Agilent
System Protocol Tester

Installation Guide

Agilent Technologies

Notices

Trademarks

Windows 2000®, Windows XP®, and Microsoft .NET Framework 1.1® are U.S. registered trademarks of Microsoft Corporation.

Installation Guides

You can find the installation guides for different components of the product on the product CD. Agilent recommends you to do not switch on the instrument before you have understood all the applicable installation instructions and have met all the installation prerequisites.

Where to find more information

You can find more information about System Protocol Tester from the following link:

http://www.agilent.com/find/spt

We continually improve our software. Therefore, we recommend you to check the following link to download and install the latest version:

http://www.agilent.com/find/sptdownload

You can also look to search a local contact for assistance on the following link:

http://www.agilent.com/find/assist

Warranty

Technology Licenses

Restricted Rights Legend

Safety Notices

CAUTION

A **CAUTION** notice denotes a hazard. It calls attention to an operating procedure, practice, or the like that, if not correctly performed or adhered to, could result in damage to the product or loss of important data. Do not proceed beyond a **CAUTION** notice until the indicated conditions are fully understood and met.

WARNING

A WARNING notice denotes a hazard. It calls attention to an operating procedure, practice, or the like that, if not correctly performed or adhered to, could result in personal injury or death. Do not proceed beyond a WARNING notice until the indicated conditions are fully understood and met.

Safety Symbols on Instruments

Indicates warning or caution. If you see this symbol on a product, you must refer to the manuals for specific Warning or Caution information to avoid personal injury or damage to the product.

Frame or chassis ground terminal. Typically connects to the equipment's metal frame.

Indicates hazardous voltages and potential for electrical shock.

Indicates that antistatic precautions should be taken.

Indicates hot surface. Please do not touch.

Indicates laser radiation turned on.

Safety requirements for electrical equipment for measurement, control, and laboratory use CAN/CSA C22.2 No. 1010.1 (1993) UL 3101, 3111 (First Editions) This equipment has also been evaluated to IEC 61010 edition 1 including amendments 1 and 2.

Notice for European Community: This product complies with the relevant European legal Directives: EMC Directive 89/336/EEC and Low Voltage Directive 73/23/EEC.
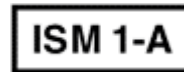
This is the symbol for an Industrial, Scientific, and Medical Group 1 Class A product.

Environmental Information

	This product complies with the WEEE Directive (2002/96/EC) marking requirements. The affixed label indicates that you must not discard this electrical/ electronic product in domestic household waste. *Product Category: With reference to the equipment types in the WEEE Directive Annex I, this product is classed as a "Monitoring and Control instrumentation" product.* **Do not dispose in domestic household waste.** **To return unwanted products, contact your local Agilent office, or see www.agilent.com/environment/product/ for more information.**

Contents

4   Testing the Installation

Index

1

System Requirements

The System Protocol Tester platform comprises various software components that are categorized into two broad categories: Controller and Client. You can install these software components on a single PC or on multiple PCs. In the first case, both the Controller and Client software are installed on the same PC. In the latter case, the Controller software is installed on the Controller (a.k.a *Server*) PC and the Client software is installed on the Client PC.

In this chapter, you will learn about the installation requirements that you need to ensure before starting installing System Protocol Tester on the Controller PC and on the Client PC.

Agilent Technologies

About the Installation Requirements

Prior to starting the installation process, ensure that all the system requirements to install the software components of the System Protocol Tester platform are in place.

In the following sections, you will learn about the requirements of the Controller and Client PCs.

Controller PC Requirements

- USB 2.0 interface for each N5308A Exerciser card is there.
- Windows 2000 (with Service Pack 3 or higher) or Windows XP (with Service Pack 2) operating system is installed.
- At least 256 MB RAM is installed. For better performance, Agilent recommends you to install 512 MB RAM or higher.
- At least 500 MB free disk space is available on the C drive.
- One 100BaseT LAN interface is installed.

  Agilent recommends to install two 100BaseT LAN interfaces for concurrent access to the corporate network or other clients.

  You can also use the USB network adapter, which comes with System Protocol Tester, as a second LAN interface.

Client PC Requirements

- Windows 2000 (with Service Pack 3 or higher) or Windows XP (with Service Pack 2) operating system is installed.
- At least 256 MB RAM is installed. For better performance, Agilent recommends you to install 512 MB RAM or higher.
- One 100BaseT LAN interface is installed.
- At least 500 MB free disk space is available on the C drive.
- Microsoft .NET Framework 1.1 is installed.

NOTE	If you do not have Microsoft .NET Framework 1.1, you can find it on the installation CD.

2

Setting Up the Hardware

Once all the system requirements are in place, you need to start setting up the hardware for the System Protocol Tester platform. This requires you to set up basic hardware for Protocol Exerciser and Protocol Analyzer.

Agilent Technologies
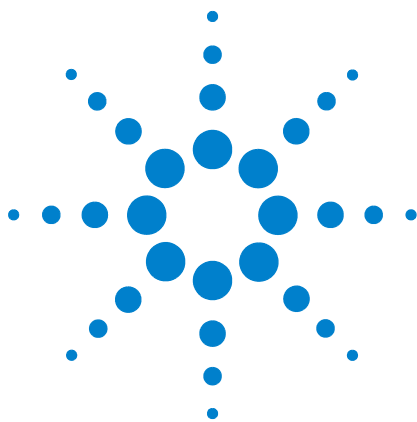
Understanding the Hardware Setup for System Protocol Tester

Before you start setting up different hardware components for System Protocol Tester, it would be a good idea to get a view of the final setup of the system.

Figure 1 shows one of the possible interconnection of N5316A Test Backplane, Exerciser Card, Midbus Probe, and Chassis.

Midbus Probe Tip

Two Slot Chassis

Exerciser Card

Metal Sheet mounted on the Backplane board

N5316A Test Backplane Board

Power Switch

N5306A I/O Module

Module Connector of a Midbus Probe plugged into Analyzer Probe of N5306A I/O Module
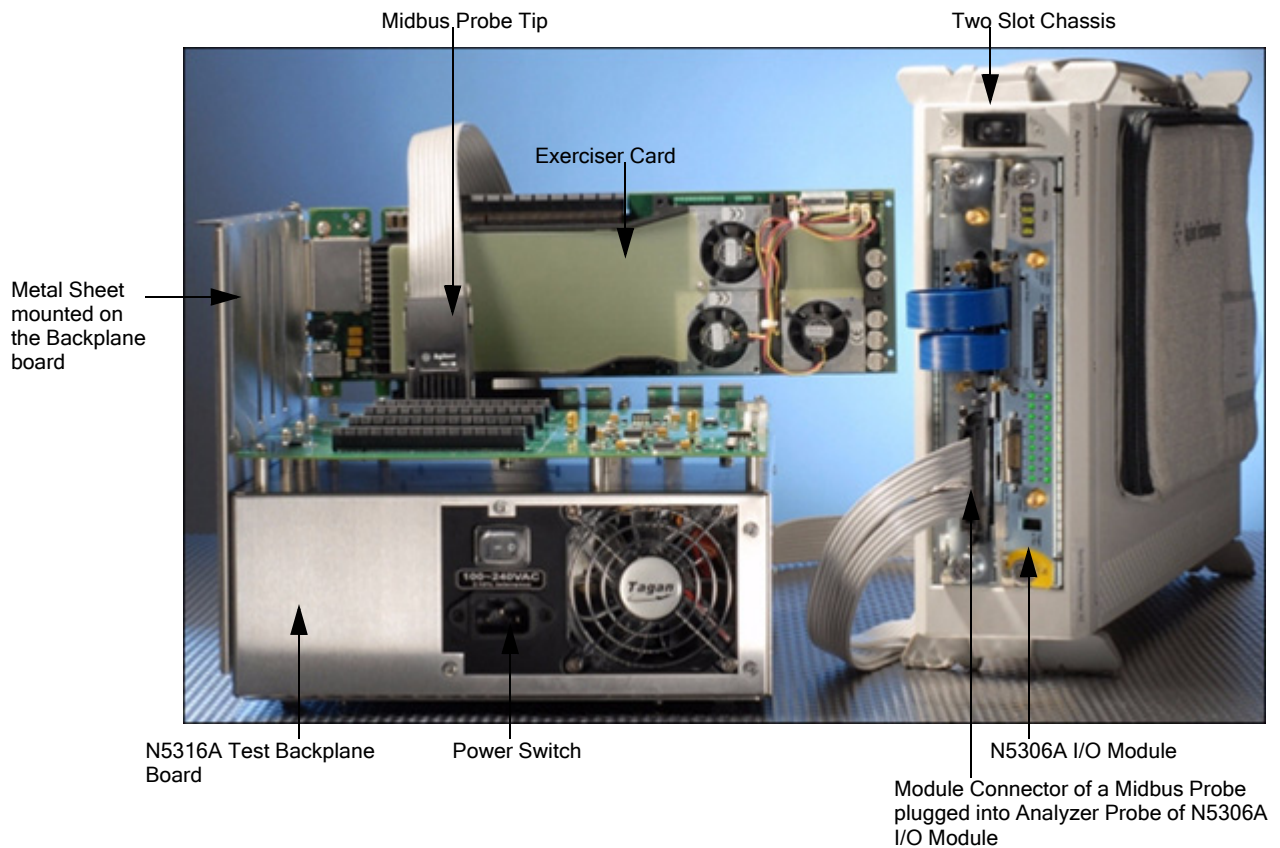
Figure 1   System Protocol Tester Hardware Setup

In the above figure:

- The two slot chassis shown is mounted with two N5306A I/O modules.
- The midbus probe is mounted on the backplane board and is also connected with the N5306A I/O module.
- The exerciser card is mounted on the backplane board.

