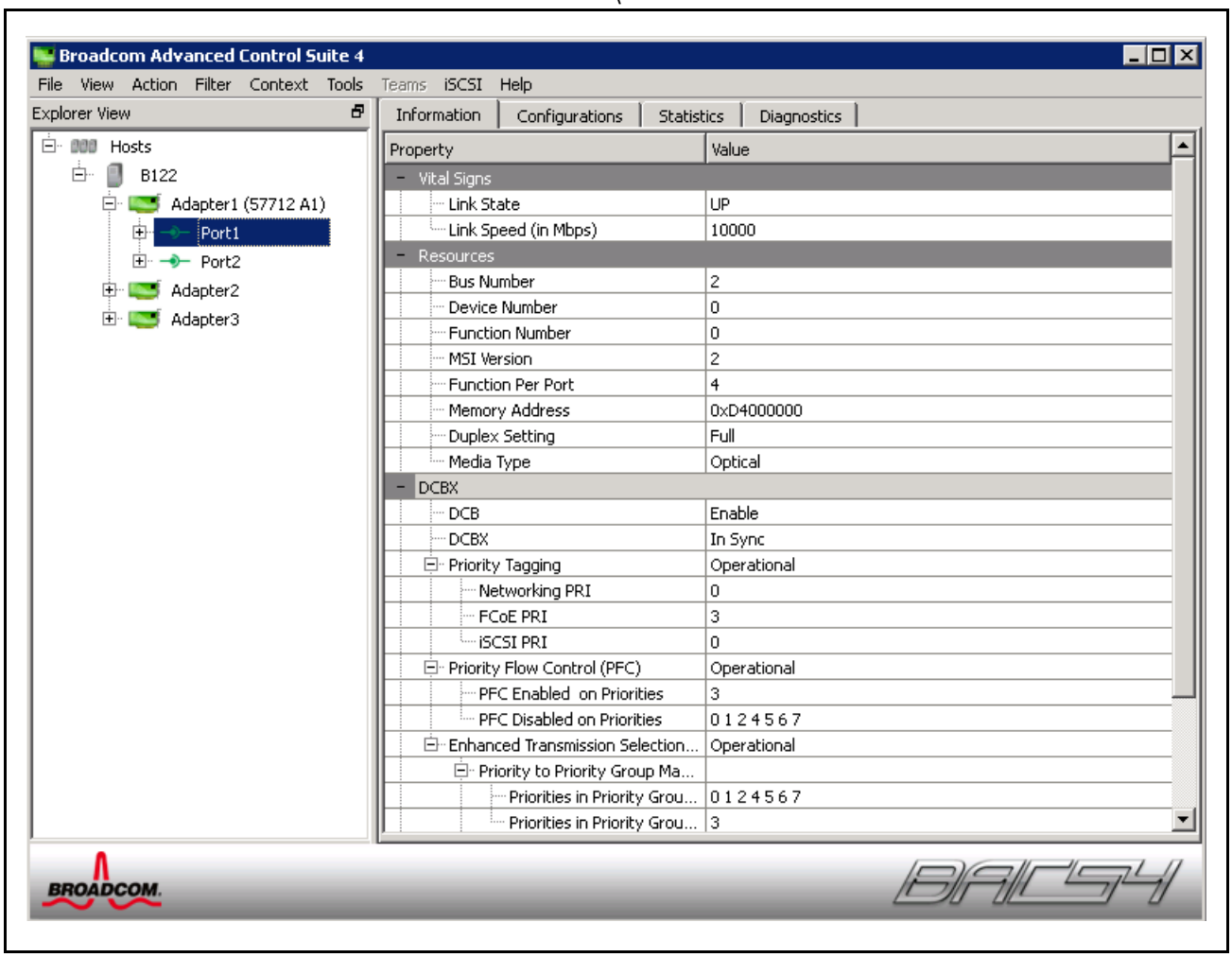


Figure 11: View Menu Item

The Tools menu allows user to configure the mode of any configuration operation as Expert Mode or Wizard Mode.

The iSCSI menu bar option allows users to configure various iSCSI related operation like discovering iSCSI discovery portals, adding and managing targets, and adding iSNS server, etc. Available options include Discovery Wizard, Manage Targets, Manage iSNS Servers and Manage Discovery Portals.

The Windows option allows users to view or close certain windows/panels. Some panels are default and they cannot be closed.

The Help menu option lists the BACS4 GUI Management Application version number and additional information like trade mark and copyright information.

Filter View

The Filter is a new feature of BACS4 GUI. With Converged Network Adapters (CNA), the number of manageable elements per adapter has increased. In multiple hosts environment, it sometimes becomes overwhelming and cumbersome for user to view/configure/manage all elements. The filter allows users to select particular type of device or function for the management. It groups selected device type for all adapters installed in all hosts and only list those devices/function. Figure 12 shows FCoE view selected. As you can see all other devices are removed and only FCoE devices are listed.

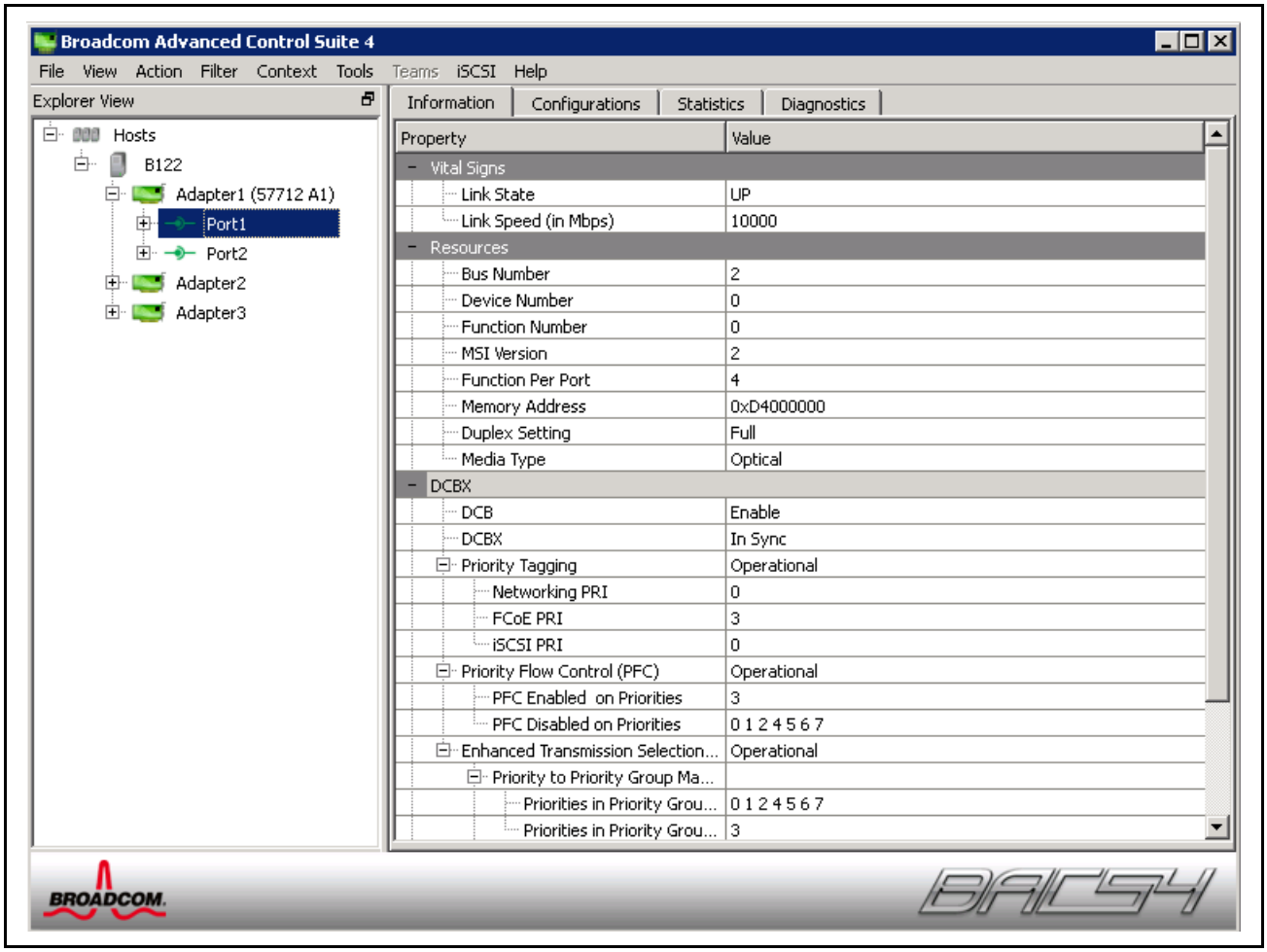


Figure 12: Filters

Launching GUI

The GUI can be launched in one of the several ways listed below.

- From Program Menu: Click the Start > All Programs > Broadcom > Broadcom Advanced Control Suit 4.
- From Control Panel: Navigate to Start > Control Panel and then click Broadcom Control Suite 4.
- From System Tray: Click Broadcom Advanced Control Suite 4 icon located in system tray.

The GUI can be closed in one of the two ways listed below.

- Click the File > Exit on the BACS4 GUI window.
- Click the X button on the upper right corner of the BACS4 GUI window.

Note: The BACSTray can be closed by right-clicking on the BACS Tray icon in the system tray. Closing the BACS Tray does not close the GUI. The BACS Tray can be started again by double clicking on the BACSTray.exe file in c:\Programs Files\Broadcom\BACS folder.

CLI

This section will describe management of the CLI client application.

CLI Architecture

The BACS4 CLI structure is somewhat unique and it is highly recommended that user get familiar with the underlying architecture before using it. There are two modes of CLI management.

- Interactive
- Noninteractive

In the noninteractive mode, the utility can take a command as an input argument and run the command producing appropriate effect/output and return meaningful exit codes.

In the interactive mode, user make connections to local as well as remote hosts and manage them by entering command in the CLI window. The output is listed in the CLI window which may be the information or error message. The interactive mode is not menu based. User is required to enter a correct command to list particular types of target before they can be managed.

Each manageable element is known as “Target”. The word target should not be mistaken for FCoE/SCSI target which usually referred to as a storage system and/or LUN. When the command is issued to list a particular target/manageable element, all the targets matching the criteria defined in the query are listed and the first element is selected by default. When the command is executed to list particular type of targets, the focus shifts from the target which was selected before the query was run to a first target in the current output. For example, when the currently selected target is FCoE device and if the user enters a command to list NDIS devices then all matching NDIS devices are listed and the first NDIS device in the list is automatically selected for the management. If user wants to manage the FCoE device which was originally selected then he must first list all the FCoE devices and then select the appropriate instance to manage it. See Figure 13 and Figure 14 below to understand the concept.

This does not apply when user issues command to list the information regarding the currently selected target.

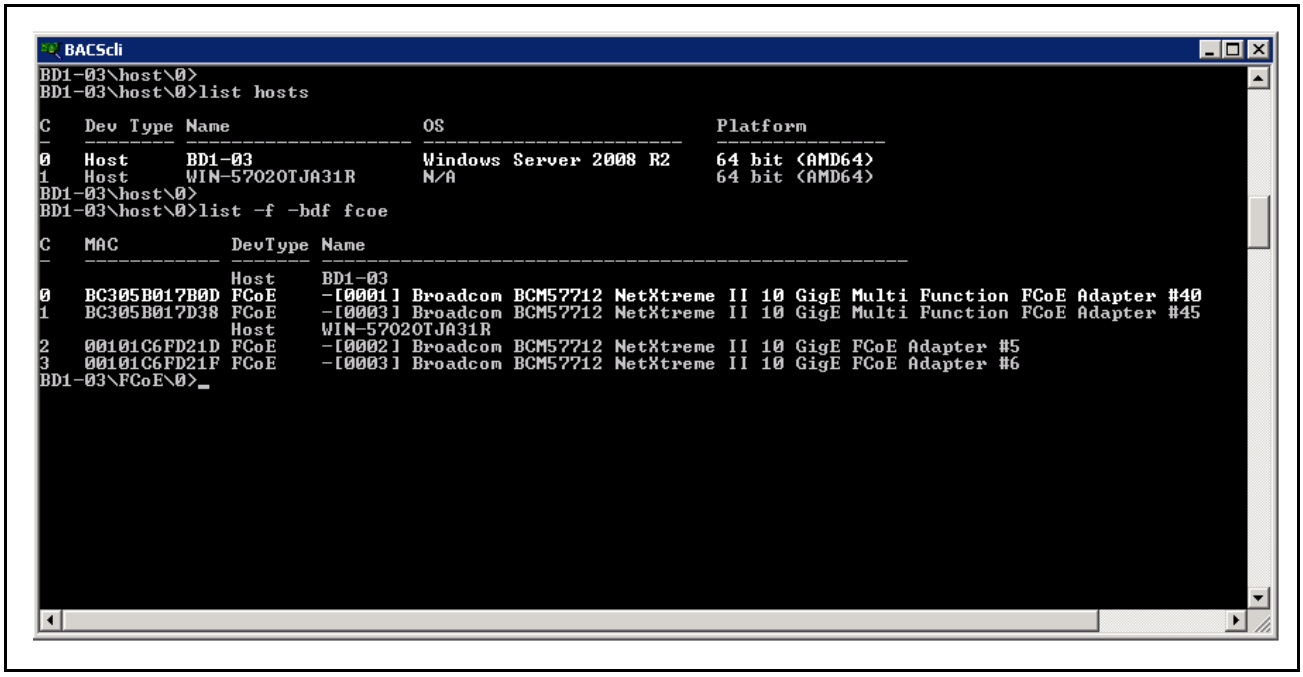


Figure 13: FCoE Device Selected

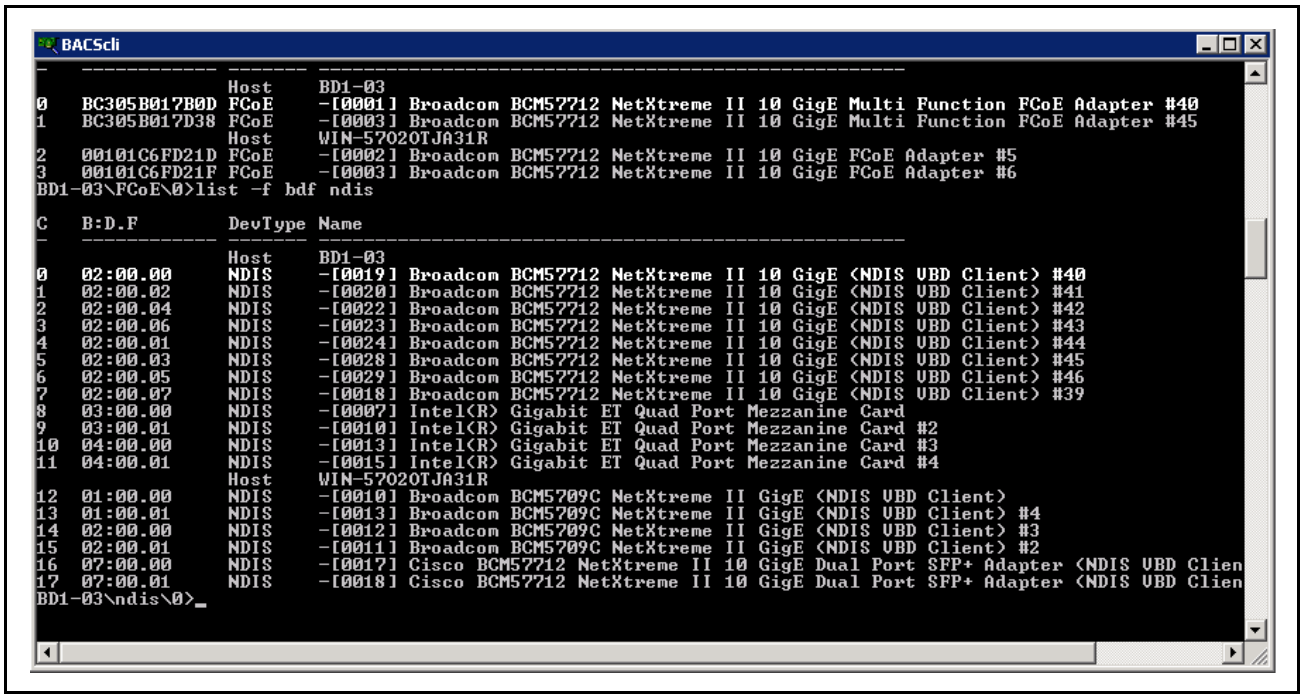


Figure 14: Focus Changed to NDIS Device

The target can be selected by indicating the instance number in the **Select** command. For example, if CLI has connection to two hosts and if there are two adapters in each host then when the command is issued to list the adapters, all adapters will be listed - grouped by the host. There will be total four entries with instance number 0 to 3. User can select any adapter by issuing the select <instance_number> command.

The CLI always displays the prompt with current focus in hierarchical manner starting with host. See "Windows System" on page 15 to understand the hierarchical structure of the CNA. When the command is entered and output is listed, the prompt changes to the first target -- starting with the host and ending with the current target following a hierarchical structure.

In the interactive mode of the CLI there is no back or forward levels. User must explicitly define the target he wants to manage if the new target is different than the currently selected target by first listing particular type of targets and then selecting the appropriate target.

All CLI commands can be broadly divided in four categories – commands to display information of the target, commands to modify the configuration of the target, commands to display the statistical counters for the target and commands to perform diagnostic test on the target.

One of the other important things to remember about the CLI is that when the configuration changes are performed, the host information must be refreshed to display the most up to date information. For host refresh, issue a command to list the host; select the appropriate host and then issue "refresh" command. User can then change the focus back to the target which was being managed.

CLI Layout Design

The CLI client is a windows executable (BACSclie.exe) and is started in the command window. See Figure 15 below.

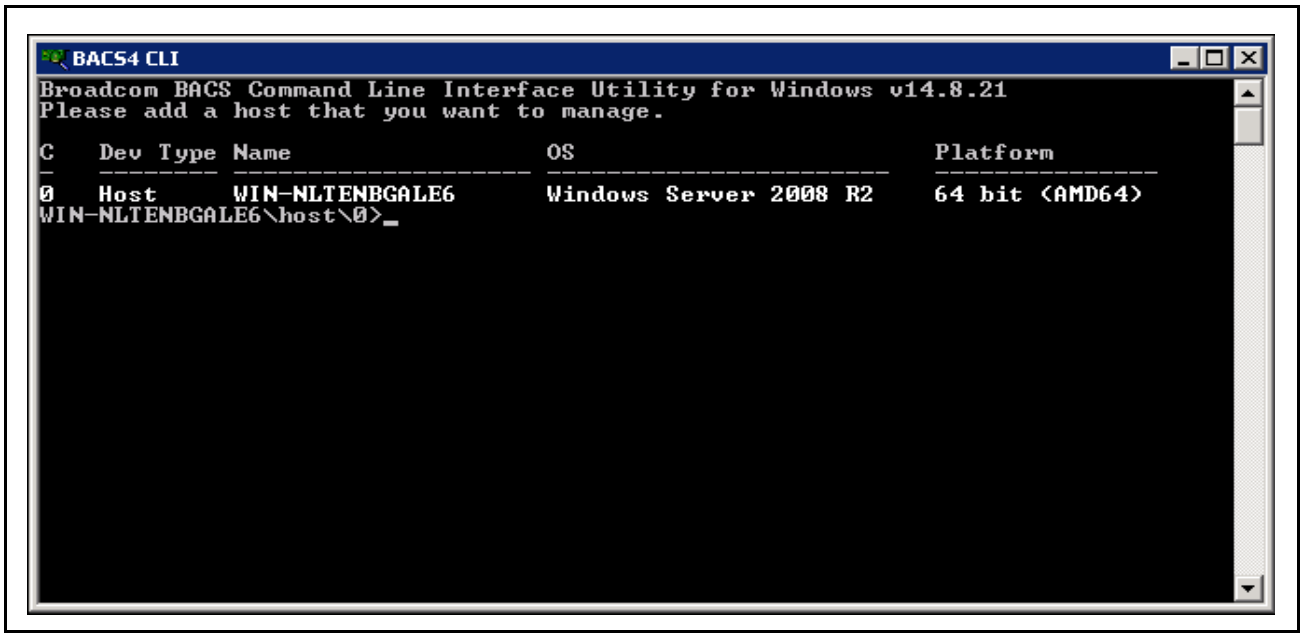


Figure 15: BACS4 CLI Window

The CLI application starts in a command line window. The BACS4 CLI window is like any other windows command line window and can be managed in same way you manipulate command line window. You can resize, minimize and close the window using the mouse. When the CLI window is closed, the connection to the managed host is lost.

Launching CLI

On Windows client, the BACS4 CLI can be launched by double clicking on BACScli.exe file installed in the Program Files\Broadcom\BACS folder.

On Linux client, the BACS4 CLI can be launched by executing on BACScli file installed in the Opt/Broadcom/BACS folder.

The CLI can be closed in one of the two ways listed below.

- Typ q at the prompt in the BACS4 CLI window.
- Click ‘X button on the upper right corner of the BACS4 CLI window.

Connecting to Host

GUI

The BACS4 GUI allows user to add one or multiple hosts for the management. The hosts can be local host or remote host.

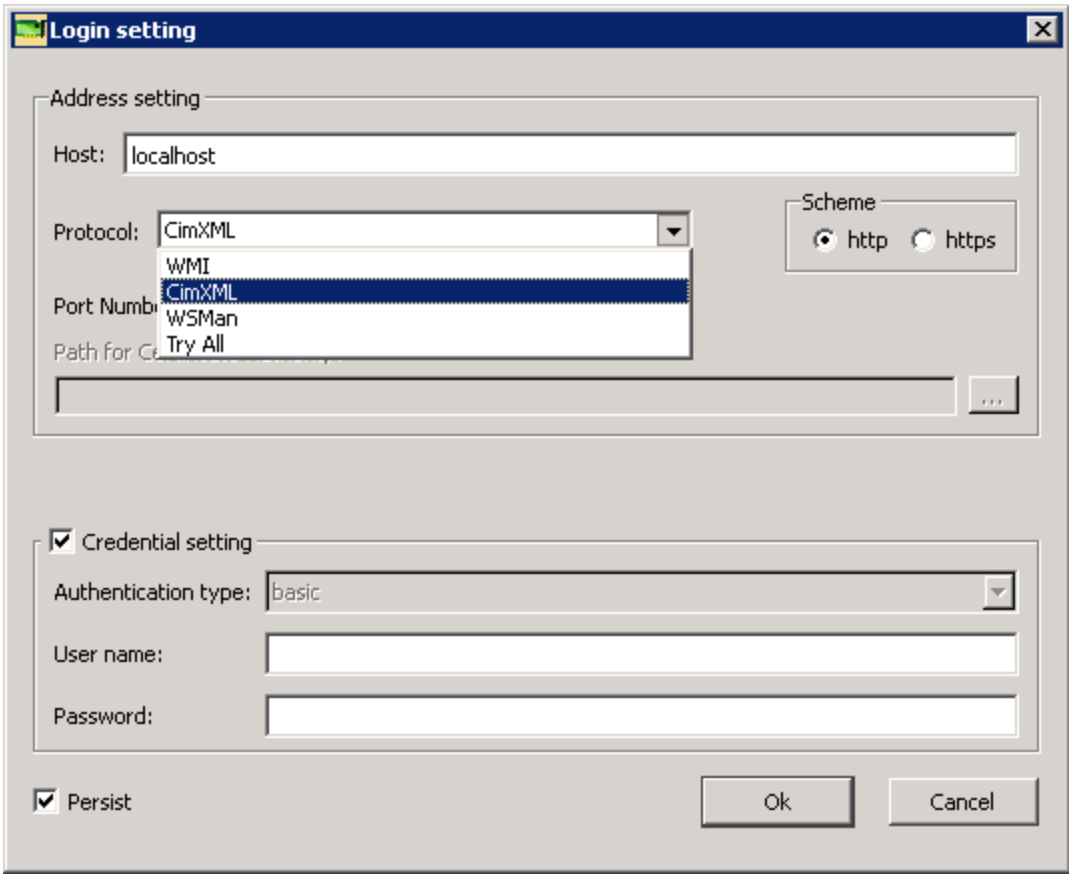


Figure 16: Connecting to Host

Add a Local Host Using the GUI

Connection to a local host is made automatically whenever GUI is opened, if GUI client detects the CIM provider installed on the local host. The local host is displayed in the Object Explorer window with the host name as identifier.

Add Remote Windows Host Using GUI

Note: See "Installation Steps" on page 24 to prepare client and managed host for remote connection.

1. Select **Hosts** in the Object Explorer windows and click Menu option **Action** > **Add Host**. Alternatively, right-click **Hosts** container in Object Explorer panel and select **Add Host**. It will bring up the dialogue box shown in Figure 16 above.
2. In the Host field, enter remote hosts host name or IP address.

3. In the protocol field, select **WMI**, **CimXML**, **WSMan** or **Try All**.

   WMI: This option will use WMI protocol to communicate with the remote window host and make connection. This is a default option selected to make the connection with Windows host.

   WSMan: Select this option if you want to use more secure protocol option while making the remote host connection. If this option is selected then user has the option of selecting “HTTP” or “HTTPS”. Selecting HTTPS will provide additional security. This option can be used to connect to Linux/Windows server from Linux/Windows client.

   CimXML: Select this option if you want to use more secure protocol option while making the remote host connection from Linux client to Linux server using CimXml. If this option is selected then user has the option of selecting “HTTP” or “HTTPS”. Selecting HTTPS will provide additional security.

   Try All: Selecting this option will force GUI client to try all applicable options one by one. User doesn’t have to select different options manually one by one, if this option is selected.

4. Select HTTPS for **Scheme** option if you want to use HTTPS for added security. Otherwise leave HTTP as default selected option.
5. Enter different value of **Port Number** if you have configured the host with nondefault port number for HTTP/HTTPS. The default value is 5985.
6. Enter username and password with administrative privilege on the remote host. You can also use user account with domain administrator privilege.
7. Select **Persist** check box if you want BACS4 GUI to remember entry for this host. If you select this option then user don’t have to add the IP address or host name of the remote host. User will still have to enter username and password.
8. Click **OK.**

   The **Path for Certificate Authority** is relevant when the HTTPS is selected under **Scheme**.

Add a Remote Linux Host Using GUI

Note: See “Installation Steps” on page 24 to prepare client and managed host for remote connection.

1. Click Menu option **Action** > **Add Host**. Alternatively, right-click Hosts container in Object Explorer panel and select **Add Host**. It will bring up the dialogue box shown in Figure 16 above.
2. In the Host field, enter remote hosts host name or IP address.
3. In the protocol field, select **CimXML**, **WSMan** or **Try All**.

   CimXML: This option will use CimXML protocol to communicate with the remote Linux host and make connection.

   WSMan: Select this option if you want to use more secure protocol option while making the remote host connection. If this option is selected then user has the option of selecting “HTTP” or “HTTPS”. Selecting HTTPS will provide additional security. While adding Windows host from Linux client GUI, you must select this option.

   Try All: Selecting this option will force GUI client to try all applicable options one by one. User doesn’t have to select options one by one if this option is selected.

4. Select HTTPS for **Scheme** option if you want to use HTTPS for added security. Otherwise leave HTTP as default selected option.
5. Enter different value of **Port Number** if you have configured the host with nondefault port number for HTTP/HTTPS. The default value is 5985.
6. Enter username and password with administrative privilege on the remote host. You can also use user account with domain administrator privilege.
7. Select **Persist** check box if you want BACS4 GUI to remember entry for this host. If you select this option then user don't have to add the IP address or host name of the remote host. User will still have to enter username and password.
8. Click **OK**

CLI

The BACS4 CLI allows user to add one or multiple hosts for the management. The hosts can be local host or remote host.

Add a Local Host Using CLI

Connection to a local host is made automatically whenever CLI is opened, if CLI client detects the CIM provider installed on the local host. The local host is displayed at the top of the CLI and the local host is automatically selected as the current object.

Add a Remote Host Using the CLI

1. Open BACS4 CLI client.
2. Connection to the local host is automatically made and selected as current object.
3. Issue the following command:

```
addhost < [ < localhost | <local host name> | <local host IP> ] |
[ -u <username> -p <password> <host name | IP address> ] >
[-a <digest | basic>]  [-n <port>] [-protocol <wmi | cimxml | wsman | all>]
[-persist]
```

   For the **Protocol** variable, select:

   - WMI: This option will use WMI protocol to communicate with the remote window host and make connection. This is a default option selected to make the connection with Windows host.
   - WSMan: Select this option if you want to use more secure protocol option while making the remote host connection. If this option is selected then user has the option of selecting "HTTP" or "HTTPS". Selecting HTTPS will provide additional security. This option can be used to connect to Linux/Windows server from Linux/Windows client.
   - CimXML: Select this option if you want to use more secure protocol option while making the remote host connection from Linux client to Linux server using CimXml. If this option is selected then user has the option of selecting "HTTP" or "HTTPS". Selecting HTTPS will provide additional security.
   - Try All: Selecting this option will force GUI client to try all applicable options one by one. User doesn't have to select different options manually one by one, if this option is selected.

4. Enter different value of **Port Number** if you have configured the host with nondefault port number for WMI/HTTP/HTTPS. The default value for WMI is 80.
5. Enter username and password with administrative privilege on the remote host. You can also use user account with domain administrator privilege.
6. Select **Persist** check box if you want BACS4 GUI to remember entry for this host. If you select this option then user don't have to add the IP address or host name of the remote host.

Troubleshooting Connection-Related Issues

The BACS4 Management Application introduces a new feature – managing remote host using the BACS4 client GUI. This section will describe most common connection related issues and troubleshooting steps.

Windows

Network cable not properly connected to the network interface of the management host.

Check if the network cable is connected properly to the network interface of the management host where GUI client is installed. Disconnect the network cable from the network interface and connect it back. Also verify that the network LED on both - network interface and switch is lit indicating a good connection.

Network cable not properly connected to the network interface of the remote managed host.

Check if the network cable is connected properly to the network interface of the management host where GUI client is installed. Disconnect the network cable from the network interface and connect it back. Also verify that the network LED on both - network interface and switch is lit indicating a good connection.

Network interface of the management host does not have network parameters configured.

Check and verify that the network interface used by BACS4 GUI client to make connection to the managed host is configured with the correct IP address, subnet mask and gateway IP address. Use the 'ping' command to verify the network connectivity to the managed host.

Incorrect credential used while making connection.

Ensure that the correct username and password are used. Verify that the CAPS LOCK is not activated on the keyboard. The local administrator account of the managed host and domain admin account have permission to connect to the managed host using the BACS4 GUI. For all other user account, refer #5 below.

User does not have enough security privileges to connect to the remote managed host.

By default, user account that has local admin privilege on the remote host or domain admin privilege, can log on to the remote managed host using the BACS4 GUI. See "Windows" on page 19 to configure the WMI access for user and group that does not have local admin or domain admin rights on the managed host.

Incorrect WMI port number used while making connection.

The port number being used to make the connection with remote host while using WMI connection should be the same as configured on the remote host. The default port number is 80.

Linux

For Linux connection issue, verify the following in addition to points mentioned above.

- Ensure that OpenPegasus is installed correctly and CIMSERVER can be started without any issue before installing the Broadcom CMPI provider.
- Broadcom CMPI Provider is installed and the version is minimum 2.1.0.
- CIMSERVER is currently running.
- Ensure that the protocol (HTTP/HTTPS) you want to use is enabled.
- If OpenPegasus was compiled from source and you have trouble connecting HTTPS, ensure that you have installed **OpenSSL** and enabled HTTPS as mentioned in “Uninstall the BACS Management Application” on page 39
- If Firewall is enabled, verify if the appropriate ports are open.
- If connection was fine before and stopped working after OpenPegasus was rebuilt, you must follow configuration steps mentioned in “Uninstall the BACS Management Application” on page 39.
- If you are using the Inbox tog-pegasus from Red Hat, it may be because of the security setting. See “Install OpenPegasus from Inbox RPM (Red Hat only).” on page 34 for detailed instructions.

Persistent Connection

While connecting to a local host or remote host user have the option to save connection elated information in the local BACS database. User doesn’t have to remember host name or IP address of all hosts they want to manage using the BACS4 GUI. This also saves time for the user form entering this information manually one-by-one.

However, the persistent database does not save user credential in the database for obvious security reason. The username and password will have to be manually added every time user selects one of the persistent connection entries to connect to it.

If persistent check box was selected while making connection for the first time, the entry with the IP address or host name will be displayed in the Object Explorer pane when GUI is opened next time. Simply select the entry, enter username, password and click OK to connect to it.

Note: All subsequent chapters list the information on the various aspects of the host management using GUI. The respective information for the CLI is listed in the Appendix A: “CLI Command Usage,” on page 143. The Appendix A: “CLI Command Usage”contains lists of all CLI commands and example to perform most common tasks. It is highly recommended that users see “CLI” on page 56 for the CLI architecture.

Managing Host

This chapter will cover details on how to manage the host. Once the host is added and selected in the Object Explorer window, user can view information about the host and make host level changes. Two tabs are displayed in the Context View pane once the host is selected:

- Information
- Configuration

View Information

The Information tab displays host related information like - operating system information and iSCSI initiator information, if there is iSCSI enabled on the host. See "View Host Information" on page 65.

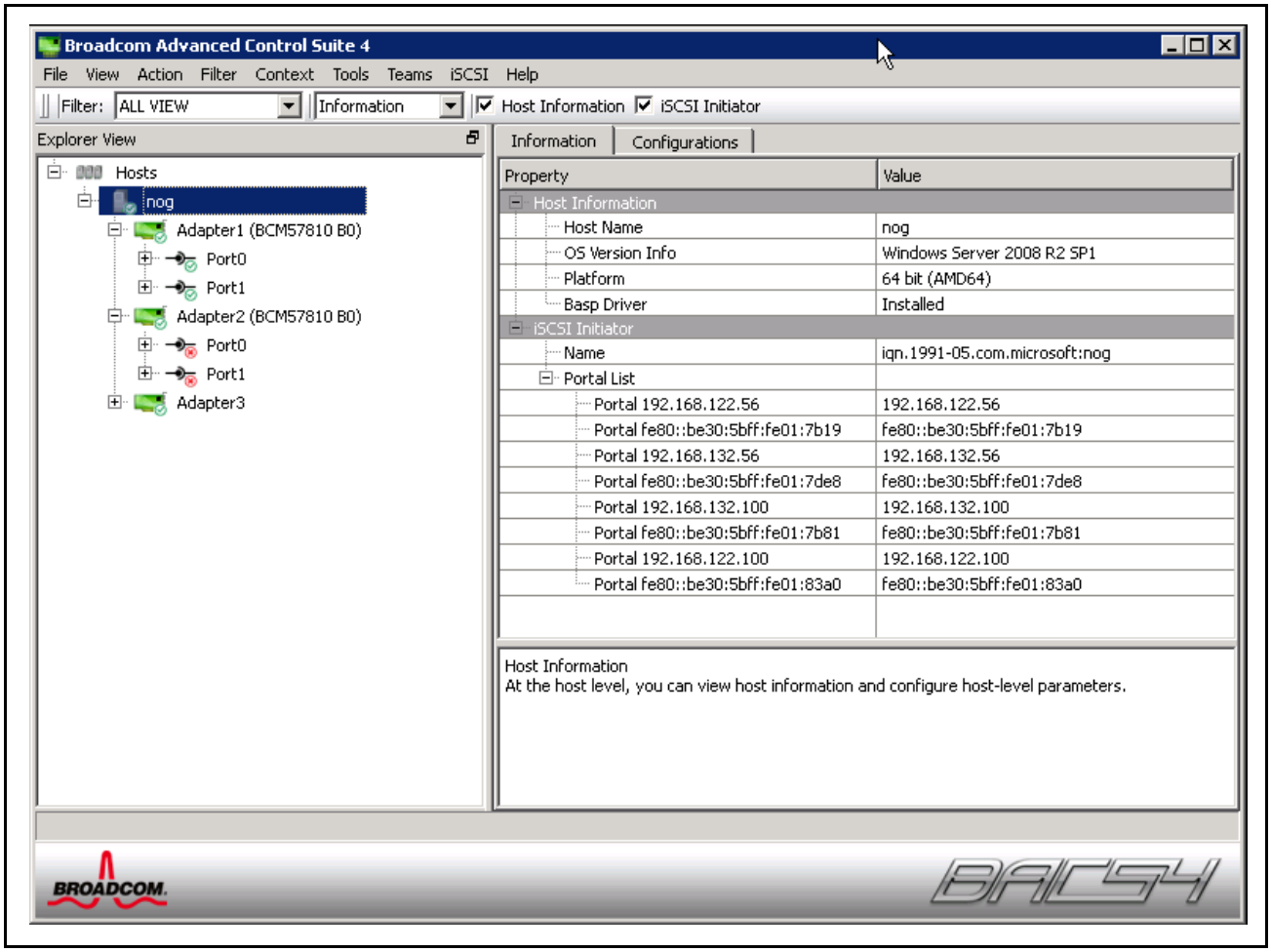


Figure 17: View Host Information

There are two sections on this tab and both displays the following information:

Host Information

Host name: Displays host name of the host.

OS Version Info: Displays the operating system name and version information.

Platform: Displays the hardware architecture platform information (32-bit, 64-bit etc.)

iSCSI Initiator

Name: Displays iSCSI initiator name in the IQN format. This information displayed only if iSCSI driver is installed and enabled.

Portal List: Displays all iSCSI portal IP address configured on the selected host. Both IPv4 and IPv6 portal IP addresses are displayed.

Configuration

Selecting Configuration tab allows user to configure or modify host level parameters. See Figure 18 below for details.

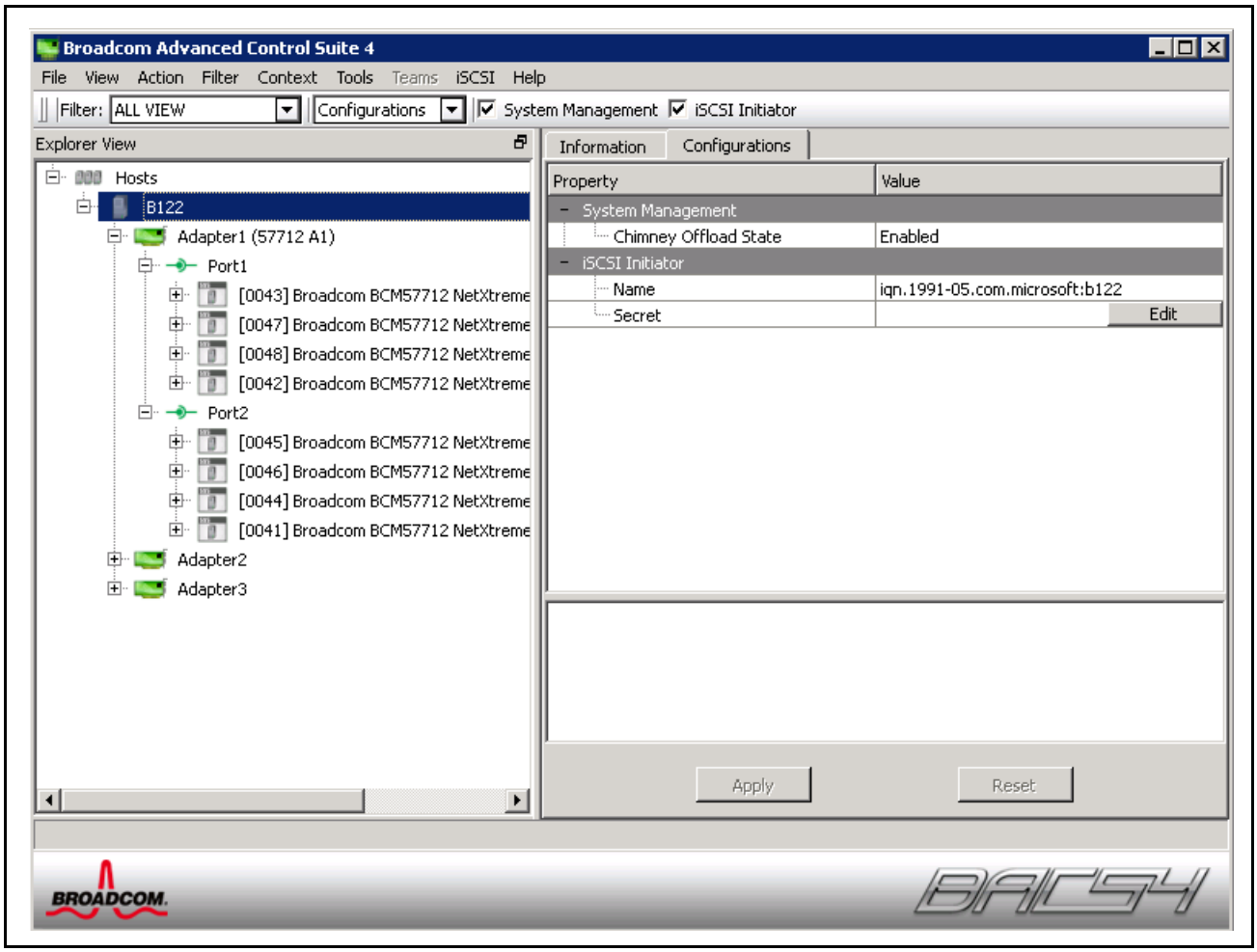


Figure 18: Configure Host information

On this tab, user can configure Chimney offload and iSCSI initiator name in the IQN format.

Chimney Offload State: The current configuration state is displayed under Value column. Click the value column against Chimney Offload State to configure chimney offload at the host level. Available options are **Enable** and **Disable**. After making changes, click **Apply** button for changes to take effect.

Note: The Linux host does not show Chimney Offload State.

iSCSI Initiator Name: The current IQN name is displayed. Click the name to modify the iSCSI initiator name of the host. Clicking on **Apply** button will make the changes as active configuration.

Boot Configuration

The Broadcom CNA supports various boot options – PXE boot, Boot from SAN and Boot from iSCSI target. It also supports some legacy boot options like RPL and BOOTP. Boot configuration can be performed very easily using the BACS4 management application using the user friendly wizard.

1. Start the Boot Configuration wizard as follows:
   a. Select host in the object explorer pane of the BACS4 GUI and then right-click to select **Boot Configurations**.
   b. Select host in the object explorer pane of the BACS4 GUI and then from the menu bar select **Action** > **Boot Configurations**.