- The metal sheet is mounted on the backplane board and is supporting the exerciser and PCIe cards.

   To mount the metal sheet on the backplane board:

   - Align the metal sheet *feeders* to the *clamps* on the the backplane board. This helps the metal to hold tight after it is properly attached to the backplane board.

   - Insert the *screw lock mouth* of the metal sheet into the *screw thread* on the backplane board.

   - Tighten the *screw lock head* of the metal sheet.

   - Connect the *fan cable* of the fans on the metal sheet to an appropriate *fan connector* on the backplane board. This completes mounting the metal sheet on the backplane board (Figure 2).
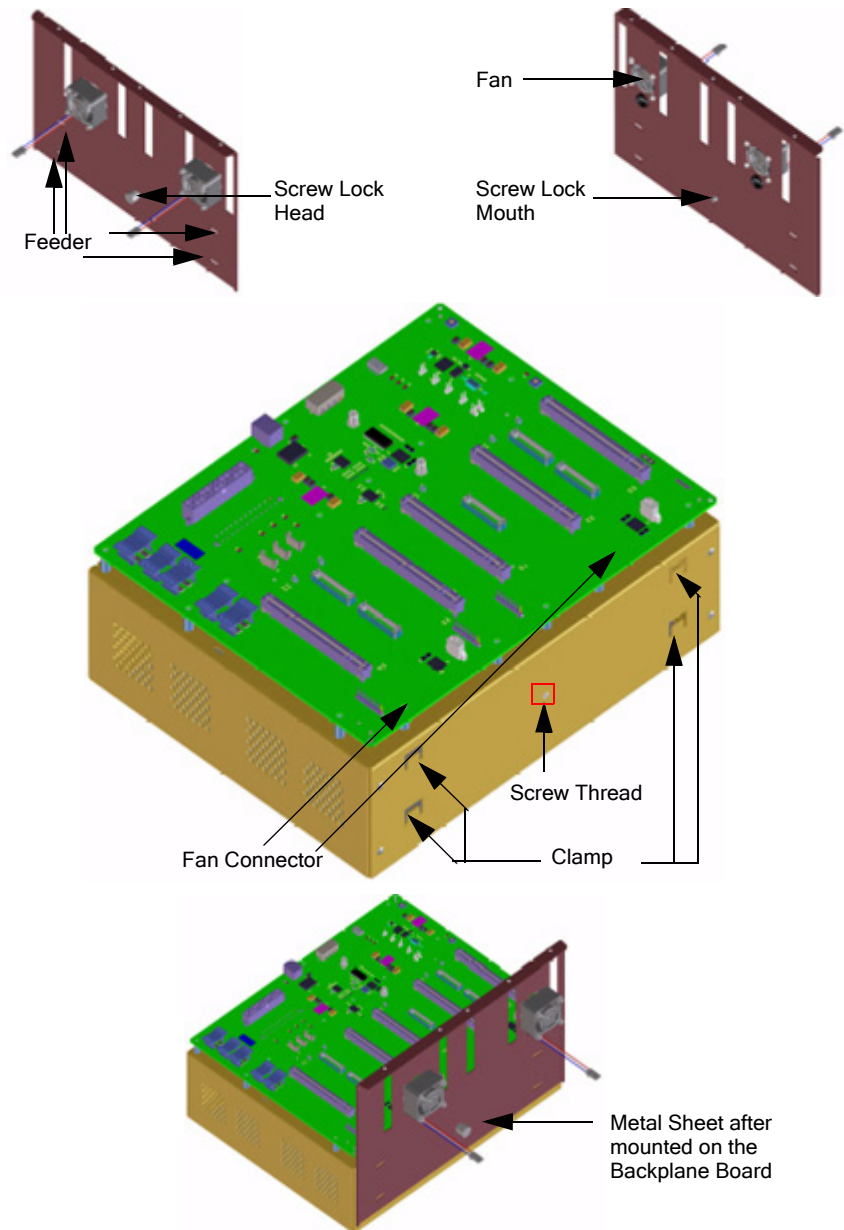
Figure 2   Mounting Metal Sheet on the N5316A Backplane Board

- The *N5316A test backplane* board for PCIe 5 Gb/s, shown in Figure 1 and Figure 2, is *passive*. This board has:
  - Five *retention modules* for midbus probe.
  - Five *PCIe connectors* for the slot interposer cards, exerciser cards, and other add-in cards (like LAN or graphic card).

• Five *REFCLK connectors* (reference clock connector), one for each PCIe connector. You use these connectors when you want to supply external clock feed to the PCIe connectors. In this situation, you use the *Y-cable*, whose tail is plugged into the external clock source and two heads into the two REFCLK connectors.

The main application of this board is in testing an add-in card, such as a LAN or graphic card, using an exerciser card and a midbus probe. In this case, you plug the exerciser card into one PCIe connector and the add-in card into the other PCIe connector. Then, you plug the midbus probe into one of the retention module between the add-in and exerciser cards. This enables you to capture and analyze the traffic flowing between the add-in and Exerciser cards.

Figure 3 highlights some of the important components of the N5316A test backplane board for PCIe 5 Gb/s.
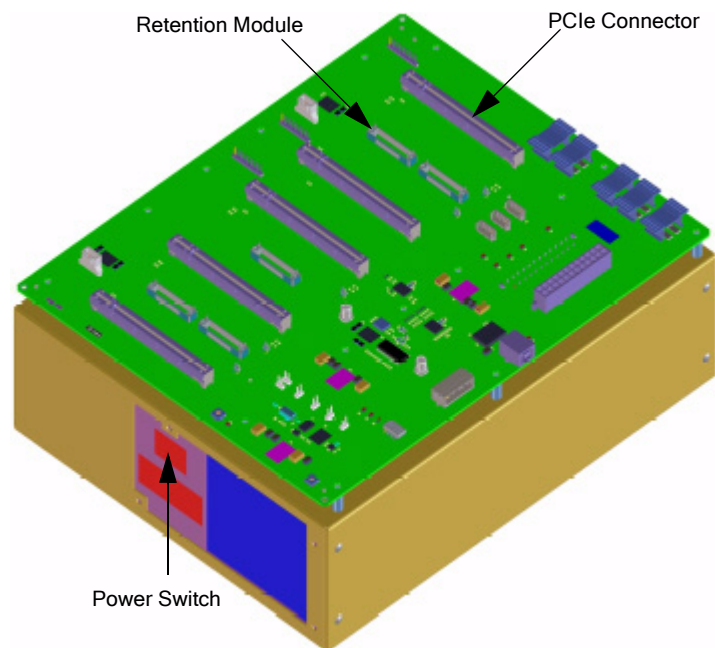
Figure 3   N5316A Backplane board

CAUTION   During normal operations, N5316A operates safely. Nevertheless, the circuits of 3.3V and 12V on PCI Express connectors and 5V on the Power Output connector are not limited and may provide currents higher than 8A. In case of failure, for example short circuit, such a circuit presents the risk of causing fire. Therefore, to limit the energy and avoid damage, we urgently recommend implementing one of the following preventive measures:

1. Limit the circuits of your product under test with a 4A IEC fuse (5A UL fuse) at the input.

2. Operate the N5316A in a fire enclosure.

Table of electrical specification is given below:

U⎓ Output	Imax Output
+3.3V	28A
+5V	42A
+12V	22A

NOTE   For complete information on the N5316A Test Backplane Board for PCIe 5 Gb/s, refer to the *Agilent System Protocol Tester, Hardware and Probing Guide*.

NOTE   For more information on setting up the exerciser card, I/O modules, chassis, and midbus probe, refer to their respective sections below in the chapter.

Setting Up the Hardware for Protocol Exerciser

In System Protocol Tester, you can set up hardware for Protocol Exerciser by plugging one or multiple exerciser cards into the motherboard or by mounting them on the backplane board.

You generally mount an exerciser card on backplane when you want to test an add-in card, such as a LAN or a graphic card.

Figure 4 displays an exerciser card.