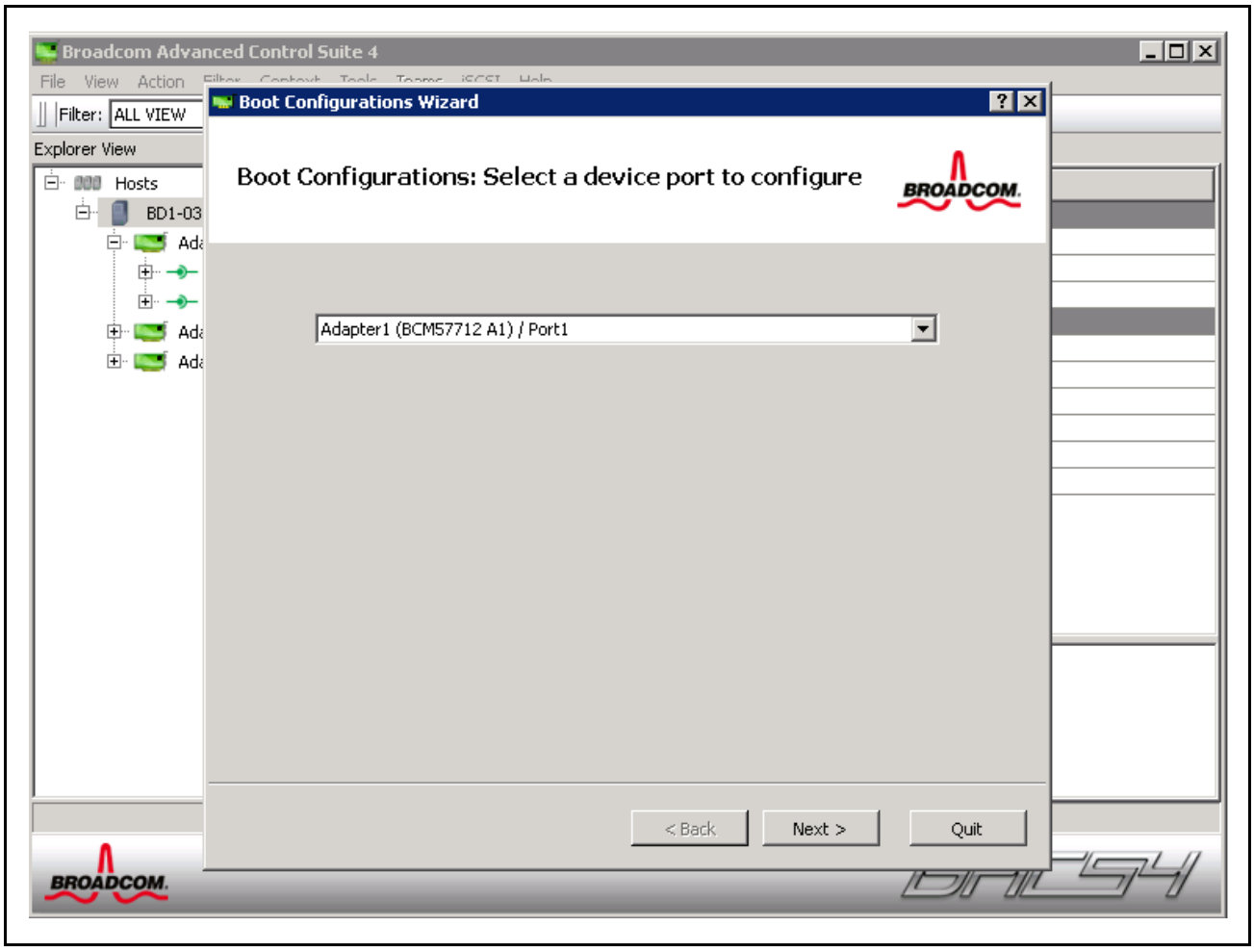


Figure 19: Boot Configuration Wizard

2. Click **Next**.
3. Configure various MBA parameters. The various parameters listed on this screen apply to all boot methods. It also has some parameters which apply to PXE boot protocol.
4. Click **Next**.
5. Select **Yes** if you want to configure FCoE Boot or iSCSI Boot related parameters now. You can start the wizard again and configure these parameters later.
6. Select **Commit all the configurations and exit the wizard** option if you want to save the configuration and then click **Finish** to exit the wizard.
7. Select **Continue to configure another device port** if you want to configure another device.

MBA Boot Parameters

The MBA boot option can be selected for the PXE boot.

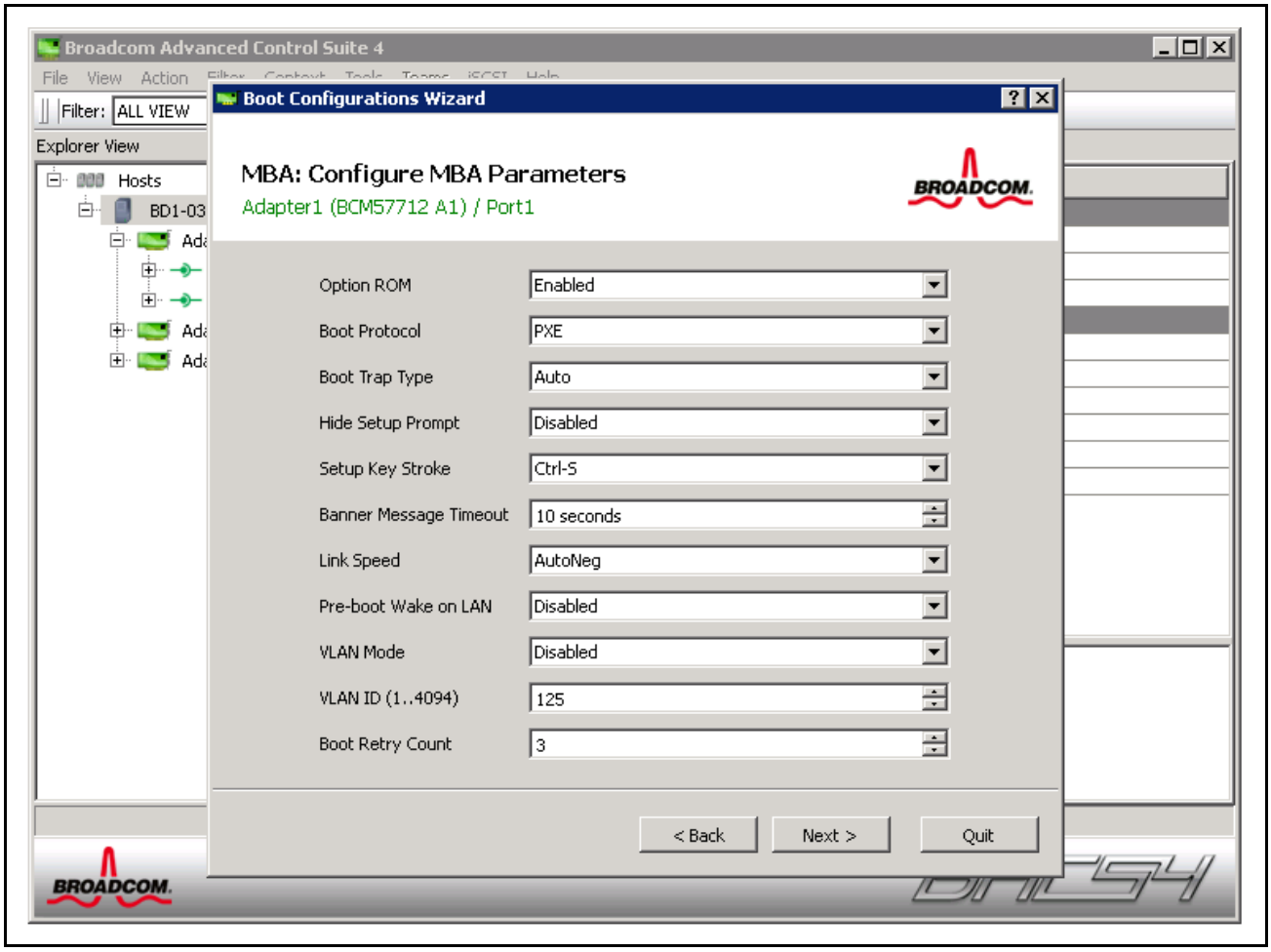


Figure 20: MBA Boot Parameters

Option ROM: Enables or Disables the option ROM. If it is disabled then adapter's boot code will not be used to scan the bootable device.

Boot Protocol: Select appropriate boot protocol. Options include PXE, RPL, BOOTP, iSCSI Boot and FCoE Boot.

Boot Trap Type: Select the appropriate boot trap type. Options include Auto, BBS, INT 18h and INT 19h.

Hide Setup Prompt: Enables or disables the setup prompt displayed when the host is booting. If enabled, it allows user to setup the boot configuration when the host is booting.

Setup Key Stroke: Select one option from Ctrl-S or Ctrl-B. This is useful if another adapter installed in the host is using one of these key combination and you want to configure different setup key stroke.

Banner Message TimeOut: User can configure any value between 0 and 14 seconds. This configures the time for which setup banner will be displayed when the host is booting.

Link Speed: Depending on the type of adapter being configured, available options varies between 100MB, 1Gb and AutoNeg.

The following options apply to PXE, RPL and BOOTP boot protocol.

Preboot Wake on LAN: Enables or disables the WoL option in preboot environment.

VLAN Mode: Enables o disables VLAN tagging during the boot process.

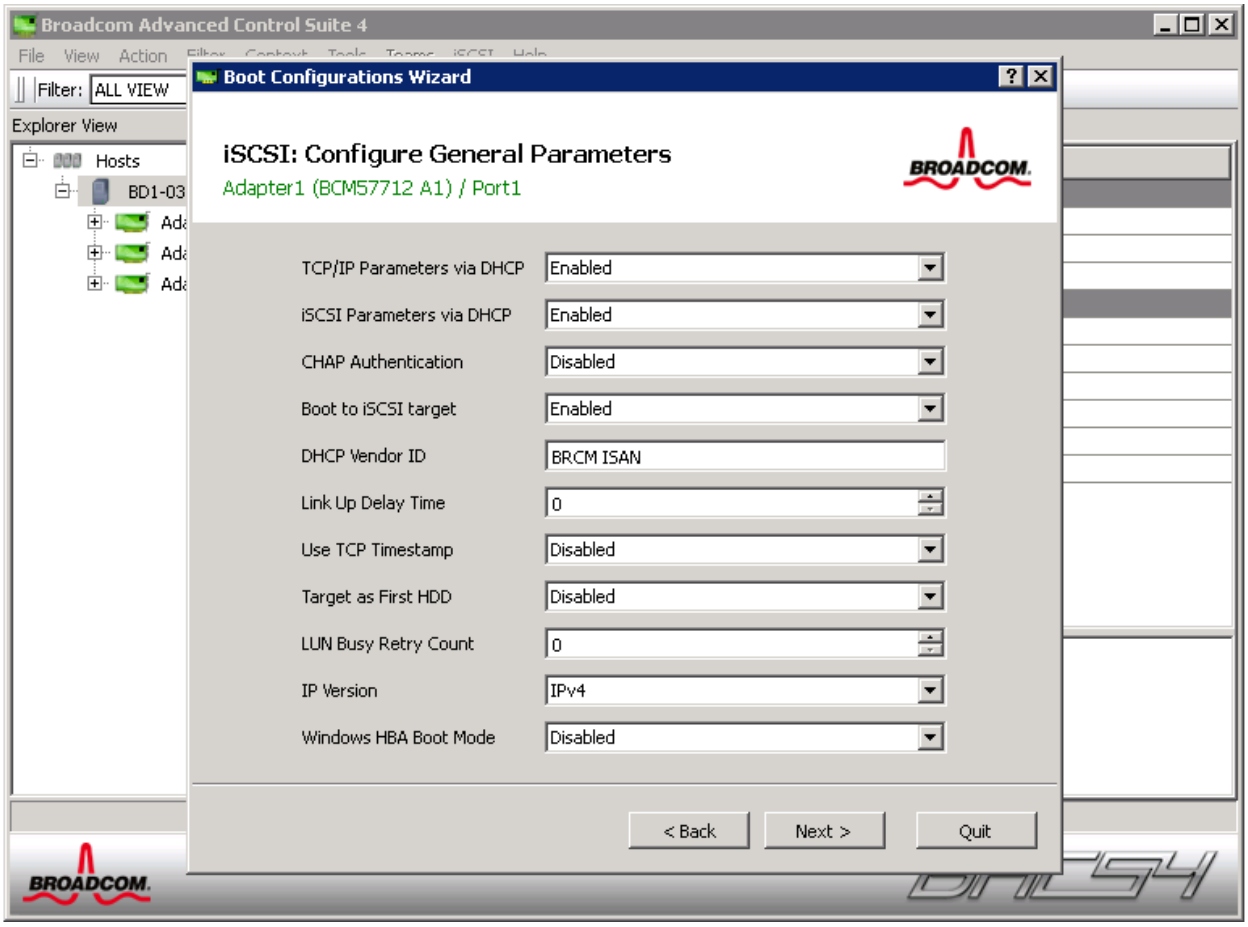
VLAN ID: User can configure any value between 1 and 4094.

Boot Retry Count: This configures number of times boot retry will be performed. Available options are any number between 0 and 7.

iSCSI Boot Parameters

Once the MBA boot parameters are configured and if iSCSI boot was selected as the boot protocol then user can configure the iSCSI boot related parameters by continuing with the MBA wizard and selecting iSCSI Boot Configurations option. Or alternatively the boot wizard can be started again and then selecting iSCSI Boot Configurations option.

1. Start the **iSCSI Boot Configuration** Wizard.



TCP/IP Parameters via DHCP: Determines if the TCP/IP parameters are obtained from DHCP server or not.

iSCSI Parameters via DHCP: Determines if boot related parameters should be obtained from DHCP or not. Refer to the DHCP administration guide to find out which options are supported for the DHCP implementation in your network.

CHAP Authentication: Enables or Disables CHAP authentication during the iSCSI boot. The target must support CHAP authentication and appropriate parameters should be configured on the target.

Boot to iSCSI Target: Available options are: Enabled, Disabled or One Time Disabled.

DHCP Vendor ID: The default vendor ID is BRCM ISAN. The same vendor ID should be configured on the DHCP server if iSCSI boot related parameters are being obtained from the DHCP server.

Link Up Delay Time: Number of seconds for which iSCSI initiator will wait for the target to become online. The number can be any value between 0 and 255 seconds.

Use TCP Timestamp: Enables or disable TCP time stamping.

Target as First HDD: Enables or disable configuring iSCSI target as first HDD device when the host is booting.

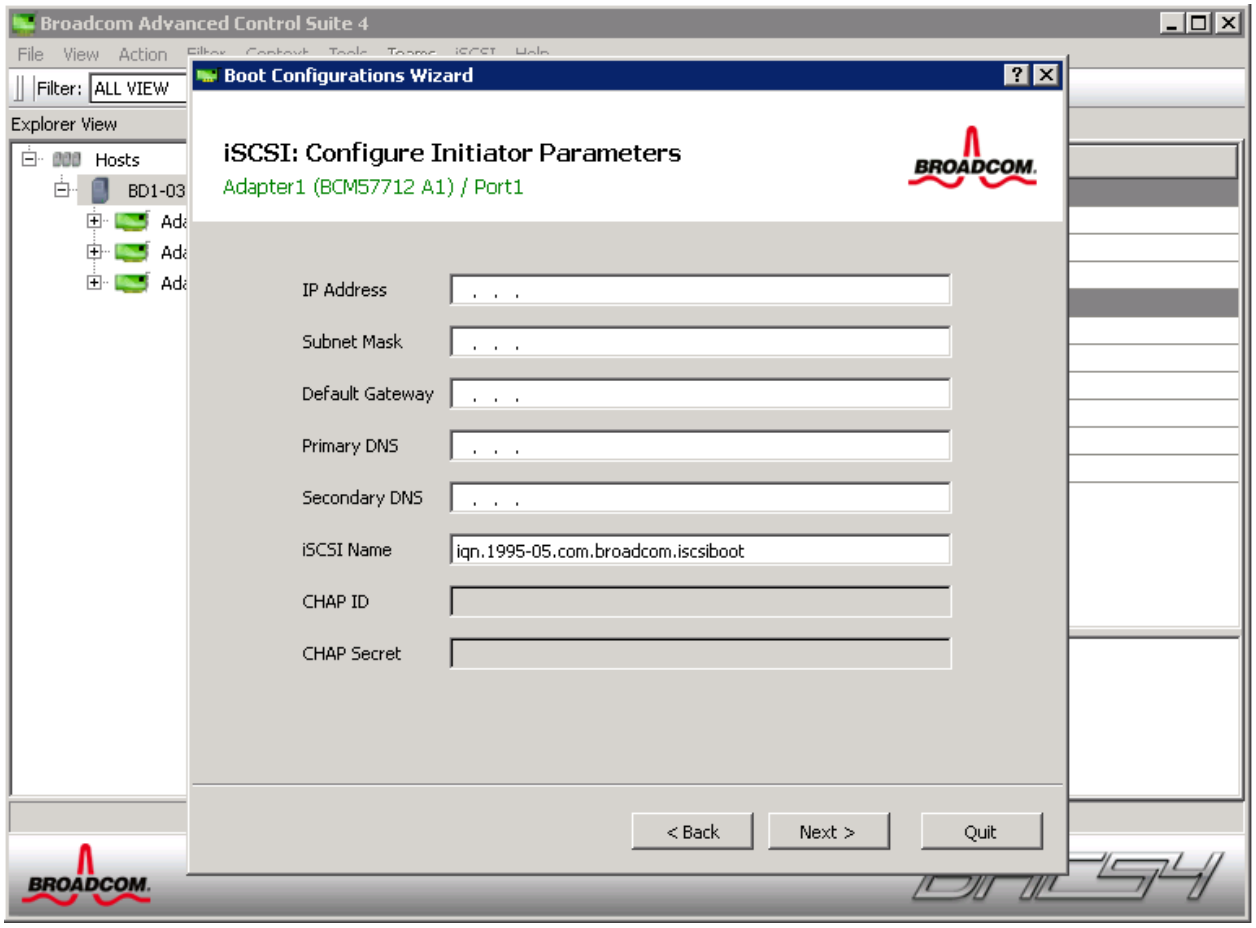
LUN Busy Retry Count: Number of times initiator will try booting from LUN when the LUN busy is returned by the iSCSI target. Number can be any value between 0 and 60.

IP Version: Configures IPv4 or IPv6 as the IP version.

Windows HBA Boot Mode: Enables or disables windows HBA boot mode.

2. Click **Next**.

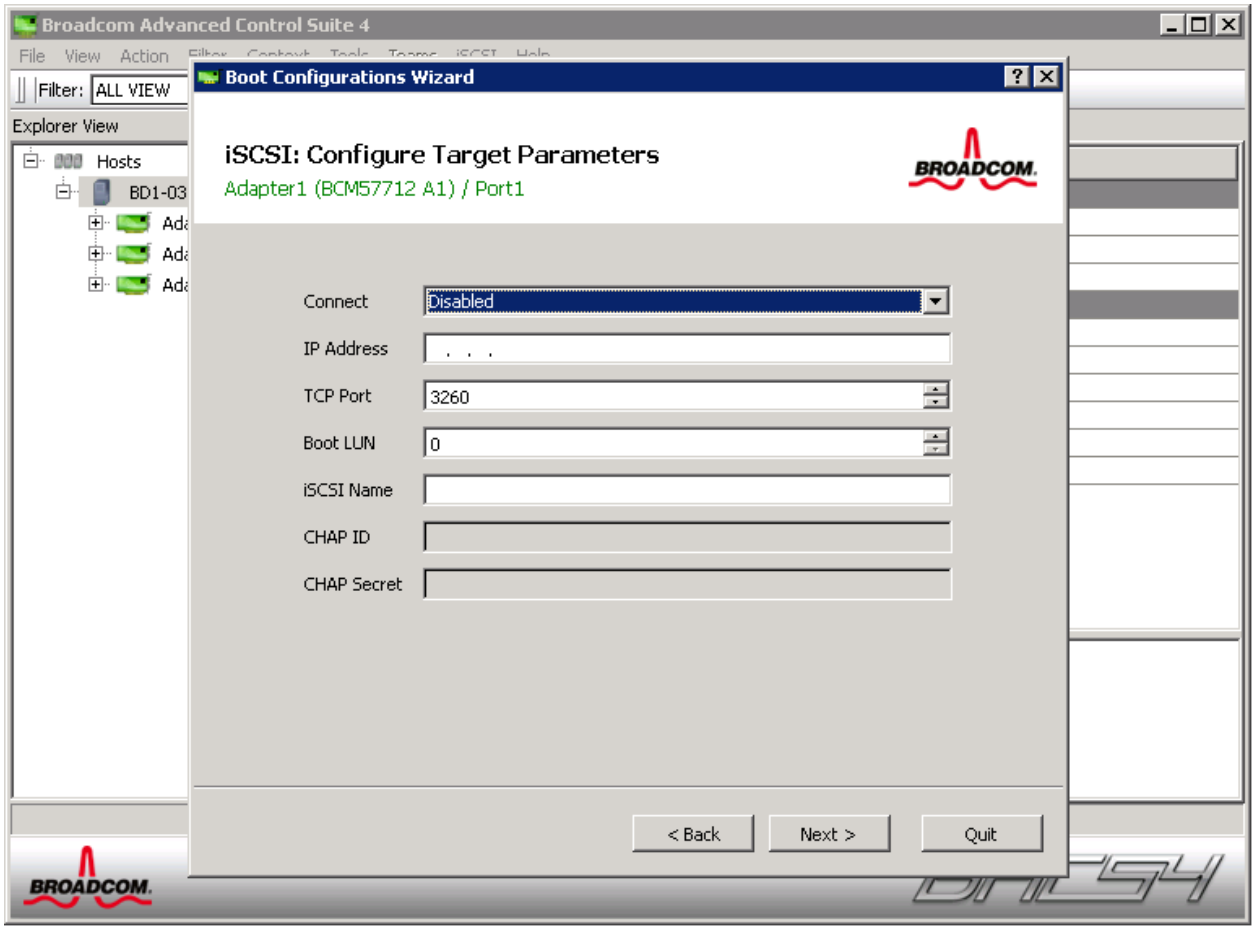
   On the next screen, initiator parameters can be configured.



Configure IP address, subnet mask, default gateway, DNS IP address, iSCSI name, CHAP ID and CHAP secret on this screen. Some options are enabled or disabled depending on the options selected on the previous screen.

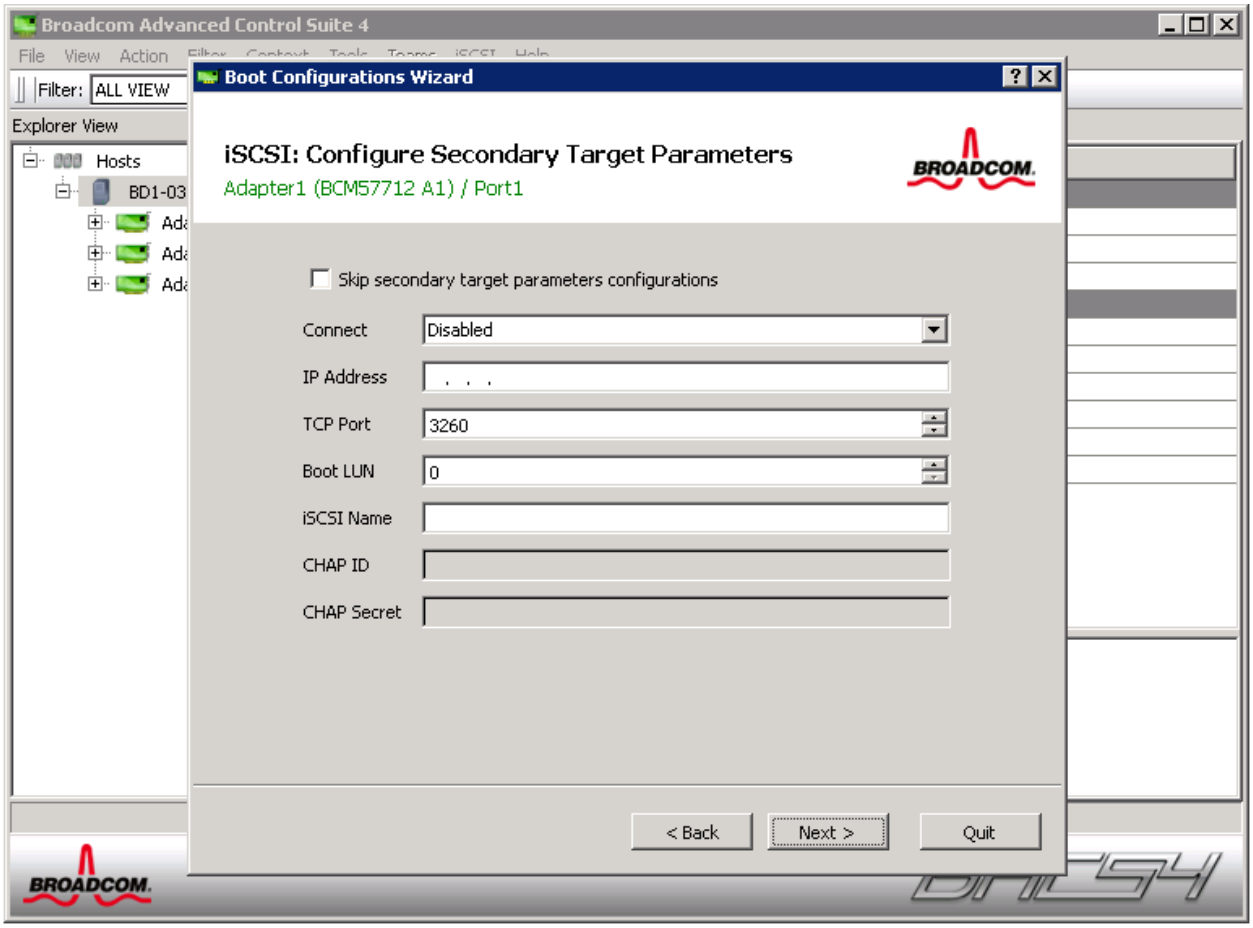
3. Click **Next**.

   On the next screen target parameters can be configured.



The parameters that can be configured on this screen are IP address, TCP port to be used, Boot LUN number, iSCSI name o the target, CHAP ID and CHAP secret. Some options are enabled or disabled depending on the options selected on the previous screen.

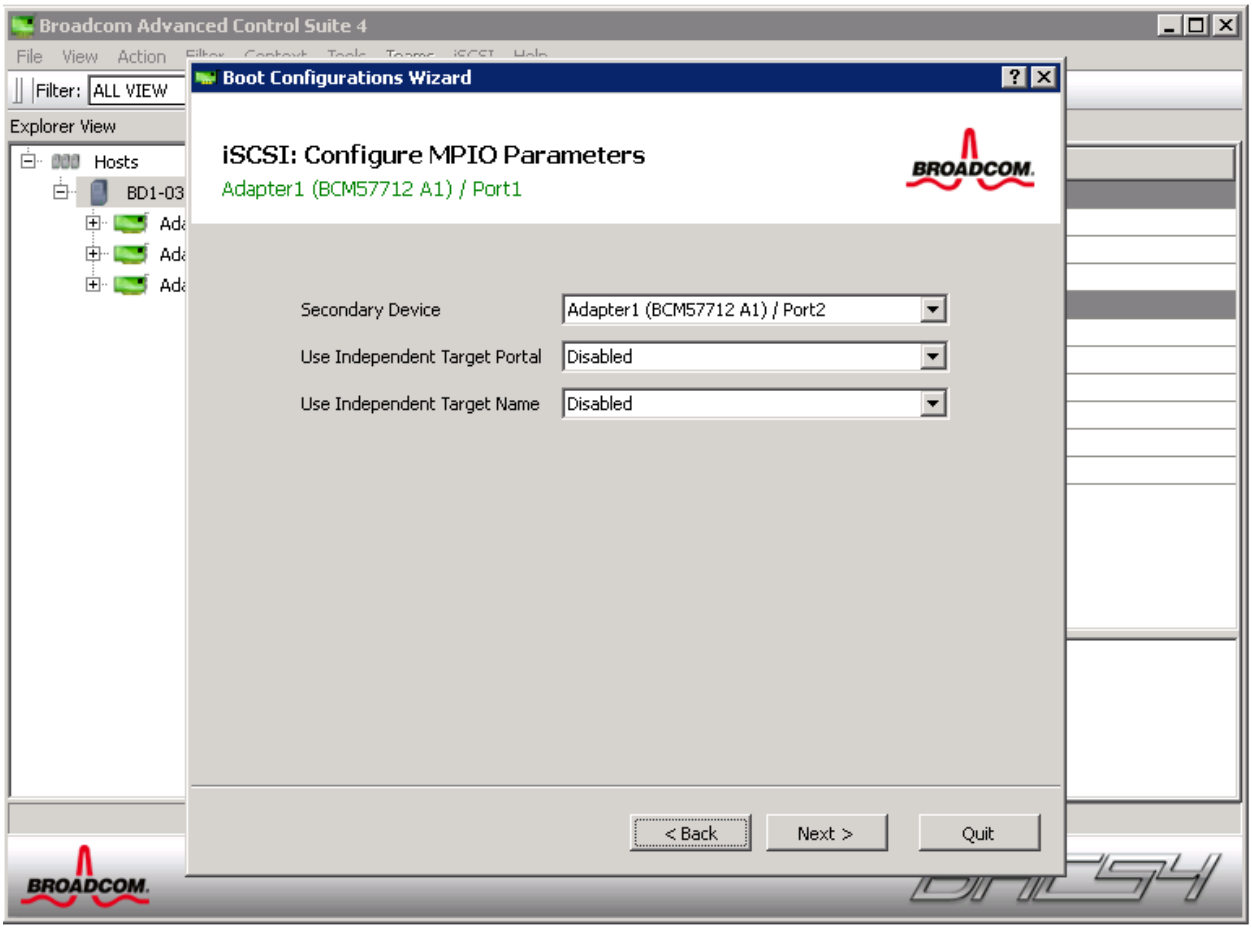
On the next screen, secondary target parameters can be configured.



You can skip the configuration by selecting **Skip secondary target parameters configurations** and then clicking on **Next**.

4. Click **Next**.

   The next screen allows users to configure MPIO parameters.



The available options to be configured are as follows:

Secondary Device: Allows user to select secondary adapter port to be configured in case the first port fails to access the boot device.

Use Independent target Portal: Enables or disable the option of using independent target portal for the secondary boot port.

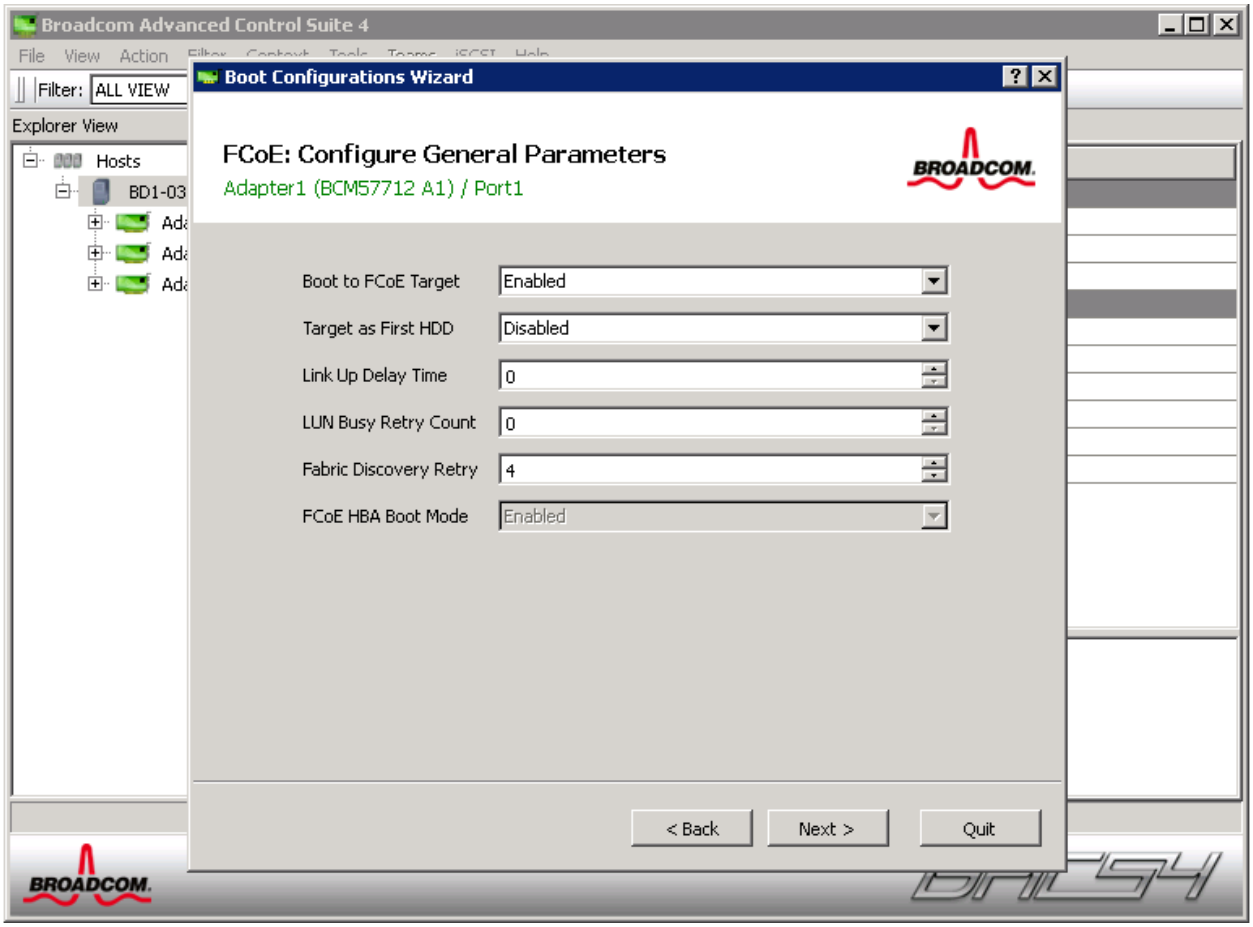
Use Independent target Name: Enables or disable the option of using independent target name for the secondary boot port.

5. Do one of the following:
   - Select **Yes** to do another configuration on the current device.
   - Select **No** and then click **Next**.
6. Select **Commit all the configurations and exit the wizard** option if you want to save the configuration and then click **Finish** to exit the wizard.
7. Select **Continue to configure another device port** if you want to configure another device.

FCoE Boot Parameters

Once the MBA boot parameters are configured and if FCoE boot was selected as the boot protocol then user can configure the FCoE boot related parameters by continuing with the MBA wizard and selecting **FCoE Boot Configurations** option. Or alternatively the boot wizard can be started again and then selecting **FCoE Boot Configurations** option.

1. Start the **FCoE Boot Configuration** Wizard.



Boot to FCoE Target: Enables or disable booting to the FCoE target.

Target as First HDD: Enables or disable configuring iSCSI target as first HDD device when the host is booting.

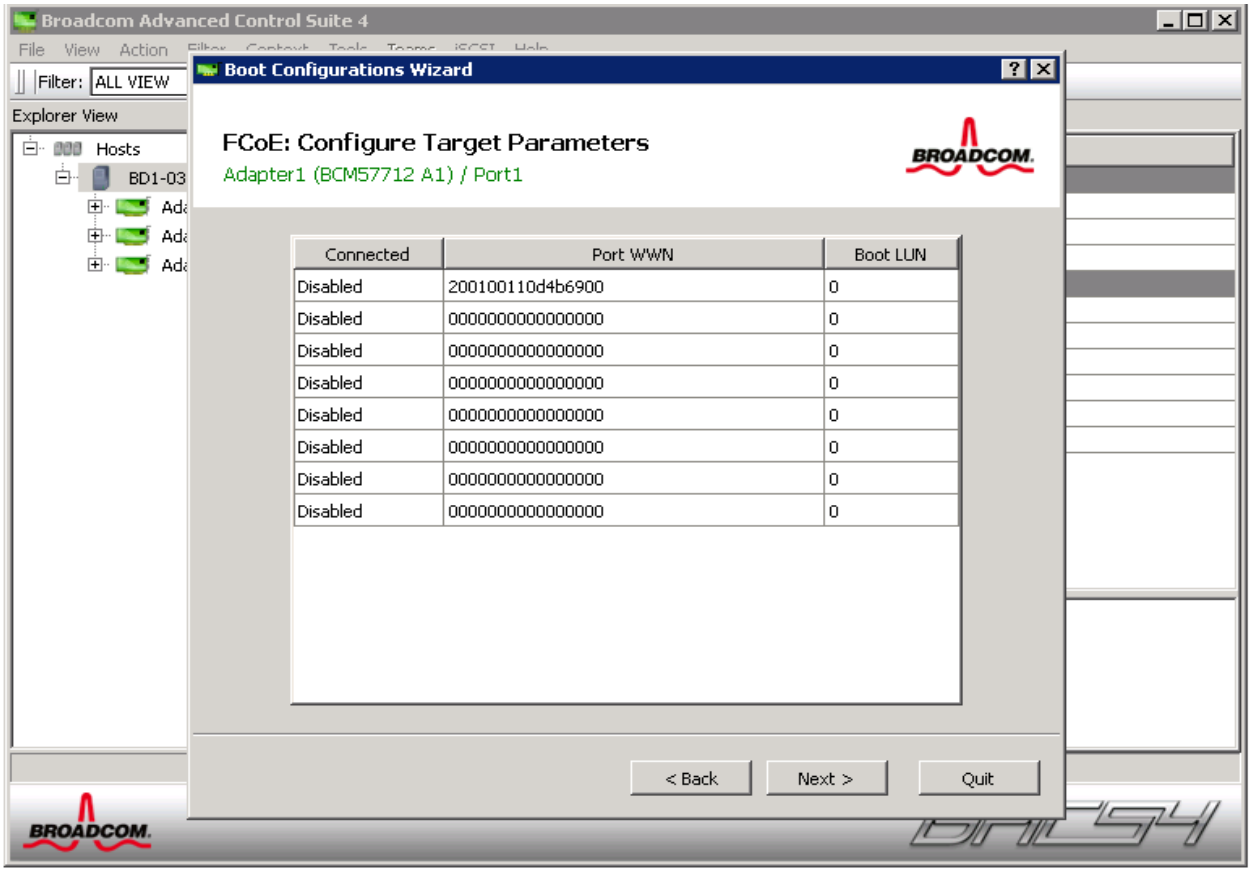
Link Up Delay Time: Number of seconds for which iSCSI initiator will wait for the target to become online. The number can be any value between 0 and 255 seconds.

LUN Busy Retry Count: Number of times initiator will try booting from LUN when the LUN busy is returned by the iSCSI target. Number can be any value between 0 and 60.

Fabric Discovery Retry: Number of times initiator will try booting from the FCoE target when the adapter port link is down.

FCoE HBA Boot Mode: Enables or disables FCoE HBA boot mode.

2. Click **Next**.



3. On the next screen, configure Port WWN and boot LUN information for all boot devices from which initiator can boot.
4. Select **Yes** if you want to Continue with another configure for the current device.
5. Or select No and then click **Next**.
6. Select **Commit all the configurations and exit the wizard** option if you want to save the configuration and then click **Finish** to exit the wizard.
7. Select **Continue to configure another device port** if you want to configure another device.

Adapter Information

The next level of device after Host in hierarchical tree in the Object Explorer window is Adapter. All installed adapters will be displayed under the connected host. The "**+**" icon near the adapter allows user to collapse or expand the tree at the adapter level.

Once the adapter is selected in the Object Explorer window, user can view information about the adapter and make adapter level changes. There are two tabs displayed in Context View pane once the adapter is selected. They are:

- Information
- Configuration (available only if NIC Partitioning is configured and enabled)

View Information

The information tab displays adapter level information like adapter hardware details and bus type. See Figure 21 for the screenshot.

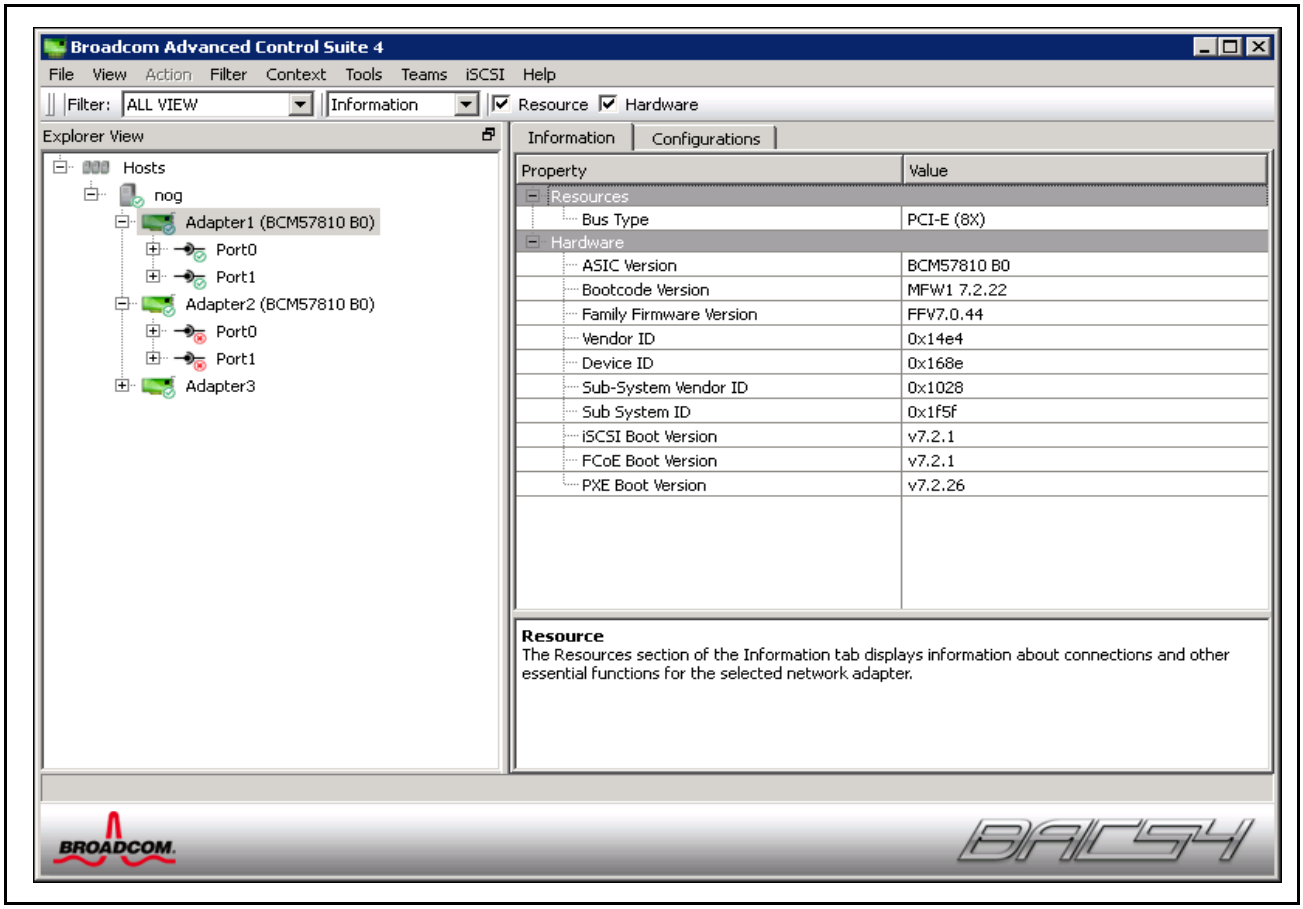


Figure 21: Adapter Information

The following give details of the information available at the adapter level.

Hardware

ASIC Version: This filed displays the model number and version number of the main chipset used in the adapter.

Bootcode Version: Displays the adapter bootcode version (not to be confused with FCoE bootcode, iSCSI bootcode and L2 bootcode version).

Family Firmware Version: Displays the firmware version of the chipset. This firmware version should not be confused with EVBD firmware version.

Vendor ID: Displays vendor ID of the adapter.

Device ID: Displays device ID of the adapter.

Sub-system Vendor ID: Displays sub-system vendor ID of the adapter.

Sub System ID: Displays sub system ID of the adapter.

iSCSI Boot Version, FCoE Boot Version, PXE Boot Version: Displays various boot code versions.