Power Supply
Connector

USB Connector
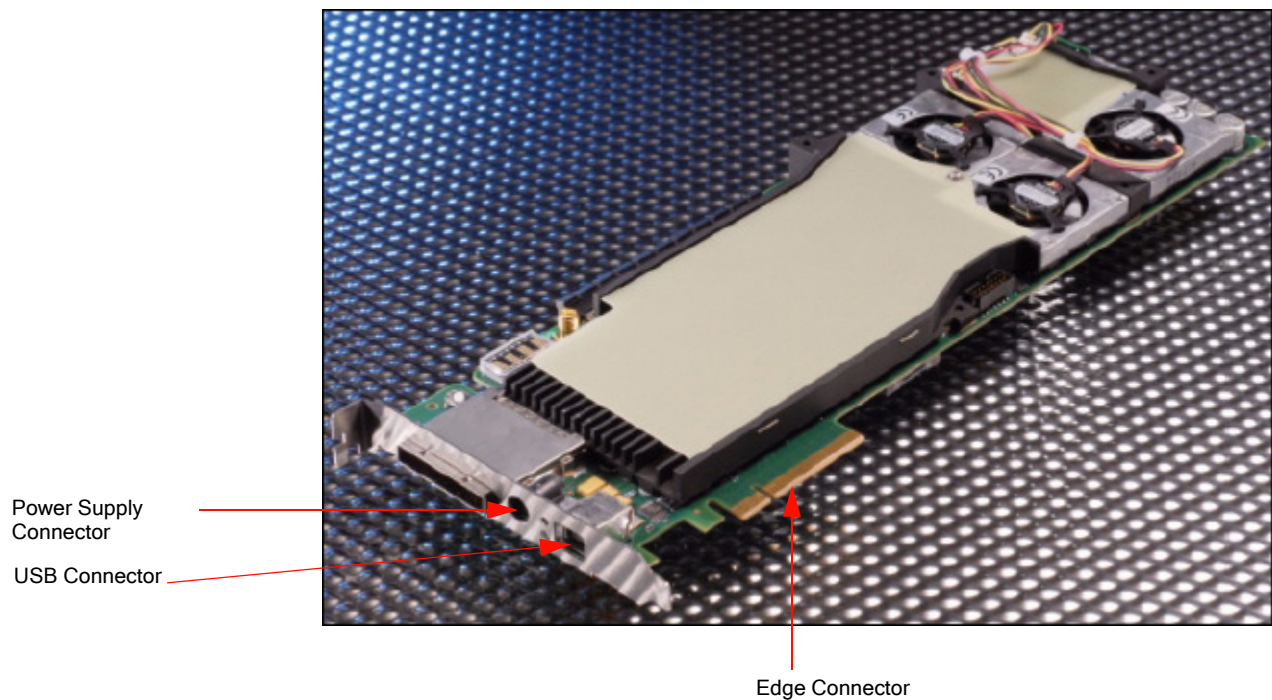
Edge Connector

Figure 4 Exerciser card

To Set Up Hardware for Protocol Exerciser

1 Plug the exerciser card's *Edge Connector* into a *PCIe Connector* on the backplane board, or into a system.

Figure 5 displays an exerciser card mounted on the backplane board.
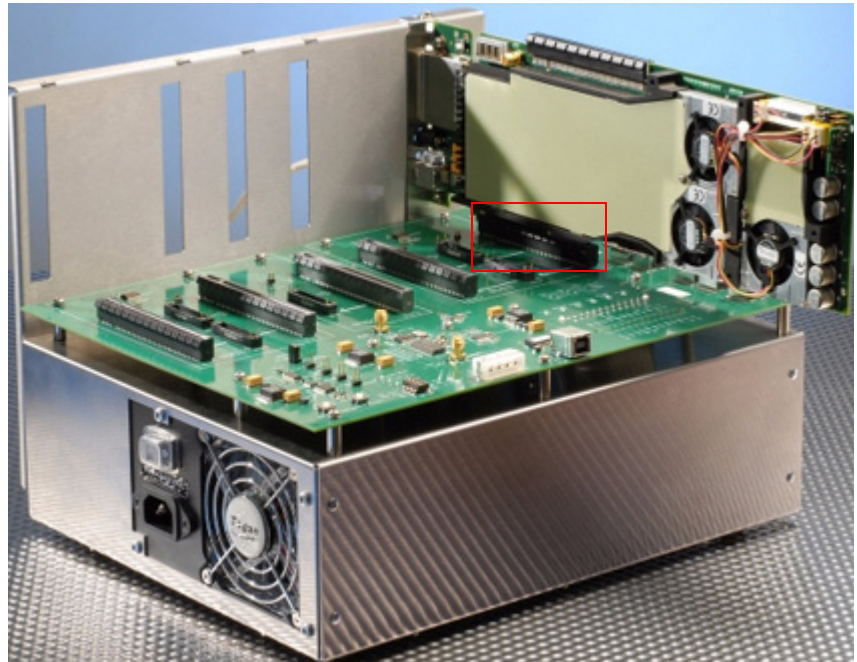
Figure 5   Exerciser Card mounted on N5316A Test Backplane

2   Connect the exerciser card with external power supply.

3   Connect the exerciser card with the Controller PC using the USB cable.

This completes the hardware setup for Protocol Exerciser.

CAUTION	Components on the I/O module are sensitive to the static electricity. Therefore, take necessary anti-static precautions, such as wear a grounded wrist strap, to minimize the possibility of electrostatic damage. Also, you should not operate a chassis with empty slots. Fill empty slots with blanking plates to ensure correct operation of the chassis.

CAUTION	This product is a plug-in printed board and has no encloser. For the purpose of safe use when utilized outside of PCI Slots, the product may only be operated under supervision and on surfaces complying with flammability class V-1 or better acc. to IEC60695 or UL94.

NOTE   You can also use an N5305A I/O module and an active probe board as an exerciser. In this case:

1 Plug the one end of the active probe board into DUT.
2 Connect the other end of the active probe board into the I/O module (N5305A I/O module). Use probe cable to connect active probe board with the I/O module.
3 Connect the chassis, comprising the I/O module, with the controller PC.
4 Start the Protocol Exerciser GUI.

For information on setting up I/O modules and chassis, and connecting chassis with the controller PC, refer to the sections given below in this chapter.

For information on using the Protocol Exerciser GUI, refer to *Agilent Protocol Exerciser, User's Guide*.

NOTE   For complete information on exerciser card, refer to *Agilent System Protocol Tester, Hardware and Probing Guide*.

Setting Up the Hardware for Protocol Analyzer

Setting up the hardware for Protocol Analyzer requires setting up the I/O modules, chassis, and midbus probe.

NOTE	The information provided in the following two sections: *Setting Up the I/O Modules* and *Setting Up the Chassis*, is also applicable to all the N5305A and N5306A I/O modules based solutions.

Setting Up the I/O Modules

To set up various I/O modules, you need to know how to attach as well as remove them to and from the chassis.

To attach an I/O module to the chassis

1 Insert the I/O module inside the empty slot and push it to adjust it inside the empty slot (Figure 6).
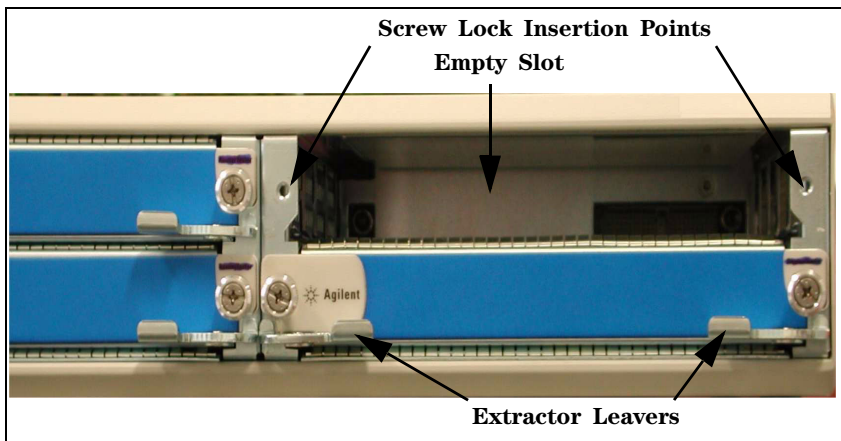
Figure 6   Chassis with an Empty Slot

2 Tighten the screw locks of the I/O module.

The I/O module is now attached to the chassis.

To remove an I/O Module from the Chassis

1 Unscrew the screw locks (Figure 7).
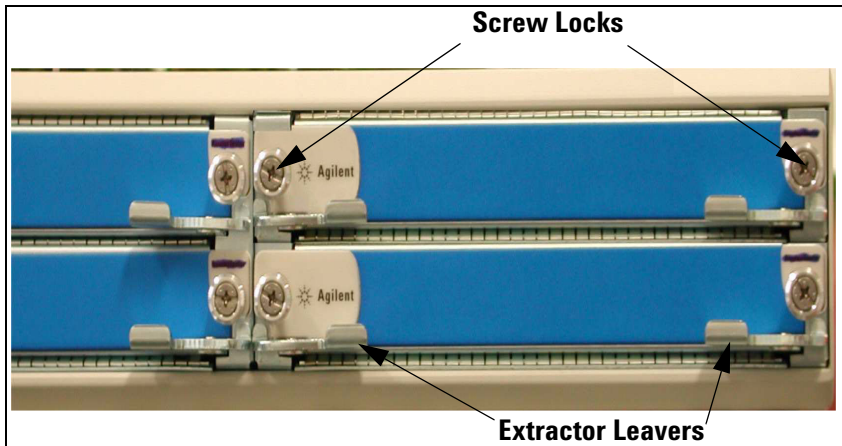
Figure 7   Chassis with I/O Modules

2 Pull the extractor levers outside the chassis.

3 Pull out the I/O module to remove it from the chassis.

Once you have removed the I/O module from the chassis, hold it by the front panel and metal case, and place it on a hard and flat surface.

WARNING	**Do not directly touch any component on the I/O module. It may be hot.**

CAUTION	Components on the I/O module are sensitive to the static electricity. Therefore, take necessary anti-static precautions, such as wear a grounded wrist strap, to minimize the possibility of electrostatic damage. Also, you should not operate a chassis with empty slots. Fill empty slots with blanking plates to ensure correct operation of the chassis.

Setting Up the Chassis

There are two types of chassis: the two-slot chassis and the four-slot chassis. You may require to use one or both types of chassis. You also require to connect the chassis to the Controller PC to establish a two-way communication link between the chassis and the Controller PC.

A single chassis is set when you are done setting up the I/O modules in it. However, to set up multiple chassis, you need to arrange them properly and ensure proper interconnections between them.

| NOTE | In the multiple chassis arrangement, the distance between the chassis position and the device under test (DUT) is limited by the length of the connector/probe cable. |

To set up multiple chassis

1 Arrange one chassis over another to form a stack of chassis. To do this:

   a Insert the rubber feet at the bottom of the four-slot chassis. These rubber feet come as accessories with a four-slot chassis.

   b Create a pile of the chassis, as shown in Figure 8.
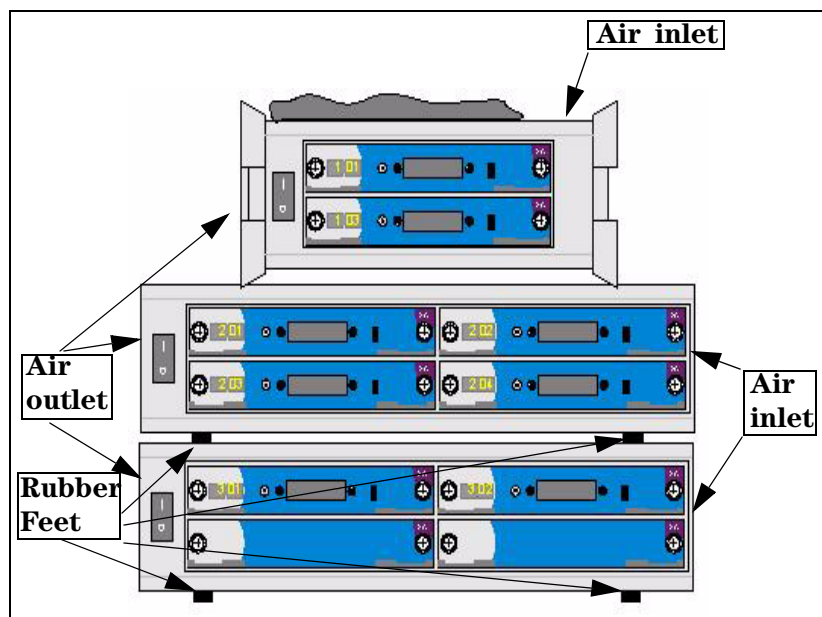
Figure 8   Pile of Chassis

NOTE	You can also mount the four-slot chassis in a standard 19-inch rack. Their accessories include two mounting brackets, screws, and clip-on hexnuts to attach them to the front posts. The rear posts of four-slot chassis are not used.

CAUTION	All chassis have ventilation holes. Do not block these holes while setting up or mounting chassis, Instead, leave at least the 50 mm (2 inches) gap free around all ventilation holes to protect the device from overheating.

2 Select the chassis you want to use as the *master chassis.*

3 Connect the master chassis with the slave chassis using the *N2X Chassis to Chassis* cable.

The N2X Chassis to Chassis cable is used to connect two N2X chassis. This cable and sync ports are color-coded, such as the *pink* color represents *Sync OUT* and the *green* color represents *Sync IN*.

Ensure that all the chassis, connected to a single controller PC, are properly interconnected using N2X Chassis to Chassis cables. This allows proper enumeration and synchronization of modules. The operation fails if any two or more chassis are not interconnected.

Figure 9 shows the interconnection between the master chassis and the slave chassis. Here, lower chassis is the master.

MDI Port   MDI-X Port

Figure 9   Interconnection between the Master and Slave Chassis

4 All chassis connected to a single controller PC need interconnection with the N2X Chassis to Chassis cables to allow proper enumeration and synchronization of modules. Operation will fail if any two or more chassis are not interconnected.

5 Connect the LAN ports (MDI and MDI‑X) of the chassis using the *Straight‑Through* LAN cables to daisy‑chain them starting from the MDI port of the master chassis to the MDI‑X port of the slave chassis.

6 Connect all the chassis to the main power.

WARNING	Do not block access to the power cord or the power switch. This helps you to immediately disconnect the power supply in case of emergency.

Setting Up the Midbus Probe

Once you are done setting up the I/O modules and chassis, set up the midbus probe.

Module Connector   Midbus Probe Tip

Figure 10   Midbus Probe

NOTE	For complete information on midbus probes, refer to the *Midbus Series 2.0 of Probes using Soft Touch Technology, User's Guide*.

To set up the midbus probe

1   Select the midbus cable (*straight, swizzled, or split*) that best suits the design.

2   Plug the midbus probe tip into the retention module on the backplane board (Figure 11).

Figure 11   Connecting Midbus Probe Tip

3   Plug the module connector into the *Analyzer Probe* slot on the N5306A I/O module (Figure 12).

This completes the hardware setup for Protocol Analyzer.
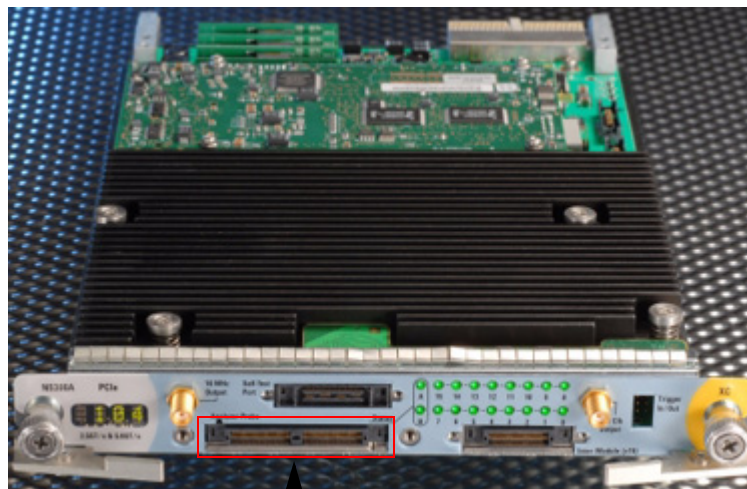
Analyzer Probe

Figure 12   N5306A I/O Module

NOTE	For complete information on N5306A I/O module, refer to the *Agilent System Protocol Tester, Hardware and Probing Guide*.

NOTE	You can also use an N5305A I/O module and an active or a passive probe board as a Protocol Analyzer hardware device. In this case:

1 Plug the one end of the active/passive probe board into DUT.
2 Connect the other end of the active/passive probe board into the I/O module (N5305A I/O module). Use probe cable to connect active/passive probe board with the I/O module.
3 Connect the chassis, comprising the I/O module, with the controller PC.
4 Start the Protocol Analyzer GUI.

For information on connecting chassis with the controller PC, refer to the following section.

For information on using the Protocol Analyzer GUI, refer to *Agilent Protocol Analyzer, User's Guide*.

Using the N5317A Cable

There may be a situation when you have the following devices only, and you need to setup Protocol Analyzer:

- Active or passive probe board
- Midbus probe
- N5306A I/O module

In this situation, you can use the N5317A cable (Figure 13).

Power Connector

Active/Passive Probe Connector

Midbus Probe Connector
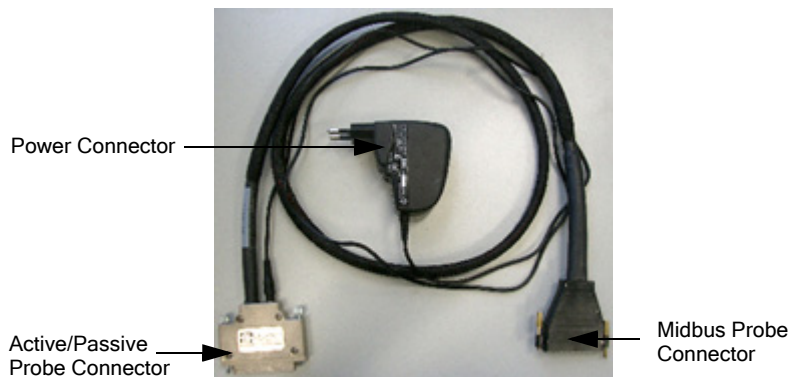
Figure 13 N5317A Cable

To Setup Protocol Analyzer Using the N5317A Cable

1 Plug the *active/passive probe connector* of the N5317A cable into the underlying active or passive probe board.

2 Plug the *midbus probe connector* of the N5317A cable into the midbus probe tip.

3 Ensure that the module connector of the midbus probe is connected with the N5306A I/O module.

4 Plug the power connector of the N5317A cable into an appropriate power switch.

5 Turn the power on.

   This sets up the Protocol Analyzer hardware using the N5317A cable.

Connecting a Chassis to the Controller PC

After setting up Protocol Exerciser and Analyzer, you can connect the master chassis to the Controller PC. For this, you can refer to the following arrangements, as applicable:

*   **No LAN interface available**: In this situation, you can use the USB network adapter, which comes with System Protocol Tester, to connect the Controller PC to the master chassis.

    The advantage of this arrangement is that you can set up a test environment easily at different places. For example, you can use a mobile instrument, such as laptop, as Controller PC and connect it directly to the chassis.

*   **Single LAN interface available**: In this situation, you can:

    *   Connect the chassis to the Controller PC through the private LAN.