Resources

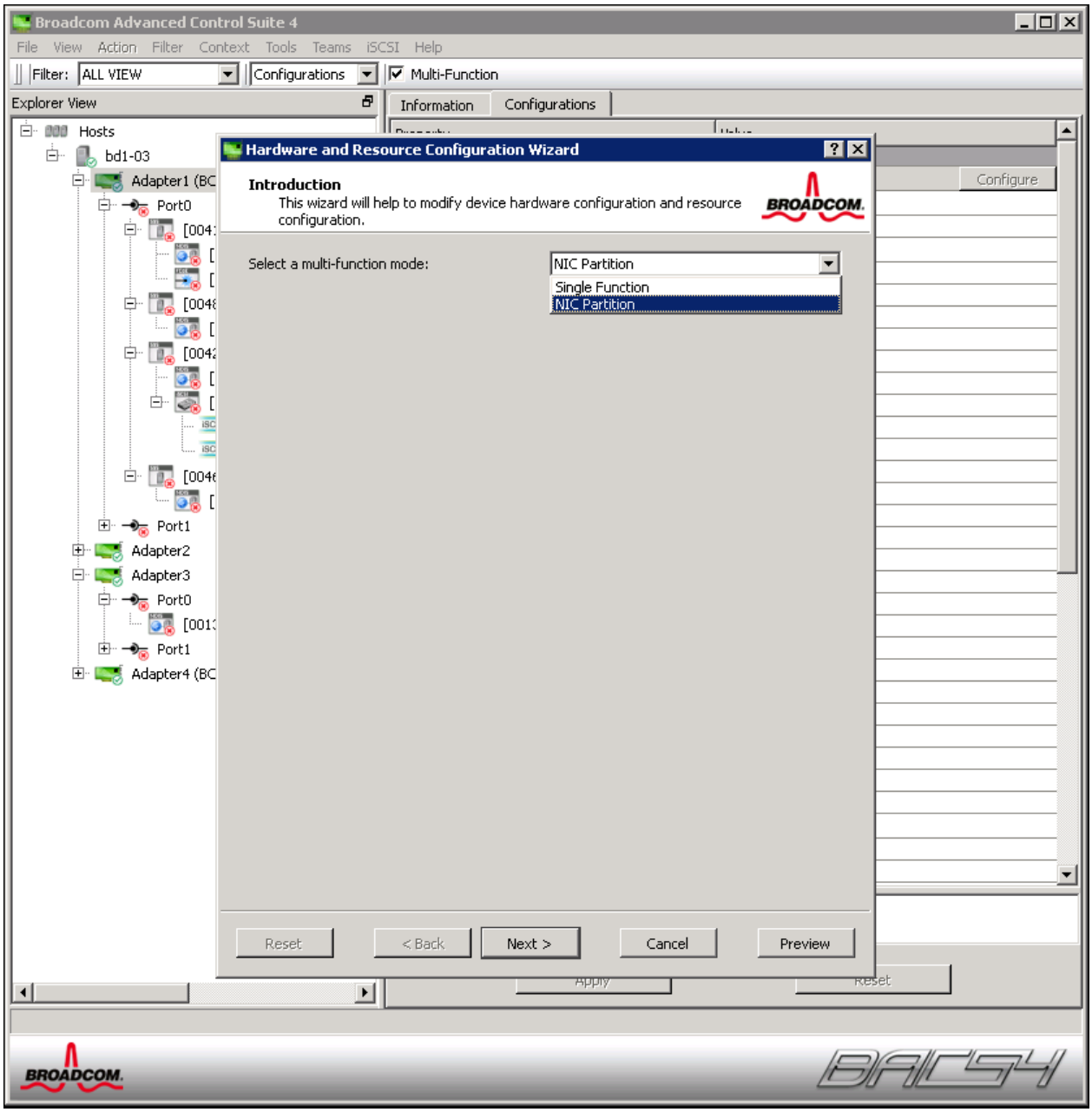
Bus Type: Displays bus type and speed where the adapter is installed. The speed of the bus shown is the negotiated value.

Configuration

The configuration tab allows user to modify adapter level configuration including enabling/disabling NIC Partitioning (NPAR).

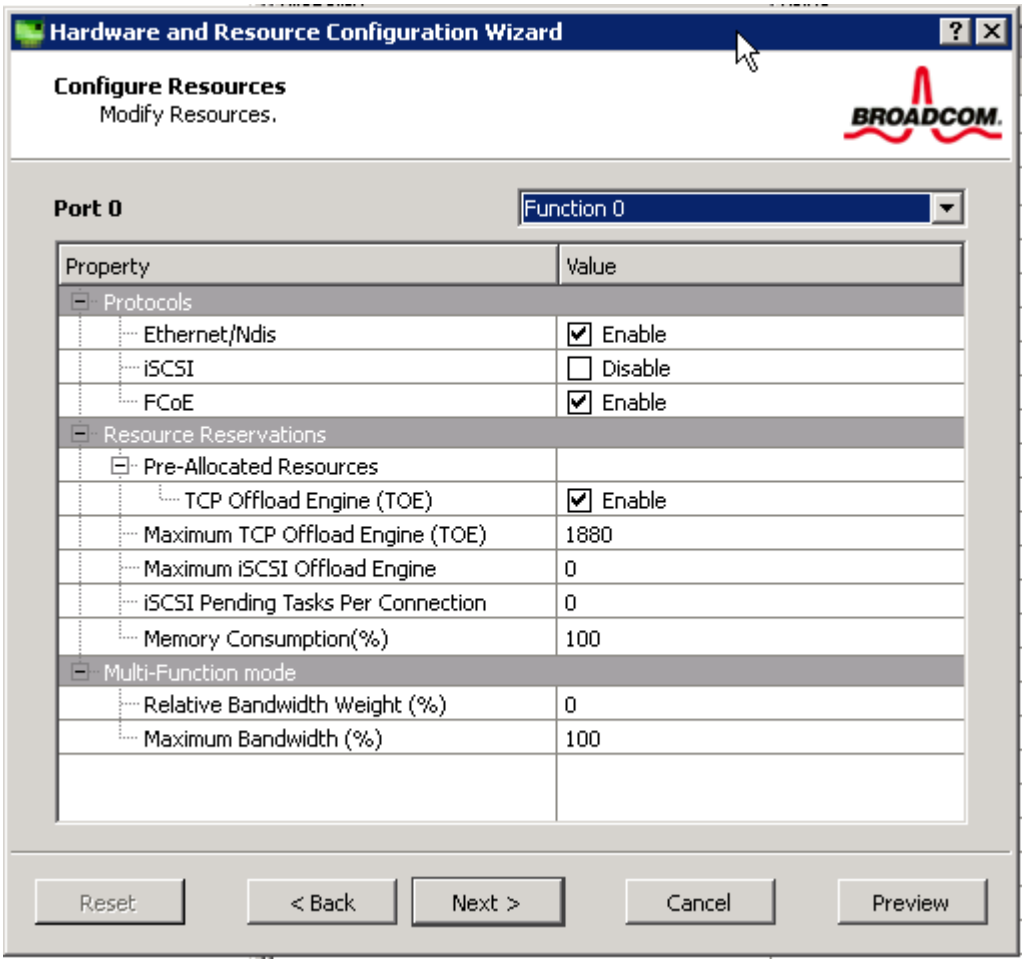
Enable/Disable NIC Partitioning (NPAR)

1. Click the “Adapter” label in the device tree.
2. Select **Configuration** tab.
3. Click **Configure** button.
4. From the drop down menu, select **NIC Partition** to enable the NIC Partitioning and click **Next**.
   This will open the wizard.
5. Select the port that needs to be configured and click **Next**. From this screen the **Flow Control** can be configured for the select port before you click **Next**.
   Flow Control: The possible values are Auto, TX Pause, RX Pause, TX/RX pause and Disable. The configuration done at the port level applies to all functions under that port. The value of the flow control is a default value for the port and the effective configuration can be different based on switch port configuration and whether DCB/DCBX is enabled or not.



See the next figure for the screenshot when the NIC Partitioning (NPAR) is enabled on the adapter.

6. Select the appropriate function.



The following properties are configurable at the function level. As stated earlier, there are four functions created under each port when the NIC Partitioning is enabled. The functions are numbered from 0 to 7. All odd function numbers (1,3,5,7) are created on one port and all even functions (0,2,4,6) are created on the remaining port.

Ethernet/NDIS: The check box (Enable/Disable) is not selected by default. That means Ethernet/NDIS capability is disabled for that function. Selecting this check box will enable the Ethernet/NDIS driver.

iSCSI: The check box (Enable/Disable) is not selected by default. That means iSCSI functionality/capability is disabled for that function. Selecting this check box will enable the iSCSI functionality.

FCoE: The check box (Enable/Disable) is not selected by default. That means FCoE functionality/capability is disabled for that function. Selecting this check box will enable the FCoE functionality.

Maximum Bandwidth: The possible value is from 0 to 100. The value is percentage of the maximum link speed allowed for that particular function. This feature configures a maximum bandwidth that particular function can use. For example, if 50 is configured as Maximum Bandwidth then it will restrict the bandwidth usage of the function to 50% of the 10Gbps or in other words to 5 Gbps.

Relative Bandwidth: The possible value is from 0 to 100. This parameter is applicable only when the ETS is disabled on the adapter port. This value defines the weight assigned to the function when the ETS is disabled and all functions are trying to transmit at the maximum link speed. It should not be confused with the percentage of the link speed like Maximum Bandwidth parameter. In case of congestion, the weight value will determine how much importance will be given by transmit scheduler to the traffic emanating from this function.

Under Resource Reservation, the following properties can be configured.

TOE: Enable/Disable TCP Offload Engine.

Maximum TCP Offload Engine and Maximum iSCSI Offload Engine: Number of maximum TOE and iSCSI offloaded connections for the function.

iSCSI Pending Tasks Per Connection: Number of maximum pending tasks that are allowed for the function selected.

Memory Consumption (%): Maximum memory consumption allowed for the function in terms of percentage.

Note: On Linux managed host, after selecting function, only the following parameters are available for modification.

L2NIC: The check box (Enable/Disable) is selected by default. Deselecting this check box will disable the Ethernet function

iSCSI: The check box (Enable/Disable) is not selected by default. That means iSCSI functionality/capability is disabled for that function. Selecting this check box will enable the iSCSI functionality.

FCoE: The check box (Enable/Disable) is not selected by default. That means FCoE functionality/capability is disabled for that function. Selecting this check box will enable the FCoE functionality.

Maximum Bandwidth: The possible value is from 0 to 100. The value is percentage of the maximum link speed allowed for that particular function. This feature configures a maximum bandwidth that particular function can use. For example, if 50 is configured as Maximum Bandwidth then it will restrict the bandwidth usage of the function to 50% of the 10Gbps or in other words to 5 Gbps.

7. Click **Next**.
8. Select another port or another function on the same port and click **Next** to configure it.
9. Alternatively, click **Apply** and exit the wizard.
10. Click **Cancel** to cancel all the configurations done in wizard earlier.
11. Click **Preview** allows user to view the configuration for all ports and functions on the adapter before applying it.

Note: The configuration of various functionality/capability is governed by the following rule.

- On one adapter port, maximum of two protocol offload can be configured.
- On a function, only one protocol offload can be configured (FCoE or iSCSI).
- The Ethernet can coexist with any protocol offload.

Valid configuration:

- Function 1: Eth, Function 2: FCoE, Function 3: iSCSI, Function 4: Eth
- Function 1: Eth + iSCSI, Function 2: FCoE, Function 3: Eth, Function 4: Eth
- Function 1: Eth + iSCSI, Function 2: Eth + FCoE, Function 3: Eth, Function 4: Eth

Invalid configuration:

- Function 1: Eth, Function 2: FCoE, Function 3: iSCSI, Function 4: FCoE
- Function 1: Eth + iSCSI, Function 2: FCoE + iSCSI, Function 3: Eth, Function 4: Eth

In the above example of invalid configurations:

- The first example is invalid because there are more than two offload protocols per port.
- The second example is invalid because there are two protocol offload on the same function.

Managing Ethernet Controller (Port)

Before we go in to details of managing Ethernet controller (Port object in Object Explorer), some level of DCBX knowledge will be helpful.

DCB/DCBX

Introduction

The Data Center Bridging Exchange Protocol is defined in 8021.Qaz specification. The DCBX defines the way in which peer exchange capability and configuration related information in converged network. With the help of DCBX protocol, the peer can detect the mismatch in the DCBX related configuration of its peer. The information unit in DCBX protocol is TLV (Time, Length, and Value) which are transmitted within LLDP frames. The DCBX database consists of three parts – Administrative Default parameters (default parameters configured on the local peer), Remote parameters (parameters configured on the remote peer) and Local parameters (operational state of the parameter on the local peer). Currently, all the parameters being exchanged with the peer can be divided in three categories: PFC TLV (Priority Flow Control), Priority Group TLV (for ETS - Enhanced Transmission Scheduling) and Application TLV.

Priority Flow Control (PFC)

Traditional IEEE 802.3 Ethernet defines an unreliable communication medium; it does not offer guarantees that a packet transmitted on the network will reach its intended destination. Upper level protocols are responsible to maintain the reliability by way of acknowledgement and retransmission.

In a network with multiple hopes, it becomes very difficult to maintain the reliability in absence of some type of feedback. In some situation, it is possible that transmitter transmit packets at faster rate than the receiver. The receiver will start dropping packets as its buffers runs out of the space. The receiver will start dropping packets without any notification to the transmitter. This is traditionally tackled with the help of Link Level Flow Control. The receiver sends Pause to the transmitter and all type of traffic will stop until the pause is cancelled. In the converged network environment, this will pose a problem since multiple types of traffic are running on

the wire. The priority flow control provides the solution. Each traffic type can be individually stopped and started using the priority field in the VLAN tag. Each traffic types can be encoded with different priority value and pause frame can refer this priority value while instructing transmitter to stop and restart the traffic. The value range for the priority field is from 0 to7 allowing eight distinct types of traffic that can be individually stopped and started. Broadcom Converged Network Adapters are fully compliant with the Priority Flow Control specification IEEE 802.1Qbb.

Enhanced Transmission Selection (ETS)

We saw earlier that PFC can create eight distinct virtual links and it can be used to define different traffic classes. This still cannot guarantee particular bandwidth to the desired traffic class. The ETS provides the prioritized processing based on the bandwidth allocation. Each traffic class or priority can be grouped in a Priority Group (PG) and it can be considered as virtual link or virtual interface queue. The transmission scheduler in the peer is responsible to maintain the allocated bandwidth for each priority Group. For example, user can configure FCoE traffic to be in a PG 0 and iSCSI traffic in a PG 1. User can then allocate each group a certain bandwidth – 60% to PG 0 and 40% to iSCSI, for example. The transmission scheduler in the peer will ensure that in the event of congestion, the FCoE traffic will be able to use at least 60% of the link bandwidth and iSCSI 40%.

The BACS4 GUI makes it very easy for users to group various traffic classes in to priority group and allocate bandwidth to each priority group.

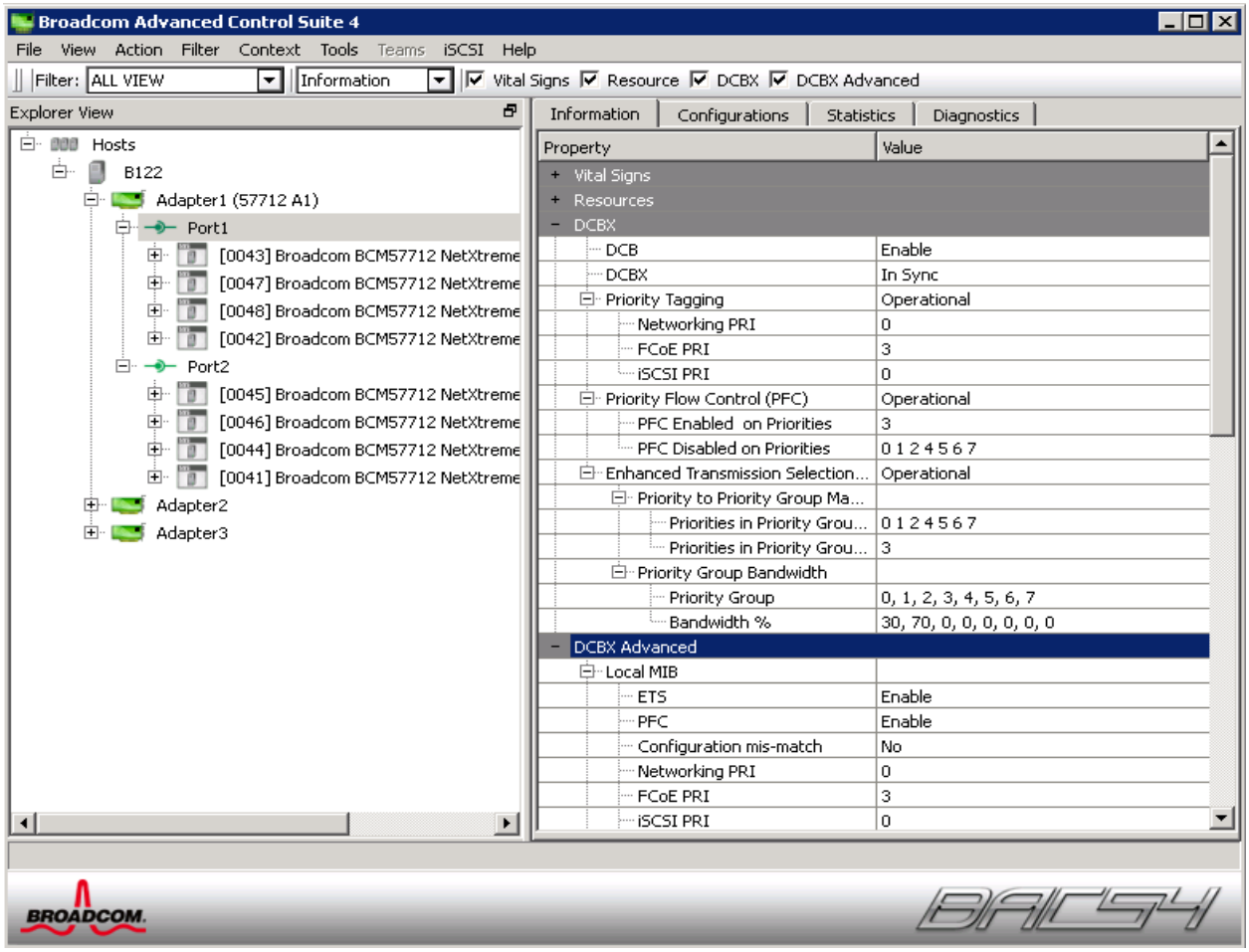
When the Ethernet controller is selected in the Object Explorer panel, the following four tabs will be displayed in the context view panel:

- Information Tab
- Configuration tab
- Statistics Tab
- Diagnostic Tab

View Port Level Information

Selecting Ethernet controller in the object explorer will allow user to view various types of information at the port level.

1. Select **PortX** (where X is either 0 or 1) below **Adapter** in the object explorer.
2. Various components of the port will be displayed below port in the object explorer. You can click the "**+**" icon near Port to expand or collapse the tree below.
3. Select the **Information** tab in the context view panel on the right side.



The information is decided in three categories as below.

DCBX

This category lists DCBX related information. The information being displayed under this section is a current operation state of various DCBX related parameters. The information is grouped as follows:

DCB: Displays if DCB is enabled or disabled. If the DCB is disabled then PFC and ETS doe not take effect.

DCBX: Displays if DCBX is in sync with its peer (switch).

Priority Tagging: Displays if the priority tagging is enabled or disabled. IUt also displays the priority tag values for FCoE, iSCSI and L2/TOE traffic.

Priority Flow Control: Displays if the PFC is operational or not. Also displays which class of traffic is using PFC.

Enhanced Transmission Selection: Displays if ETS is operation or not. Also displays priority to priority group (PG) mapping and bandwidth (in terms of percentage of the total link bandwidth) assigned to each priority group.

DCBX

This category lists some advanced DCBX related information. The information is grouped under two major sections – Local MIB and Remote MIB. The parameters displayed under each section are roughly the same as mentioned in "DCBX" on page 85.

The Local MIB parameters are the default parameters configured on the adapter port. The values mentioned in this section take effect if the DCB is enabled on the adapter but the DCBX sync fails between adapter port and the switch.

The Remote MIB parameters are the DCB parameters configured on the remote peer (switch) port.

Resource

This section lists various resource related parameters as listed below.

- Bus number: The PCI bus number for the selected physical port.
- Device Number: The PCI device number for the selected port.
- Function Number: The PCI function number for the selected port.
- MSI version: The MSI version number for the selected port.
- Function per port: The current number of virtual functions crated on the port. This number is always "4" if NIC Partitioning is enabled and configured on the adapter.
- Memory Address: The memory address being used by the port in the host memory.
- Duplex settings: The duplex setting for the physical port.
- Media Type: The connector medium for the physical port.

Vital Signs

This section lists important vital signs and its state to give a quick status of the port to the user.

- Link State: Indicates if the link on the port is Up or Down.
- Link Speed: States the current link speed of the port in Mbps. For Converged Network Adapter, the value is always 10000.

Configure Port Level Information

This section will describe various parameters that can be configured at the port level. The primary configuration that can be performed at the port level involves configuring DCBX related parameters. Many DCX related parameters are dependent on each other and so the configuration needs to be done with utmost care. Some parameters cannot be configured independently. To make this process very easy, BACS4 uses wizard style method for DCBX configuration. Some parameters can be independently configured.

To understand the configuration process, it is important to define various configuration states for the adapter. Let us examine those one by one.

DCB Enabled and DCBX enabled

The default configuration for the port is as shown on Figure 22 and described below.

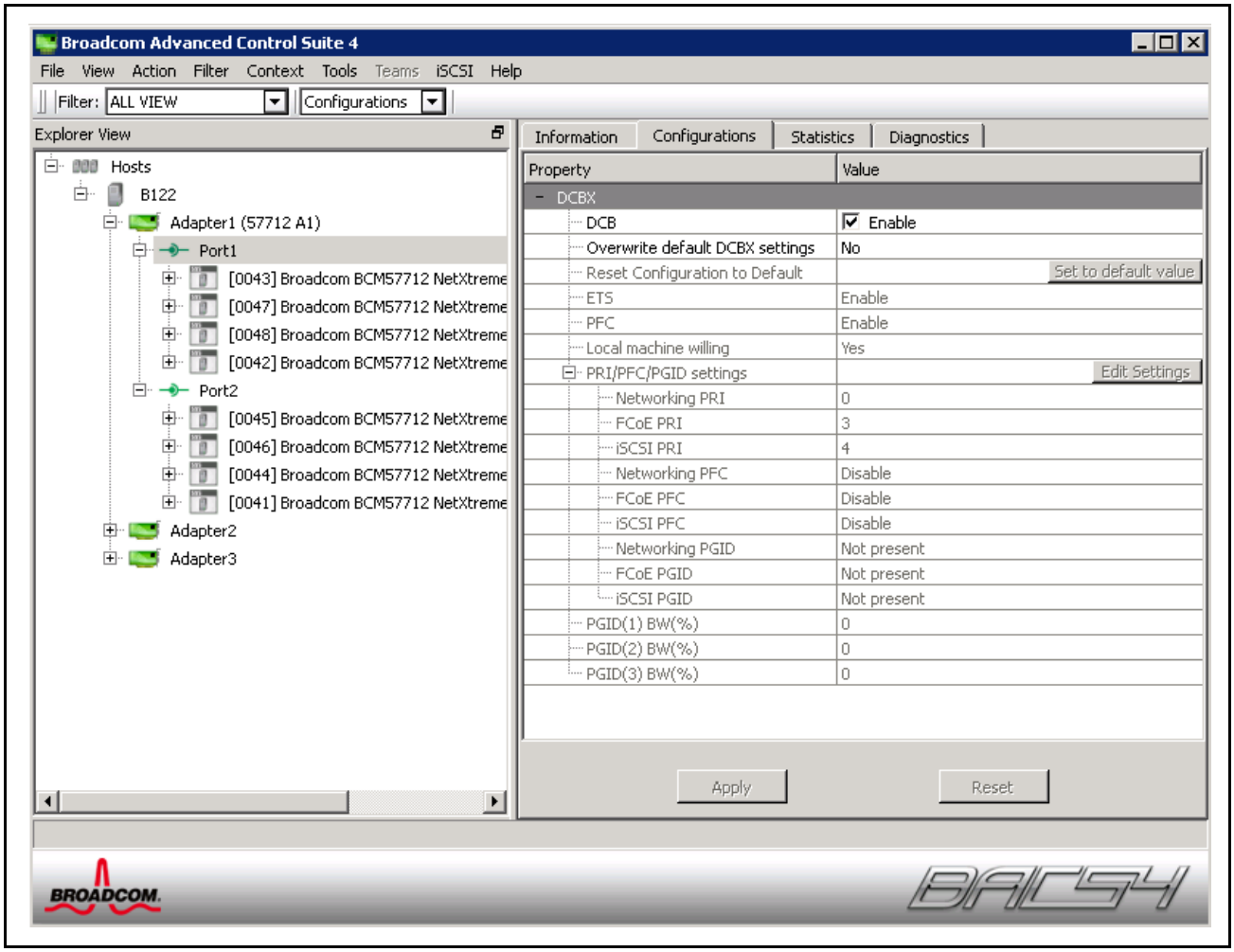


Figure 22: Configure Port

The default setting has DCB and DCBX enabled on the port. The Overwrite default DCBX Settings is configured as 'No'. This ensures that adapter's default DCBX configuration saved in the NVRAM is considered as Administrative parameter (see "Introduction" on page 83 for details).

With DCB enabled, the adapter has PFC and ETS capability enabled. With DCBX enabled, the adapter will "negotiate" various DCBX parameters with its peer. The adapter's default configuration is 'willing'. That means, adapter will accept the DCBX parameter values from its peer and configure itself accordingly. At the end of the negotiation, adapter's Local Parameters will be a copy of the Remote Parameters.

This is the most common configuration and satisfies most customers' need. The entire DCB/DCBX related configuration is performed at the switch level and adapter accepts the DCBX setting (PFC, ETS etc.) from switch. The management is simplified with this approach.

DCB and DCBX Enabled with Nondefault Settings

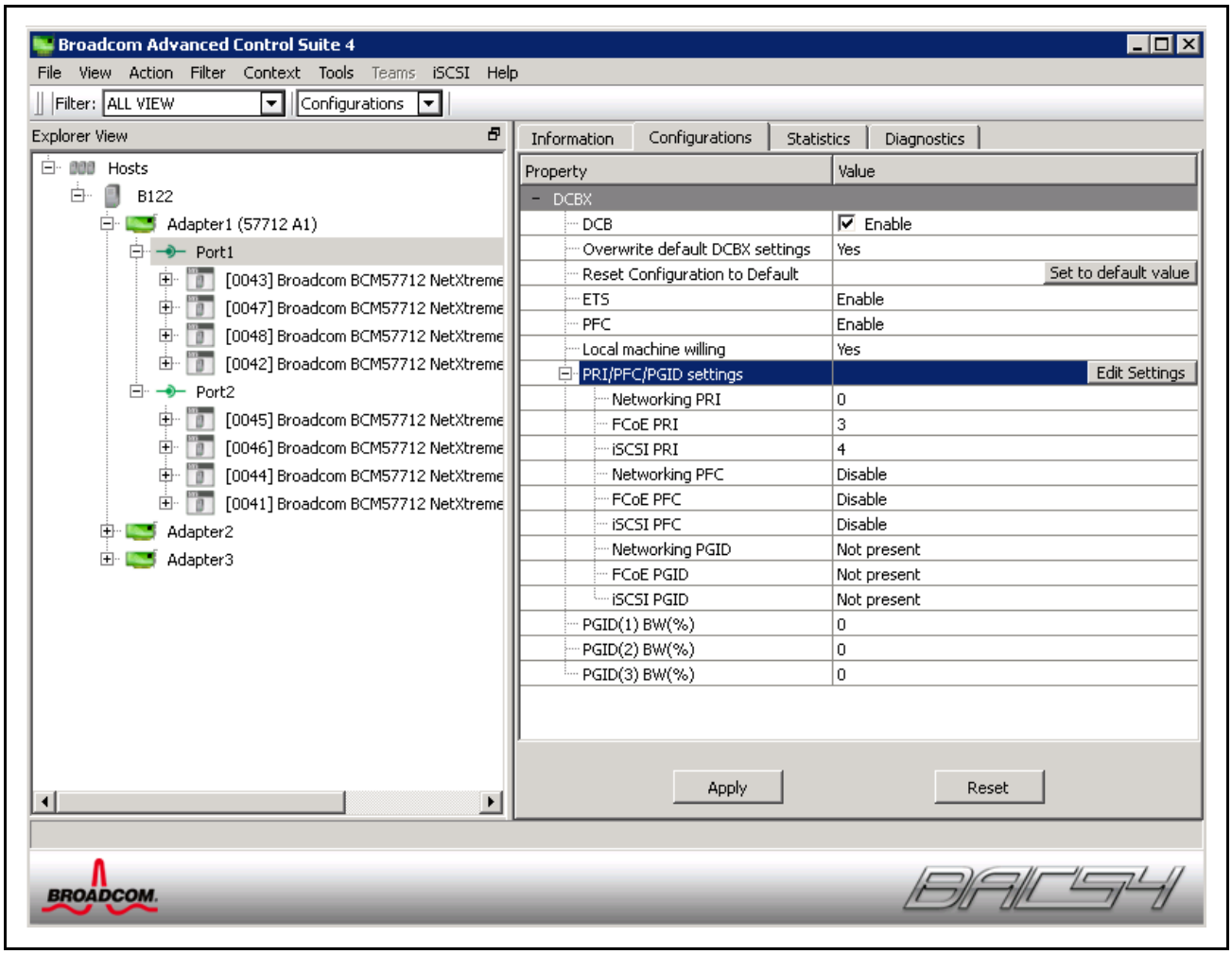


Figure 23: Configure Port with Nondefault settings

If user select “Yes” for Overwrite default DCBX settings parameter, then many parameters below it, becomes enabled for modification. User can click the Edit Settings button against PRI/PFC/PGID settings property to start the wizard. If DCBX is enabled then changing any parameters does not have much effect. The adapter will accept the DCBX parameters from switch. At the end of the negotiation, adapter’s Local Parameters will be a copy of the Remote Parameters.

To modify the Administrative parameters, follow this procedure.

1. Select **Overwrite default DCBX settings** and select “Yes”.
2. Click **Edit Settings** button against **PRI/PFC/PGID settings**.
3. On **Step 1**, select Priority value you want to configure for three traffic classes – Ethernet, FCoE and iSCSI.

Note: You can select the same priority value for more than one traffic type.

4. On **Step 2**, assign PGID value to each traffic type (in other words assign PGID to priority). If you select same priority value for more than one traffic type then you will see those traffic class combined in step 2.
5. On **Step 3**, configure PFC for each traffic types. If you select same priority value for more than one traffic type then you will see those traffic class combined in step 3.
6. Finally, assign the desired bandwidth to each PGID.

Note: The total bandwidth for all PGID should not exceed 100%.

7. Click the **Apply** button for changes to take effect.

DCB Enabled, DCBX Disabled with Nondefault Settings

If the user has enabled DCB, disabled DCBX and modified the Administrative parameters, the operation state of the adapter will be as follows.

- The adapter will have DCB related capabilities enabled. In other words, the adapter will support priority flow control and ETS for the egress traffic.
- The Administrative parameters configured above will take effect.
- The adapter will not send LLDP frames with DCBX TLV to the peer.

1. Select **Overwrite default DCBX settings** and select **Yes**.
2. Click the **Edit Settings** button against **PRI/PFC/PGID settings**.
3. On **Step 1**, select the Priority value you want to configure for three traffic classes – Ethernet, FCoE and iSCSI.

Note: You can select same priority value for more than one traffic type.

4. On **Step 2**, assign the PGID value to each traffic type (in other words assign PGID to priority). If you select same priority value for more than one traffic type, you will see those traffic class combined in step 2.
5. On **Step 3**, configure the PFC for each traffic types. If you select same priority value for more than one traffic type, you will see those traffic class combined in step 3.
6. Finally, assign desired bandwidth to each PGID.

Note: The total bandwidth for all PGID should not exceed 100%.

7. Click the **Apply** button for changes to take effect.

DCB Disabled

If the user uncheck the DCB Enable check box then the DCB feature will be disabled at the port level. The operational flow control will be Link Level flow control instead of priority flowcontrol (see"Priority Flow Control (PFC)" on page 83 for details of PFC) depending on the adapter settings and switch settings. The ETS will be disabled (see "Enhanced Transmission Selection (ETS)" on page 84 for details on ETS). Although not a common configuration, BACS4 gives user the ability to configure adapter in this way.

Statistic

The Statistics tab displays various statistical counters at the port level.

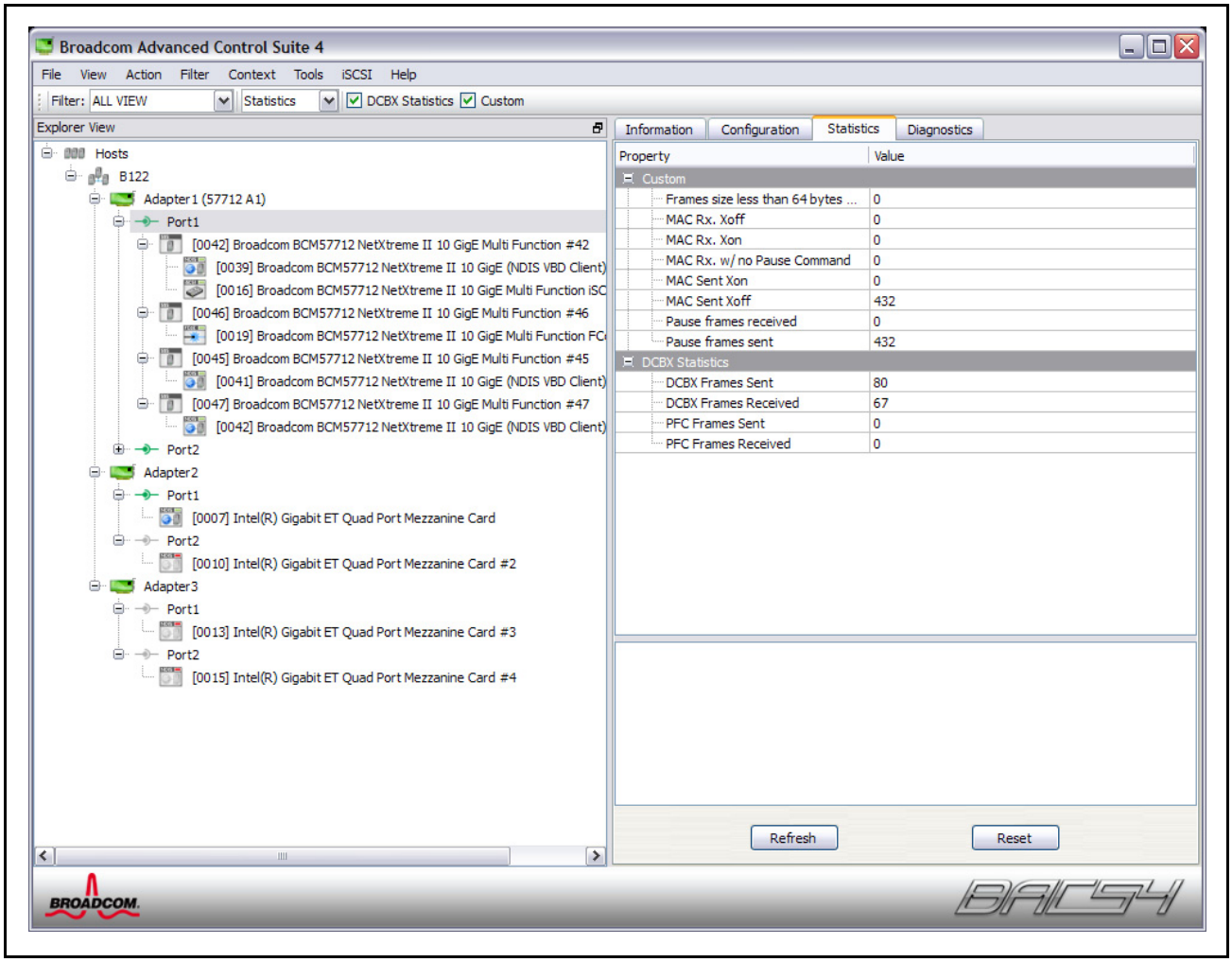


Figure 24: Statistics Tab for Port

There are two buttons at the bottom the tab as follows.

Refresh**:** Clicking this button will refresh the Statistics information immediately. If this button is not clicked then statistical counter information is refreshed every 5 seconds.

Reset: Clicking on this button will reset all counters on the Statistics tab. All counter values will be set to 0.

Diagnostics

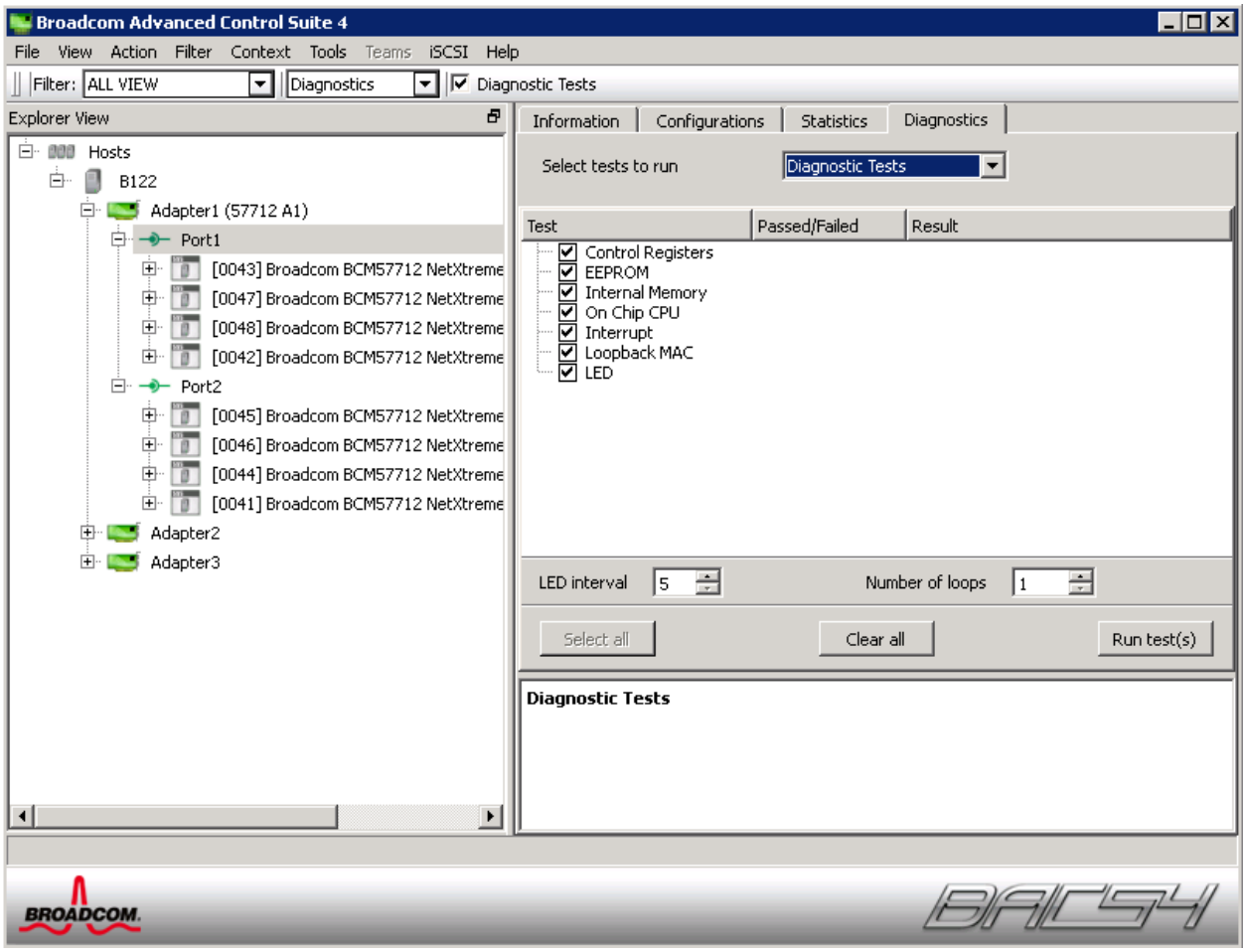
This tab allows user to run various diagnostics tests. In normal situation it may not be necessary to run tests. Some tests will disrupt the I/O running on the adapter. The diagnostics tests should be run with utmost care and by the individual who is aware of the effects of the tests on the functioning of the adapter. In some cases, Broadcom support team may ask users to run some diagnostics tests while debugging any issue.

There are two main categories of tests which can be run at the port level. They are defined in details below.

Diagnostic Tests

Follow this procedure to run **Diagnostics** tests.

1. On the **Select test to run** drop down menu, select **Diagnostic Test**.
2. Select one or more of the following tests.
   - Control Registers
   - EEPROM
   - Internal Memory
   - On Chip CPU
   - Interrupt
   - Loopback PHY
   - LED



3. Select value for **Number of loops**. This will determine how many iteration of each test will run.
4. Select appropriate value of **LED Interval**.
5. Click **Clear all**, if you want to deselect all tests and start all over again.
6. Clicking on **Select all** will select all available tests.
7. Click **Run Test(s)** to start running the selected tests.
8. Click **Yes** when the warning message is displayed indicating that network connection will be disrupted while the tests are running.
9. Once the test starts, an information window will open giving the status of the test.
10. User has the option of stopping the long running test, if they desired to do so.

    At the end of the tests, the result will be displayed indicating how many tests passed and how many failed under **Passed/Failed** column.

    The **Status** column displays the current status (Running/Completed) of the test.

Note: Some Diagnostics tests are not available on Linux managed hosts.

Managing PCI Function

One level below Ethernet controller object (Port) is a PCI function. This represents VBD driver of the adapter. The following three tabs are available for PCI function object.

- Information Tab
- Configuration Tab
- Statistics Tab

Information

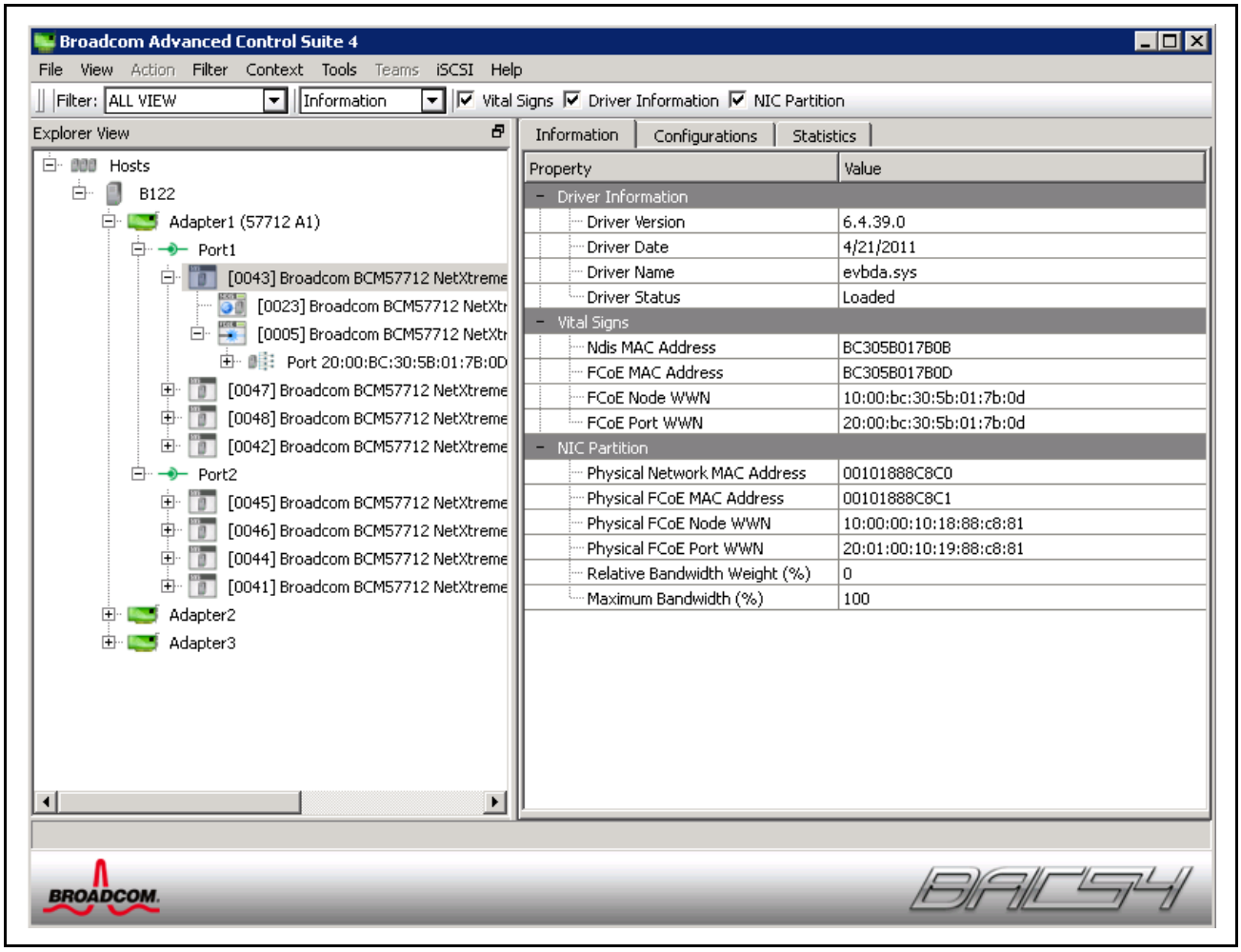


Figure 25: Information tab for PCI Function

Note: Depending on the offload functions created under PCI function, information being displayed will vary. For example, if the FCoE offload is created then FCoE related information will be displayed.