    *   Use the USB network adapter, which comes with System Protocol Tester, as a second LAN interface.

    The advantage of this arrangement is that you can access the Controller PC from anywhere within the corporate LAN. For example, multiple Client PCs can access the Controller PC through the corporate LAN.

NOTE	The two-slot chassis and the four-slot chassis have the same connector assembly at the rear.

To connect the master chassis to the Controller PC

*   Connect the MDI-X port of the master chassis to the Controller PC using the standard LAN cable.

*   Or, connect the MDI-X port of the master chassis to the USB network adapter using the standard LAN cable.

NOTE	Do not connect the USB cable of the USB network adapter with the Controller PC until installation wizard prompts you for it.

3

Installing System Protocol Tester

Once you have set up the hardware, you can start installing the software components that come with the installation CD of the System Protocol Tester platform.

If you are planning to install these software on a single PC, then you first need to run the installation file. After this, you need to configure the Dynamic Host Configuration Protocol (DHCP) service on your Windows operating system.

However, if you are planning to install these software on multiple PCs, then you first need to configure the Controller PC to set up the FTP service, and to modify the firewall security and the DCOM server. After this, you can run the installation file and configure the DHCP service.

Agilent Technologies

About Configuring the Controller PC

You need to configure the Controller PC to enable communication between the Controller and Client PCs for data interchange.

In order to configure the Controller PC, you need to set up the FTP service, and configure the firewall service and the DCOM server.

In this section, you will learn about:

- Setting Up the FTP
- Setting Up the Firewall
- Configuring DCOM

NOTE	You do not have to configure the Client PC if you have planned to install both the Controller and Client software on a single PC.

Setting Up the FTP

On the Controller PC, you need to install and enable the FTP service to download firmware for various test modules. For this requirement, System Protocol Tester provides a third- party FTP server named WARftp.

Remember the following about WARftp while installing System Protocol Tester:

- WARftp is automatically installed and configured while installing System Protocol Tester.
- WARftp is installed only when the default FTP service is not installed on the Controller PC.
- Do not install WARftp prior to installing System Protocol Tester.
- Uninstall WARftp if it is already installed, as it halts the installation of System Protocol Tester.

NOTE	WARftp restricts many organizations, such as government organizations, from using it. For more information on using WARftp, please refer to www.warftp.org. Also, please refer to the license notes to find out if you can use WARftp.

If you are not allowed to use WARftp, you can use the FTP server that comes with the Windows operating system. In Windows, FTP is a part of Internet Information Services (IIS).

In this section, you will learn:

To Install FTP

1 Click **Start > Settings > Control Panel**.

The Control Panel window appears.

2 Double-click the **Add/Remove Programs** icon.

The Add/Remove Programs window appears.

3 Click the **Add/Remove Windows Components** button.

The Windows Components Wizard dialog box appears.

4 Select the **Internet Information Services (IIS)** check box in the Components list box.

5 Click **Details**.

The Internet Information Services (IIS) dialog box appears.

6 Select the **File Transfer Protocol (FTP) Server** check box in the Subcomponents of Internet Information Services (IIS) list box.

This automatically selects the **Common Files** and **Internet Information Services Snap-In** check boxes.

7 Click **OK**.

This saves the changes you made and closes the Internet Information Services (IIS) dialog box.

8 Click **Next** to install IIS.

9 Click **Finish** to complete the installation process.

To Enable FTP

1 Click **Start > Settings > Control Panel**.

The Control Panel window appears.

2 Double-click the **Administrative Tools** icon.

The **Administrative Tools** window appears.

3   Double-click the **Services** icon.

     The **Services** window appears.

4   Select the **FTP Publishing Service** service from the Name column.

5   Select **Action > Start** to enable FTP.

Setting Up the Firewall

On the Controller PC, you need to configure firewall to enable communication between the Controller PC and the test modules. If you do not configure it properly, then firewall may fail System Protocol Tester by preventing communication between the Controller PC and test modules. Firewall may also prevent the serial I/O modules to acquire an IP address (through DHCP services), update their firmware (through FTP service), and download the FPGA code.

The System Protocol Tester GUI can run on two operating systems: Windows 2000 (with Service Pack 3 or higher) or Windows XP (with Service Pack 2).

Windows 2000 (with Service Pack 3 or higher) does not provide any default firewall. Therefore, if you are using Windows 2000, then you have to separately install and configure firewall as per your needs. However, Windows XP (with Service Pack 2) provides a default active firewall. You only need to configure it to enable communication between the Controller PC and test modules.

NOTE	This guide provides instructions to configure the default firewall that comes with Windows XP. For adding programs to other firewall software, please refer the documentation provided with the respective firewall software.

To configure firewall on Windows XP

1   Click **Start > Settings > Control Panel**.

     The Control Panel window appears.

2   Double-click the **Windows Firewall** icon.

     The Windows Firewall dialog box appears.

3   Click the **Exceptions** tab.

4   Click **Add Programs**.

The **Add a Program** dialog box appears.

5 Select **Protocol Analyzer** from the **Programs** list box.

6 Click **OK**.

7 Repeat steps 4 to 6 for Protocol Exerciser.

8 Click **OK**.

NOTE	An error message, *Cannot download embedded software to the modules*, indicates that I/O modules cannot get the embedded software and FPGA images from the Controller PC. This error message generally occurs due to improper configuration of the subnet mask, or because firewall is not properly configured for System Protocol Tester.

Configuring DCOM

You need to configure DCOM to allow the Client software to communicate with the Controller software.

In this section, you will learn:

- To configure the DCOM server on Windows XP
- To configure the DCOM server on Windows 2000

To configure the DCOM server on Windows XP

1 Click **Start > Settings > Control Panel**.

The Control Panel window appears.

2 Double-click the **Administrative Tools** icon.

The Administrative Tools window appears.

3 Double-click the **Component Services** icon.

The Component Services window appears.

4 Select the **Component Services** icon under **Console Root**.

5 Click the **Configure My Computer** icon on the toolbar.

The My Computer dialog box appears.

6 Select the **Default Properties** tab.

7 Ensure the following:

- **Enable Distributed COM on this computer** is selected.
- **Default Authentication Level** is **None**.
- **Default Impersonation Level** is **Identity**.

8 Select the **COM Security** tab.

9 Modify access permissions.

To allow local and remote access to anonymous:

a Click **Edit Limits**. The Access Permission dialog box appears.

b Select **ANONYMOUS LOGON** in the **Group or user names** list box.

c Select the **Allow** check box for the **Local Access** and **Remote Access** options in the **Permissions for ANONYMOUS LOGON** list box.

d Click **OK**.

To allow local and remote access to everyone:

a Click **Edit Default**. The Access Permission dialog box appears.

b Select **Everyone** in the **Group or user names** list box.

c Select the **Allow** check box for the **Local Access** and **Remote Access** options in the **Permissions for Everyone** list box.

d Click **OK**.

10 Modify launch and activation permissions.

To allow launch and activation permissions to anonymous:

a Click **Edit Limits**. The Access Permission dialog box appears.

b Select **ANONYMOUS LOGON** in the **Group or user names** list box.

c Select the **Allow** check boxes for the **Local Launch**, **Local Activation**, **Remote Launch**, and **Remote Activation** options in the **Permissions for ANONYMOUS LOGON** list box.

d Click **OK**.

To allow launch and activation permissions to everyone:

a Click **Edit Default**. The Access Permission dialog box displays.

b Select **Everyone** in the **Group or user names** list box.

c Select the **Allow** check boxes for the **Local Launch**, **Local Activation**, **Remote Launch** and **Remote Activation** options in the **Permissions for Everyone** list box.

d Click **OK**.

11 Click **Apply**.

12 Click **OK**.

The Component Services window appears.

13 Expand the **Component Services > Computers > My Computer** icon under **Console Root**.

14 Select the **DCOM Config** icon under **My Computer**.

This displays a list of processes in the **DCOM Config** pane on the right.

15 Right-click the **ResourceManager** icon in the DCOM Config pane.

16 Click **Properties** from the short-cut menu.

The ResourceManager Properties dialog box appears.

17 Click the **Identity** tab.

18 Select one of the following option buttons:

- **The interactive user**: Select to specify that the application runs using the identity of the user who is currently logged on to the computer. The security credentials of the currently logged on user are used when the application is authenticated to access resources. The disadvantage is if no one is logged on, then nothing will work.

- **The launching user**: Select to specify that the application runs using the security credentials of the user who launched the application in order to be authenticated in the domain. The launching user can be same as the interactive user.

19 Click the **Security** tab.

20 Modify access permissions for everyone.

To modify the access permissions for everyone:

a Select **Customize** in the Access Permissions section.

b Click **Edit**.

c Select **Everyone** in the **Group or user names** list box.

d Select the **Allow** check boxes for the **Local Access** and **Remote Access** options in the **Permissions for Everyone** list box.

e Click **OK**.

21 Modify launch and activation permissions for anonymous and everyone.

To modify the launch and activation permissions for anonymous and everyone:

a Select **Customize** in the Launch and Activation Permissions section.

b Click **Edit**.

c Select **Everyone** in the **Group or user names** list box.

d Select the **Allow** check boxes for the **Local Launch**, **Local Activation**, **Remote Launch** and **Remote Activation** options in the **Permissions for Everyone** list box.

e Select **ANONYMOUS LOGON** in the **Group or user names** list box.

f Select the **Allow** check boxes for the **Local Launch**, **Local Activation**, **Remote Launch** and **Remote Activation** options in the **Permissions for ANONYMOUS LOGON** list box.

g Click **OK**.

22 Click **Apply**.

23 Click **OK**.

The Component Services window appears.

24 Repeat steps 15 to 23 for **sessionexec**.

25 Select **File > Exit**.

26 Restart the PC.

To configure the DCOM server on Windows 2000

1 Select **Start > Run**.

The Run dialog box appears.

2 Type dcomcnfg in the **Open** editable drop-down list.

3 Click **OK**.

The Distributed COM Configuration Properties dialog box appears.

4 Click the **Application** tab.

5 Select **ResourceManager** from the Applications list box.

6 Click **Properties**.

The ResourceManager Properties dialog box appears.

7 Click the **Security** tab.

8 Select the **Use custom access permissions** option.

9 Click **Edit**.

The Register Value Permissions dialog box appears.

10 Click **Add**.

The Add Users and Groups dialog box appears.

11 Click **Search**.

The Find Account dialog box appears.

12 Type in the user name, to whom you want to grant access to the Controller PC, in the **Find User or Group** text box.

13 Click **Search**.

The search result is displayed in the Search Result list box.

14 Select the user name from the Search Result list box.

15 Click **Add**.

This adds the selected user name to the Add Names list box in the Add Users and Groups dialog box.

16 Select **Allow Access** from the **Type of Access** drop-down list.

17 Click **OK**.

This saves the user settings and adds its details in the Name list box of the Registry Value Permission dialog box.

18 Click **OK**.

This closes the Registry Value Permission dialog box and takes you back to the ResourceManager Properties dialog box.

19 Repeat steps 8 to 18 for the **Use custom launch permissions** and **Use custom configuration permissions** options.

20 Click **Apply**.

21 Click **OK**.

The Distributed COM Configuration Properties dialog box appears.

22 Repeat steps 4 to 21 for the *sessionexec* application.

23 Select the **Default Properties** tab.

24 Ensure the following:

- **Enable Distributed COM on this computer** is selected.
- **Default Authentication Level** is **None**.
- **Default Impersonation Level** is **Identity**.

25 Click **Apply**.

26 Click **OK**.

27 Restart the PC.

About Installing System Protocol Tester

Once you have prepared the system for installation, you can start installing System Protocol Tester on it. There are two ways to install System Protocol Tester. One is to install without using the USB network adapter, and the other is to install using the USB network adapter.

In this section, you will learn:

- To Install System Protocol Tester without the USB Network Adapter
- To Install System Protocol Tester with the USB Network Adapter

NOTE	Before moving to the next section, uninstall the N2X software if it is installed on the Controller PC.

NOTE	We continually improve our software. Therefore, we recommend you to check the following link to download and install the latest version:

http://www.agilent.com/find/sptdownload

To Install System Protocol Tester without the USB Network Adapter

1 Insert the installation CD in the CD drive.

The InstallShield wizard appears.

If the InstallShield wizard does not appears automatically, do the followings:

a Access the CD drive using Windows Explorer.

b Double-click the Setup.exe file.

2 The Agilent System Protocol Tester Setup window appears with the welcome screen of the installation wizard.

3 Click **Next**.

The Question dialog box appears if one or more legacy components are installed on your computer. This dialog box displays a list of installed legacy components, and prompts if you want to remove them.

Do the following:

a Click **Yes**. The uninstallation process starts. A message box appears that prompts if you want to remove QuickTest.

b Click **Yes**. This uninstalls QuickTest and other legacy components.

The Software License Agreement dialog box appears.

4 Click **Yes**.

The Choose installation location dialog box appears.

5 Specify the location where you want to install System Protocol Tester.

Do the following to specify the desired location to install System Protocol Tester:

a Click **Browse**. The Choose Folder dialog box appears.

b Select the location where you want to install System Protocol Tester.

c Click **OK**.

6 Click **Next**.

The Select Components screen appears.

7 Select the System Protocol Tester components you want to install.

8 Click **Next**.

The Setup Type dialog box appears.

9 Do one of the followings:

a Select the **Client Installation** list item if you want to install only the Client software on your PC.

b Select the **Controller PC Installation (includes client)** list item if you want to install both the Controller and Client software on your PC.

10 Click **Next**.

The Install extra components dialog box appears.

11 Select those extra components, which you want to install with the current System Protocol Tester installation, from the **Components** list box.

12 Click **Next**.

The Start copying files dialog box appears.

13 Click **Next**.

This installs System Protocol Tester and displays the ReadMe File dialog box.

14 Clear the **View Readme.txt** check box if you do not want to view the `Readme.txt` file.

15 Clear the **Run USB network adapter Config Helper** check box.

16 Click **Next**.

The Agilent System Test Protocol Setup complete dialog box appears.

17 Select **Yes, I want to restart my computer now**.

18 Click **Finish**.

To Install System Protocol Tester with the USB Network Adapter

1 Repeat steps 1 to 14 from the previous section.

2 Select the **Run USB network adapter Config Helper** check box.

3 Click **Next**.

A message box appears that prompts you to attach the USB network adapter to the Controller PC.

4 Attach the USB network adapter to the Controller PC.

5 Click **Yes**.

A message box, displaying the USB network adapter and DHCP settings, appears.

6 Click **Yes**.

A message box, displaying the Settings successfully modified message, appears.

7 Click **OK**.

The Agilent System Test Protocol Setup complete dialog box appears.

8 Select **Yes, I want to restart my computer now**.

9 Click **Finish**.

NOTE If you are using the USB network adapter, and has already used the Config Helper tool to configure the LAN interface and DHCP, jump to "Testing the Installation on page 47.

About Setting Up the DHCP Service

DHCP is a communications protocol that lets network administrators centrally manage and automate the assignment of IP addresses in a computer network. DHCP lets a network administrator supervise and distribute IP addresses from a central point and automatically sends a new IP address when a computer is plugged into a different place in the network.

The DHCP server installed with System Protocol Tester does not use the standard DHCP port. Rather, it uses the following special ports to avoid any interference with the DHCP server running within your corporate LAN:

- **7901**: This port is used to listen to the requests sent from a serial I/O module.
- **7902**: This port is used to listen to the responses/answers sent from the Controller PC.

Setting up the DHCP service for System Protocol Tester requires you to configure the LAN card and configure the DHCP service.

Configuring the LAN interface

You need to configure the LAN card on the Controller PC to establish a private LAN connection between the Controller PC and the chassis.

To configure the LAN interface

1 Click **Start > Settings > Control Panel**.

   The Control Panel window appears.

2 Double-click the **Network and Dial-up Connections** icon.

   The Network and Dial-up Connections window appears.

3 Select the icon that represents LAN card for private network.

4 Click **File > Properties**.

   The Properties dialog box for the selected LAN card appears.

5 Click the **General** tab.

6 Select the **Internet Protocol (TCP/IP)** check box in the **Components checked are used by this connection** list box.

7 Click **Properties**.

The Internet Protocol (TCP/IP) dialog box appears.

8 Select **Use the following IP address**.

9 Type in the following information in the **IP address**, **Subnet mask**, and **Default gateway** text boxes.

```
IP address: 10.0.0.1
```

```
Subnet mask: 255.0.0.0
```

10 Click **OK**.

11 Click **OK**.

Configuring DHCP

To configure DHCP, you need to update the DHCP configuration file (`dhcpd.conf`), restart the DHCP service, and update the DHCP registry file (`dhcpd.reg`) and the system registry.

In this section, you will learn to:

- To update the DHCP configuration file
- To restart the DHCP service
- To update the DHCP registry file and the system registry

To update the DHCP configuration file

1 Go to the `c:\dhcpdnt` directory.

2 Open the `dhcpd.conf` file in a text editor.

3 Modify the `subnet`, `netmask`, and `range dynamic-bootp` parameters, as desired.

4 Save the `dhcpd.conf` file.

5 Close the `dhcpd.conf` file.

NOTE	Before you move to the next section, ensure that the controller PC is connected with the chassis.

To restart the DHCP service

1   Click **Start - Settings - Control Panel**.

The Control Panel window appears.

2   Double-click the **Administrative Tools** icon.

The Administrative Tools window appears.

3   Double-click the **Services** icon.

The Services window appears.

4   Select **dhcpdNT** under the **Name** column.

5   Click **Action > Restart**.

This assigns IP addresses to the serial I/O modules according to the new settings.

To update the DHCP registry file and the system registry

1   Go to the `c:\dhcpdnt` directory.

2   Open the `dhcpd.reg` file in a text editor.

3   Modify the `Interface.0` parameter with the IP address of the LAN card that is connected to serial I/O modules.

The address you specify here should be within the subnet and is used as the DHCP server.

4   Save the `dhcpd.reg` file.

5   Close the `dhcpd.reg` file.

6   Double-click the `dhcpd.reg` file in Windows Explorer.

The Registry Editor dialog box appears asking if you want to update the system registry using the `dhcpd.reg` file.

7   Click **Yes**.

The Registry Editor message box displays prompting that the system registry has been successfully updated.

8   Click **OK**.

Updating the DHCP configuration file to use MAC addresses

If you do not want to use DHCP, then you can use MAC addresses of the serial I/O modules to assign them their IP addresses. For this, you need to update the DHCP configuration file in order to prepare it for using MAC addresses of the serial I/O modules.