The following information is provided under this tab under Vital Signs and Driver Information.

Vital Signs

NDIS MAC Address: Displays the MAC address of the NDIS function.

iSCSI MAC Address: Displays the MAC address of the iSCSI function.

FCoE Node WWN: Displays the World Wide Node Name of the FCoE function.

FCoE Port WWN: Displays the World Wide Port Name of the FCoE function.

Note: On Linux hosts, in addition to the above mentioned fields, the following fields are available — **Permanent MAC address, IPv4 Address, IPv6 Address, MTU.**

Driver Information

Driver Version: Displays the version information of the installed EVBD driver.

Driver Date: Displays the date version information of the installed EVBD driver.

Driver Name: Displays the file name of the installed EVBD driver.

Driver Status: Displays whether driver is loaded or not loaded.

Note: The Linux managed host does not have **Driver Date** field.

NIC Partition

This section is displayed only if the NIC partition is enabled on the adapter port.

Physical network MAC Address: Displays the physical network MAC address of the function.

Physical FCoE MAC Address: Displays the FCoE MAC address of the function. This MAC address is used in the FIP frames.

Physical FCoE Node WWN: Displays the FCoE node WWN of the function, if the FCoE offload is enabled for the function.

Physical FCoE Port WWN: Displays the FCoE port WWN of the function, if the FCoE offload is enabled for the function.

Physical iSCSI MAC Address: Displays the iSCSI MAC address of the function. This MAC address is used in the iSCSI frames.

Relative Bandwidth Weight (%): Displays the relative bandwidth weight assigned to the function. The value depicts the relative share that the partition will get for transmission, relative to the other partitions on the port. This setting takes effect only when the ETS is disabled on the adapter port. When the ETS is enabled, the ETS configuration takes effect. The sum of all relative bandwidth weight on all functions per port should be 100.

Maximum Bandwidth (%): Displays the maximum bandwidth assigned to the function. This setting set a cap on the maximum transmission bandwidth on that partition. This setting takes effect only when the ETS is either enabled or disabled on the adapter port. Each function can have the value of 100% since this value is a cap on the individual function.

Configuration

The Configuration tab allows user to configure PCI Function (EVBD driver) related parameters. The configuration of the PCI function is divided in two main categories:

- Advanced
- Resource Reservation

The Advanced section allows configuring parameters which should e modified only by someone who is familiar with the effect of the changes. If you are unsure of you should change these parameters, contact Broadcom Technical support.

Advanced

Pause On Exhausted Host Ring: Not available on Linux managed hosts. There are two possible scenarios that can trigger pause frames to be generated: a host ring buffer is exhausted or the on-chip buffers are depleted. With RSS enabled inside the system, it is possible to achieve better Ethernet throughput if no pause frames are being generated in a case where a host ring buffer (of multiple RSS rings) is exhausted. The default is Disabled.

Speed & Duplex: Not available if NPAR is enabled. This field allows user to manually configure the speed and duplex characteristics of the port.

Set Properties to Default Values: Clicking on this field sets the properties of EVBD driver parameters to its default values.

Flow Control: Not available if NPAR is enabled. Manually configure the flow control for the select LAN device. Possible options are TX Enabled, RX Enabled, RX & TX Enabled and Auto (Default).

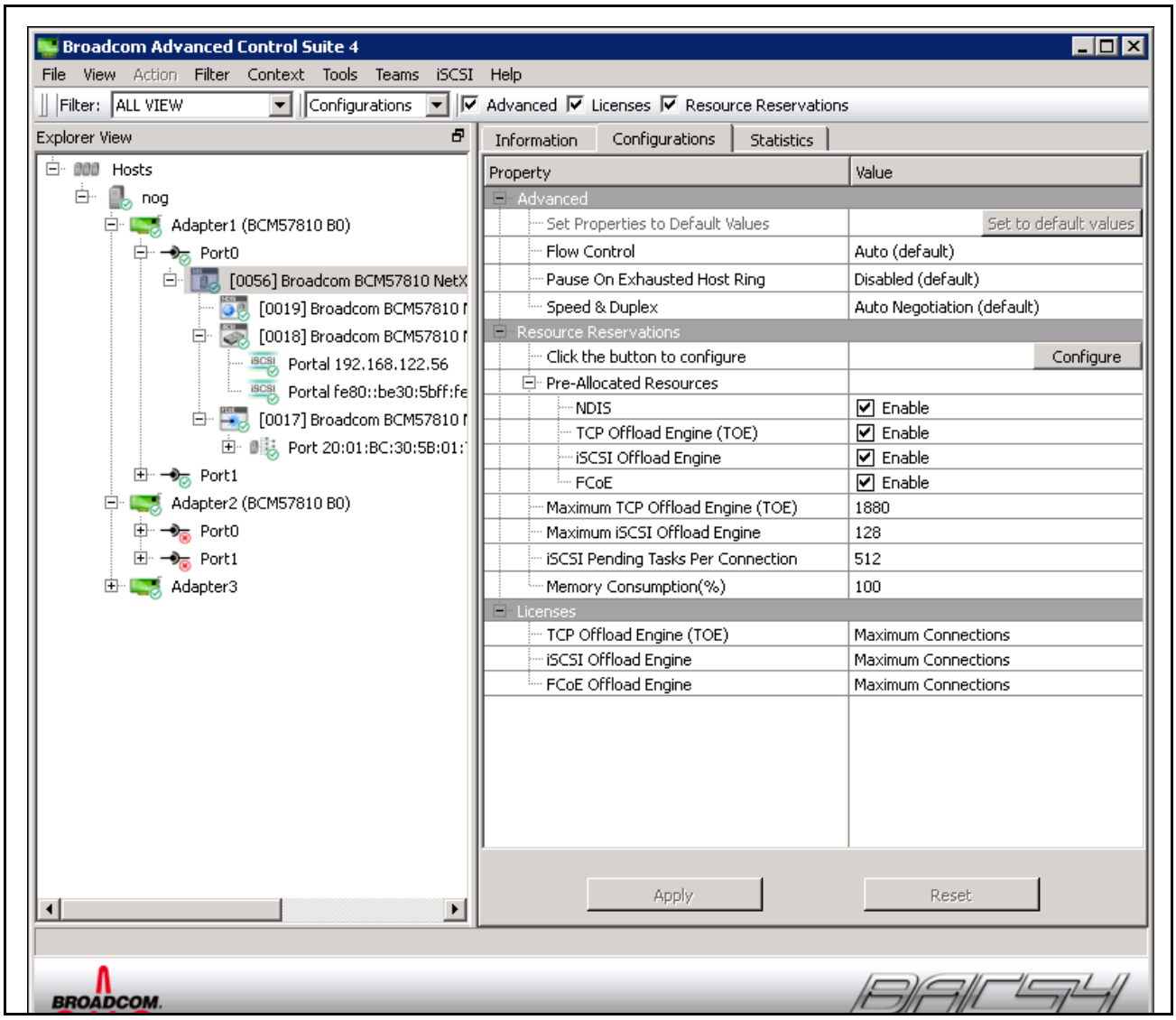


Figure 26: Configure PCI Function

On Linux managed hosts, the following properties are available for modification.

Jumbo Packet: This field allows user to manually configure the MTU size.

Receive Buffer: This field allows user to manually configure the receive buffer size. The maximum allowed value is 4078.

TCP Segmentation Offload: This field allows user to manually enable/disable the TCP segmentation offload.

Transmit Buffer: This field allows user to manually configure the transmit buffer size. The maximum allowed value is 4078.

Resource Reservation

Note: This section is not available on Linux managed hosts.

Pre-Allocated Resources: Under this subsection there are several check boxes available – for NDIS, TOE offload, iSCSI and FCoE. All protocol functions whose check boxes are unchecked are disabled. The text False against the protocol indicates that the protocol is disabled. You can selectively check any box to enable the corresponding protocol offload function.

Maximum TCP Offload Engine Connections: This field defines the maximum number of connections available for TOE offload. The maximum number of allowed connections is 8192.

Maximum iSCSI Offload Engine Connections: This field defines the maximum number of connections available for iSCSI offload. The maximum number of allowed connections is 128.

Pending Tasks per Connection: This field defines the maximum number of outstanding tasks per connection. The maximum value that can be configured is 512.

Memory Consumption: This defines how much percentage of the total memory can be used by PCI function (EVBD driver). The maximum value is 100 and can be configured in the quanta of 25%.

Note: When the NIC Partitioning (NIC PAR) feature is enabled and configured, some parameters cannot be configured at the PCI function (or EVBD driver) level. The parameters which cannot be modified with NIC Partitioning enabled are – Pre-allocated Resources, Maximum TCP Offload Engine Connections, Maximum iSCSI Offload Engine connections, Pending Tasks Per Connection, and FCoE connections.

License

Note: Displays various licences configured on the adapter port.

Statistics

The **Statistics** tab displays various statistical related counters.

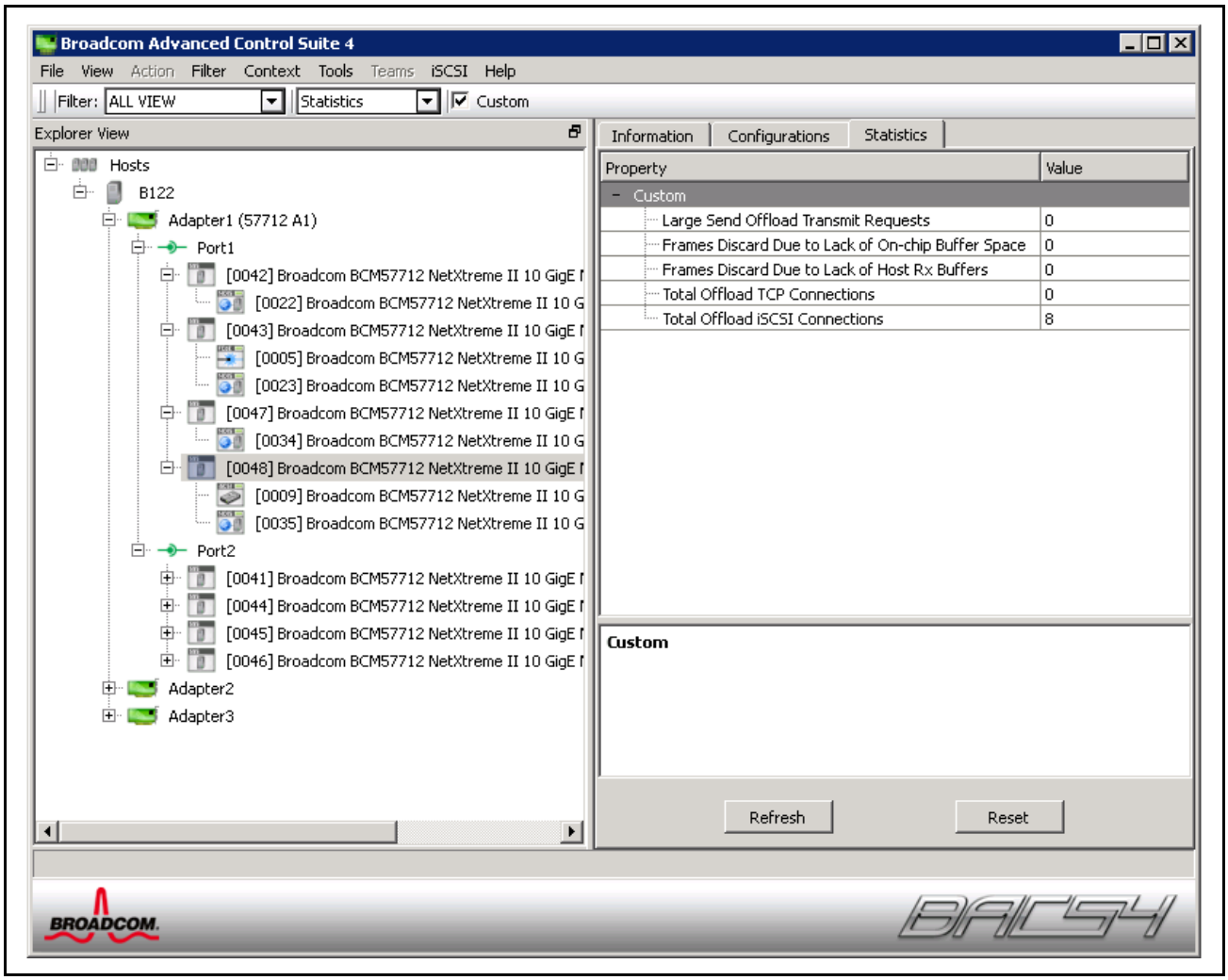


Figure 27: Statistical Information for PCI Function

There are two buttons at the bottom the tab as follows.

Refresh: Clicking on this button will refresh the **Statistics** information immediately. If this button is not clicked then statistical counter information is refreshed every 5 minutes [Verify this]

Reset: Clicking on this button will reset all counters on the **Statistics** tab. All counter values will be set to 0.

Managing LAN Device

The LAN function represents the Ethernet (NDIS) functionality available under the PCI Function. User can view current values of various NDIS driver parameters, configure NDIS driver parameters, view attached FCoE targets and LUN information by selecting FCoE object in object explorer panel.

Note: On Linux hosts, there is no separate LAN device function available. The LAN device function is configured at the PCI function level. See "Managing PCI Function" on page 93 to configure LAN functionality.

The available tabs for the NDIS function are as follows:

- Information Tab
- Configuration Tab
- Diagnostics Tab
- Statistics Tab

Information

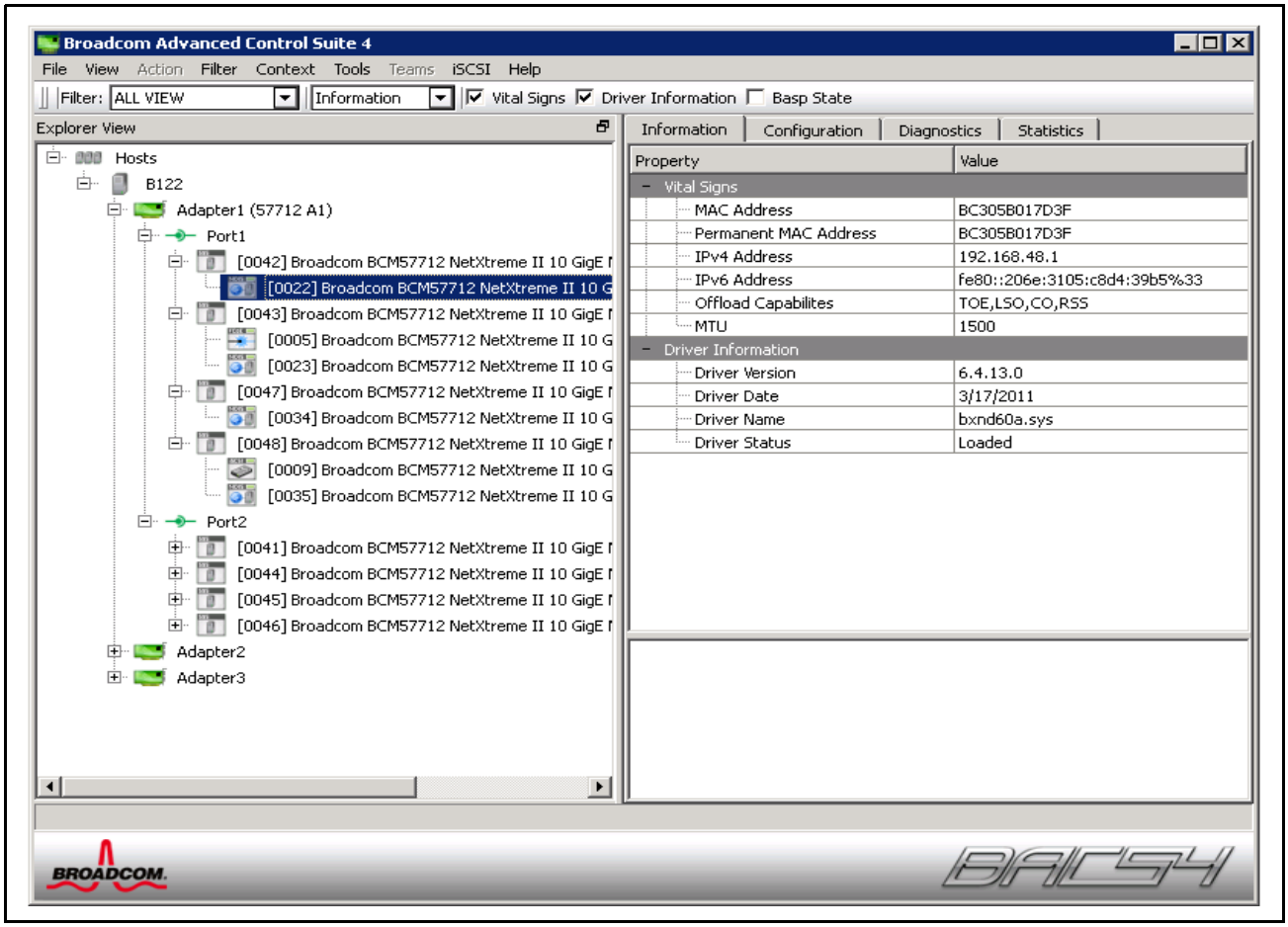


Figure 28: Information Tab for LAN Function

The Information tab has the following two sections and related parameters under it.

Driver Information

Driver Version: Displays the NDIS driver version information.

Driver Name: Displays installed NDIS driver file name.

Driver Status: Displays if NDIS driver is loaded or not.

Driver Date: Displays NDIS driver release date.

Vital Signs

MAC Address: Displays the current MAC address configured for the selected LAN device.

Permanent MAC Address: Displays the burned-in MAC address for the selected LAN device. This value cannot be modified.

IPv4 Address: Displays the current IPv4 address assigned to the selected LAN device.

IPv6 Address: Displays the current IPv6 address assigned to the selected LAN device.

Offload Capabilities: Displays the list of protocol or features (e.g. TOE, LSO, CO, RSS etc.) which can be offloaded on the selected LAN device.

MTU Size: Displays the current MTU size configured for the selected LAN device.

Configuration

The configuration tab allows users to modify some of the configurable parameters of the NDIS driver.

1. Select **LAN function** in the Object Explorer window.
2. Click the **Configuration** tab.
3. The following parameters can be configured at the configuration tab.

   Set properties to default values: By clicking on this field, user can set all NDIS driver parameters to its default values.

   Interrupt Moderation: Enables interrupt moderation, which limits the rate of interrupt to the CPU during packet transmission and packet reception. The disabled option allows one interrupt for every packet transmission and packet reception. Enable is the default option.

   Jumbo packet: Enables the network adapter to transmit and receive oversized Ethernet frames that are greater than 1514 bytes, but less than or equal to 9600 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. To increase the size of the received frames, raise the byte quantity in 500-byte increments.

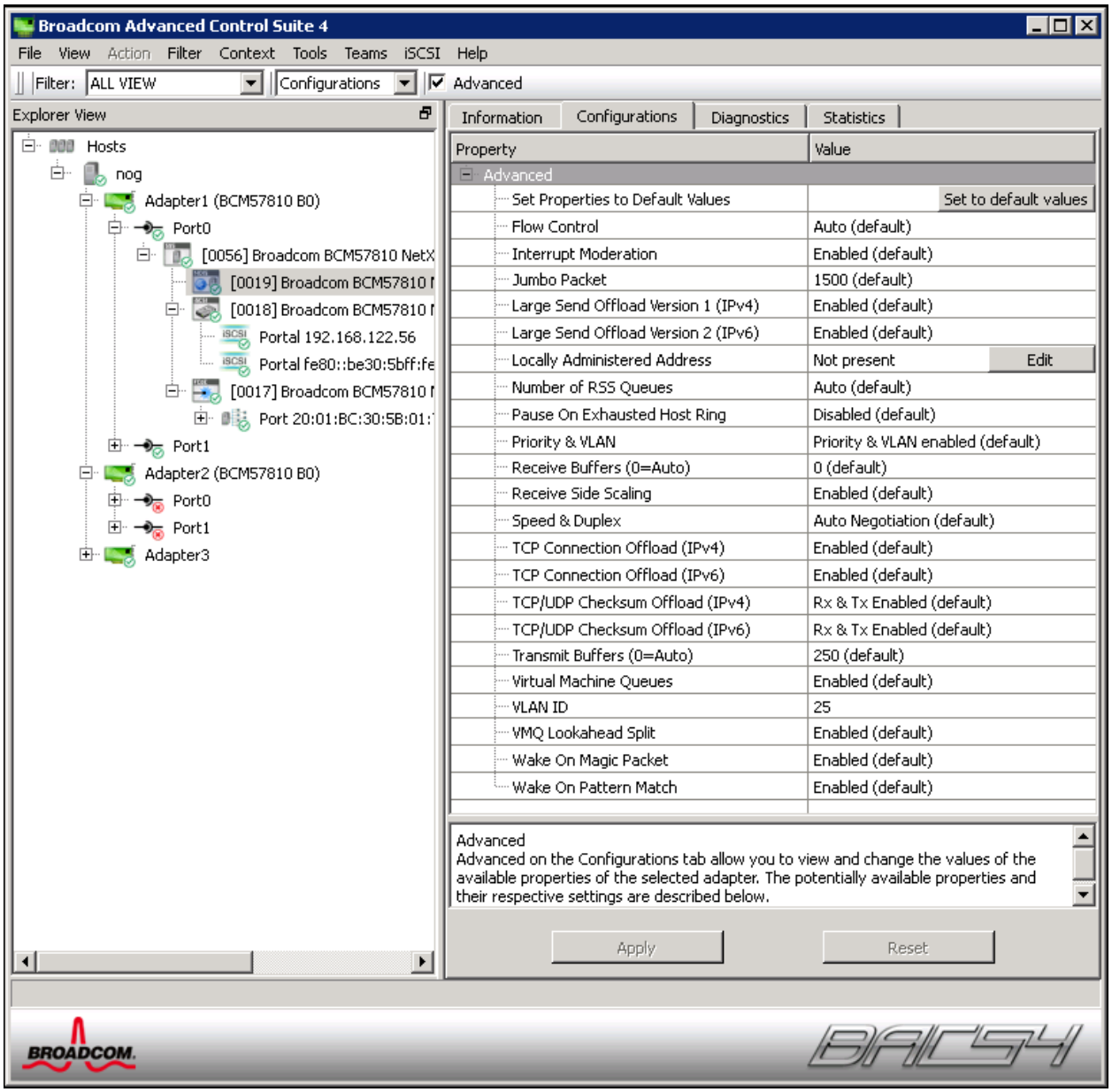


Figure 29: Configuration Tab for LAN Device

Note: If **Jumbo Packet** is set to 5000 bytes or greater on Converged Network Adapters, ensure that **Flow Control** is set to **Auto** to prevent the system performance from performing at less than optimal levels. This limitation exists on a per-port basis.

Flow Control: Manually configure the flow control for the select LAN device. Possible options are TX Enabled, RX Enabled, RX & TX Enabled and Auto (Default).

IPv4 Large Send Offload: Normally, the TCP segmentation is done by the protocol stack. When you enable the Large Send Offload property for IPv4, the TCP segmentation for IPv4 traffic can be done by the network adapter. The default setting for this property is Enabled.

IPv6 Large Send Offload: Normally, the TCP segmentation is done by the protocol stack. When you enable the Large Send Offload property for IPv6, the TCP segmentation for IPv6 traffic can be done by the network adapter. The default setting for this property is Enabled.

Number of RSS Queues: Allows configuring RSS queues from 1 to 16. Options are 1, 2, 4, 8, 16 and Auto. The Auto is a default setting.

Priority and VLAN: Enables the priority and VLAN capability on the adapter. Available options are Priority & VLAN enabled, Priority & VLAN disabled, Priority enabled, VLAN enabled.

Receive Buffers (0=Auto): Configures the number of receive buffers at the LAN unction level. The default setting is “0’ which means driver automatically configures optimum number of buffers. User can configure any value between 0 and 3000.

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

TCP Connection Offload (IPv4): Enables and disables TOE offload when using the IPv4 protocol. The default setting for this property is Enabled.

TCP Connection Offload (IPv6): Enables and disables TOE offload when using the IPv6 protocol. The default setting for this property 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. Applies to IPv4 traffic.

IPv6 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. Applies to IPv6 traffic.

Transmit Buffers (0=Auto): Configures the number of transmit buffers. Transmit buffers are data segments that allow the network adapter to monitor transmit packets in the system memory. The range of valid transmit buffers is 0 to 5000 in increments of 50 with 0 transmit buffers as the default value.0

Virtual Machine Queues: Enables or disables the virtual machine queue capability. The default setting is Enabled.

VMQ Lookahead Split: Enables or disabled the look ahead capability when the VMQ (Virtual Machine Queue) is enabled. The default is Enabled.

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.
- Do not assign a Locally Administered Address on any physical adapter that is a member of team.
- Do not assign a Locally Administered Address on any iSCSI boot-enabled device.

Pause On Exhausted Host Ring: There are two possible scenarios that can trigger pause frames to be generated: a host ring buffer is exhausted or the on-chip buffers are depleted. With RSS enabled inside the system, it is possible to achieve better Ethernet throughput if no pause frames are being generated in a case where a host ring buffer (of multiple RSS rings) is exhausted. The default is Disabled.

Wake Up Capabilities: This defines the Wake On LAN configuration on the adapter. Possible values are – None, Magic packet, Wake up Frame and Both. The Both is default.

VLAN ID: Configures the VLAN ID value for the LAN function. The default value is “0”.

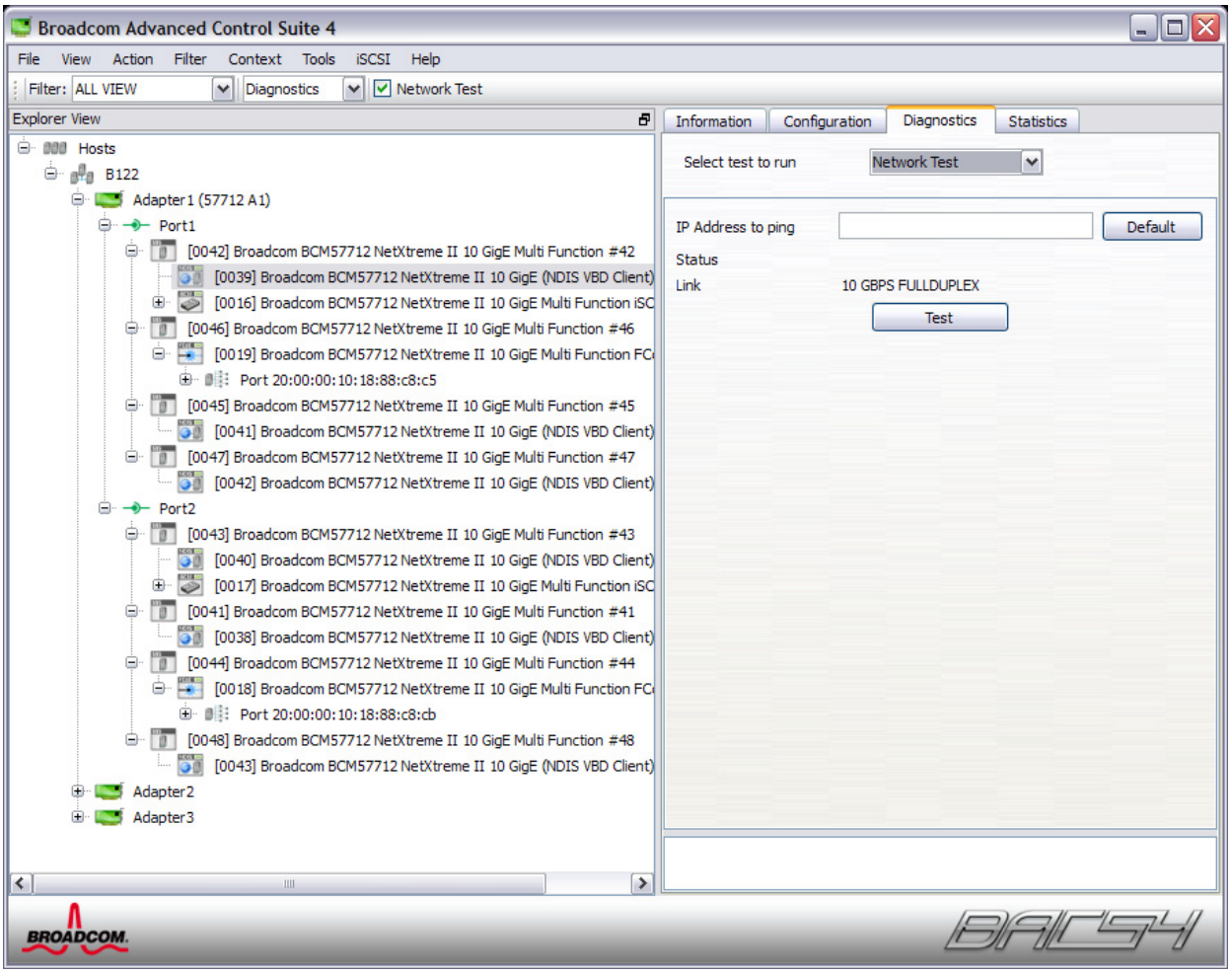
Diagnostics

This tab allows user to run Network diagnostics test. User can run the Ping test to verify the network connectivity.

1. Select the appropriate **LAN device** in the object explorer panel.
2. In the **IP Address to Ping** field, enter the IP address of the network device with which connectivity needs to be tested.
3. Click Test button to initiate the testing.
4. The test progress bar will be displayed when the LAN device is running the test.
5. At the end of the test, the test result will be displayed indicating if the test was successfully or failure.

   The test results will also be displayed against **Status** field.

   The **Link** field displays the current link speed with the duplex settings.
6. Click **OK** to complete the test.



Statistics

This tab displays various statistical counters for the LAN device.

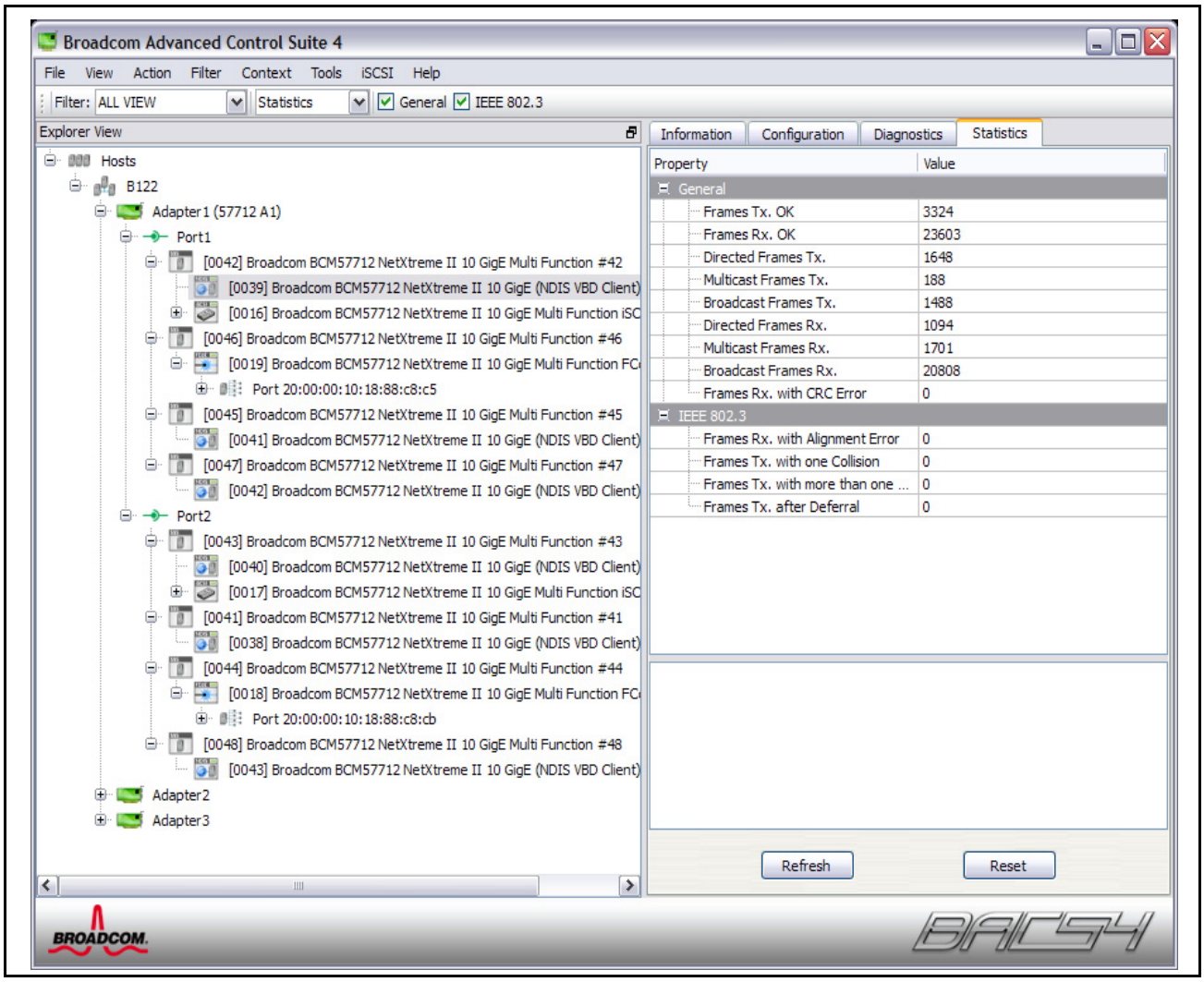


Figure 30: Statistics tab for LAN Device

There are two buttons at the bottom the tab as follows.

Refresh: Clicking on this button will refresh the **Statistics** information immediately. If this button is not clicked then statistical counter information is refreshed every 5 minutes [Verify this]

Reset: Clicking on this button will reset all counters on the **Statistics** tab. All counter values will be set to 0.

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. For a comprehensive description of the technology and implementation considerations of the teaming software, see your Broadcom network adapter user guide.

Note: Currently, Teaming configuration using BACS4 is allowed only on hosts running Windows operating system. Teaming on Linux hosts can be configured using the Linux Bonding driver and configuration utility. Refer to the Linux operating system Teaming/Bonding documentation to configure Team on Linux host.

Teaming can be accomplished by either of the following methods:

- Using the Broadcom Teaming Wizard
- Using Expert Mode

Note the following:

- For further information regarding teaming protocols, see your Broadcom network adapter user guide.
- BASP is available only if a system has one or more Broadcom network adapters installed.
- The TCP Offload Engine (TOE), 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.
- If an adapter is included as a member of a team and you change any advanced property, then you must rebuild the team to ensure that the team's advanced properties are properly set.
- If an adapter with a TOE key is included as a member of a team and you remove the TOE key, then you must rebuild the team to ensure that the team does not appear as a TOE-enabled team.
- You must have administrator privileges to create or modify a team.
- In a FEC/GEC or 802.3ad type team, disabling the device driver(s) of a team member that has IPMI enabled may prevent a successful failover since IPMI maintains link with the attached switch.
- Do not assign a Locally Administered Address on any physical adapter that is a member of a team.

Team Type

You can create four types of load balance teams:

- Smart Load Balance™ and Failover
- Link Aggregation (802.3ad) (TOE is not applicable)
- Generic Trunking (FEC/GEC)/802.3ad-Draft Static (TOE is not applicable)
- 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.

Note: TOE is not applicable for Link Aggregation team type.

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.

Note: TOE is not applicable for FEC/GEC Generic Trunking team type.

SLB (Auto-Fallback Disable)

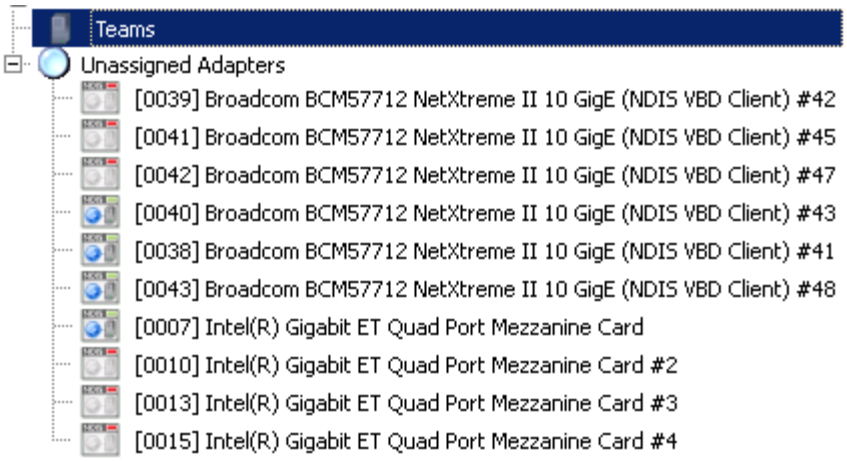
This team is identical to Smart Load Balance and Failover, with the following exception: when the standby member is active, if a primary member comes back online, the team continues using the standby member rather than switching back to the primary member. This type of team is supported only for situations 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.

Create Team Using 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. Select the **Team view** option on the Filter drop down menu, below the menu bar at the top of the BACS4 window, or from the **View** menu, select **Navigate**, then **Team**.
2. Click **Teams** at the top of the Team Management pane, or select one of the listed adapters.
3. **Create** or **Edit** a team:

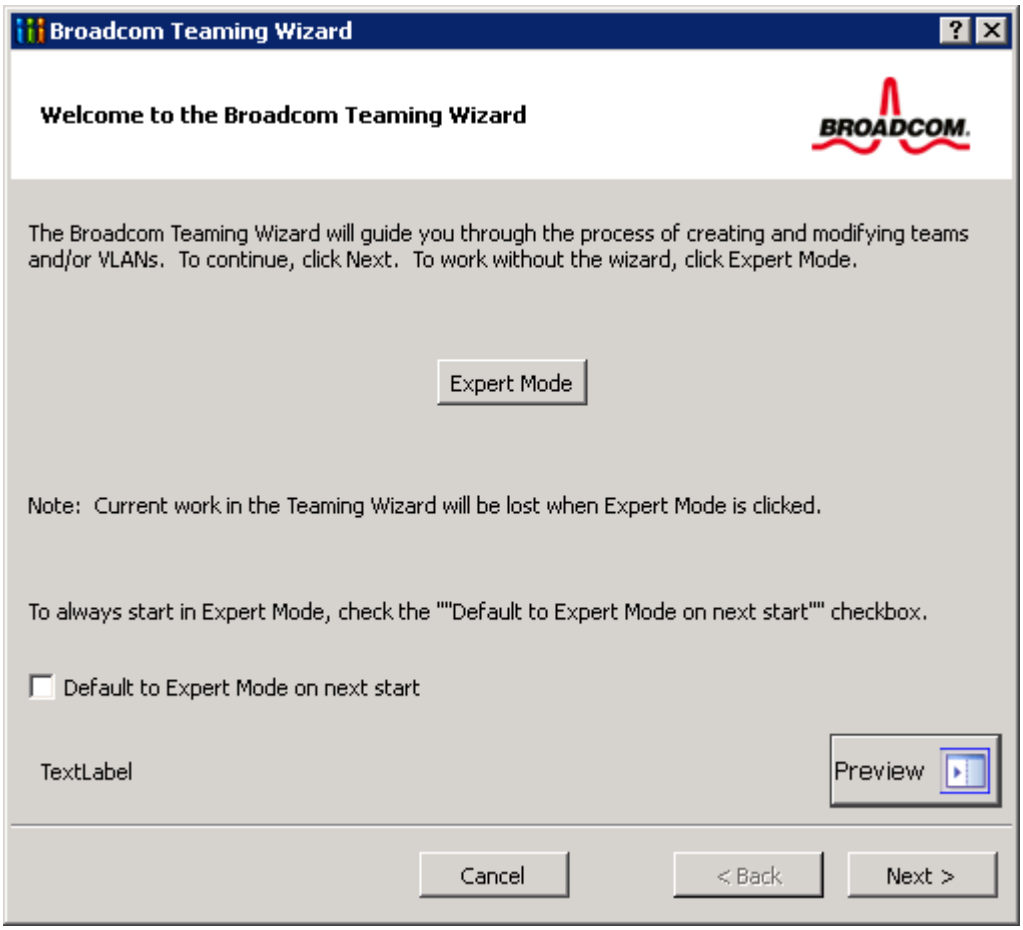
   To create a new team, select **Create a Team** from the **Team** menu, or right-click one of the devices in the **Unassigned Adapters** section and select **Create a Team**. This option is not available if there are no devices listed in the **Unassigned Adapters** section, which means all adapters are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



To configure an existing team, select **Edit Team** from the **Team** menu, 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.

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.

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



5. 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: & \ / : * ? < > |

6. 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.
7. 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**.

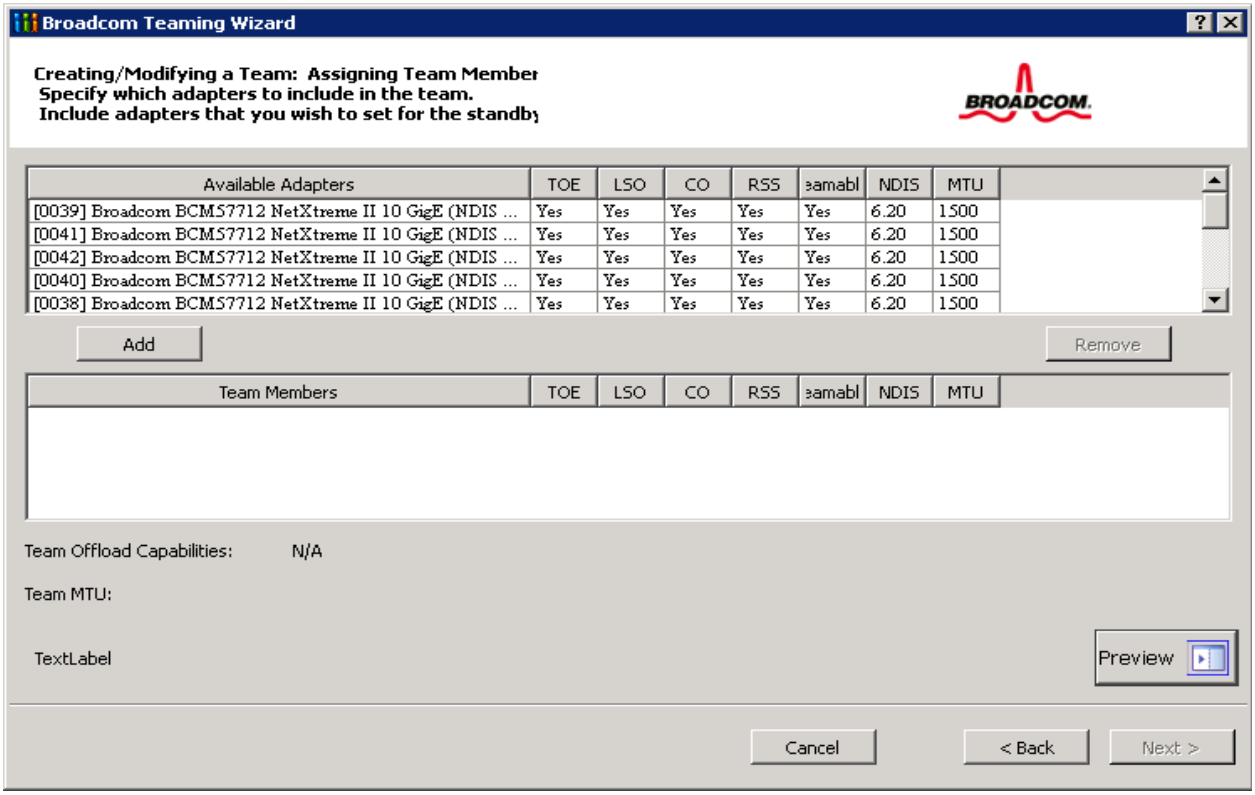
Note: There must be at least one Broadcom network adapter assigned to the team.