To update the DHCP configuration file for using MAC addresses

1 Go to the `c:\dhcpdnt` directory.

2 Open the `dhcpd.conf` file in a text editor.

3 Comment out the following statements:

`boot-unknown-clients true;`

`range dynamic-bootp <range of ip addresses for modules>;`

To comment out these statements, insert the # symbol in the beginning.

Commenting these statements disables the automatic configuration of the IP addresses.

4 Uncomment the following function for each serial I/O module:

`#host <hostname for module>{`

`# hardware ethernet <MAC address of the module>;`

`# fixed-address <ip address to be assigned to this module>;`

`#}`

5 Replace the `<hostname for module>` parameter with the name of the serial I/O module.

6 Replace the `<MAC address of the module>` parameter with the MAC address of the serial I/O module.

You can find the MAC address of the serial I/O module on its label.

7 Replace the *<ip address to be assigned to this module>* parameter with the IP address of the serial I/O module.

The IP address of the serial I/O module should be within the defined subnet.

8 Save the `dhcpd.conf` file.

9 Restart the DHCP service.

For information on restarting the DHCP service, refer to

10 Reboot the serial I/O modules.

The new IP addresses are assigned to the serial I/O modules.

About Uninstalling the USB Network Adapter

Once you have used the USB network adapter in the installation process, you can remove it. However, doing this does not releases the IP address assigned to the USB network adapter. Therefore, any attempts to use that port displays an error, which prompts that the IP address is already assigned to a device. To avoid this situation, uninstall the USB network adapter before physically removing it from the computer.

To uninstall the USB network adapter

1 Right-click the **My Computer** icon.

2 Select **Manage** from right-click menu.

The Computer Management window appears (Figure 14).
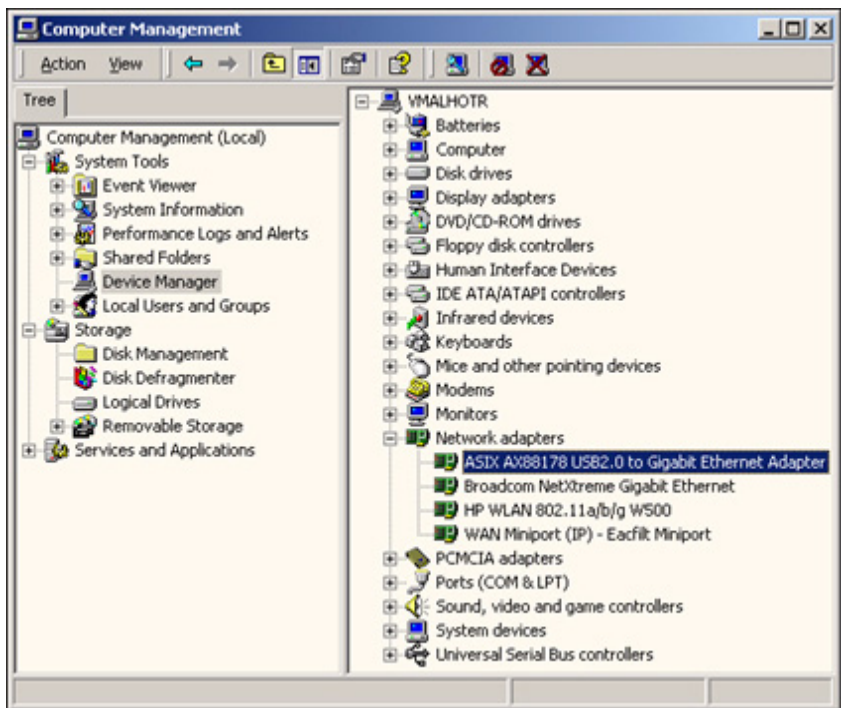
Figure 14   Computer Management window

3 Click the **System Tools > Device Manager** icon under the Tree tab.

This displays an expandable list of options in the right panel of the Computer Management window.

4 Expand the **Network adapters** icon.

A list of network adapters attached to your computer is displayed.

5 Right-click the option that represents the USB network adapter.

6 Select **Uninstall** from the context menu.

The Confirm Device Removal message box appears (Figure 15).
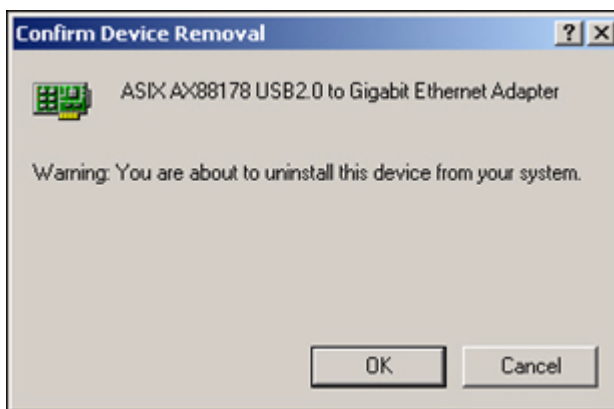
Figure 15 Confirm Device Removal message box

7 Click **OK**.

This uninstalls the USB network adapter. You can now remove the USB network adapter from the computer and assign its IP address to some other device.
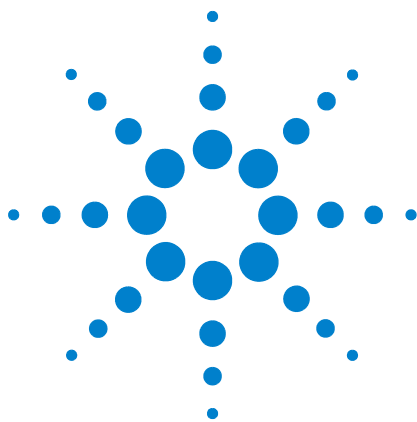
4

Testing the Installation

Once you have installed the System Protocol Tester platform, the next step is to test the installation.

In this chapter, you will learn to power up and power down the system, and to verify the hardware setup using the diagnostic tool.

Agilent Technologies

How to Power Up the System

After installing the System Protocol Tester platform, find out if it is starting up fine.

The following procedure tells you about how to power up the system.

To Power Up the System

1 Power up the Controller PC.

Powering up the Controller PC starts the AgtResourceManager service. This service keeps track of all the chassis that are connected to the Controller PC.

2 Power up the Ethernet switch or hub if you have connected the chassis through an Ethernet switch or hub.

3 Power up all the chassis that are connected to the Controller PC.

You can power up the chassis using the power switch, which is at the front of each chassis.

Powering up the chassis also boots the serial I/O modules that are installed in it.

4 View the matrix display of the serial I/O modules.

While booting, serial I/O modules display the following sequence:

BHW1 – BHW2 – BNET – BIP – BAPP –

KHW1 – KHW2 – KNET – KIP – KAPP

After booting, serial I/O modules display their numbers along with a trail of pixel snake around the border of the display area.

NOTE If some problem occur while booting, the code shows what stage was reached. A message may also gets scrolled across the display area.

NOTE To find out more information on System Protocol Tester, access online help. To access online help, click **Start > Programs > Agilent System Protocol Tester > Online Help**.

How to Power Down the System

The following procedure tells you about how to power down the system.

To Power Down the System

1 Shut down the Controller PC.

2 Switch off the Controller PC.

3 Switch off the chassis.

How to Verify the Hardware Setup

Agilent System Protocol Tester provides a diagnostic tool that you can use to verify if the setup for the System Protocol Tester platform or any of its hardware module is properly arranged.

NOTE	This diagnostic tool can be run only from the Controller PC.

Accessing the Diagnostic Tool

To access the diagnostic tool:

• Select the **Start > Programs > Agilent System Protocol Tester > Diagnostics** menu command.

The main Diagnostics Tool window appears (Figure 16).
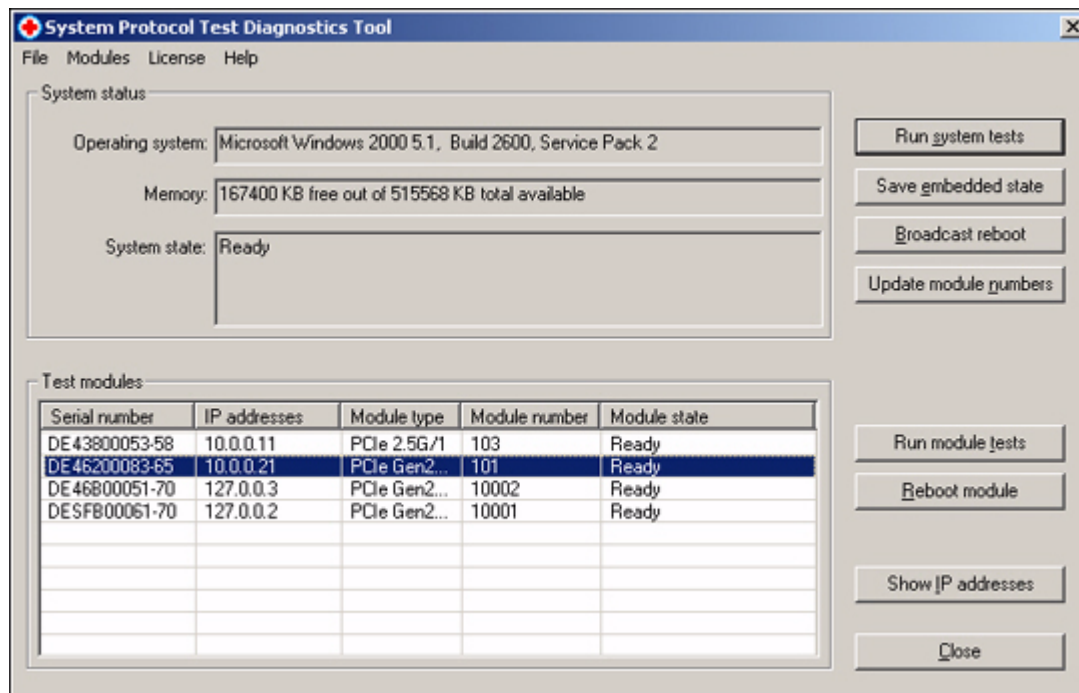
Figure 16   Diagnostics Tool window

| NOTE | Before you run any module test, ensure that no System Protocol Tester application, such as Protocol Analyzer or Protocol Exerciser, is running. |