A team created with a single adapter will not have load balancing or failover capabilities.

The TCP Offload Engine (TOE), Large Send Offload (LSO) and Checksum Offload (CO) columns indicate if the TOE, LSO, Jumbo MTU, and/or the CO properties are supported for the adapter. The TOE, LSO, Jumbo MTU, 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 the following:

- If an adapter is included as a member of a team and you change any advanced property, then you must rebuild the team to ensure that the team's advanced properties are properly set.
- If an adapter with a TOE key is included as a member of a team and you remove the TOE key, then you must rebuild the team to ensure that the team does not appear as a TOE-enabled team.
- 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.



1. 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.
2. 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**.
3. If you want to configure LiveLink, select **Yes**, otherwise select **No**, then click **Next**.

4. 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).
5. 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 12).

6. 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**.

   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.
7. 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**.

   All of the member IP addresses must be in the same subnet as the subnet of the probe targets.
8. 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 20. of this procedure).
9. 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.

   VLANs can only be created when all team members are Broadcom adapters.
10. Type the VLAN name and then click **Next**.

    The team name cannot exceed 39 characters, cannot begin with spaces, and cannot contain any of the following characters: & \ / : * ? < > |
11. 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 19. of this procedure).
12. Type the VLAN tag value and then click **Next**. The value must be between 1 and 4094.
13. 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.

    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.
14. 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.

    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.

15. 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, and team customization options in the **Configurations** tab.

Create Team 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 "Create Team Using Teaming Wizard" on page 107.

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

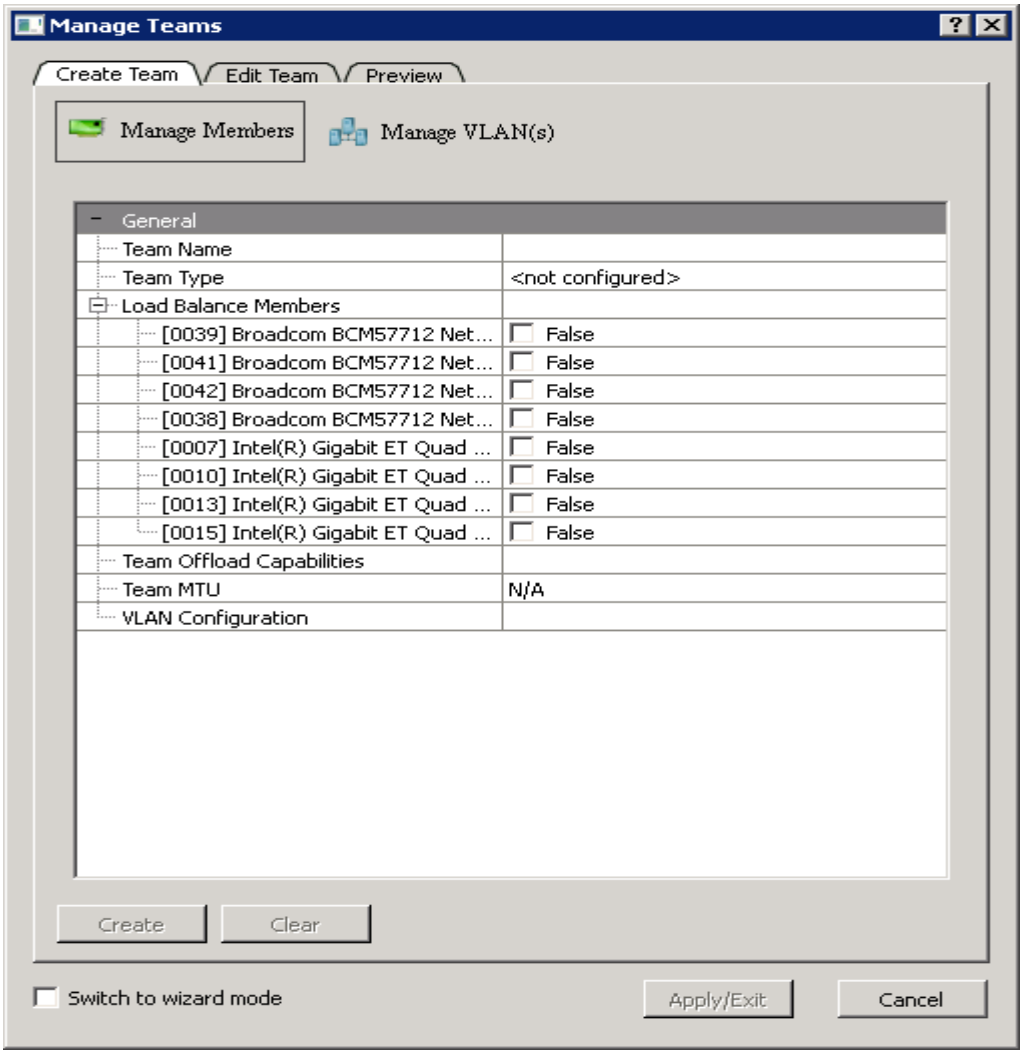
Creating a Team

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

1. Select the **Team view** option on the Filter drop down menu, below the menu bar at the top of the BACS4 window, or from the **View** menu, select **Navigate**, then **Team**.
2. Click **Teams** at the top of the Team Management pane, or select one of the listed adapters.
3. From the **Team** menu, select **Create a 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.
4. Click **Expert Mode**.

   If you want to always use Expert Mode to create a team, click **Default to Expert Mode on next start**.
5. Click the **Create Team** tab.

   The **Create Team** tab appears only if there are teamable adapters available.
6. Click the **Team Name** field to enter a team name.
7. Click the **Team Type** field to select a team type.
8. Click **Manage Members** at the top of the window.



9. Assign any available adapter or adapters to the team by moving the adapter from the **Available Adapters** list to the **Load Balance Members** list. There must be at least one adapter in the **Load Balance Members** list.
10. You can assign any other available adapter to be a standby member by selecting it from the **Standby Member** list.

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

    A team created with a single adapter will not have load balancing or failover capabilities.

    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: If an adapter is included as a member of a team and you change any advanced property, then you must rebuild the team to ensure that the team's advanced properties are properly set.

- If an adapter with a TOE key is included as a member of a team and you remove the TOE key, then you must rebuild the team to ensure that the team does not appear as a TOE-enabled team.
- 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.

1. Click **OK** to accept your changes to the team members.
2. Click **Create** to save the team information.
3. Repeat steps 6 through 12 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.
4. Click **Apply/Exit** to create all the teams you have defined and exit the Manage Teams window.
5. Click **Yes** when the message is displayed indicating that the network connection will be temporarily interrupted.

   Note the following:

   - 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 reenable it, you must first disable and reenable all team members before you reenable 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.
6. 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.

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.

If the **Statistics** tab is not visible, then from the **View** menu, select **Navigate**, then **Team Management**, and then **Statistics**.

If the **General** section is not visible, then from the **Context View** tab on the right side of the window, select **Statistics** and then select **General**.

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

Managing FCoE Function

The FCoE function represents the FCoE functionality available under the PCI Function. User can view current values of various FCoE driver parameters, configure FCoE driver parameters, view attached FCoE targets and LUN information by selecting FCoE object in object explorer panel.

The available tabs for the FCoE function are as follows:

- Information Tab
- Configuration Tab
- Statistics Tab

Information Tab

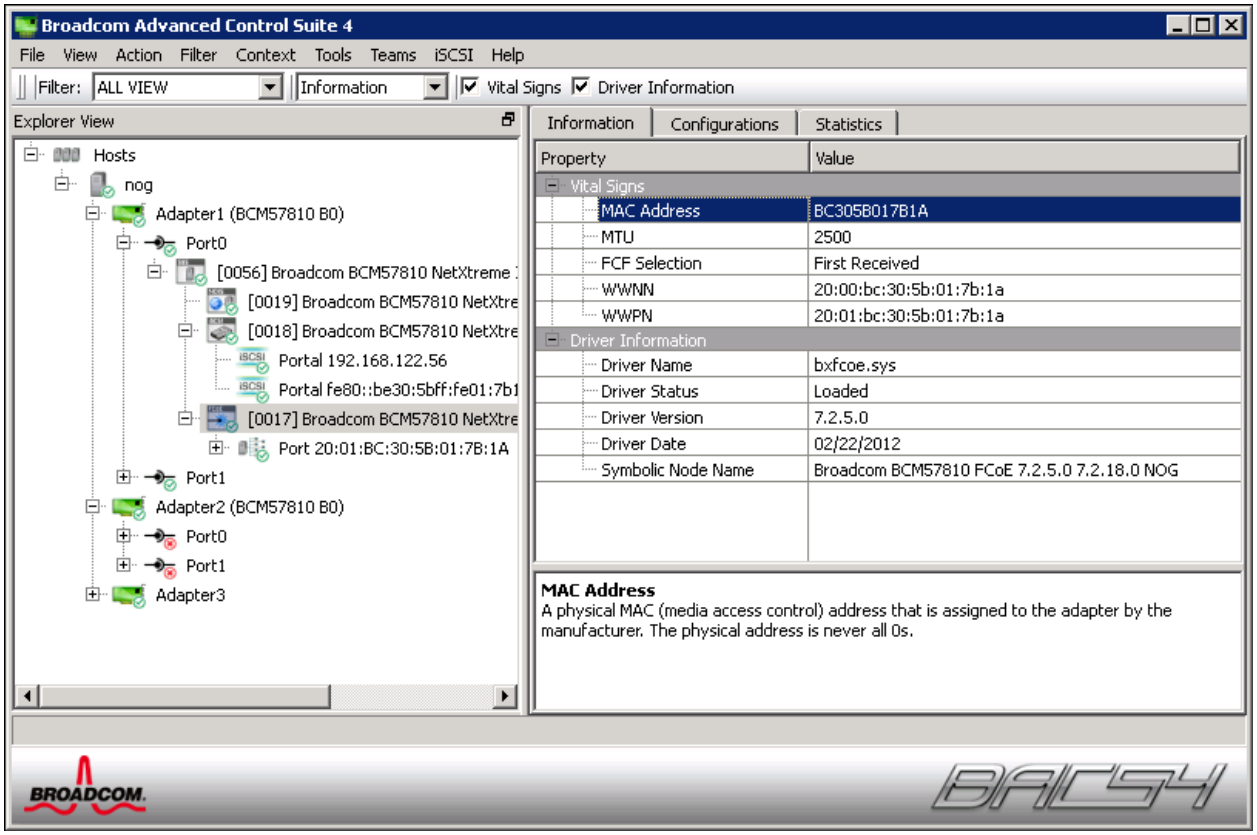


Figure 31: Information Tab for FCoE Function

The Information tab has the following two sections and related parameters under it.

Driver Information

Driver Name: Displays installed FCoE driver file name.

Driver Status: Displays if driver is loaded or not.

Driver Version: Displays the driver version information.

Driver Date: Displays driver release date.

Symbolic Node Name: Displays the symbolic Node name. This information is helpful in debugging login issue.

Vital Signs

MAC Address: Displays the current burned-in FCoE MAC address configured for the FCoE function.

MTU: Displays the MTU size configured for the FCoE function. The default value is 2500.

FCF Selection: Displays the current FCF selection method configured for the FCoE function. In a multiple fabric scenario the selection method plays important role in selecting FCF for login.

WWPN and WWNN: Displays user configured WWPN and WWNN for the FCoE function. This value is different than the burned-in WWPN and WWNN.

Configuration

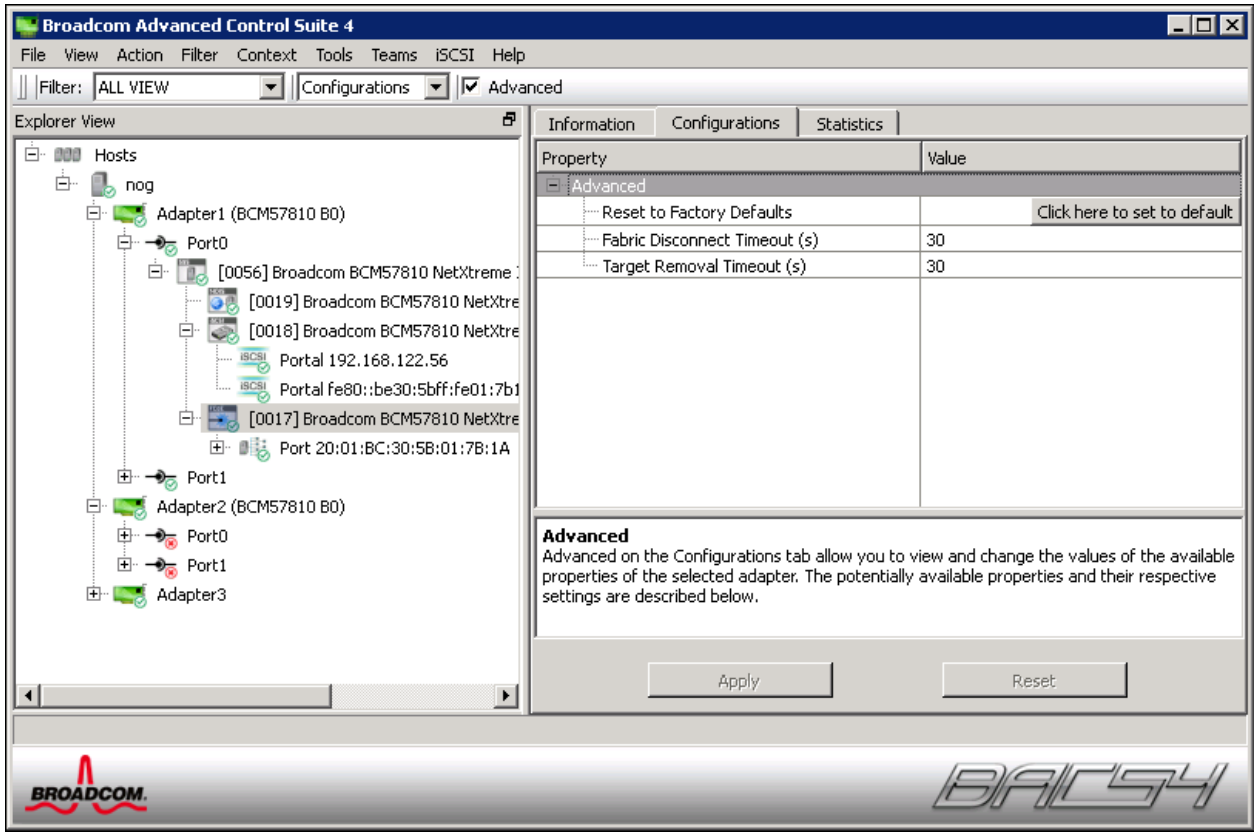
The configuration tab allows users to modify some of the configurable parameters of the FCoE driver.

1. Select **FCoE function** in the Object Explorer window.
2. Click the **Configuration** tab.
3. The following parameters can be configured at the configuration tab.

   Fabric Disconnect timeout: Configures the fabric disconnect timeout value. If the connection to the fabric is not restored before the timeout value expires, all targets discovered on the fabric are removed from the operating system.

Note: The Fabric Disconnect timeout value must be less than or equal to the Target Removal timeout value.

Target Removal Timeout: Configures the target removal timeout value. Provided the connection to the fabric remains active, if the connection to a target is not restored before the timeout value expires, then the individual target is removed from the operating system.



Reset to Factory Defaults: Resets the value to the factory default values.

Statistics

This tab displays various statistical counters for the FCoE function.

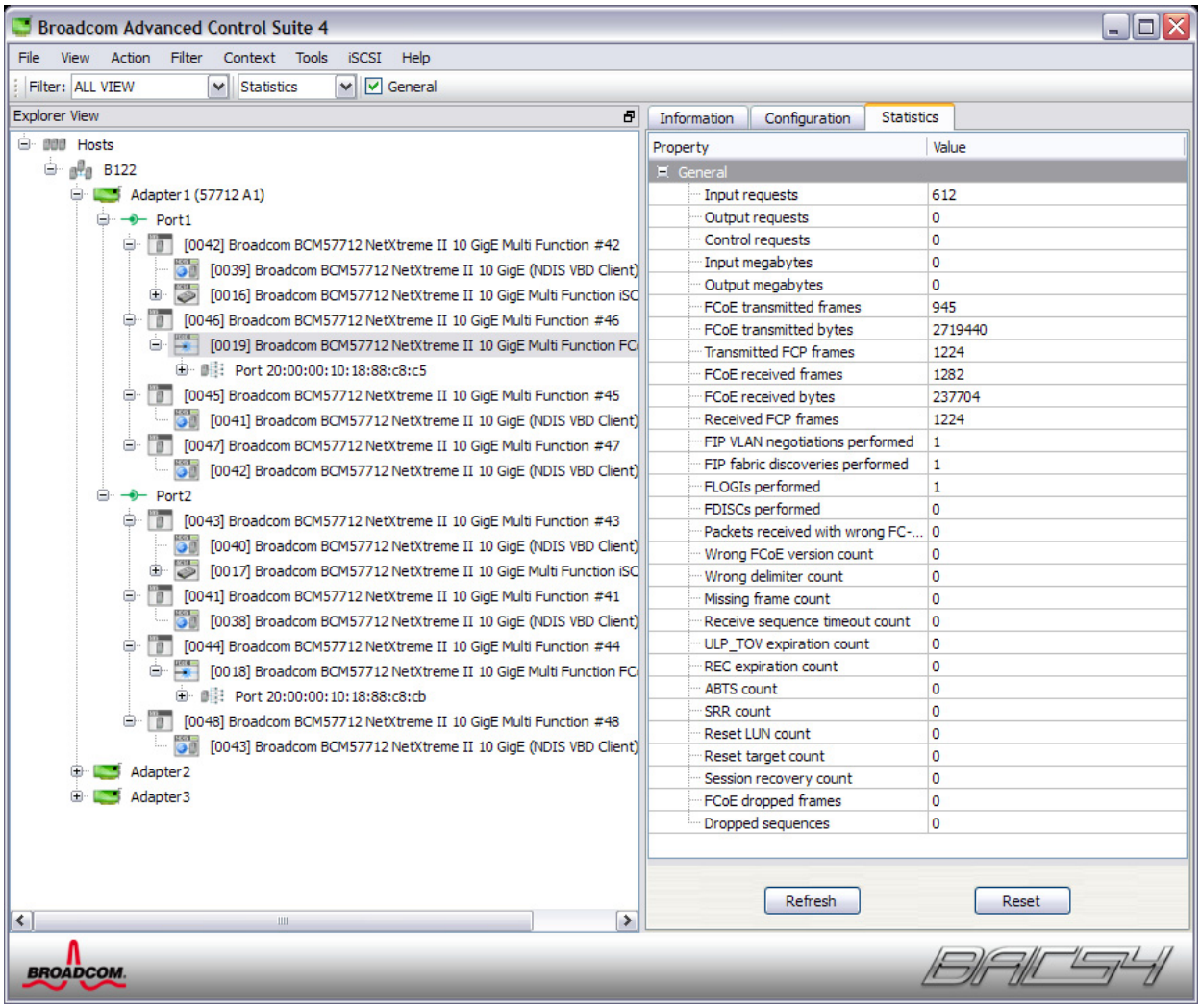


Figure 32: Statistical Information for FCoE Function

The BACS4 displays large number of statistical counters information for the FCoE function. This gives user wide variety of information to better manage the converged network environment.

There are two buttons at the bottom the tab as follows.

- **Refresh:** Clicking this button will refresh the **Statistics** information immediately. If this button is not clicked then statistical counter information is refreshed every 5 seconds.
- **Reset:** Clicking this button will reset all counters on the **Statistics** tab. All counter values will be set to 0.

N_Port

One level below FCoE function is the physical representation of the **N_Port**. This object in the Object Explorer window is identified by WWPN of the **N_Port**. There is one tab for the **N_Port** object as below.

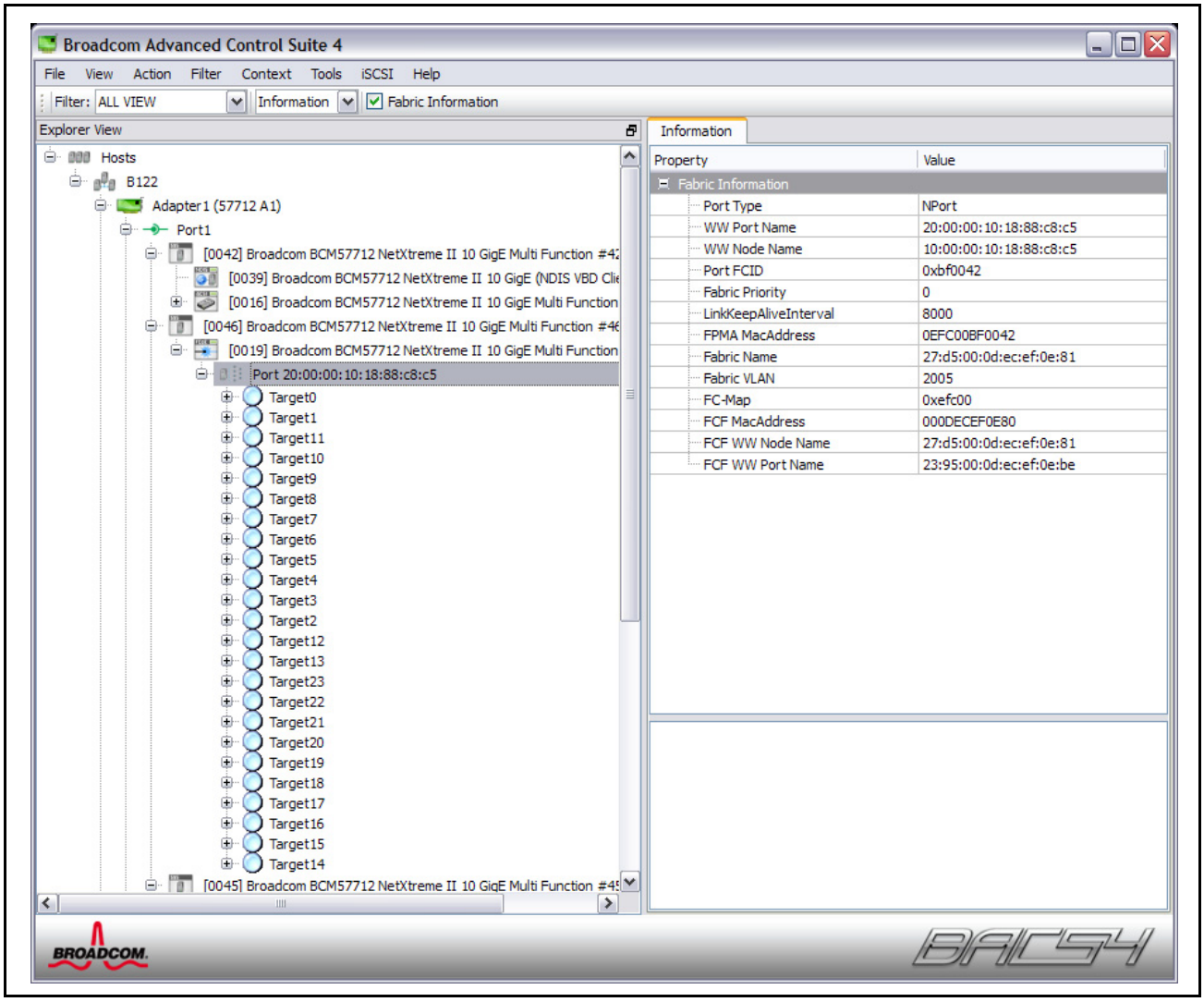


Figure 33: Information tab for N_Port

Information

The **N_Port** object is not a configurable object. The **Information** tab provides the following information.

Port Type: Displays the port type. For N_Port the value is always NPort.

WW Port Name: Displays the WWPN (World Wide Port name) of the N_Port.

WW Node Name: Displays WWNN (World Wide Node name) of the N_Port.

Port FCID: Displays FCID (Fibre Channel ID) of the N_Port.

Fabric Priority: Displays the fabric priority of the attached fabric. Relevant in the multi-fabric topology.

LInkKeepAliveInterval: Displays the current value of the Link Keep Alive value is milliseconds.

FPMA MACAddress: Displays the FPMA (Fabric Provided MAC Address) for the N_Port.

Fabric name: Displays the fabric name, which is a WWPN of the of the switch port connected to the N_Port.

Fabric VLAN: Displays the FCoE VLAN ID of the N_Port. This should not be confused with the VLAN ID for the Ethernet traffic.

FC-Map: Displays the current FC-Map value defined on the switch.

FCF MacAddress: Displays the MAC address of the switch which usually is a management port Mac address of the switch.

FCF WW Node Name: Displays the WWNN of the switch port connected to the N_Port.

FCF WW Port Name: Displays the WWPN of the switch port connected to the N_Port.

Target Port

One level below FC N_Port is the physical representation of the FC targets connected to it. This object in the Object Explorer window is identified by label **TargetX** (where X is the numerical value). There is one tab for the **Target** object as below.

Information

The **Target** object is not a configurable object. The **Information** tab provides the following information.

FCID: Displays the FCID (Fibre Channel ID) of the target.

WW Port Name: Displays the WWPN (World Wide Port name) of the selected target.

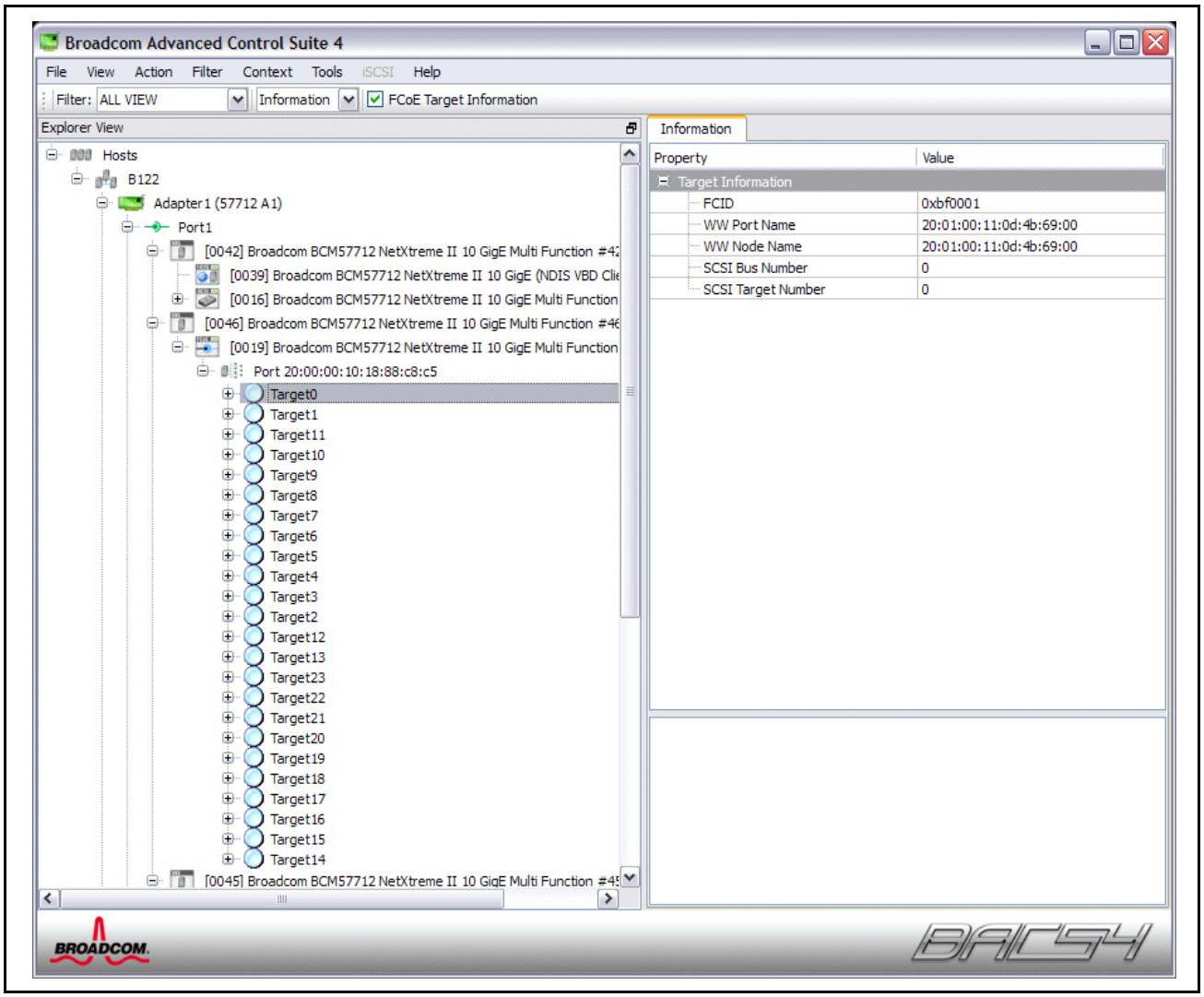


Figure 34: Information Tab for FC Target

WW Node Name: Displays WWNN (World Wide Node name) of the selected target.

SCSI Bus Number: Displays the SCSI bus number of the selected target.

SCSI Target Number: Displays the SCSI target number of the select target.

LUN

One level below **Target** Port is the physical representation of the LUN connected to it. This object in the Object Explorer window is identified by label **LUNx** (where X is the numerical value). There is one tab for the **LUN** object as below.

Information

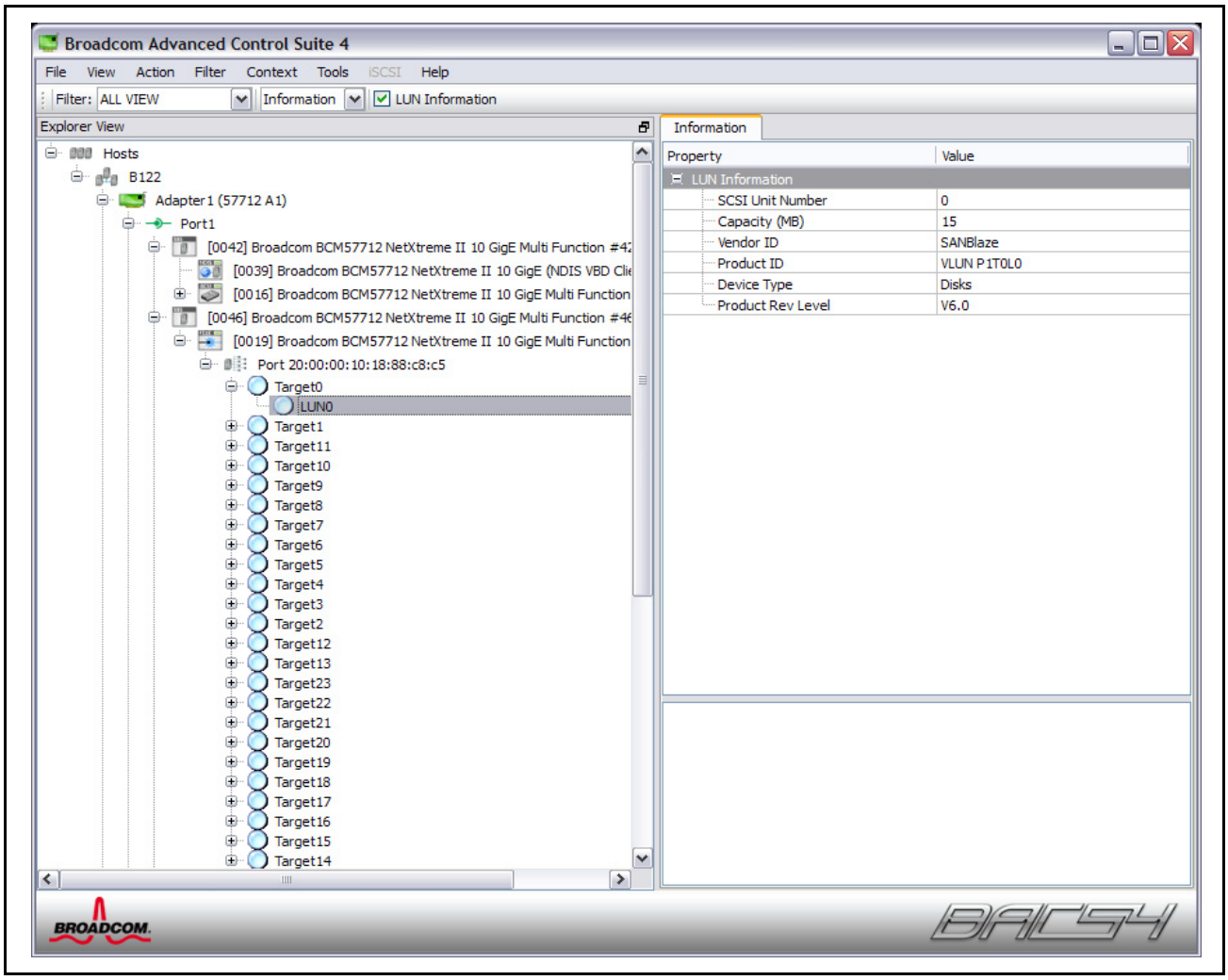


Figure 35: Information Tab for LUN

The **LUN** object is not a configurable object. The **Information** tab provides the following information.

SCSI Unit Number: Displays the SCSI LUN number of the selected LUN.

Capacity: Displays the capacity of the LUN in MB.

Vendor ID: Displays the vendor ID of the selected LUN. This usually represents the manufacturer of the storage system where the LUN is created.

Product ID: displays the model number of the storage system where the LUN is created.

Device Type: Displays the device type of the LUN.

Product Rev Level: Displays the software/Firmware version number of the LUN.

Managing iSCSI Device

The iSCSI function represents the iSCSI functionality available under the PCI Function. User can view current values of various iSCSI driver parameters, configure iSCSI driver parameters, view attached iSCSI targets and LUN information by selecting iSCSI object in object explorer panel.

The available tabs for the iSCSI function are as follows:

- Information Tab
- Configuration Tab
- Diagnostic Tab
- Statistics Tab

Note: The Diagnostic and Statistics tab are not available on Linux managed hosts.

Information

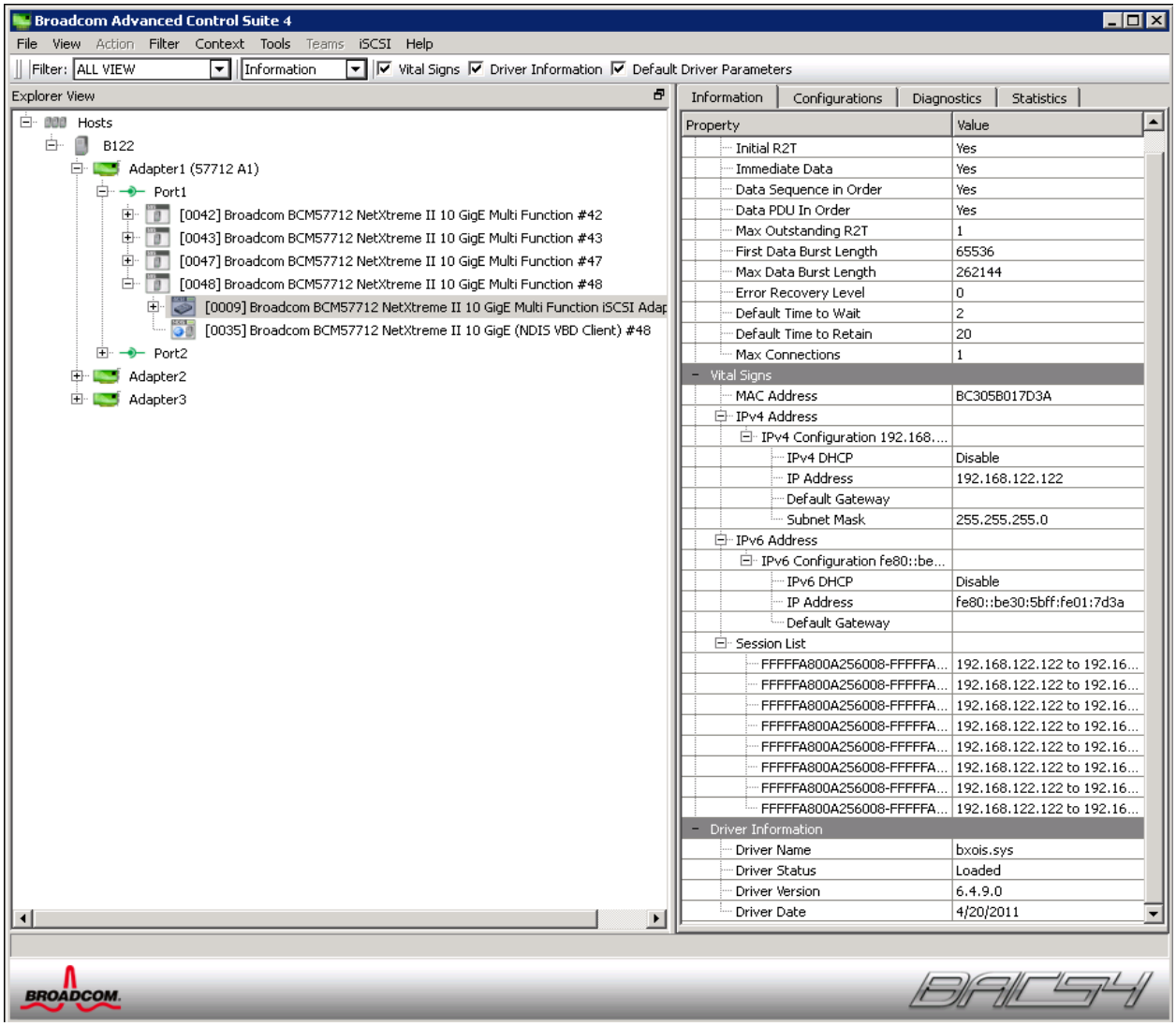


Figure 36: Information Tab for iSCSI Device

The Information tab has the following two sections and related parameters under it.

Driver Information

Driver Name: Displays installed iSCSI driver file name.

Driver Status: Displays if iSCSI driver is loaded or not.

Driver Version: Displays the iSCSI driver version information.

Driver Date: Displays iSCSI driver release date.

Vital Signs

MAC Address: Displays the current burned-in iSCSI MAC address configured for the iSCSI function.

Session List: Displays the current list of iSCSI sessions created by the initiator. The information includes the session numbers and the iSCSI target portal IP addresses.

IPv4 Addresses

IPv4 DHCP: Displays whether IPv4 address is statically configured or if DHCP is assigning the IP address.

IP Address: Display the current value of IPv4 address.

Default Gateway: Displays the default gateway IP address.

Subnet Mask: Display the current value of the subnet mask.

IPv6 Addresses

IPv6 DHCP: Displays whether IPv6 address is statically configured or if DHCP is assigning the IP address.

IP Address: Display the current value of IPv6 address.

IPv6 Scope ID: Displays the current value of IPv6 scope ID.

IPv6 Flow Info: Displays the current value of IPv6 flow info.

Default Gateway: Displays the default gateway IP address.

Default Driver Parameters

*I*nitial R2T: Displays if Initial R2T is enabled or not.

Immediate Data: Displays if Immediate Data is configured or not.

- If ImmediateData is set to Yes and InitialR2T is set to Yes (default), then only immediate data are accepted in the first burst.
- If ImmediateData is set to No and InitialR2T is set to Yes, then the initiator will not send unsolicited data.
- If ImmediateData is set to No and InitialR2T is set to No, then the initiator will send unsolicited immediate data, but MAY send one unsolicited burst of Data-Out PDUs.
- If ImmediateData is set to Yes and InitialR2T is set to No, then the initiator MAY send unsolicited immediate data and/or one unsolicited burst of Data-Out PDUs.

Data Sequence in Order: Displays if Data sequence in order is enabled or disabled.

Data PDU in Order: Displays if Data PDU in order is enabled or disabled.

Max Outstanding R2T: Displays the current configured value of maximum outstanding R2T.

First Data Burst Length: Display the maximum length of the data in bytes, initiator will send in the first frame.

Max Data Burst Length: Display the maximum length of the data in bytes, initiator will send during the iSCSI session.

Error Recovery Level: Displays the current level of error recovery configured.

Default Time to Wait: Displays the current value of default time to wait.

Default Time to Retain: Displays the current value of default time to retain.

Max Connections: Displays the current value of maximum connections allowed.

Configuration

The configuration tab allows users to modify some of the configurable parameters of the iSCSI driver.

1. Select iSCSI **function** in the Object Explorer window.
2. Click the **Configurations** tab.
   The following parameters can be configured at the configurations tab.
   VLAN ID: Allows user to configure VLAN ID for the selected iSCSI interface.
   MTU: Allow configuring MTU for the iSCSI interface.
   IPv4 Configuration: Determines if iSCSI interface acquires the IPv4 address from DHCP or not.

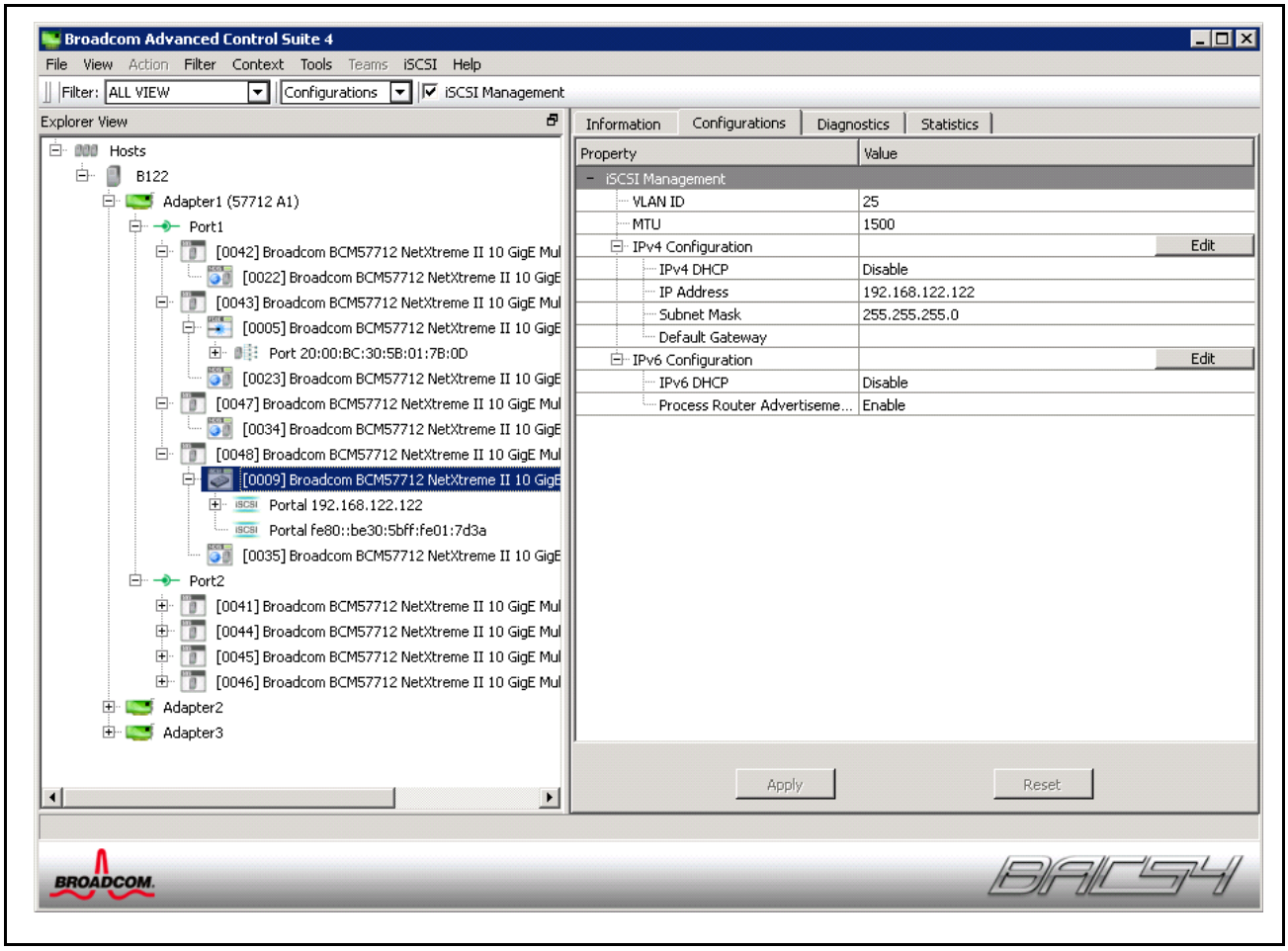


Figure 37: Configuration Tab for iSCSI Device

IP Address: If DHCP is disabled then allows user to configure static IP address for the iSCSI interface.

Subnet Mask: Allows user to configure subnet mask for the iSCSI interface.

Default gateway: Allows user to configure default gateway for the iSCSI interface.

IPv6

IPv6 DHCP: Determines if iSCSI interface acquires the IPv6 address from DHCP or not.

Process Router Advertisements: Determines if iSCSI interface will process the router advertisement or not.

Diagnostics

The **Diagnostic** will allow user to perform an iSCSI ping to any IP address.

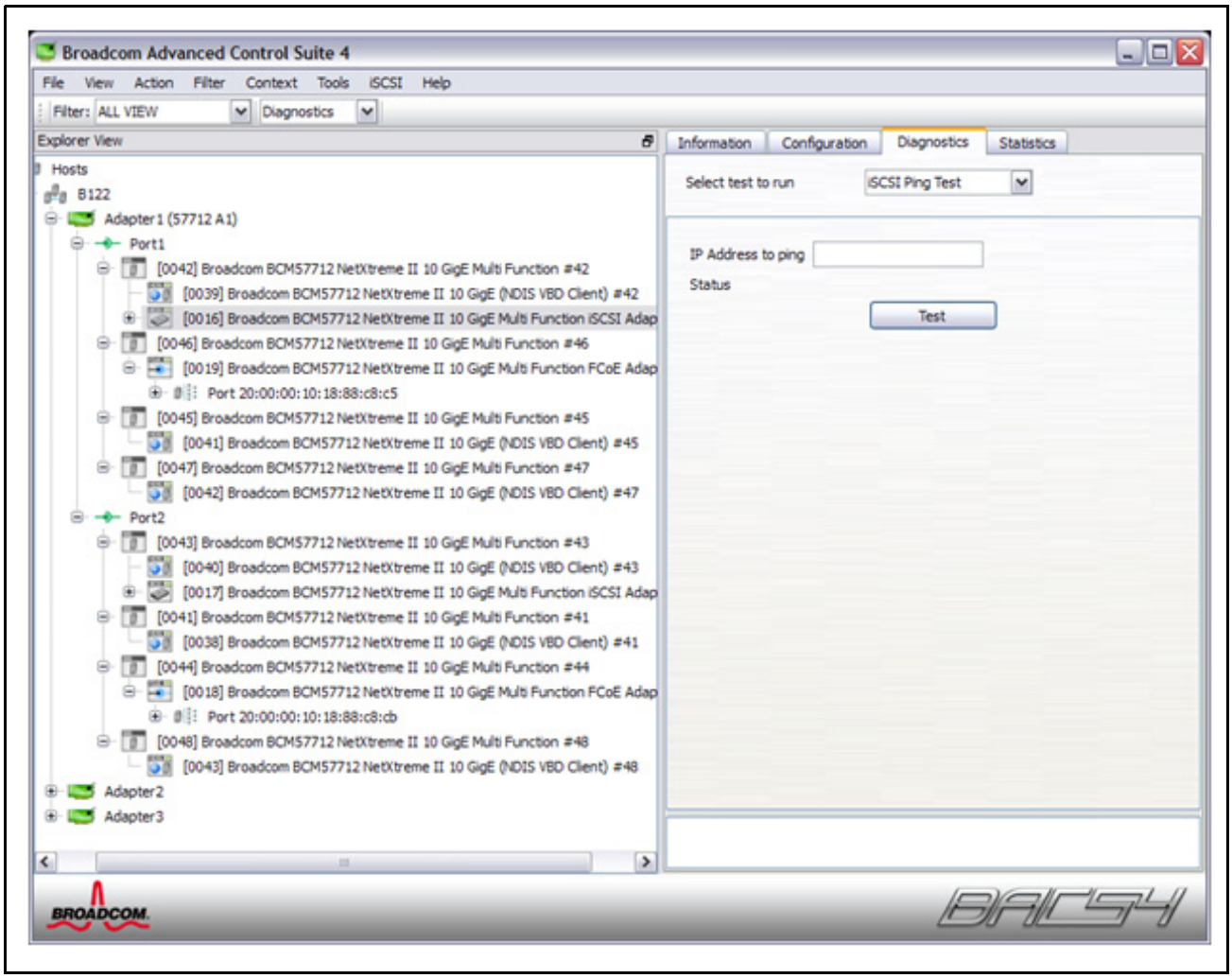


Figure 38: Diagnostics Tab for iSCSI Device

1. Select the appropriate iSCSI interface in the object explorer panel.
2. Select **Diagnostic** tab.
3. Select **iSCSI Ping Test** from **Select test to run** drop down menu.
4. Enter valid IP address for which the connectivity needs to be tested in **IP Address to ping** field.
5. Click **Test** button.
   The **Status** at the end of the test will give the test result.

Note: This tab is not available on Linux host.

Statistics

The **Statistics** allow a user to look at various statistical counters for the iSCSI interface.

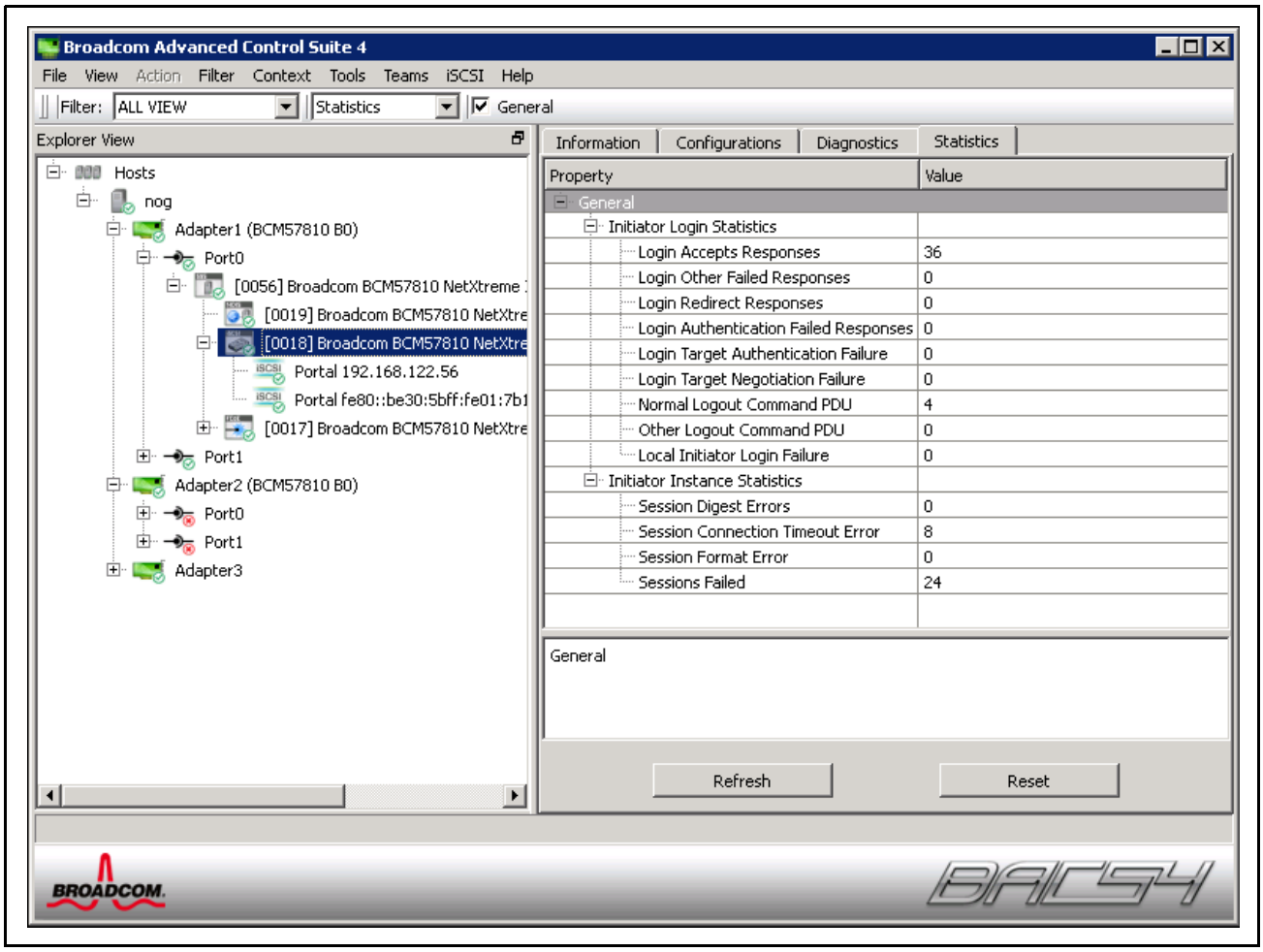


Figure 39: Statistics Tab for iSCSI Device

Note: This tab is not available on Linux managed hosts.

There are two buttons at the bottom the tab as follows.

Refresh: Clicking this button immediately refreshes the **Statistics** information. If this button is not clicked, the statistical counter information is refreshed every 5 seconds.

Reset: Clicking this button resets all counters on the **Statistics** tab to 0.

iSCSI Management Overview

The iSCSI management can be divided into three sections.

- Managing iSCSI Discovery Portals
- Managing iSCSI Targets
- Connection using the iSNS server

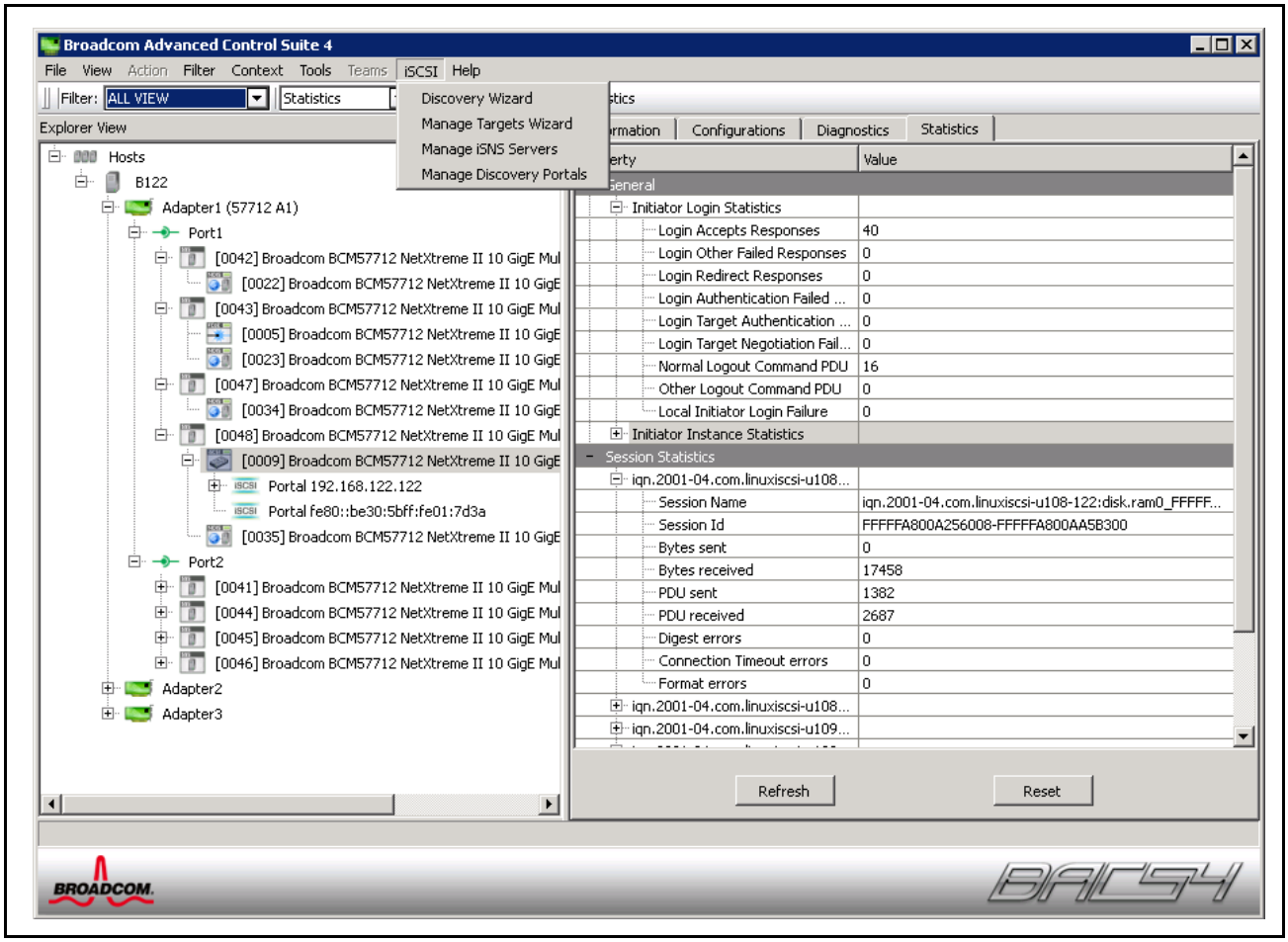


Figure 40: iSCSI Management

The first step in creating iSCSI sessions to iSCSI targets is to define the iSCSI Discovery Portal. It can be easily done in BACS4 via the Managing Discovery Portals" wizard. An iSCSI portal is a target IP address and port number pair. If the port number is not specified then default port number of 3260 is used. Discovery is the process of an initiator requesting target portal for a list of it's targets. Most of the time, using discovery on a target portal is the proffered way to get connected. You can however, alternatively specify the portals and targets you wish to use. The third way of discovery and connecting to the target is by way of iSNS (Internet Storage Name Service) server.

Managing iSCSI Discovery Portals

Managing discovery portal can be performed using the “Manage Discovery Portals” wizard, using the procedure below.

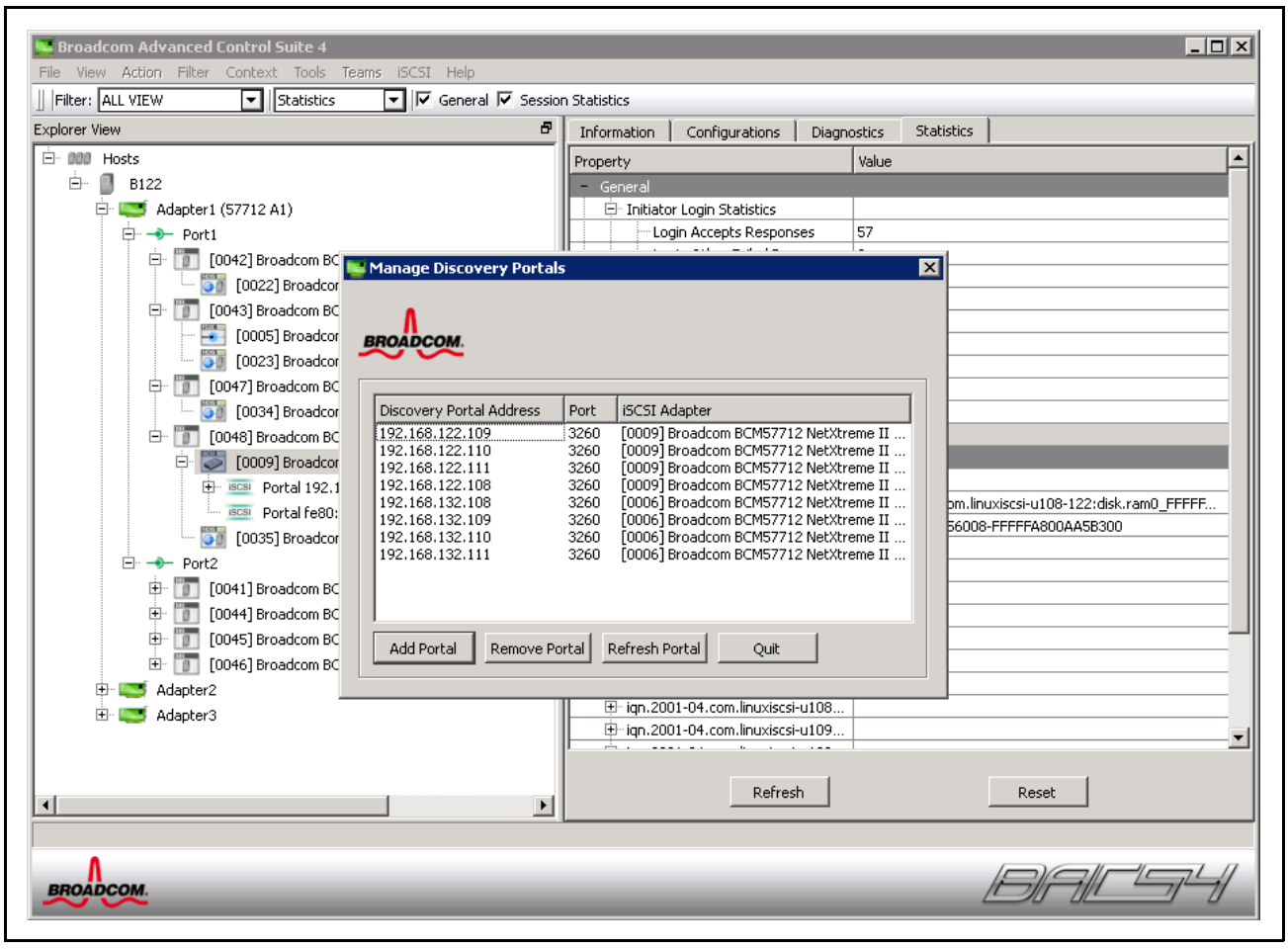
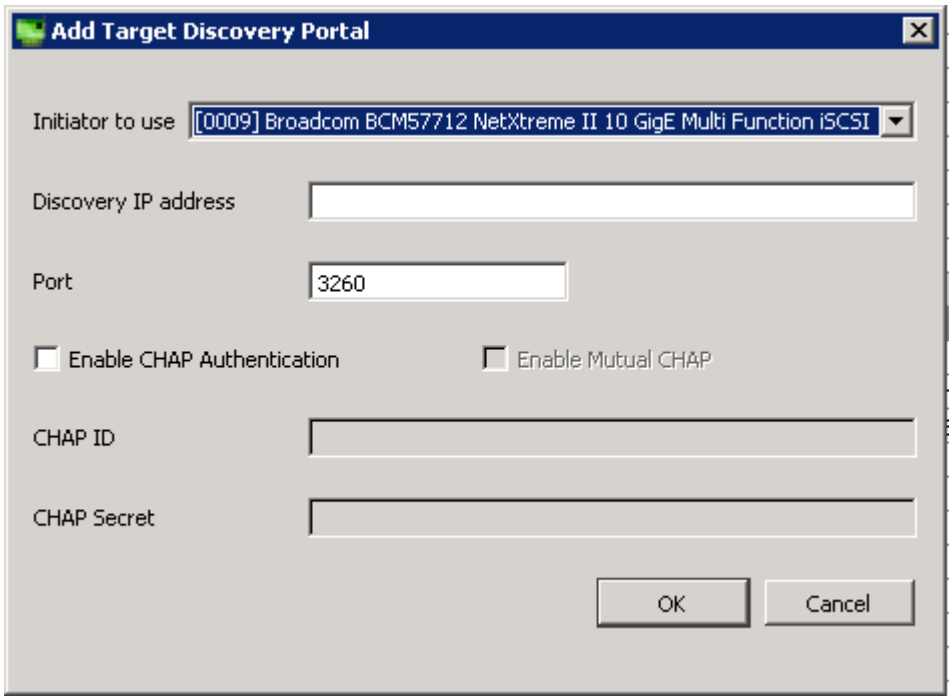


Figure 41: Manage Discovery Portals

1. Select the appropriate iSCSI interface in the objet explorer panel.
2. Select menu option **iSCSI**.
3. Select **Manage Discovery Portals**.
4. Click **Add Portal button**.



5. Select the initiator under the **Initiator to use** drop down menu.
6. Enter the **Discovery IP address**. This is the IP address of the iSCSI target.
7. Enter the **Port** number. The default port number is 3260.
8. If CHAP is configured on the target then select the **Enable CHAP Authentication** check box.
9. Select **Enable Mutual CHAP** check box if two way CHAP authentication is configured. In two way authentication both initiator and target authenticate each other.
10. Enter the CHAP ID string in **CHAP ID** field.
11. Enter the **CHAP Secret**. This CHAP ID and secret should be configured on the target before selecting this option on the initiator.
12. Click **OK**.

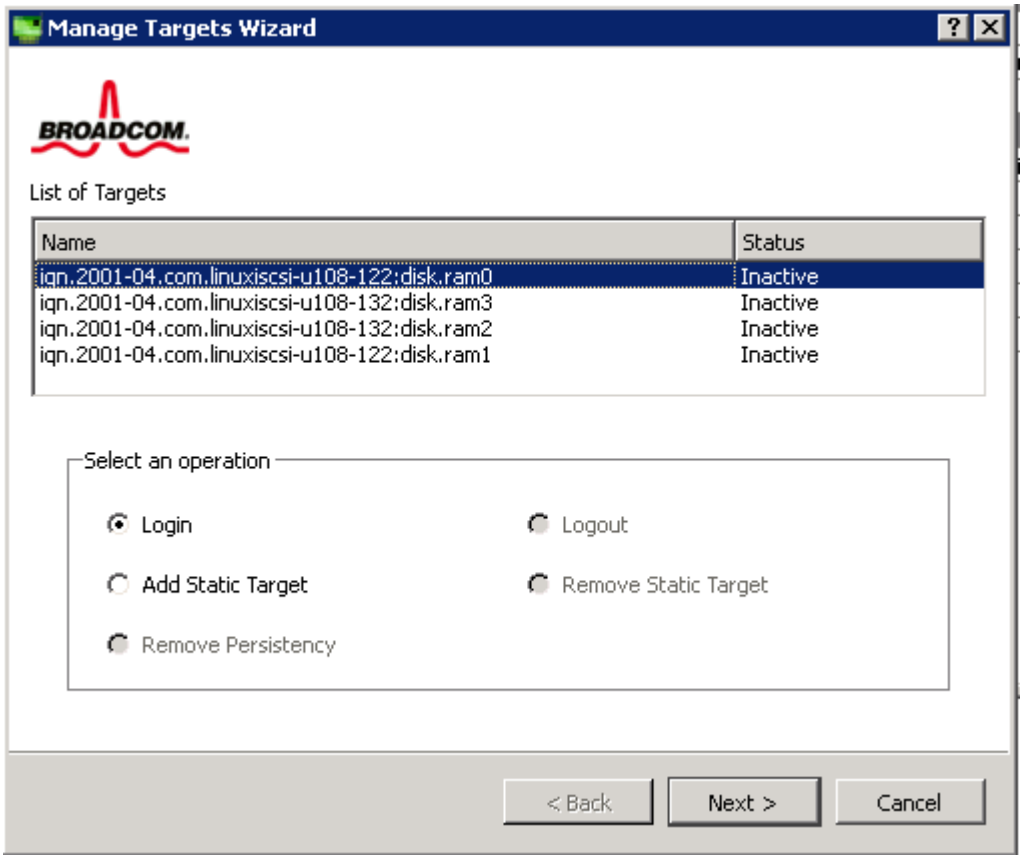
    The newly added Target IP address will be displayed in the Manage Discovery Portal dialogue box.
13. Repeat this procedure if you want to add more target IP addresses.
14. Click **Quit,** to exit the wizard.

Managing Targets Wizards

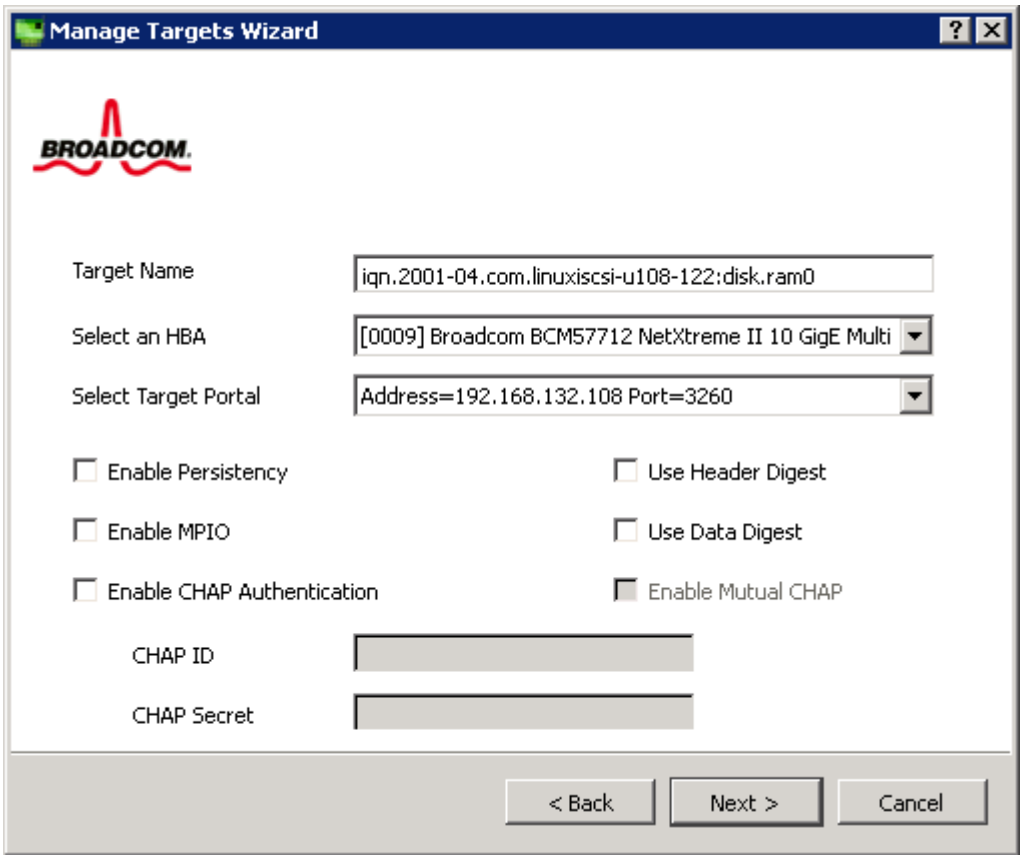
Once the Target portal IP address is configured, proceed with the managing targets. The Manage Targets wizard allows user to login to the target, logout of the targets, ad static target, remove static target and remove persistency.

Logging on to the Targets

1. Select **iSCSI** menu option.
2. Select **Manage Targets Wizard** option. A dialogue box similar to the one shown below will be displayed. All targets discovered on the target IP address will be displayed in the main window.



3. Select the target and verify that **Login** radio button is selected.
4. Click **Next**. The dialogue box similar to the one below will be displayed.
5. Select appropriate initiator from the **Select an HBA** drop down menu, if you have multiple initiators installed in the host.



6. Select appropriate target portal from **Select Target Portal** drop down menu.
7. The following options are available on this dialogue box:

   Enable Persistency: Selecting this option will enable the persistence connection to the target between the reboot.

   Enable MPIO: Selecting this option will enable the failover option for the target. The Microsoft failover software component (MPIO) is required to be installed on the host.

   Use Header Digest: Select this option if you want to enable the header digest for the target. Target should be configured with header digest for this option to work.

   Use Data Digest: Select this option if you want to enable the data digest for the target. Target should be configured with data digest for this option to work.

   Enable CHAP Authentication: Selecting this option will enable the CHAP authentication. The target should be configured for CHAP authentication and CHAP secret should be configured. This is a one way authentication in which only target authenticates the initiator. The secret is set just for the target and all initiators that want to access that target need to use the same secret to start a logon session with the target.

   Enable Mutual CHAP: Select this option if two way authentication is required between initiator and target. With this option selected, the target and the initiator authenticate each other. A separate secret is set for each target and for each initiator.
8. Click **Next**.
9. If you have more targets to manage, select **Manage more targets** and click **Next**.

10. Otherwise, select **Exit wizard** and click **Next**.

11. Click **Finish** to exit the wizard.

Logging Out of the Targets

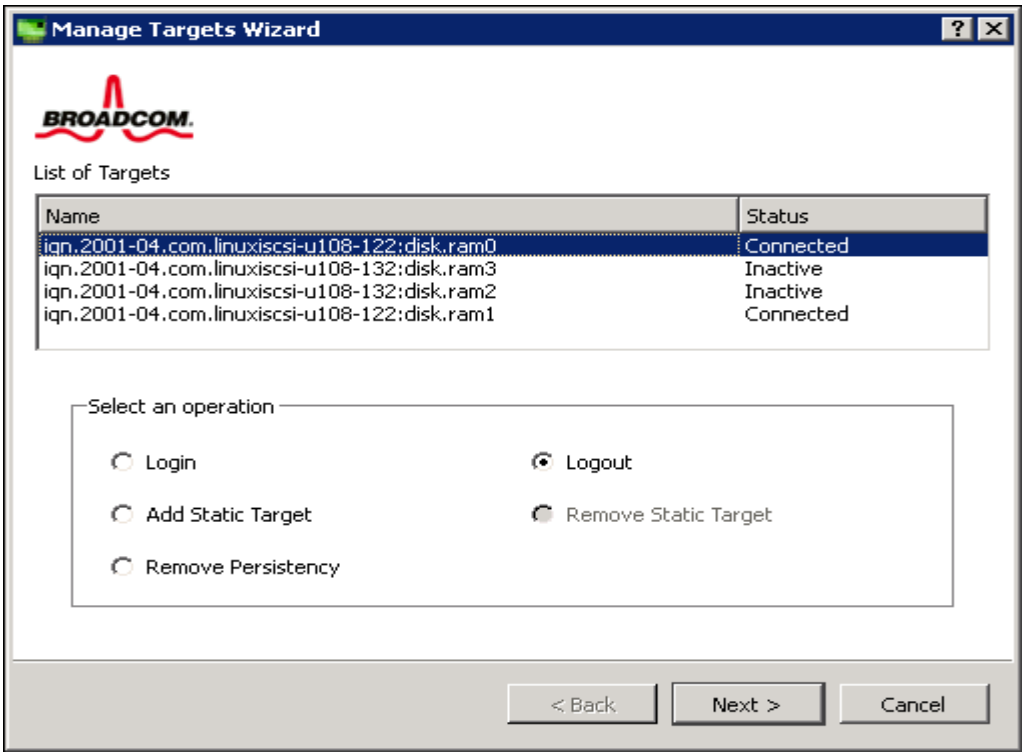


Figure 42: Manage Targets—Login

1. Select **iSCSI** menu option.
2. Select **Manage Targets Wizard** option. A dialogue box similar to the one in Figure 42 will be displayed. The **Status** column displays if initiator has logged in to the target or not.
3. Select the target to which initiator has active login session.
4. Select radio button **Logout**.
5. Click **Next**.
6. Select the session ID and click **Logout**.
7. Click **Next**.
8. If you have more targets to manage then select **Manage more targets** and click **Next**.
9. Otherwise, select **Exit wizard** and click **Next**.
10. Click **Finish** to exit the wizard.

Add Static Target

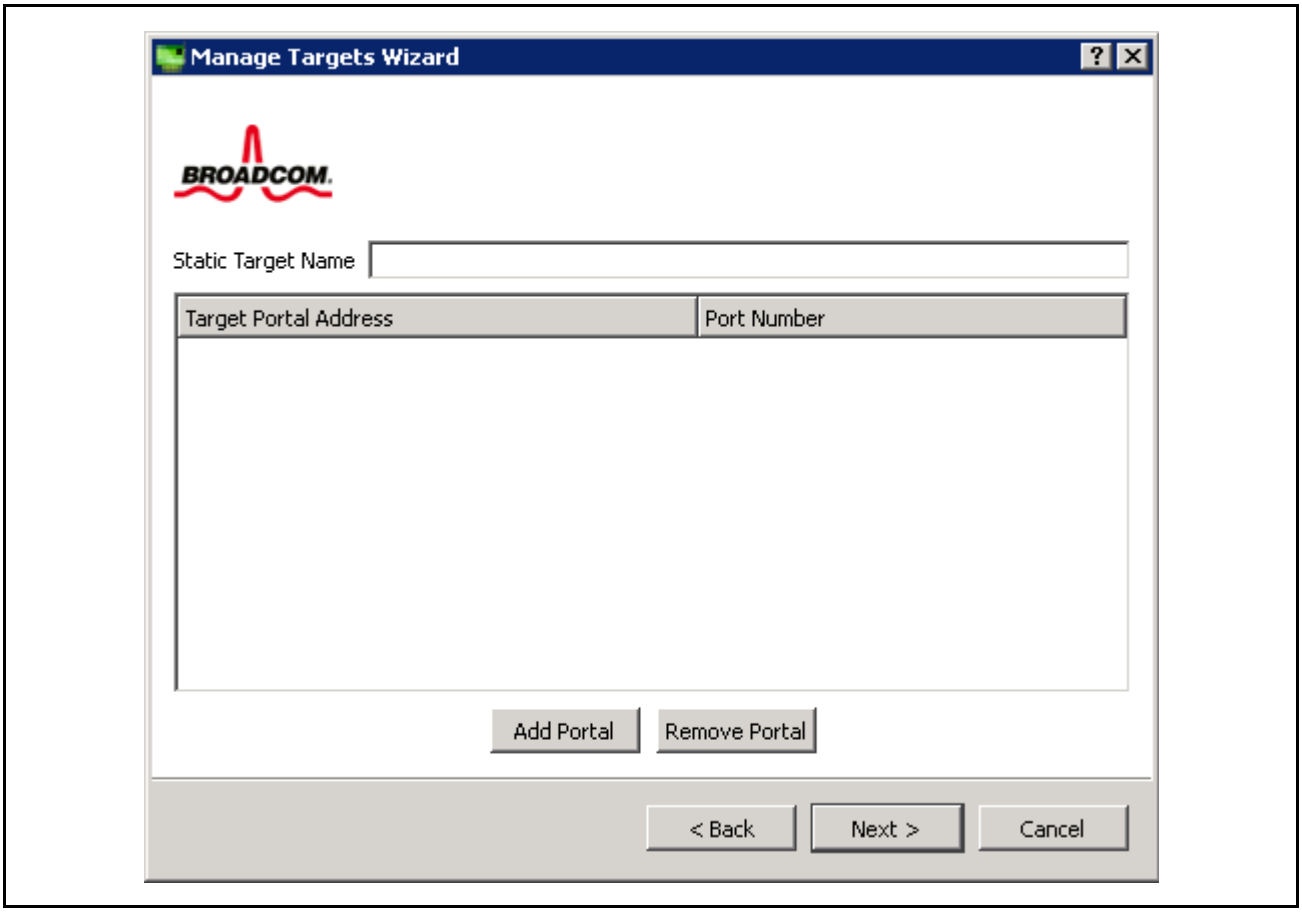


Figure 43: Add Static Target

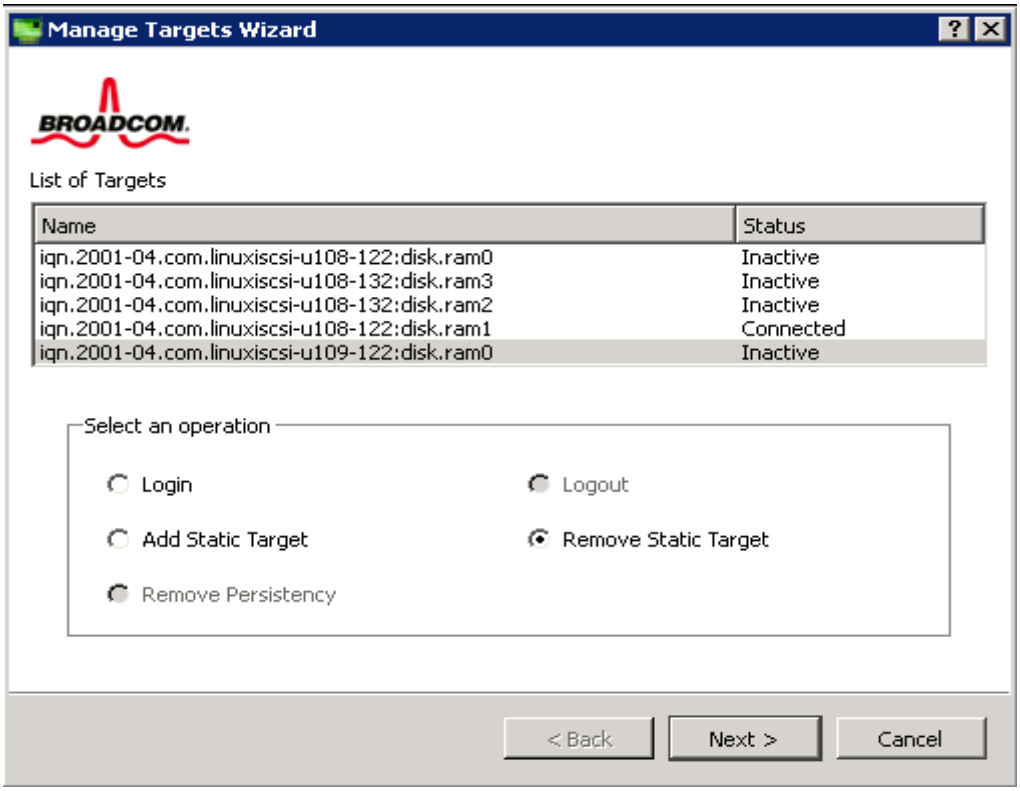
1. Select **iSCSI** menu option.
2. Select **Manage Targets Wizard** option. A dialogue box similar to the one in Figure 42 will be displayed.
3. Select radio button **Add Static Target.** A dialogue box similar to the one in Figure 43 will be displayed.
4. Click **Add Portal** button.
5. Enter the IP address of the target in **Target IP Address** field.
6. Enter the correct **Port** number. The default port number is 3260.
7. Once the target portal IP address is added successfully, enter in the name of the target in the **Static Target Name**.
8. Click **Next**.
9. If you have more targets to manage then select **Manage more targets** and click **Next**.
10. Otherwise, select **Exit wizard** and click **Next**.
11. Click **Finish** to exit the wizard.

12. To login to the static target added above, follow procedure mentioned in "Logging on to the Targets" on page 133.

Remove the Static Target

To remove the static target, there should not be an active login session on the target. Follow the steps mentioned in "Logging Out of the Targets" on page 135 to log out of the target. Once the initiator has logged out of the target, follow the procedure below to remove the static target.

1. Select the **iSCSI** menu option.
2. Select the **Manage Targets Wizard** option. A dialog box similar to the one in "Remove the Static Target" on page 137 will be displayed.
3. Select the static target that needs to be removed.
4. Select the **Remove Static Target** radio button.
5. Click **Next**.
6. If you have more targets to manage, select **Manage more targets** and click **Next**.
7. Otherwise, select **Exit wizard** and click **Next**.
8. Click **Finish** to exit the wizard.



Remove Persistency

To remove the persistency, there should not be an active login session on the target. Follow the steps mentioned in "Logging Out of the Targets" on page 135 to log out of the target which has a persistent configuration. Once the initiator has logged out of the target, follow the procedure below to remove the persistency.

1. Select the **iSCSI** menu option.
2. Select the **Manage Targets Wizard** option.
3. Select the static target that needs to be removed.
4. Select the **Remove Persistency** radio button.
5. Click **Next**.
6. If you have more targets to manage, select **Manage more targets** and click **Next**.
7. Otherwise, select **Exit wizard** and click **Next**.
8. Click **Finish** to exit the wizard.

Managing iSNS Servers

The iSNS protocol is an in industry standard designed to facilitate the automated discovery, management and configuration of iSCSI devices on a TCP/IP network. The iSNS server uses the Internet Storage management Service (iSNS) to provide provides central database of all iSCSI initiators and iSCSI targets for the easy management in a heterogeneous storage network.

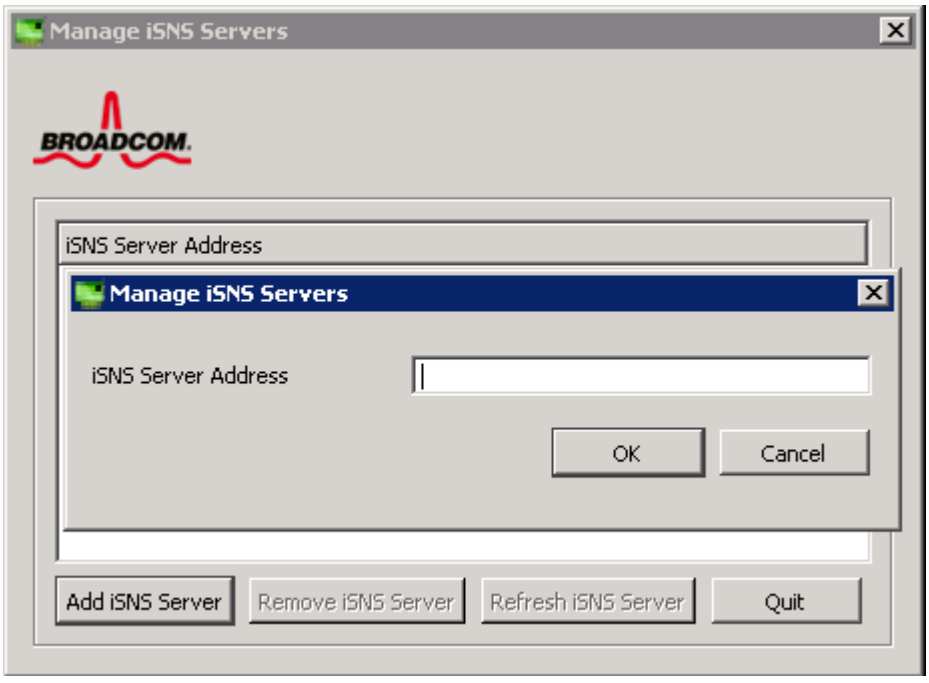


Figure 44: Add iSNS Server

1. Select the **iSCSI** menu option.
2. Select the **Manage iSNS Servers** option. See Figure 44.
3. Enter the IP address of the iSNS server.
4. Click **OK**.
5. Click **Quit** to exit the wizard.