To Test the Module using the Diagnostic Tool

1 Connect midbus probe with the Self-Test Port component of the N5306A I/O module.

To do this:

a Plug the module connector into the Analyzer Probe slot.

b Plug the midbus probe *tip* in the *Side B* of the loopback connector. While doing this, ensure that the while bullet on the midbus probe *tip* is facing the *upper section* of the Side B (Figure 17).
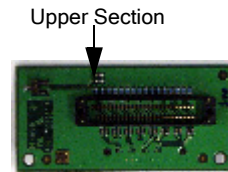
Upper Section

Figure 17   Upper section of Side B

c Plug the *Side A* of the *loopback connector* in the Self-Test Port.

Figure 18 shows the loopback connector.

Side B ──────────➤   ◄────── Side A
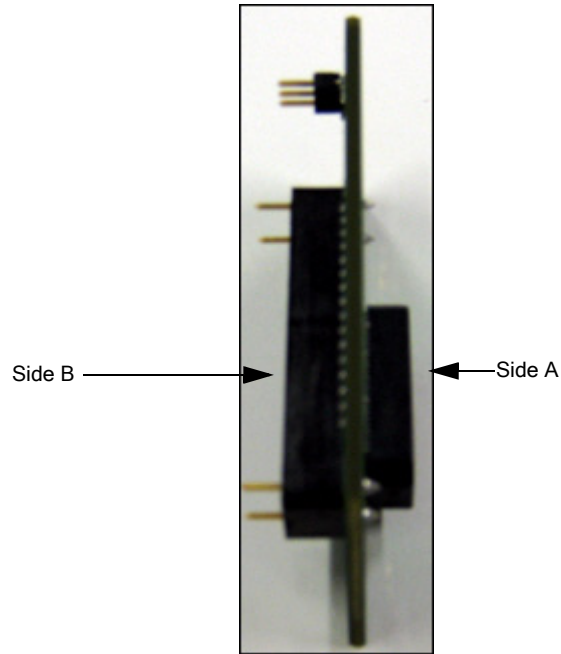
Figure 18   Loopback Connector

NOTE	Skip this step if you only want to test the DDR memory (DDR_Test). This step is needed only when you want to test the signal integrity of the I/O module's receivers (PRBS_Gen1_External_Loopback and PRBS_Gen2_External_Loopback).

2 Select the module, which you want to diagnose, in the Test modules section (Figure 16).

3 Click **Run module tests**.

The Self Diagnostics window appears (Figure 19).
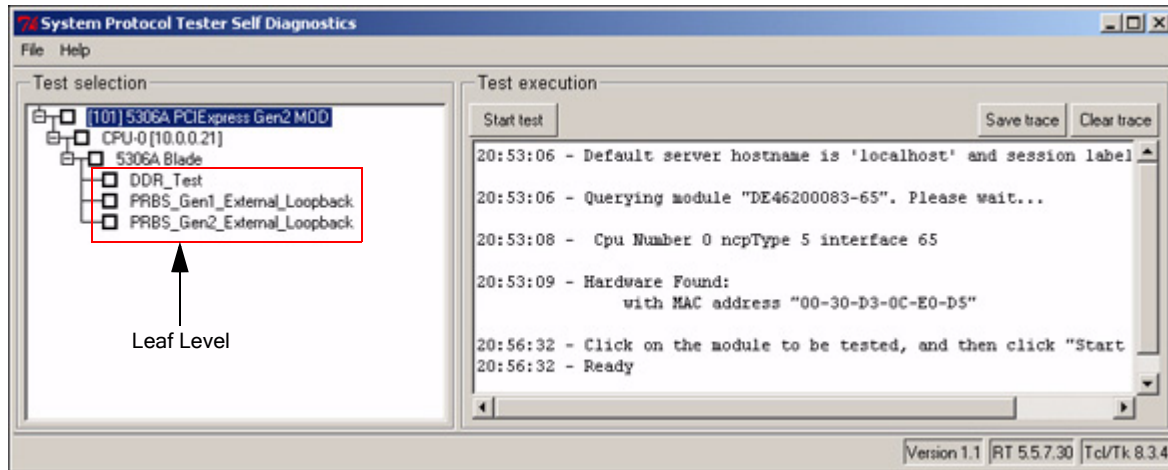
Figure 19   Self Diagnostics window

4 Expand the tree in the **Test selection** section to the *leaf level*.

The leaf level has the following diagnostic tests for the underlying module:

- **DDR_Test**: Use this test to verify if the DDR memory of the module is functioning properly.
- **PRBS_Gen1_External_Loopback**: Use this test to verify the signal integrity of the I/O module's receivers at the speed 2.5 Gb/s.
- **PRBS_Gen2_External_Loopback**: Use this test to verify the signal integrity of the I/O module's receivers at the speed 5 Gb/s.

NOTE	Owing to the continuous improvement of the product, there can be more diagnostic tests available in the tool.

5 Select one or more diagnostic tests, as desired.

6 Click **Start test** in the **Test execution** section.

Once the test completes, with success or fail result, its details are shown in the Text execution section (Figure 20).
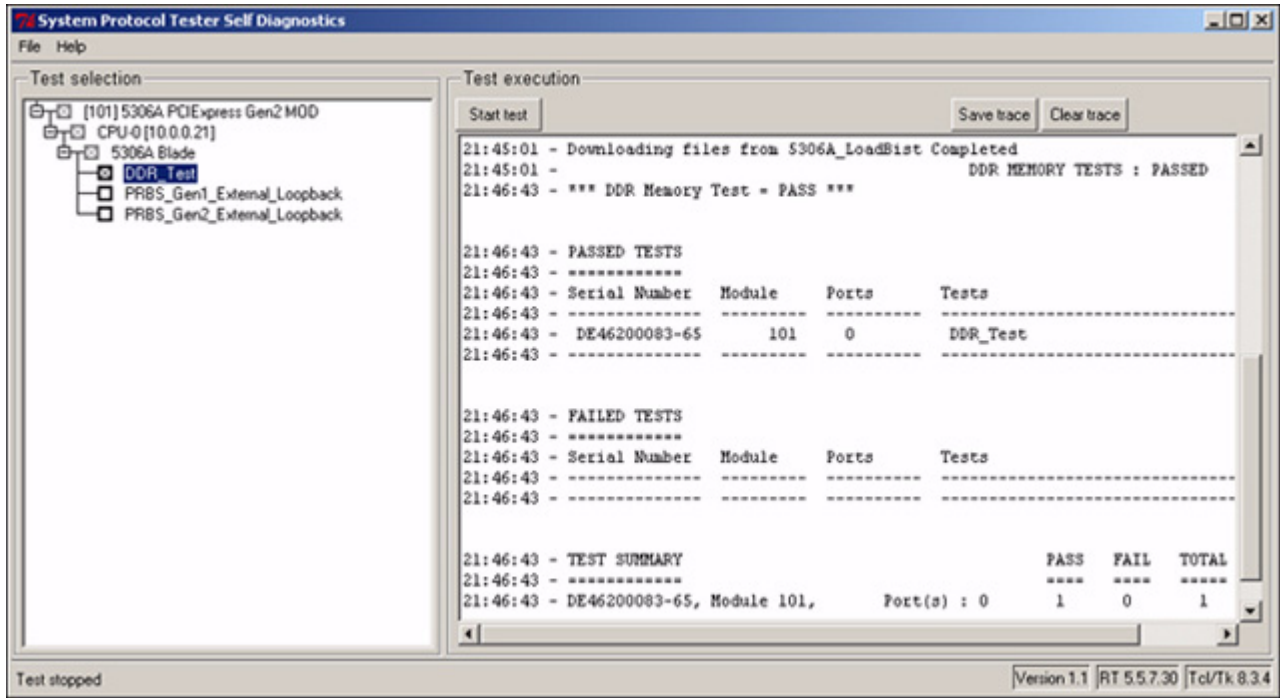
Figure 20   DDR test result after execution

| NOTE | If you used the straight midbus probe cable, then all MGTs show PASS. However, if you used the swizzle midbus probe cable, then depending on which of the two midbus probe tips used, only 8 MGTs show PASS. |

7 Click **Save trace** to save the test details.

This displays the **Save trace text** dialog box. Here, browse to the destination folder, and then save the test details in a file for later reference.

8 Click **Clear trace** to remove the test details from the Test execution section.

9 Select **File > Exit** to close the Self Diagnostic window.

Doing this also closes the main Diagnostics Tool window.

Index

Agilent Technologies