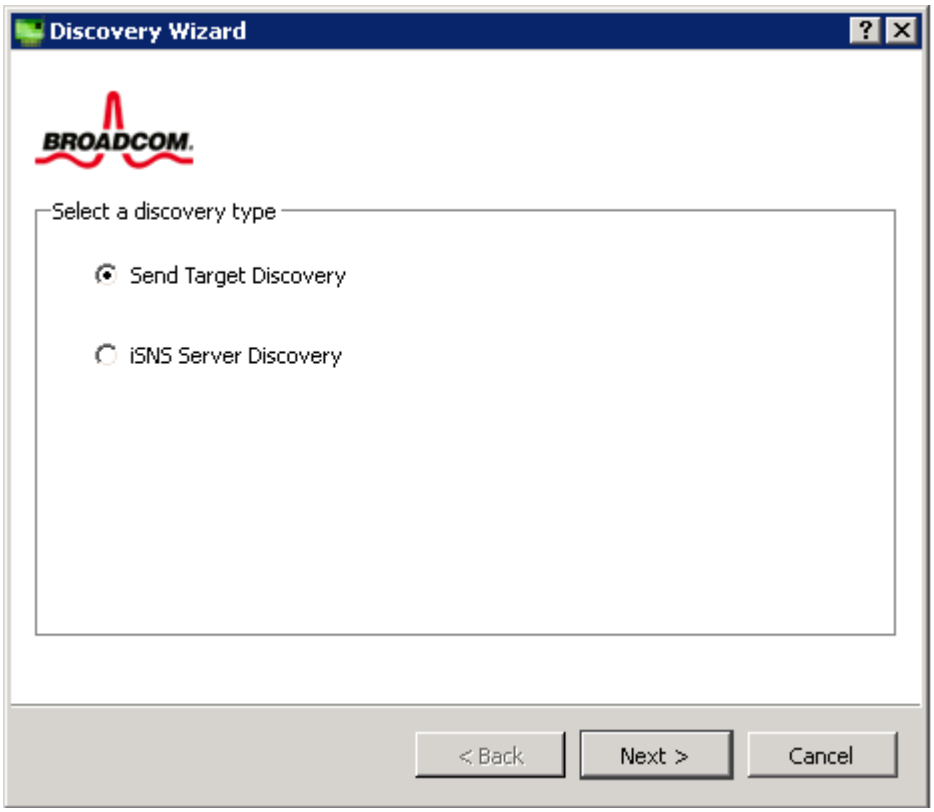
Once the targets register themselves with the iSNS server, the Manage Target Wizard can be used to login to the target.

Discovery Wizard

The Discovery Wizard option combines two operations in a one simple to use wizard. This option is designed for those users who are less familiar with iSCSI management function. It accomplishes this task by giving users an option to configure IP address for the initiator port and then define the discovery portals in a single wizard. It also gives user an option to use iSNS server IP address configuration. The wizard stars with an option to select method of discovery -- Send Target Discovery or iSNS Server Discovery.

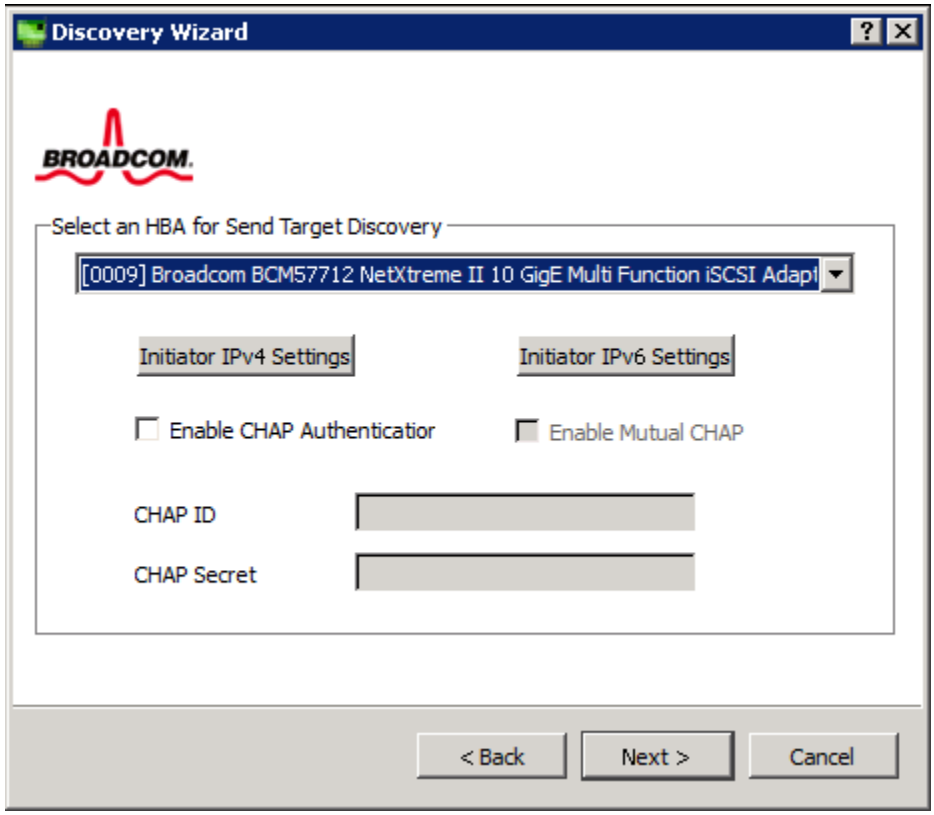
Send Target Discovery

1. Select **iSCSI** menu option.
2. Select the **Discovery Wizard** option.



3. Select **Send Target Discovery** option.

4. Click **Next**.
5. Select the adapter you would like to manage under **Select an HBA for Send Target Discovery** drop down menu.



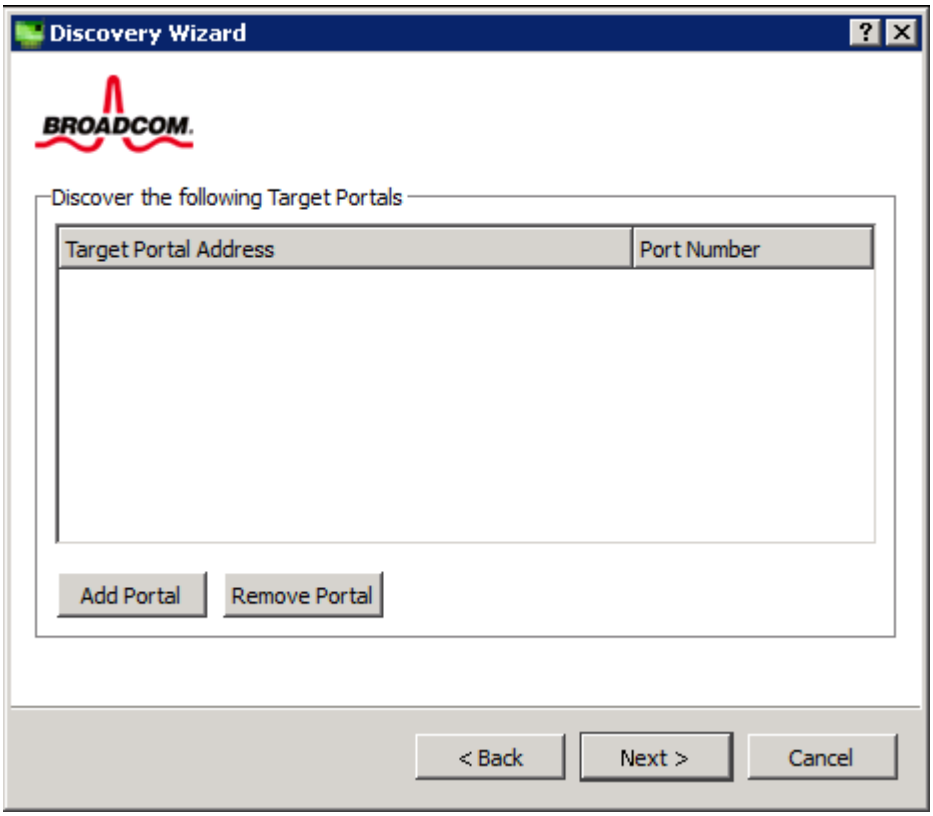
6. Click **Initiator IPv4 Settings** or **Initiator IPv6 Settings** to configure IPv4 address or IPv6 address related parameters for the adapter port.

   You can also configure DHCP for the adapter port.

7. Select **Enable CHAP Authentication** or **Enable Mutual CHAP**, if CHAP authentication is desired.

   Enable CHAP Authentication: Selecting this option will enable the CHAP authentication. The target should be configured for CHAP authentication and CHAP secret should be configured. This is a one way authentication in which only target authenticates the initiator. The secret is set just for the target and all initiators that want to access that target need to use the same secret to start a logon session with the target.

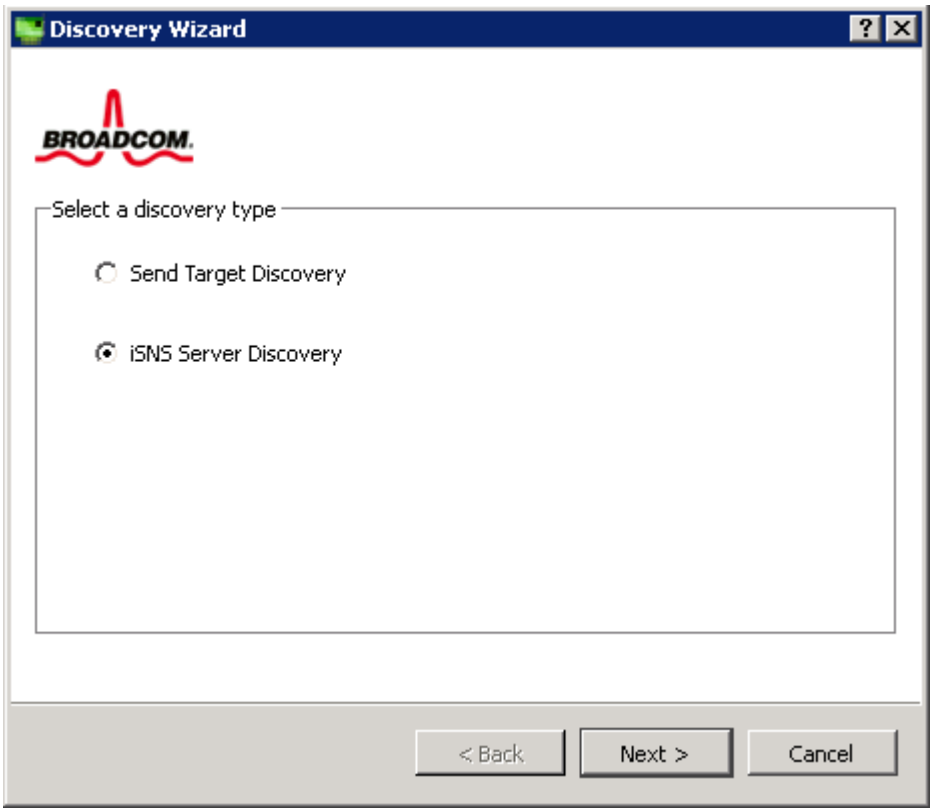
   Enable Mutual CHAP: Select this option if two way authentication is required between initiator and target. With this option selected, the target and the initiator authenticate each other. A separate secret is set for each target and for each initiator.



8. Click **Add Portal** button to add target portal IP address and click **Next**.
9. Enter the IP address of the target on the next dialogue box and click **Next**.
10. Click **Finish** to exit the wizard.
11. Follow the procedure in "Logging on to the Targets" on page 133 to login to the targets discovered above.

iSNS Server Discovery

1. Select **iSCSI** menu option.
2. Select **Discovery Wizard** option.
3. Select **iSNS Server Discovery** option.
4. Click **Next**.
5. Enter the IP address of the iSNS server in the **iSNS Server Address** field.
6. Click **Next**.



7. Enter the IP address of the iSNS server in the **iSNS Server Address** field.
8. Click **Next**.
9. Click **OK** when an informational message is displayed.
10. Click **Finish** to exit the wizard.
11. Follow procedure mentioned in "Logging on to the Targets" on page 133 to login to the targets discovered above.

Appendix A: CLI Command Usage

POSIX-Compliant Commands

```
BACScli [-t <target type>] [-f <target ID format>] [-i <target ID>] [-r <IP address>] [-n <port>]
[-a digest | basic] [-u <username>] [-p <password>] <command string>
```

- The -t option is used to select the type of the target, it must be followed by the <target type> that can be VBD, NDIS, iSCSI, iSCSI Portal, iSCSI Target, TEAM, VNIC, FCOE, FCoE Target, PhyAdapters, PhyPorts, HOST or system.
- The -f option is used to select the format of the <target ID> used in the -i option. The <target ID format> can be MAC, BDF, or NAME.

  The MAC and BDF are used to select a device of a <target type>.

  The NAME is used to select either a Team or a Virtual adapter.
- The -i option is used to select the target identified by the <target ID>.

  The <target ID> can be the Ethernet MAC address (using the NDIS device's MAC address for Ethernet and using the iSCSI device's MAC address for iSCSI Hardware Offload and using the teaming MAC address for VDB), the PCI Bus/Device/Function number, or the name of a Team/Virtual adapter.
- The -r option is used to specify an IP address of a host to be accessed.
- The -n option is used to select a port on a host to be accessed.
- The -a option is used to select either digest or basic authentication mode.

  The default authentication mode is basic.
- The -u option is used to specify a user name.
- The -p option is used to specify password.
- The <command string> includes the command, its options, parameters, and values for the command. <command string> have to be specified within the double quotes, but if the <command string> contains only one command without any option or command argument, the double quotes is optional.
- If any name or parameter contains special character such as '^', '&' and so on, it needs to be specified in double quotes, "^" for example.

The following lists the available commands:

add: Add team configuration from a file

adddiscoveryportal: Add a discovery portal to the host

addhost: Add a remote host for management

addisnsserver: Add the IP address or DNS name of an iSNS server to the list of iSNS servers

addtarget: Manually configure a target and optionally persist that target

bootcfg: Use this command to do MBA/FCoE/iSCSI boot configuration

cablediag: Run cable diagnostic tests on the selected PhyPort device

cfg: Configure parameter of the selected device

createnpivport: Create an NPIV port

diag: Configure and conduct a diagnostic test

discoverhost: Search and add remote hosts from a range of IP addresses

fallback: Fallback to primary adapters from standby

help: List available commands

info: Display adapter information of the selected NIC

list: List target items in different views

listisnsservers: Display the list of iSNS server addresses that are persisted by the iSCSI Initiator service.

listdiscoveryportals: Display the list of persisted target portals

log: Log all input and output into a file

login: Log in to an iscsi target

logout: Log out of an iscsi target

networkdiag: Run network diagnostic test on the selected NDIS device

q: exit the program

refresh: Scan the system for hardware/configuration changes

refreshall: Scan all systems for hardware/configuration changes

refreshdiscoveryportal: Perform a SendTargets operation to the target portal

refreshisnsserver: Refresh the list of targets discovered from the specified iSNS server

remove: Remove a team

removediscoveryportal: Remove discovery portal from the host

removeallhosts: Remove all hosts from the host management list

removehost: Remove a host from the host management list

removeisnsserver: Remove the IP address or DNS name of the iSNS server from the persisted list of iSNS servers

removenpivport: Remove an NPIV port

removepersistenttarget: Remove a target from the list of persistent targets

removetarget: Remove a target from the list of persisted targets

resetsessionstats: Display session statistics for all or the selected session

resetstats: Reset the statistics

restore: Restore team configuration from a file

save: Save team configuration to a file

select: Select an adapter or List available adapters

sessions: Display list of iSCSI sessions on the selected iSCSI adapter.

sessionstats: Display session statistics for all or the selected session

showsel: Show the selected target item

stats: Display statistic information of the selected NIC

unassigned: Display adapters that are not yet part of a team

version: Display the version of this program

Applicable Commands for Each Item View

All:

- addhost
- discoverhost
- help
- list
- log
- q
- removeallhosts
- removehost
- select
- showsel
- version

FCoE:

- cfg
- createnpivport
- info
- removenpivport
- resetstats
- stats

FCoETarget:

info

FCPort:

info

Host:

- adddiscoveryportal
- addisnsserver
- addtarget
- cfg
- info
- listdiscoveryportals
- listisnsservers
- login
- logout
- refresh
- refreshall
- refreshdiscoveryportal
- refreshisnsserver
- removediscoveryportal
- removeisnsserver
- removepersistenttarget
- removetarget

iSCSI:

- cfg
- info
- login
- logout
- pingtest
- resetsessionstats
- resetstats
- sessions
- sessionstats
- stats

iSCSIPortal:

- info
- resetsessionstats
- sessionstats

iSCSITarget:

- info
- login
- logout
- removepersistenttarget
- resetsessionstats
- sessionstats

LUN:

info

NDIS:

- cfg
- info
- networkdiag
- resetstats
- stats

PhyAdapter:

- cfg
- info

PhyPort:

- bootcfg
- cablediag
- cfg
- diag
- info
- resetstats
- stats

Teamview:

- add
- fallback
- info
- Remove
- resetstats
- restore
- save
- stats
- unassigned

VBD:

- cfg
- info
- resetstats
- stats

VNIC:

- info
- networkdiag
- resetstats
- stats

Command Syntax

```
add [-h <host>] <file>
```

- The `add <file>` command adds team configuration from the specified <file>. The existing team configuration is preserved and a new team(s) is added to the system from the configuration file.
- This command is only available if the active selection is a team and/or in the team view.
- The `-h` option is needed if there is no team selected and application need to know which host the teams will be added to.

  Example:
  `add "c:\test.txt"`

```
adddiscoveryportal  {-m <iSCSI HBA MAC Address>} {-i <TargetPortalAddress>}
[-n <TargetPortalSocket>] [-u <CHAP name>] [-p <CHAP secret>] [-mu]
```

- Adds a static target portal to the list of target portals to which the iSCSI initiator service transmits SendTarget requests.
- If a value was not specified for the `-n` option, the default 3260 port number is used.
- If the CHAP name and CHAP secret are both not empty, CHAP authentication is used for login.
- `-mu` specifies the Mutual CHAP Authentication type is used.
- The `adddiscoveryportal` command is available in the context of a host.

```
addhost < [ < localhost | <local host name> | <local host IP> ] |
[ -u <username> -p <password> <host name | IP address> ] >[-a <digest | basic>]  [-n <port>]
[-protocol <wmi | cimxml | wsman | all>][-scheme <http | https>] [-persist]
```

- `-u` <username> is used to specify a user name.
- `-p` <password> is used to specify password.
- `[-a <digest | basic>]` is used to select either digest or basic authentication mode.

  The default authentication mode is basic.
- The `[-n <port>]` option is used to specify a port.
- The `[-protocol <wmi | cimxml | wsman |all>]` option is used to specify connection protocol.

`wmi` is for Windows host, `cimxml` is for the Linux host, `wsman` can be used for both window and Linux host and `all` is to try all protocol for unknown host types.

- `host name` is the name of a host to be connected.
- `IP address` is the IP address of a host to be connected.
- The `[-persist]` option indicates the host information will be saved to the persistent hosts file when user closes the bacscli application with the `-q` command. All the hosts in the saved file are automatically connected when BACSCLI starts. Use Ctrl+break to break the operation of connecting to the persistent remote hosts.

```
addisnsserver {-i <iSNS Server Address>}
```

- Adds the iSNS server identified by the `-i` option input parameter.
- The `addisnsserver` command is available in the context of a host.

```
addtarget {-t <TargetName>} {-i <TargetPortalAddress>} {-n <TargetPortalSocket>}
```

- Adds the specified target to the list of static targets.
- The `addtarget` command is available in the context of a host.

```
bootcfg [-t {iscsi | fcoe | mba}] [-o show [General | Initiator | Target | MPIO]]
[-o {save <filename.xml> | restore <filename.xml>}]
```

- This command is only available in the context of a physical port.
- This command displays the current iSCSI/FCoE/MBA boot configuration or one of its subcategory boot configuration, or saves the current iSCSI/FCoE/MBA boot configuration to a file, or restores the iSCSI/FCoE/MBA boot configuration from a file.
- The format of the file is xml.

```
cablediag
```

- The 'cablediag' command runs cable diagnostic tests on the selected device.
- This command is available on a Broadcom based NetXtremeI physical port device and/or NetXtremeII physical port device.
- Ctrl+break to stop the test.

```
cfg Advanced [[default]|[parameter]|[parameter=value]]
```

- The `cfg Advanced` command gets/sets the advanced parameters of the device.
- The `cfg Advanced default` command sets all advanced parameters to their default values.
- Both parameter and value are case insensitive and have to be specified within the double quotes. If it doesn't have any space or special characters inside, the double quotes are optional. If the value has a special character (such as &), a double quote can be used around &.
- No space is allowed around the '=' in the 'parameter=value'.
- The `cfg Advanced` command displays all advanced parameters and their current settings.
- The `cfg Advanced parameter` displays the current setting and all valid settings of the specified parameter.
- `cfg Advanced parameter=value` sets the specified value to the specified parameter.

- The parameter specified has to be one of those parameters that are displayed by the `cfg Advanced` command.
- The value specified has to be one of the valid settings of the parameters that are displayed by the `cfg advanced parameter`.
- This command is available if the actively selected device is a NDIS device.

  Example:

  - `cfg Advanced "Flow Control"="Auto"`
  - `cfg Advanced`
  - `cfg Advanced "Flow Control"`

`cfg Power [value]`

- The `cfg Power` command gets/sets Power Management of the device.
- The `value` is case insensitive and has to be specified within the double quotes. If it doesn't have any space or special characters, the double quotes is optional.
- The `cfg Power` command displays the current setting of the Power Management.
- `cfg Power value` sets the Power Management setting to the specified value. The <value> can be either Enable or Disable.
- This command is only available if the actively selected device is a NDIS device and is Power Management capable.

`cfg Licenses`

- The `cfg Licenses` command displays all License parameters and their current settings.
- This command is only available if the actively selected device is a VBD device and belongs to NetxtremeII family of devices.

`cfg Resource [[key]|[key=value]]`

- The `cfg Resource` command gets/sets the Resource keys of the device.
- Both key and value are case insensitive and have to be specified within the double quotes. If there are no spaces or special characters inside, the double quotes are optional.
- No space is allowed around the = in the `key=value`.
- The `cfg Resource` command displays all Resource Reservation keys and their current settings.
- This command is only available if the actively selected device is a VBD device and belongs to NetxtremeII family of devices.

  `cfg Resource` uses <key> and <value> to configure the Resource Reservation parameters. The use of <key> and its valid <value> are listed as follows:

  – The <key> CONFIGURABLE displays all the configurable Resource Reservation parameters with their current setting and valid settings. It does not require any <rsc_value>.

  – The <key> CONFIG sets the Offload Configuration to either First Come First Served or Reserved Resources. It does require the <value> that can be either FCFS or RSVD.

  – The <key> NDIS sets Preallocated Resources for NDIS to either Enable or Disable. It does require the <value> that can be either Enable or Disable.

- The <key> TOE sets Preallocated Resources for TOE to either Enable or Disable. It does require the <value> that can be either Enable or Disable.
- The <key> iSCSI sets Preallocated Resources for iSCSI to either Enable or Disable. It does require the <value> that can be either Enable or Disable.
- The <key> FCOE sets Preallocated Resources for FCOE to either Enable or Disable. It does require the <value> that can be either Enable or Disable.
- The <key> TOECONN sets TOE Connections to the number allowed in the range displayed in `cfg Resource CONFIGURABLE` command. It does require the <value> that has to be a number.
- The <key> iSCSICONN sets iSCSI Connections to the number allowed in the range displayed in `cfg Resource CONFIGURABLE` command. It does require the <value> that has to be a number.
- The <key> iSCSIPT sets iSCSI Pending Task per Connection to the valid numbers specified in `cfg Resource CONFIGURABLE` command. It does require the <value> that has to be a number.
- The <key> TOEPROTOCOL sets TOE Protocol Type to the valid settings specified in `cfg Resource CONFIGURABLE` command. It does require the <value> that has to be either Ipv4 or IPv6.
- The <key> iSCSIPROTOCOL sets the iSCSI Protocol Type to the valid settings specified in `cfg Resource CONFIGURABLE` command. It does require the <value> that has to be either Ipv4 or Ipv6.
- The <key> MEMCONSUMPTION sets the iSCSI Memory Consumption to the valid settings specified in `cfg Resource CONFIGURABLE` command. This command only applies to 57710/57711 adapter. It does require the <value> to be a percentage value from 25% - 100% with the increment of 25%.
- The <key> TOERSS sets the TOE RSS to either Enable or Disable. This command only applies to 57710/ 57711 adapter. It does require the <value> that can be either Enable or Disable.

Examples:

a. `cfg Resource Configurable`

b. `cfg Resource TOE=Disable`

c. `cfg Resource MEMCONSUMPTION=75`

`cfg iSCSIMgmt [[key]|[key=value]]`

- The cfg iSCSIMgmt command gets/sets the iSCSIMgmt keys of the device.
- Both key and value are case insensitive and have to be specified within the double quotes. If there are no spaces or special characters inside, double quotes are optional.
- No space is allowed around the = in the key=value.
- The cfg iSCSIMgmt command displays all iSCSI Management keys and their current settings.
- The cfg iSCSIMgmt key displays the current setting and all valid settings of the specified key.
- The cfg iSCSIMgmt key=value sets the specified value to the specified key.
- This command is only available if the actively selected device is a iSCSI device and belongs to NetxtremeII family of devices.

  The cfg iSCSIMgmt use <key> and <value> to configure the iSCSI Management parameters. The use of <key> and its valid <value> are listed as follows:

  - The <key> IPV4DHCP enables the DHCP of IPv4. The <value> can only be Enable. To disable DHCP, use IPV4ADDR to set the static IPv4 address and the DHCP automatically disables.
  - The <key> IPV4ADDR sets the static IPv4 address. The <value> is the IPv4 address. It l automatically disable the DHCP of IPv4.

- The <key> IPV4MASK is used to set the IPv4 Subnet mask. The <value> is the IPv4 Subnet mask.
- The <key> IPV4GATEWAY is used to set the default IPv4 gateway address. The <value> is the IPv4 gateway address.
- The <key> IPV6DHCP is used to enable the DHCP of IPv6. The <value> can only be Enable. To disable DHCP, use IPV6ADDR to set the static IPv6 address and the DHCP will automatically disable.
- The <key> IPV6PRA sets Process Router Advertisement. The <value> can be either Enable or Disable.
- The <key> IPV6ADDR is used to set the static IPv6 address. The <value> is the IPv6 address. It automatically disables the DHCP of IPv6.
- The <key> IPV6PL sets the IPv6 address subnet prefix length. The <value> is the IPv6 address subnet prefix length.
- The <key> IPV6DG is used to set the IPv6 default gateway address. The <value> is the IPv6 default gateway address.
- The <key> IPV6DGPL is used to set the IPv6 default gateway address subnet prefix length. The <value> is the IPv6 default gateway subnet prefix length.
- The <key> VLANID is used to set the Vlan ID for the iSCSI The <value> is the range of 0 — 4094.
- The <key> MTU is used to set the MTU for the iSCSI. The <value> is in the range of 1500 to 9600.

Note the following:

- When system is booted up through iSCSI HBA with a IPv4 address, the above IPv4 related parameters will be nonconfigurable, and not available in cfg iSCSIMgmt command.
- When system is booted up through iSCSI HBA with a IPv6 address, the above IPv6 related parameters will be nonconfigurable, and not available in cfg iSCSIMgmt command.

Example:

- `cfg iSCSIMgmt`
- `cfg iSCSIMgmt VLANID=3`
- `cfg iSCSIMgmt IPV4ADDR=172.16.100.140`

`cfg iSCSIBoot [[key]|[key=value]]`

- The 'cfg iSCSIBoot' command is to get/set iSCSIBoot keys of the device.
- Both key and value are case insensitive and have to be specified within the double quotes. If there are no spaces or special characters, double quotes are optional.
- No space is allowed around the = in key=value.
- The cfg iSCSIBoot command displays all iSCSIBoot keys and their current settings.
- The cfg iSCSIBoot key displays the current setting and all valid settings of the specified key.
- The cfg iSCSIBoot key=value sets the specified value to the specified key.
- This command is only available if the actively selected device is a NDIS device and the system is on a iSCSI boot using the selected NDIS device.

  The cfg iSCSIBoot use <key> and <value> to configure the iSCSI Management parameters. The use of <key> and its valid <value> are listed as follows:

  - The <key> 'CDUMP' is used to set the iSCSI Crash Dump. The <value> can be either Enable or Disable.

  Example:

  `cfg iSCSIBoot CDUMP=Enable`

`cfg OOBMgmt [-ipv4|ipv6|hostname] [[key]|[key=value]]`

- The cfg OOBMgmt command is to get/set OOBMgmt keys of the selected device.
- Both key and value are case insensitive and have to be specified within the double quotes. If it doesn't have any space or special characters, double quotes is optional.
- No space is allowed around the = in the key=value.
- This command is only available if the actively selected device is a NDIS device and is out-of-band management capable.
- The option `-ipv4|ipv6|hostname` is used to set the value of property Management Console Address. Among them:
  - -ipv4: verify the input value with IPv4 format
  - -ipv6: verify the input value with IPv6 format
  - -hostname: verify the input value with hostname format

    When none of the above options is given, it will be treated as the option `-hostname` is given.

    In addition, it will be ignored when one these options is put with other parameter together, and no error occurs.

Example:

- `cfg OOBMgmt`
- `cfg OOBMgmt "Heartbeat Retransmit Interval"`
- `cfg OOBMgmt "Heartbeat Retransmit Interval"=200`
- `cfg OOBMgmt "Management Console Address"=10.2.2.1`
- `cfg OOBMgmt -ipv4 "Management Console Address"=10.2.2.1`

`cfg Systoe [value]`

- The cfg Systoe command enables or disables TCP offload in chimney for the system. For Win7 kernel and later, user can also set TCP offload to automatic.
- The cfg Systoe command displays the current TCP Offload Chimney State.
- The cfg Systoe value enables or disables TCP offload in chimney for the system. For Win7 quotes are optional, command can also set TCP offload to automatic. This command is only available to the system target.

`cfg iSCSIInitiator [value]`

- The cfg iSCSIInitiator command is to display the name of iSCSI Initiator of the system.
- The cfg iSCSIInitiator name command is to set the name of iSCSI Initiator of the system.

`cfg iSCSISecret <value>`

The cfg iSCSISecret command is to set the CHAP secret of iSCSI Initiator of the system.

`cfg dcbx [ [-c <filename>] | [-s <filename>] ]`

- The `cfg dcbx` command configures DCBX settings on the selected physical port device.

- `cfg dcbx` displays the current configuration.
- `cfg dcbx -s` filename saves the current configuration into a XML file.
- `cfg dcbx -c` filename configures the DCBX settings from the specified XML file.
- This command is only available if the actively selected device is a physical port and DCBX configuration is allowed (like in 10G devices).

`cfg Advanced [[key]|[key=value]] under FCoE device level`

- The `cfg Advanced` command is used to configure FCoE settings.
- Both key and value are case insensitive and have to be specified within the double quotes. If it doesn't have any space or special characters, the double quotes are optional.
- No space is allowed around the = in the key=value.
- This command is only available if the actively selected device is a FCoE device.

```
cfg Multi-Function ["Multi-Function mode" | -s <filename> | -c <filename> |
-p port# [-f function#] key]
```

- The `cfg Multi-Function` command is used to configure physical adapter NIC partition settings.
- `cfg Multi-Function` displays the current configuration.
- `cfg Multi-Function -s filename` saves the current configuration into a XML file.
- `cfg Multi-Function -c filename` configures the NIC settings from the specified XML file.
- Use `cfg Multi-Function -c filename` to disable Multi-Function by setting <MultiFunctionMode> to SingleFunction. See "DCBX" on page 85 and "Resource" on page 86.
- `cfg multi-function -p 0 -f 2 \"FCoE\` displays port0 function2 FCoE configuration. The default function number is the first function of the specified port.
- All keys are case insensitive.

  Valid keys:
  - Multi-Function mode, -p and -f options not required.
  - FlowControl
  - Ethernet/Ndis
  - iSCSI
  - FCoE
  - MaxBandwidth
  - RelativeBandwidth
  - AFEX VIF Profile
  - AFEX VIF Profile List, -f option not required

`createnpivport {{-s <x:xx>} | {{-p <WWPN>} {-n <WWNN>}}}`

- -s: save mode, only 3 digits(1-3) allow to change.

  For example: 2x:xx:00:10:18:aa::bb::cc.

  Other digits are from current WWPN/WWNN.
- This command is available in the context of a FCoE HBA selection.

- Creates a NPIV port.

```
diag {[-c REG ] [-c MII ] [-c EEP] [-c MEM] [-c CPU] [-c INT] [-c MACLB ][-c PHYLB]
[-c LED] | [-c ALL]} [-l <cnt> ] [ -v <LEDIntv> ]
```

- The `diag` command is to configure the parameters of the Diagnostic test and run the test.
- The `diag` command displays all the tests available for the current selected target if no option is specified.
- If -l is not specified, the default iteration will be 1.
- If -v is not specified, the default LED interval will be 5.
- This command is available on a Broadcom based NetXtremeI physical port device and/or NetXtremeII physical port device.
- Ctrl+break to stop the test.

  Each individual test is indicated by the option as follows:
  - The `-c REG` is to run Control Register test.
  - The `-c MII` is to run MII Register test.
  - The `-c EEP` is to run EEPROM test.
  - The `-c MEM` is to run Internal Memory test.
  - The `-c CPU` is to run OnChip CPU test.
  - The `-c INT` is to run Interrupt test.
  - The `-c MACLB` is to run MAC Loopback test.
  - The `-c PHYLB` is to run PHY Loopback test.
  - The `-c LED` is to run LED test with the LEDIntv value.
  - The `-c ALL` is to run all the above tests.

  Example:
  - `diag -c ALL -l 3 -v 5`
  - `diag -c CPU -c LED -v 5`

```
discoverhost -s <start IP address> -e <end IP address> -u <username> -p <password>
[-a <digest | basic>] [-n <port>] [-protocol <wmi | cimxml | wsman | all>]
[-scheme <http | https> [-persist]
```

- `-s <start IP address>` is used to specify the starting IP address of searching range.
- `-e <end IP address>` is used to specify the ending IP address of searching range.
- `-u <username>` is used to specify a user name.
- `-p <password>` is used to specify password.
- `[-a <digest | basic>]` is used to select either digest or basic authentication mode.

  The default authentication mode is basic.
- `[-n <port>]` option is used to specify a port.
- `[-protocol <wmi | cimxml | wsman |all>]` option is used to specify connection protocol. `wmi` is for Windows host, `cimxml` is for Linux host, `wsman` can be used for both window and Linux host and `all` is to try all protocol for unknown host types.
- `host name` is the name of a host to be connected.

- `IP address` is the IP address of a host to be connected.
- `[-persist]` option indicates the host information will be saved to the persistent hosts file when user closes bacscli application with `q` command. All the hosts in the saved file will be automatically connected when BACSCLI starts.
- Ctrl+break to stop the operation.

`fallback`

- Fallback to primary adapters from standby.
- This command is only applicable for SLF-AFD team type.
- This command is only available in teamview view listing.

`help`

Lists the available commands

`info [ all | vitalsigns | driver | hardware | resource | os | initiator | dcbx | nicpartition ]`

Displays adapter information of the selected NIC. This version of the `info` command is available if the actively selected device is a NDIS device.

- `all`: Display information of all categories.
- `vitalsigns`: Display Vital Signs information.
- `driver`: Display Driver information.
- `hardware`: Display Hardware information.
- `resource`: Display Resource information.
- `os`: Display host operating system information.
- `initiator`: Display iscsi initiator information.
- `dcbx`: Display DCBX information.
- `nicpartition`: display NIC partition information.

Example:

- `info all`
- `info vitalsigns`

`info [all | members | livelink | general]`

Display adapter information of the selected team in the teamview view.

- `all`: Display all the information for a team.
- `members`: Display member devices for a team.
- `livelink`: Display livelink information for a team.
- `general`: Display general information for a team.

`list [-f MAC|BDF] [-b] [-r] [-h <host>][<view>]`

Lists the target items in different views.

Note:

- If `-f MAC` option is used, devices will be identified using the MAC address.
- If `-f BDF` option is used, devices will be identified using the bus/device/function numbers, the bus/device/function numbers are in HEX format.
- If `-f` option is not specified, the default behavior is to identify devices using MAC address.
- `-f MAC` option is not applicable to hosts, phyadapters & phyports devices because a single MAC address does not applicable to them.
- If `-b` option is useful only in the 'teamview'. If specified, the view will only list the team names for selection.
- If `-b` option is not specified, the default behavior is to list teams and the (physical/virtual) members that constitute the team.
- The `-h` option is useful in most of the commands. If specified, the view will only reflect the target list corresponding to the specified host.
- The `-r` option forces to reconnect, it is only valid when 'hosts' is used. This option is useful when users want to reconnect to a host which is recovered from reboot or linkdown.
- The `list` command is available in all views.
- Ctrl+break to stop the operation.

The available views are defined as follows:

- `devcon`: List devices by connection.
- `teamview`: List of teams and the devices that participate in a team.
- `ndis`: list NDIS devices.
- `vbd`: list VBD devices.
- `iscsi`: List iSCSI devices.
- `fcoe`: List FCoE devices.
- `iscsitargets`: List iSCSI targets.
- `fcoetargets`: List FCoE targets.
- `phyadapters`: List physical adapters on the system.
- `phyports`: List physical ports on the system.
- `hosts`: List the connected hosts.
- `luns`: List the LUNs.
- `vnic`: List virtual adapters in the system.
- `iscsiportal`: List iscsi portal devices.
- `fcport`: List FC port devices.

Example:

- `list -f MAC`
- `list`

`listisnsservers`

- Displays list of iSNS servers.
- `listisnsservers` command is available in the context of a host.

`listdiscoveryportals {-h <host>}`

- Displays the list of persisted target portals that the iSCSI initiator service will use for discovery for the specified host.
- `listdiscoveryportals` command is available in the context of a host.

`log [<file>]`

`file` is the log file name to save all the input and output. Without `file`, the current log file is closed. This command is available in all views.

`login {-m <iSCSI HBA MAC Address>} {-t <TargetName>} [-h <host>] [-i <TargetPortalAddress> ] [-n <TargetPortalSocket>] [-u <CHAP name>] [-p <CHAP secret>] [-b] [-e] [-d] [-o]`

- `login` command is available in the context of a host, in thecontext of a iSCSI device or in the context of a iSCSI Target.
- `-h` is only required when command is using on iSCSI target context, because a target might connect to HBA on different host.
- `-i` is an optional parameter. If '-i' option was specified, it mandatory to specify the '-n' option as well. That is, if the target portal IP address was specified, it is mandatory to specify the target port number as well.
- `login` operation will be performed using the HBA identified by the `-m` parameter and the target (identified by the `-t` parameter) and the target portal address.
- If CHAP name and CHAP secret are both not empty, then CHAP authentication will be used for login.
- Using the `-b` option specifies whether the connection should persist across reboot sessions.
- Using the `-e` option specifies use header digest for login.
- Using the `-d` option specifies use data digest for login.
- Using the `-o` option specifies enable MPIO.
- Using the `-mu` option specifies Mutual CHAP Authentication type.

`logout {-s <SessionId>} [-h <host>]`

- The `logout` command is available in the context of a host or in the context of a iSCSI device or in the context of a iSCSI Target.
- `-h` is only required when command is using on iSCSI target context, because a target might connect to HBA on different host.
- The logout operation will be performed on the specified session.

`networkdiag [-p <ipaddr>]`

- The `networkdiag` runs network diagnostic tests on the selected device.
- The `-p <ipAddr>` is the IP address used for the test, if this option is not specified, test uses the IP address found in the Gateway IP addresses list.
- This command is available on all NDIS device selections.
- Ctrl+break to stop the test.

Example:

```
networkdiag -p 10.10.10.10
```

`q`

Exit the program

`refresh`

- Scans the system for hardware/configuration changes
- This command is only available in host views.

`refreshall`

- Scans all systems for hardware/configuration changes
- This command is only available in host views.
- Ctrl+break to stop to the operation.

```
refreshdiscoveryportal  {-m <iSCSI HBA MAC Address>} {-i <TargetPortalAddress>}
[-n <TargetPortalSocket>]
```

- Performs a SendTargets operation to the target portal and includes the discovered targets into the list of targets maintained by the service
- The refreshdiscoveryportal command is available in the context of a host.
- If a value was not specified for the -n option, the default 3260 port number is used.

```
refreshisnsserver {-i <iSNS Server Address>}
```

- Refreshes the list of targets discovered from the specified iSNS server.
- The refreshisnsserver command is available in the context of a host.

```
remove {-c all | <team name>}
```

- The remove command removes the specified team or all teams.
- The `remove -c all` removes all the teams in the system.
- The `remove <team name>` removes the specified team.
- The `remove` removes the active/selected team.
- This command is only available if the active selection is a team and/or in the teamview view.

  Example:

  - `remove -c all`
  - `remove "Team1"`

`removeallhosts`

Example:

```
removeallhosts
```

```
removediscoveryportal  {-m <iSCSI HBA MAC Address>} {-i <TargetPortalAddress>}
[-n <TargetPortalSocket>]
```

- Removes a portal from the list of portals that iSCSI initiator service sends SendTargets request to discover targets.
- The removediscoveryportal command is available in the context of a host.
- If a value was not specified for the `-n` option, the default 3260 port number is used.

```
removehost  <host name | IP address>
```

- `host name` is the name of a host to be disconnected.
- `IP address` is the IP address of a host to be connected.

```
removeisnsserver {-i <iSNS Server Address>}
```

- Removes the iSNS server as identified by the `-i` option input parameter.
- This command is available in the context of a host.

```
removenpivport  {-p <WWPN>}
```

- This command is available in the context of a FCoE HBA selection.
- Removes a NPIV port.

```
removepersistenttarget  {-t <TargetName>} [-h <host>]
```

- The removepersistenttarget command is available in the context of a host or in the context of a iSCSI Target.
- Removes a target from the list of persistent targets.
- `-t` is only required when the command is used on the host, in context of a iSCSI Target. The `-t` option must not exist.
- `-h` is only required when the command is used on the iSCSI target, because a target might connect to HBA on different host.

```
removetarget {-t <TargetName>}
```

- Removes the static target as identified by the `-t` option input parameter.
- The removetarget command is available in the context of a host.

```
resetsessionstats [<sessionid>]
```

- Resets statistics information for all sessions or for a specified session.
- If `sessionid` was specified, the statistics for that session are reset.
- This command is only available if the active selection is a iSCSI device.

```
resetstats
```

- The 'resetstats' command will reset the statistics of the selected device.
- This command is available in all context where the 'stats' command is applicable.

`restore [-h <host>] <file>`

- `restore <file>` restores the team configuration from the specified <file>. Existing team configurations are lost.
- This command is only available if the active selection is a team and/or in the teamview view.
- `-h` option is needed if there is no team selected and the application needs to know to which host the teams will be restored.

Example:
`restore "c:\test.txt"`

`save {-f MAC|BDF} <file>`

- The save command saves the team configuration to the specified <file> in the specified format.
- The `save -f MAC <file>` saves the team configuration to the specified <file> in MAC format.
- The `save -f BDF <file>` saves the team configuration to the specified <file> in BDF format; bdf numbers are in HEX format.
- This command is only available if the active selection is a team and/or in the teamview view.

Example:

- `save -f MAC "c:\test.txt"`
- `save -f BDF "c:\test.txt"`

`select [<index>]`

- Selects a target from the current view or display the selected target in the current view if <index> is not specified.
- This command is available in all views.

`sessions`

- Displays a list of iSCSI sessions on the selected iSCSI adapter.
- This command is only available if the actively selected device is an iSCSI device.

`sessionstats [<sessionid>]`

- Displays statistics information for all sessions or for a specified session.
- If sessionid was specified, the statistics for that session are displayed.
- This command is only available if the active selection is a iSCSI device.

`showsel`

Shows the selected target item.

`stats [all | general | IEEE | basp ]`

- The stats command displays the statistic information for the selected device.
- This command is available on all NDIS device selections.

Example:

- `stats`
- `stats all`
- `stats basp`

`stats [all | login | instance | custom]`

- If the `login` argument was specified, the stats command displays the login statistics of the selected iSCSI adapter.
- If the `instance` argument was specified, the stats command displays the instance statistics of the selected iSCSI adapter.
- If the `custom` argument was specified, the stats command displays the custom statistics of the selected iSCSI adapter.
- If the `all` option was specified, the stats command displays all the statistics information for the selected iSCSI adapter.
- If the no parameter was specified, the stats command displays all the statistics information for the selected iSCSI adapter.
- This command is available on all iSCSI device selections.

`unassigned [-h <host>]`

- Displays the adapters that are not yet part of a team.
- This command is only available in teamview view listing.
- `-h` option is needed if there is no team selected and application needs to know the host to which the unassigned nics belong.

`version`

Displays the version of this program

Legacy Commands (Used by BACScli v1.0.10 or Earlier)

These commands are deprecated, and only supported to provide the backward compatibility. It is recommended to use the new POSIX-compliant commands listed in "POSIX-Compliant Commands" on page 143.

`BACScli [ -mac MAC | -bdf BDF ] [Command]`

The following lists the available commands:

help: List the available commands.

q: Exit the program.

dev: Select an adapter or list the available adapters.

bdf: Display the PCI Bus/Device/Function number of all devices.

log: Log all input and output into a file.

version: Display version of this program.

info: Display adapter information of the selected NIC.

stats: Display statistic information of the selected NIC.

cfg: Configure parameter of the selected device.

diag: Configure and conduct a diagnostic test.

Appendix B: How-To and Examples

How to Enter Interactive Mode

Enter `BACScli` without additional parameters to enter into the Interactive mode of BACScli.

Example:

`BACScli` enters into interactive mode.

How to Exit Interactive Mode

Enter `q` command while in the Interactive mode of BACScli.

Example:

`q` exit from Interactive mode.

How to List Target Adapters of Different Views in the Command Line Interface mode

In Command Line Interface mode, use the `BACScli list <view>` command to list all the target adapters of the desired <view>.

Example:

- `BACScli list NDIS` lists all NDIS adapters in the system.
- `BACScli list devcon` lists all adapters by connection.

How to Obtain Context-Sensitive Help for Each Command

In interactive mode, the keyword `help` or `?` is applicable to show help for its particular command.

Example:

- `cfg Advanced help` displays help text for the advanced configuration for the selected device.
- `info ?` displays help text for the information of the selected adapter.

In the command line interface mode, use the following syntax to obtain the help text for a specific operation

Example:

- `BACScli -t NDIS -f mac -i 0010181a1b1c info help` displays all the help text for the information of the selected NDIS adapter.

- `BACScli -t NDIS -f mac -i 0010181a1b1c "cfg Advanced help` displays help for the Advanced configuration of the selected NDIS adapter and their current settings.

How to Switch Between Different Views of Target Adapters in Interactive Mode

In Interactive mode, use the `list [-f MAC|BDF] [<view>]` command to switch between different view of target adapters. The default view of the BACScli is `devtype` in the Interactive mode. All target adapters of the selected view are listed and the selected default adapter is high-lighted.

Example:

- `list -f MAC NDIS` lists all NDIS devices that are present in the system with MAC address as identifiers.
- `list -f BDF NDIS` lists all NDIS devices that are present in the system with Bus/Device/Function numbers as identifiers, the Bus/Device/Function numbers are in HEX format.
- `list -f MAC devcon` lists all adapters by the connection identifying devices using their MAC address.
- `list -f BDF devcon` lists all adapters by the connection identifying devices using their Bus/Device/Function address, the Bus/Device/Function numbers are in HEX format.

In the command line interface mode, use the following syntax to list devices in different views:
`BACScli “list [-f MAC|BDF][<view>]”`

Example:

- `BACScli "list -f MAC NDIS"` lists all NDIS devices that are present in the system with MAC address as identifiers.
- `BACScli "list -f BDF NDIS"` lists all NDIS devices that are present in the system with Bus/Device/Function numbers as identifiers, the Bus/Device/Function numbers are in HEX format.
- `BACScli "list -f MAC devcon"` lists all adapters by the connection identifying devices using their MAC address.
- `BACScli "list -f BDF devcon"` lists all adapters by the connection identifying devices using their Bus/Device/Function address, the Bus/Device/Function numbers are in HEX format.

How to Select a Target for the Command to Operate on in CLI Mode

In Command Line Interface mode, use the `-t`, `-f`, and `-i` option to uniquely select the target for the following <command string> to operate on it.

Example:

- `BACScli -t NDIS -f mac -i 0010181a1b1c info` displays the adapter information of the selected NDIS adapter whose current MAC address is 00:10:18:1a:1b:1c.
- `BACScli -t VBD -f mac -i 0010181a1b1d info` displays the adapter information of the selected VBD adapter whose current MAC address is 00:10:18:1a:1b:1d.

- `BACScli -t iSCSI -f mac -i 0010181a1b1e info` displays the adapter information of the selected iSCSI adapter whose current MAC address is 00:10:18:1a:1b:1e.
- `BACScli -t TEAM -f name -i Team1 "info"` displays the team information of the selected ('Team1') team.
- `BACScli -t VNIC -f name -i VLAN1 "info"` displays the virtual adapter information which is identified by a VLAN name (VLAN1).

How to Select a Target in Interactive Mode

In Interactive mode, use the select [<index>] command to select the target from the target adapters of current view. Use the 'showsel' command to display the selected target adapter. Any command entered at this point will apply to the selected target adapter.

Example:

- `list NDIS` and `select 3` selects the third adapter from the list of all target adapters of NDIS view.
- `list devcon` and `select 5` selects the fifth adapter from the list of all target adapters of devcon view.

How to Get Information on a Selected Target

In CLI mode, use `BACScli -t <target type> -f <format> -i <target ID> info [ all | vitalsigns | driver | hardware | resource | members | livelink | general ]` command to get information of the selected target. This command is available for NDIS, VBD and team.

Example:

- `BACScli -t NDIS -f mac -i 0010181a1b1c "info"` displays all the information of the selected NDIS adapter.
- `BACScli -t NDIS -f mac -i 0010181a1b1c "info vitalsigns"` displays the Vital Signs information of the selected NDIS adapter.
- `BACScli -t NDIS -f mac -i 0010181a1b1c "info resource"` displays the Resources information of the selected NDIS adapter.
- `BACScli -t VBD -f mac -i 0010181a1b1d "info driver"` displays the driver information of the selected VBD adapter.
- `BACScli -t NDIS -f mac -i 0010181a1b1c "info hardware"` displays the hardware information of the selected NDIS adapter.
- `BACScli -t NDIS -f mac -i 0010181a1b1c "info all"` displays all the information of the selected NDIS adapter.
- `BACScli -t TEAM -f name -i team1 "info all"` displays all the information of the selected team.
- `BACScli -t TEAM -f name -i team1 "info members"` displays all the information of the selected team.
- `BACScli -t TEAM -f name -i team1 "info livelink"` displays livelink settings of the selected team.
- `BACScli -t TEAM -f name -i team1 "info general"` displays the general information of the selected team.
- `BACScli -t TEAM -f name -i team1 "info"` displays all the information of the selected team.

- `BACScli -t TEAM -f name -i "^"Team1 "info"` displays the team information of the selected ('^Team1') team. If team name contains special character, it needs to be specified inside double quotes.
- `BACScli -t VNIC -f name -i "^"VLAN1 "info"` displays the virtual adapter information which is identified by a VLAN name ('^VLAN1'). If VLAN name contains special character, it needs to be specified inside double quotes.

In Interactive mode, use `list <view>` and `select <idx>` commands to select the desired target device. Use `info [ all | vitalsigns | driver | hardware | resource ]` command to get information of the selected target.

Example:

- `info` or `info all` displays all the information about the selected target.
- `info vitalsigns` displays vitalsigns information of the selected target.
- `info resource` displays vitalsigns information of the selected target.
- `info driver` displays vitalsigns information of the selected target.
- `info hardware` displays vitalsigns information of the selected target.
- `info members` displays all the information of the selected team.
- `info livelink` displays livelink settings of the selected team.
- `info general` displays the general information of the selected team.

How to Configure a Selected Target's Advance Parameters

In CLI mode, use the `BACScli -t <target type> -f <target format> -i <target ID> cfg Advanced [param|param=value]` command to display and configure the Advanced parameters for the selected target.

Example:

- `BACScli -t NDIS -f mac -i 0010181a1b1c "cfg Advanced"` displays all Advanced parameters of the selected NDIS adapter and their current settings.
- `BACScli -t NDIS -f mac -i 0010181a1b1c "cfg Advanced \"802.1p QOS\""` displays the current setting and all valid settings of the specified Advanced parameter "802.1p QOS".
- `BACScli -t NDIS -f mac -i 0010181a1b1c "cfg Advanced \"802.1p QOS\"=\"Enable\""` sets the Advanced parameter, '802.1p QOS', to 'Enable'.
- `BACScli -t NDIS -f mac -i  0010181a1b1c "cfg advanced \"Flow Control\"=\"Rx "&" TX enabled\""` sets the Advanced parameter, 'Flow Control', to 'RX & TX enabled'.

In Interactive mode, use `list <view>` and `select <idx>` commands to select the desired target device. Use `cfg Advanced [param|param=value]` to display and configure the Advanced parameters of the selected target.

Example:

- `cfg Advanced` displays all Advanced parameters of the selected adapter and their current settings.
- `cfg Advanced "802.1p QOS"` displays the current setting and all valid settings of the 802.1p QOS Advanced parameter.
- `cfg Advanced "802.1p QOS"="Disable"` sets the 802.1p QOS parameter to Disable.

How to Display a Selected Target's Licenses

In CLI mode, use `BACScli -t <target type> -f <target format> -i <target ID> cfg licenses` to display the Licenses' of the selected target.

Example:

`BACScli -t VBD -f mac -i 0010181a1b1d "cfg Licenses"` displays all Licenses of the selected VBD adapter and their current settings.

In Interactive mode, use the `list <view>` and `select <idx>` commands to select the desired target device. Use the `cfg Licenses` command to display the Licenses of the selected target.

Example:

- `cfg Licenses` displays all Licenses parameters of the selected adapter and their current settings.

How to Configure the iSCSI Parameter for a Selected Target

In CLI mode, use the `BACScli -t <target type> -f <target format> -i <target ID> cfg iSCSIMgmt [key|key=value]` command to display and configure the iSCSI parameter of the selected target.

Example:

- `BACScli -t iSCSI -f mac -i 0010181a1b1e "cfg iSCSIMgmt"` displays all iSCSI Management keys of the selected iSCSI adapter and their current settings.
- `BACScli -t iSCSI -f mac -i 0010181a1b1e "cfg iSCSIMgmt \"IPV4DHCP\""` displays the current setting and all valid settings of the IPV4DHCP key.
- `BACScli -t iSCSI -f mac -i 0010181a1b1e "cfg iSCSIMgmt \"IPV4DHCP\"=\"Enable\""` sets the `IPV4DHCP` key to `Enable`.

In Interactive mode, use `list <view>` and `select <idx>` commands to select the desired target device. Use `cfg iSCSIMgmt [key|key=value]` command to display and configure the `iSCSI parameter` of the selected target.

Example:

- `cfg iSCSIMgmt` displays current settings of all iSCSI Management parameters of the selected adapter and their current settings.
- `cfg iSCSIMgmt "IPV4DHCP"`displays the current setting and all valid settings of the IPV4DHCP key.
- `cfg iSCSIMgmt "IPV4DHCP"="Enable"` sets IPV4DHCP to Enable.

How to Configure the Resources for a Selected Target

In CLI mode, use 'BACScli -t <target type> -f <target format> -i <target ID> cfg Resource [key|key=value]' command to display and configure the 'Resource parameter' of the selected target.

Example:

- `BACScli -t VBD -f mac -i 0010181a1b1d "cfg Resource"` displays all Resource Reservation keys and their current settings.
- `BACScli -t VBD -f mac -i 0010181a1b1d "cfg Resource \"CONFIGURABLE\""` displays all configurable Resource Reservation keys with their current settings and valid settings.
- `BACScli -t VBD -f mac -i 0010181a1b1d "cfg Resource \"CONFIG\"=\"RSVD\""` sets the Offload Configuration to Reserved Resources.
- `BACScli -t VBD -f mac -i 0010181a1b1d "cfg Resource \"TOECONN\"=\"50\""` sets the TOE Connections to 50. The command is valid only when the Offload Configuration is in Reserved Resources.
- `BACScli -t VBD -f mac -i 0010181a1b1d "cfg Resource \"iSCSI\"=\"Disable\""` set the Preallocated Resources for iSCSI to Disable.

  All reserved resources for iSCSI is released.

  The command is valid only when the Offload Configuration is in Reserved Resources.

In Interactive mode, use `list <view>` and `select <idx>` commands to select the desired target device.

Use the `cfg Resource [key|key=value]` command to display and configure the `Resource parameter` of the selected target.

Example:

- `cfg Resource` displays all Resource Reservation parameters of the selected adapter and their current settings.
- `cfg Resource "CONFIGURABLE"` displays all configurable Resource Reservation parameters with their current settings and valid settings.
- `cfg Resource "CONFIG"="FCFS"` set the Offload Configuration to First Come First Served.
- `cfg Resource "iSCSICONN"="20"` set the iSCSI Connections to 20. The command is valid only when the Offload Configuration is in Reserved Resources.
- `cfg Resource "TOE"="Disable"` set the Preallocated Resources for TOE to Disable. All reserved resources for TOE is released. The command is valid only when the Offload Configuration is in Reserved Resources.

How to Configure OOBMgmt for a Selected Target

In CLI mode, use `BACScli -t <target type> -f <target format> -i <target ID> cfg iSCSIMgmt [key|key=value]` command to display and configure the iSCSI parameter of the selected target.

Example:

- `BACScli -t NDIS -f mac -i 0010181a1b1c "cfg OOBMgmt"` displays all OOB Management parameters and their current settings or information.
- `BACScli -t NDIS -f mac -i 0010181a1b1c "cfg OOBMgmt \"Heartbeat Transmit Interval\""` displays Heartbeat Transmit Interval current settings and its valid input.
- `BACScli -t NDIS -f mac -i 0010181a1b1c "cfg OOBMgmt \"Heartbeat Transmit Interval\"=\"50\""` sets the Heartbeat Transmit Interval to 50 seconds.

In Interactive mode, use 'list <view>' and 'select <idx>' commands to select the desired target device. Use `cfg OOBMgmt [key|key=value]` command to display and configure the 'OOBMgmt parameter' of the selected target.

Example:

- `cfg OOBMgmt` displays all OOB Management parameters of the selected adapter and their current settings.
- `cfg OOBMgmt "Heartbeat Transmit Interval"` displays Heartbeat Transmit Interval current settings and its valid input.
- `cfg OOBMgmt "Heartbeat Transmit Interval"="50"` sets the Heartbeat Transmit Interval to 50 seconds.

How to Configure Systoe for the System

In CLI mode, use `BACScli -t System "cfg Systoe [value]"` command to display and configure the TCP Offload of system chimney.

Example:

- `BACScli -t system "cfg Systoe"` displays current Chimney Offload State.
- `BACScli -t system "cfg Systoe Enabled"` enables current Chimney Offload State.
- `BACScli -t system "cfg Systoe Disabled"` disables current Chimney Offload State.
- `BACScli -t system "cfg Systoe Automatic"` sets current Chimney Offload State to automatic (Win7 kernel and later).

In Interactive mode, use `list System` and by default the system is selected because there is only system. Use `cfg Systoe [value]` command to display and configure the TCP Offload of system chimney.

Example:

- `cfg Systoe` displays current Chimney Offload State.
- `cfg Systoe Enabled` enables current Chimney Offload State.
- `cfg Systoe Disabled` disables current Chimney Offload State
- `cfg Systoe Automatic` sets current Chimney Offload State to automatic (Win7 kernel and later).

How to Get Statistics for a Selected Target

In CLI mode, use `BACScli -t <target type> -f <target format>  -i <target ID> "stats <options>"`.

Example:

- `BACScli -t NDIS -f mac -i 0010181a1b1c "stats"` displays all statistics of the selected NDIS adapter.
- `BACScli -t NDIS -f mac -i 0010181a1b1c "stats general"` displays general statistics of the selected NDIS adapter.
- `BACScli -t NDIS -f mac -i 0010181a1b1c "stats IEEE"` displays IEEE statistics of the selected NDIS adapter.
- `BACScli -t NDIS -f mac -i 0010181a1b1c "stats BASP"` displays BASP statistics of the selected NDIS adapter.

- `BACScli -t NDIS -f mac -i 0010181a1b1c "stats all"` displays all the statistics information of the selected NDIS adapter.
- `BACScli -t iSCSI -f mac -i 0010181a1b1e "stats login"` displays login statistics information of the selected iSCSI device.
- `BACScli -t iSCSI -f mac -i 0010181a1b1e "stats instance"` displays instance statistics information of the selected iSCSI device.
- `BACScli -t iSCSI -f mac -i 0010181a1b1e "stats custom"` displays custom statistics information of the selected iSCSI device.
- `BACScli -t iSCSI -f mac -i 0010181a1b1e "stats all"` displays all the statistics information of the selected iSCSI device.
- `BACScli -t iSCSI -f mac -i 0010181a1b1e "stats"` displays all the statistics information of the selected iSCSI device.
- `BACScli -t TEAM -f name -i asdf "stats"` displays all the statistics information for the asdf team.
- `BACScli -t VNIC -f name -i asdf "stats"` displays all the statistics information for the virtual adapter whose VLAN name is asdf.

In Interactive mode, the target type and target identifiers need not be specified and the stats command will be based on the active target selection.

Example:

- `stats` displays all statistics of the selected NDIS adapter.
- `stats general` displays general statistics of the selected NDIS adapter.
- `stats IEEE` displays IEEE statistics of the selected NDIS adapter.
- `stats BASP` displays BASP statistics of the selected NDIS adapter.
- `stats all` displays all the statistics information of the selected NDIS adapter.
- `stats login` displays login statistics information of the selected iSCSI device.
- `stats instance` displays instance statistics information of the selected iSCSI device.
- `stats custom` displays custom statistics information of the selected iSCSI device.
- `stats all` displays all the statistics information of the selected iSCSI device.
- `stats` displays all the statistics information of the selected iSCSI device.
- `stats` displays all the statistics information for the selected team.
- `stats` displays all the statistics information for the selected virtual adapter.

How to Reset Statistics for a Selected Target

- This command is not applicable in the CLI mode.
- In Interactive mode, type `resetstats` to reset all statistical information for a selected/active NDIS/VNIC/ iSCSI/team.

How to Run Diagnostic Tests for a Selected Target

In CLI mode, use `BACScli -t <target type> -f <target format> -i <target ID> diag {[-c REG ] [-c MII ] [-c EEP] [-c MEM] [-c CPU] [-c INT] [-c MACLB ] [-c PHYLB] [-c LED] | [-c ALL]} [-l <cnt> ] [ -v <LEDIntv> ]` command to run NIC diagnostics tests for the selected target. This command is available for NDIS and VBD adapters.

Example:

- `BACScli -t NDIS -f mac -i 0010181a1b1c "diag"` displays all the diagnostics tests available for the current selected target.
- `BACScli -t NDIS -f mac -i 0010181a1b1c "diag -c MII -c LED"` runs MII and LED test for the selected NDIS adapter.
- `BACScli -t VBD -f mac -i 0010181a1b1d "diag -c all -l 5 -v 8"` runs all the tests for 5 times with LED test interval 8 milliseconds for the selected VBD adapter.

In Interactive mode, use 'list <view>' and 'select <idx>' commands to select the desired target device.

Use `diag {[-c REG ] [-c MII ] [-c EEP] [-c MEM] [-c CPU] [-c INT] [-c MACLB ] [-c PHYLB] [-c LED] | [-c ALL]} [-l <cnt> ] [ -v <LEDIntv> ]'` command to run diagnostics tests for the selected target.

Example:

- `diag` displays all the diagnostics tests available for the current selected target.
- `diag -c MII -c LED` runs MII and LED test for the selected NDIS adapter.
- `diag -c all -l 5 -v 8` runs all the tests five times with an LED test interval of 8 milliseconds for the selected VBD adapter.

How to Run Cable Diagnostic Tests for a Selected Target

In CLI mode, use `BACScli -t <target type> -f <target format> -i <target ID> cablediag` to run cable diagnostics test for selected target. This command is available for NDIS and VBD adapters.

Example:

- `BACScli -t NDIS -f mac -i 0010181a1b1c "cablediag"` runs the cable diagnostics test for the current selected NDIS adapter.
- `BACScli -t VBD -f mac -i 0010181a1b1d "cablediag"` runs the cable diagnostics test for the current selected VBD adapter.

In Interactive mode, use `list <view>` and `select <idx>` commands to select the desired target device. Use `cablediag` to run cable diagnostics test for selected target.

Example:

`cablediag` runs the cable diagnostics test for the current selected NDIS adapter.

How to Run Network Diagnostic Tests on a Selected Target

In CLI mode, use `BACScli -t <target type> -f <target format> -i <target ID> networkdiag [-p <IP address>]` to run cable diagnostics test for selected target. This command is available for NDIS and virtual adapters.

Example:

- `BACScli -t NDIS -f mac -i 0010181a1b1c "networkdiag -p 192.168.1.5"` runs the network test for the current selected NDIS adapter.
- `BACScli -t VNIC -f mac -i 0010181a1b1c "networkdiag"` runs the network test for the current selected virtual adapter. Since there is no IP address specified, BACScli uses the gateway address for the test.

In Interactive mode, use `list <view>` and `select <idx>` commands to select the desired target device. Use `networkdiag [-p <IP address>]` to run cable diagnostics test for selected target.

Example:

- `networkdiag -p 192.168.1.5` runs the network test for the current selected NDIS adapter.
- `networkdiag` runs the network test for the current selected virtual adapter.

How to Create a Team Configuration

In CLI mode, use `BACScli -t TEAM "add <config file name>"` to add a team using a configuration file.

Example:

- `BACScli -t team "add o:\temp\asdf1.bcg"`

In the interactive mode, use `add <config file name>` to add a team using a configuration file.

Example:

```
add o:\temp\asdf1.bcg
```

How to Restore a Team Configuration

n CLI mode, use `BACScli -t TEAM "restore <config file name>"` to restore teams using a configuration file.

Example:

```
BACScli -t team "restore o:\temp\asdf.bcg"
```

In the interactive mode, use `restore <config file name>` to restore teams using a configuration file.

Example:

restore o:\temp\asdf.bcg

How to Save a Team Configuration

In CLI mode, use `BACScli -t TEAM "save {-f MAC|BDF} <file_path_name>"` to save the current teaming configuration to a file.

Example:

- `BACScli -t team "save -f MAC o:\temp\asdf.bcg"`. Saves the current teaming configuration to a file named `asdf.bcg` with adapters identified using the MAC address.
- `BACScli -t team "save -f BDF o:\temp\asdf.bcg"`. Saves the current teaming configuration to a file named `asdf.bcg` with adapters identified using the bus/device/function numbers, the Bus/Device/Function numbers are in HEX format.

In the interactive mode, use `save {-f MAC|BDF} <file_path_name>` to save the current teaming configuration to a file from within the teamview view listings.

Example:

- `save -f MAC o:\temp\asdf.bcg`. Saves the current teaming configuration to a file named `asdf.bcg` with adapters identified using the MAC address.
- `save -f BDF o:\temp\asdf.bcg`. Saves the current teaming configuration to a file named `asdf.bcg` with adapters identified using the bus/device/function numbers, the Bus/Device/Function numbers are in HEX format.

How to Remove One or More Teams

In CLI mode, use `BACScli -t team -f name -i <team name> "remove"` to remove one or more teams from the system.

Example:

- `BACScli -t team -f name -i asdf "remove"`. Removes a team named `asdf` from the system.
- `BACScli -t team "remove -c all"`. Removes all teams from the system.

In the interactive mode, use `remove {-c all | <team_name>| }` to remove one or more teams from the system.

Example:

- `remove asdf` removes a team named `asdf` from the system.
- `remove -c all` removes all teams from the system.
- `remove` Removes the active/selected team from the system.

How to Display Unassigned Adapters

- In CLI mode, use `BACScli -t TEAM unassigned` to display list of unassigned adapters.
- In the interactive mode, use `unassigned` to restore teams using a configuration file.

How to Switch Between Primary and Standby Adapters in a Team

- In CLI mode, use `BACScli -t TEAM "unassigned"` to display list of unassigned adapters.
- In the interactive mode, use `unassigned` to restore teams using a configuration file.

Examples of Other commands

- `help` displays a list of available commands.
- version displays the version of BACScli.
- `log <file>` turns on the log and log all the information to <file>.
- `log` turns off the log.
- `showsel` displays the current selected target.

Appendix C: Configuration File Usage

Team Configuration File

Syntax

The syntax plain text file is defined as follows. The team parameters can be specified either using NO_LIVELINK_PARAMS or using LIVELINK_PARAMS.

TEAM_CFG

[TEAM_CFG]

...

1. Each 'TEAM_CFG' with NO_LIVELINK_PARAMS is defined as follows:
   name: team_name
   [type: team_type]
   pnic: MAC_address
   [pnic: MAC_address
   ...]
   [snic: MAC_address]
   [[ip: IP_address
   smask: subnetmask]
   |[vname: VLAN_name
   vid: VLAN_ID
   [ip: IP_address
   smask: subnetmask]]
   ...]

2. Each 'TEAM_CFG' with LIVELINK_PARAMS is defined as follows:
   name: livelinkteam_name
   [type: livelink_team_type]
   target_ip: ip1
   [target_ip: ip2
   target_ip: ip3
   target_ip: ip4]
   [retry: 3]
   [freq: 2000]
   [retry_freq: 2000]

[livelink_vid: 1234]
[pnic: MAC_address|PCIINFO
livelink_ip: ll_ip
livelink_ipv6: ll_ipv6
pnic: MAC_address|PCIINFO
livelink_ip: ll_ip
pnic:...]
[snic: MAC_address|PCIINFO
livelink_ip: ll_ip]
[[ip: IP_address
smask: subnetmask]
|[vname: VLAN_name
vid: VLAN_ID
[ip: IP_address
smask: subnetmask]]
...]

A configuration file MUST contain at least one team configuration. `BACScli.exe` will recognize `name` as starting point of a team configuration section. All lines after name will apply to the `team_name` until another name or end of file is encountered. Each team configuration MUST contain at least one physical network adapter or the configuration of the team will be ignored.

If `type` is missing, the default is set to Smart Load Balancing (SLB).

There are four team types: SLB = 0, GEC = 1, LACP = 2 and SLB-AFD = 4.

If `ip` is set, `smask` must also be set or `ip` will be ignored.

If `ip` is not set, DHCP will be used.

Team IP can be set if no VLAN are configured. If any VLAN is configured, the team IP will be ignored. Multiple VLAN configurations are allowed. Each VLAN configuration allows an optional static IP information. Each IP must be couple with `smask` or will be ignored.

Note that there must at least one white space or tab between the tag (name, pnic, etc.) and the value pair (team_name, MAC_address, etc.) in each line.

The keywords before semicolons are case sensitive.

Examples

1. A sample of the TeamConfig.txt configuration file with NO_LIVELINK_PARAMS:
name: BRCMTeam
type: 1
pnic: 00101801794D

pnic: 00:0B.2
vname: VLAN2
vid: 2
vname: VLAN3
vid: 3
ip: 172.16.8.3
smask: 255.255.255.0
vname: VLAN4
vid: 4
ip: 172.16.8.4
smask: 255.255.255.0
vname: VLAN5
vid: 5
ip: 172.16.8.5
smask: 255.255.255.0

2. A sample of the TeamConfig.txt configuration file with LIVELINK_PARAMS:

name: LiveLinkTeam
type: 0
target_ip: 172.16.8.66
target_ip: 172.16.8.77
target_ip: 172.16.8.88
target_ip: fc01::101
livelink_vid: 1234
pnic: 00101801794D
livelink_ip: 172.16.8.10
livelink_ipv6: fc01::218
pnic: 01:0D.0
livelink_ip: 172.16.8.11
snic: 02:03.00
livelink_ip: 172.16.8.20
vname: VLAN2
vid: 2
vname: VLAN3
vid: 3
ip: 172.16.8.3
smask: 255.255.255.0
vname: VLAN4
vid: 4
ip: 172.16.8.4

smask: 255.255.255.0

vname: VLAN5

vid: 5

ip: 172.16.8.5

smask: 255.255.255.0

Boot Configuration XML File

iSCSI Example

```
<?xml version="1.0" encoding="UTF-8"?>

    <iSCSIBootConfiguration>
        <BACScli><Version>v14.8.0</Version></BACScli>
        <iSCSIGeneral>
            <TCPIPviaDHCP>Disabled</TCPIPviaDHCP>
            <iSCSIPviaDHCP>Disabled</iSCSIPviaDHCP>
            <CHAPAuthentication>Enabled</CHAPAuthentication>
            <BoottoiSCSITarget>Disabled</BoottoiSCSITarget>
        </iSCSIGeneral>
        <IscsiInitiator>
            <IPAddress>10.13.241.147</IPAddress>
            <SubnetMask>255.255.254.0</SubnetMask>
            <DefaultGateWay>10.13.241.1</DefaultGateWay>
            <PrimaryDNS>10.10.10.10</PrimaryDNS>
            <SecondaryDNS>20.20.20.20</SecondaryDNS>
            <iSCSIName>iqn</iSCSIName>
            <CHAPID>user</CHAPID>
            <CHAPSecret>password</CHAPSecret>
        </IscsiInitiator>
        <IscsiTarget>
            <Connect>Enabled</Connect>
            <IPAddress>10.13.241.147</IPAddress>
            <TCPPort>26535</TCPPort>
            <BootLun>255</BootLun>
            <iSCSIName>iname</iSCSIName>
            <CHAPID>admin1</CHAPID>
            <CHAPSecret>password1</CHAPSecret>
        </IscsiTarget>
        <IscsiSecTarget>
            <Connect>Enabled</Connect>
            <IPAddress>192.168.145.112</IPAddress>
            <TCPPort>34589</TCPPort>
            <BootLun>2</BootLun>
            <iSCSIName>name</iSCSIName>
            <CHAPID>user</CHAPID>
            <CHAPSecret>passwd</CHAPSecret>
        </IscsiSecTarget>
        <IscsiMPIO>
            <EnableMPIO>Enabled</EnableMPIO>
            <SecondaryDevice>Adapter2 (57712A1) / Port2</SecondaryDevice>
```

```
            <UseIndependentTargetPortal>Enabled</UseIndependentTargetPortal>
            <UseIndependentTargetName>Enabled</UseIndependentTargetName>
        </IscsiMPIO>
    </iSCSIBootConfiguration>
```

NIC Partition Config Example

```
<?xml version="1.0" encoding="UTF-8" ?>
  <MultiFunctionConfiguration>
    <Version>2</Version>
    <MultiFunctionMode>NIC Partition</MultiFunctionMode>
    <PortConfig>
      <Port>0</Port>
      <FlowControl>Auto</FlowControl>
      <FunctionConfig>
        <Function>0</Function>
        <EthernetNdis>Enable</EthernetNdis>
        <iSCSI>Enable</iSCSI>
        <FCoE>Disable</FCoE>
        <RelativeBandwidth>1</RelativeBandwidth>
        <MaxBandwidth>0</MaxBandwidth>
      </FunctionConfig>
      <FunctionConfig>
        <Function>2</Function>
        <EthernetNdis>Enable</EthernetNdis>
        <iSCSI>Disable</iSCSI>
        <FCoE>Disable</FCoE>
        <RelativeBandwidth>1</RelativeBandwidth>
        <MaxBandwidth>0</MaxBandwidth>
      </FunctionConfig>
      <FunctionConfig>
        <Function>4</Function>
        <EthernetNdis>Enable</EthernetNdis>
        <iSCSI>Disable</iSCSI>
        <FCoE>Disable</FCoE>
        <RelativeBandwidth>1</RelativeBandwidth>
        <MaxBandwidth>0</MaxBandwidth>
      </FunctionConfig>
      <FunctionConfig>
        <Function>6</Function>
        <EthernetNdis>Enable</EthernetNdis>
        <iSCSI>Disable</iSCSI>
        <FCoE>Disable</FCoE>
        <RelativeBandwidth>97</RelativeBandwidth>
        <MaxBandwidth>0</MaxBandwidth>
      </FunctionConfig>
    </PortConfig>
    <PortConfig>
      <Port>1</Port>
      <FlowControl>Auto</FlowControl>
      <FunctionConfig>
        <Function>1</Function>
        <EthernetNdis>Enable</EthernetNdis>
        <iSCSI>Disable</iSCSI>
        <FCoE>Disable</FCoE>
        <RelativeBandwidth>10</RelativeBandwidth>
        <MaxBandwidth>0</MaxBandwidth>
```

```
        </FunctionConfig>
        <FunctionConfig>
          <Function>3</Function>
          <EthernetNdis>Enable</EthernetNdis>
          <iSCSI>Enable</iSCSI>
          <FCoE>Disable</FCoE>
          <RelativeBandwidth>20</RelativeBandwidth>
          <MaxBandwidth>0</MaxBandwidth>
        </FunctionConfig>
        <FunctionConfig>
          <Function>5</Function>
          <EthernetNdis>Enable</EthernetNdis>
          <iSCSI>Disable</iSCSI>
          <FCoE>Disable</FCoE>
          <RelativeBandwidth>30</RelativeBandwidth>
          <MaxBandwidth>0</MaxBandwidth>
        </FunctionConfig>
        <FunctionConfig>
          <Function>7</Function>
          <EthernetNdis>Enable</EthernetNdis>
          <iSCSI>Disable</iSCSI>
          <FCoE>Disable</FCoE>
          <RelativeBandwidth>40</RelativeBandwidth>
          <MaxBandwidth>0</MaxBandwidth>
        </FunctionConfig>
      </PortConfig>
    </MultiFunctionConfiguration>

  <?xml version="1.0" encoding="UTF-8" ?>
    <MultiFunctionConfiguration>
      <Version>2</Version>
      <MultiFunctionMode>VNTag</MultiFunctionMode>
      <PortConfig>
        <Port>0</Port>
        <FlowControl>Auto</FlowControl>
        <FunctionConfig>
          <Function>0</Function>
          <EthernetNdis>Enable</EthernetNdis>
          <iSCSI>Enable</iSCSI>
          <FCoE>Disable</FCoE>
          <RelativeBandwidth>1</RelativeBandwidth>
          <MaxBandwidth>0</MaxBandwidth>
          <VNTagVIFProfile>file_name</VNTagVIFProfile>
        </FunctionConfig>
        ...
      </PortConfig>
      <PortConfig>
      ...
      </PortConfig>
    </MultiFunctionConfiguration>
```

Example: Disable NIC Partition Through the XML Config File

```
<?xml version="1.0" encoding="UTF-8" ?>
  <MultiFunctionConfiguration>
    <Version>2</Version>
```

```
    <MultiFunctionMode>SingleFunction</MultiFunctionMode>
  </MultiFunctionConfiguration>
```

Appendix D: Exit Codes

```
==============
BACSCLI_OK                                0       // Upgrade firmware OK
BACSCLI_QUIT                              1       // Quit program
BACSCLI_PARAM_ERROR                       2       // Not correct parameters
BACSCLI_ADAPTER_NOT_FOUND                 3       // Adapter not found
BACSCLI_CANNOT_LOCK_ADAPTER               4       // Cannot lock adapter
BACSCLI_GET_CLOSE_EVENT                   5       // Get close event
BACSCLI_INIT_FAILED                       6       // Initialization failed
BACSCLI_UNSUPPORTED_BMAPI_VER             7       // BMAPI is too old
BACSCLI_UNKNOWN_COMMAND                   8       // Unknown command
BACSCLI_MALLOC_ERROR                      9       // memory allocation error
BACSCLI_BMAPI_ERROR                       10      // BMAPI call returns error
BACSCLI_OS_NOT_SUPPORTED                  11      // OS is not supported
BACSCLI_NO_ADVANCED_PARAMS                12      // No Advanced Parameter for the NIC
BACSCLI_INVALID_ADVANCED_PARAM_DETECTED   13      // Invalid Advanced Parameter detected
BACSCLI_INVALID_ADVANCED_PARAM_SPECIFIED  14      // Invalid Advanced Parameter specified
BACSCLI_INVALID_ADVANCED_VALUE_SPECIFIED  15      // Invalid Advanced Value specified
BACSCLI_FEATURE_NOT_SUPPORTED_FOR_NIC     16      // Feature not supported for the NIC
BACSCLI_SET_ADVANCED_PARAM_ERROR          17     // Failed to set the Advanced Parameter with new
value
BACSCLI_SYSTEM_REBOOT                     18      // System Reboot required
BACSCLI_UNSUPPORT_PLATFORM                19      // System platform is not supported
BACSCLI_NOT_ENOUGH_PRIVILEGE              20      // Current user does not have enough privilege
BACSCLI_READ_LICENSE_FILE_ERROR           21      // Error in reading license file
BACSCLI_INVALID_LICENSE_KEY               22      // Invalid license key
BACSCLI_INVALID_ISCSI_PARAM_SPECIFIED     23     // Invalid iSCSI Management Parameter specified
BACSCLI_INVALID_ISCSI_VALUE_SPECIFIED     24      // Invalid iSCSI Management Value specified
BACSCLI_INVALID_RSC_PARAM_SPECIFIED       25      // Invalid Resource Parameter specified
BACSCLI_INVALID_RSC_VALUE_SPECIFIED       26      // Invalid Resource Value specified
BACSCLI_FEATURE_NOT_SUPPORTED_IN_FCFS     27      // Feature not supported in FCFS mode
BACSCLI_PARAM_IS_READ_ONLY               28     // This parameter can't be modified, Administrator
authority required.
BACSCLI_NULL_IP_ADDRESS                   29      // The current IP address is NULL.
BACSCLI_CANNOT_UNLOCK_ADAPTER             30      // Failed to unlock adapter.
BACSCLI_INVALID_VALUE_SPECIFIED           31      // Invalid value specified
BACSCLI_NIC_IS_PART_OF_GEC_LACP_TEAM      32      // NIC is part of a GEC/LACP Team.
BACSCLI_REGISTRY_ACCESS_ERROR             33      // Error in accessing Registry.
BACSCLI_NOT_AN_ISCSI_BOOT_DEVICE          34      // This is not an iSCSI Boot device.
BACSCLI_INVALID_IP_ADDRESS                35      // Invalid IP Address.
BACSCLI_DUPLICATE_IP_ADDRESS              36      // Duplicate IP Address.
BACSCLI_TEAM_DRIVER_NOT_LOAD              37     // NIC( %s ) driver has to be loaded to make it
a member of a team.
BACSCLI_NDIS6_DRIVER_REQUIRED38      // Ndis6 driver is required for the NIC to join the Team in
Windows Vista and later.
BACSCLI_TEAM_UNKNOW_NIC39      // Unknown NIC ( %s ).
BACSCLI_INVALID_SUBNET_MASK               40      // Invalid subnet mask.
BACSCLI_INVALID_CMD                       41      // Invalid command.

BACSCLI_NOT_YET_IMPL                      1000    // This functionality is not yet implemented.
BACSCLI_UNWIND                            1001    // Unwind to the parent processor
BACSCLI_NOT_APPLICABLE                    1002    // Command not applicable
```

```
BACSCLI_NO_TARGET_SEL                        1003    // No active target selection.
BACSCLI_INVALID_CONTEXT                      1004    // Not a valid context
BACSCLI_INVALID_FORMAT                       1005    // Invalid format selection
BACSCLI_INVALID_TARGET_ID                    1006    // Invalid target identifier
BACSCLI_FILE_DOES_NOT_EXIST                  1007    // File does not exist
BACSCLI_INVALID_TEAM_NAME                    1008    // Supplied team name is invalid
BACSCLI_TEAM_COMMIT_FAILED                   1009    // Failed to commit the team operation.
BACSCLI_TEAM_REMOVE_FAILED                   1010    // Failed to remove the team.
BACSCLI_CANNOT_OPEN_FILE                     1011    // Failed to open the file handle.
BACSCLI_ERR_CANNOT_SET_IPADDR                1012    // Failed to set ip address.
BACSCLI_ERR_CANNOT_GET_NIC_PCI_INFO          1013    // Failure retrieving NIC information
BACSCLI_ERR_RETRIEVE_IP_ADDR                 1014    // Error retrieving IP address information
BACSCLI_FAILED_GET_INFO                      1015    // Failed to get info from the DataContainer
BACSCLI_WRONG_OPTION_FLAG                    1016    // General team config file parsing error.
BACSCLI_EXCEEDMAXVLAN                        1017    // Only a maximum of 64 VLANs are allowed.
BACSCLI_CANNOT_CREATE_LIVE_LINK              1018    // Live link support only applied to SLB team
BACSCLI_EXCEED_MAX_TARGET_IP                 1019    // Live link support allows up to 4 link
BACSCLI_TOO_MANY_PHY_NIC                     1020    // Only up to a maximum of 8 nics are allowed
in a team.
BACSCLI_CANNOT_CREATE_FECGEC_8023AD          1021    // Cannot create FECGEC or 802.3ad team with
standby adapter.
BACSCLI_LL_IP_TARGET_IP_TYPE_MISMATCH        1022    // Invalid IPv6 Address
BACSCLI_INVALID_RANGE                        1023    // Value is out of range.
BACSCLI_INVALID_INTERVAL                     1024    // Invalid probe retry frequency
BACSCLI_DUPLICATE_OPTION                    1025    // The same option has been specified previously
BACSCLI_DUPLICATE_MAC_ADDRESS                1026    // Duplicate adapter physical MAC address
BACSCLI_DUPLICATE_VLANID                     1027    // Duplicate VLAN name
BACSCLI_TEAM_ALREADY_EXISTS                  1028    // Team with the specified name already exists
BACSCLI_CANNOT_MATCH_MAC_ADDR                1030    // Cannot find device using the specified MAC
address.
BACSCLI_NO_TEAM_TO_CONFIG                    1031    // No team to configure.
BACSCLI_CANNOT_CREATE_TEAM                   1032    // Failure while creating team
BACSCLI_NO_LINK_FOR_IP_CFG                  1033    // No link is present in team to set ip address.
BACSCLI_ONE_OR_MORE_CREATE_FAILED            1034    // Creation of one or more teams failed.
BACSCLI_TEAM_NO_MEMBER                  1035   // A team is required to have at least one valid member
BACSCLI_NO_BRCM_NIC_IN_TEAM                  1036    // Team requires at least one Broadcom NIC.
BACSCLI_ONLY_BROADCOM_NIC_FOR_VLAN         1037   // Only Broadcom certified adapters are supported
in VLAN.
BACSCLI_CANNOT_SET_IPADDR                1038   // Failed to assign ip address on the virtual adapter.
BACSCLI_INVALID_CFG                          1039    // Invalid configuration
BACSCLI_SET_ADVANCE_PARAM_FAILED             1040    // Failed to set advanced parameter
BACSCLI_INTERNAL_ERROR_INVALID_DATA          1041    // Invalid or NULL data found
BACSCLI_INVALID_PARAMETER                    1042    // Invalid Parameter. Parameter is too few
BACSCLI_NIC_NOT_SUPPORTED                1043   // The current NIC is not supported for this operation
BACSCLI_SET_ASF_FAILED                       1044    // Failed to set the ASF Table
BACSCLI_SET_POWER_MGMT_FAILED               1045    // Failed to set Power Management configuration
BACSCLI_INVALID_TARGET_CMD                   1046    // command/target identifier is invalid
BACSCLI_NO_ISCSI_SESSIONS                    1047    // No iSCSI sessions exists on the system
BACSCLI_SET_MGMT_OBJ_FAILED                  1048    // Failed to set Management Object
BACSCLI_SHOW_USAGE       1049    // If we want to show usage
BACSCLI_CANNOT_CONNECT_WMI1050    // Cannot connect WMI
BACSCLI_EXCEEDMAXTAGGEDVLAN                1051    // Only a maximum of 63 tagged VLANs are allowed.
BACSCLI_NO_TEAM_AVALIABLE                    1052    // There is no team to save.
BACSCLI_NOT_CONFIGURABLE                     1053    // Not Configurable.
BACSCLI_CANNOT_SUSPEND_RESUME_DRIVER         1054    // Failed to suspend or resume the driver.
BACSCLI_CANNOT_RESTART_DRIVER1055    // Failed to restart the driver.
```

Connecting everything®

BROADCOM CORPORATION
5300 California Avenue
Irvine, CA 92617

Phone: 949-926-5000
Fax: 949-926-5203
E-mail: info@broadcom.com
Web: www.broadcom.com

BACS4-SWUM100-R August 09, 2012