

Intelligent Test Framework Software Solutions Reference Guide



Version 3.1

ITFSS 03.10 p 1204

January 2005



Agilent Technologies



© Agilent Technologies, Inc. 2001-2005. All rights reserved.

No part of this manual may be reproduced in any form or by any means (including electronic storage and retrieval or translation into a foreign language) without prior agreement and written consent from Agilent Technologies, Inc. as governed by United States and international copyright laws.

Additional Notices


The material contained in this document is subject to change without notice.

Agilent Technologies makes no warranty of any kind with regard to this material, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Agilent Technologies shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this material.

Adobe®, Acrobat® are U.S. registered trademarks of Adobe Systems Incorporated.

Notepad®, WordPad®, Excel®, Windows®, and Microsoft® are U.S. registered trademarks of Microsoft Corporation.

Other trademarks and copyrights are owned by the respective companies mentioned in this document.



ITF Software Solutions Reference Guide

1 Overview of the ITF Software Solutions

Overview.....	1-2
Architecture of the Intelligent Test Framework 3.1	1-3
Key Features of ITF 3.1 Architecture.....	1-4
ITF 3.1 Server and Tester Communication	1-4
ITF 3.1 Server and ART/AQT Communication	1-6
ITF Server and System Administration	1-8
ITF Software Applications.....	1-9
Agilent Repair Tool	1-9
Agilent Quality Tool.....	1-9

2 Changing Preset Values

Overview.....	2-2
Changing the Port Number of the ITF Server.....	2-3
Changing the Web Application Port Number of the ITF Server	2-4
Changing the ITF Server Name and Port Number stored on the Tester Controller	2-5
Changing the Port Number of the Agent on the Tester Controller.....	2-6

3 Changing Log Levels for Logging

Overview.....	3-2
Changing the Log Level	3-3
Special Case for ITF Server.....	3-4

4 Backing up and Restoring ITF Data

Overview.....	4-2
Stopping the ITF and SQL Services	4-3
To stop the ITF services.....	4-3
To stop the SQL services	4-3
Phase 1: Backing up ITF Data	4-4
Preparing Backup data (Optional)	4-4
Estimated Speed of the Backup Process	4-4
Creating Backup Files on Tape.....	4-5
Phase 2: Restoring ITF Data.....	4-10
Starting the ITF and SQL Services	4-13
To start the SQL services.....	4-13
To start the ITF services	4-13

5 Understanding Drives and Drive Arrays

Overview.....	5-2
Drive Array.....	5-3
Array Controller.....	5-4
Fault Tolerance	5-5
RAID 1.....	5-6
Advantages.....	5-6
Disadvantage.....	5-6
RAID 5 - Distributed Data Guarding (Distributed Parity Blocks)	5-7
Advantages.....	5-7
Disadvantages	5-7
LED Patterns on the Hard Drive.....	5-8

6 Gathering Information for Technical Support

7 Useful Network Utilities

Overview.....	7-2
Ipconfig.....	7-3
Ping.....	7-4
Traceroute.....	7-5
Netstat.....	7-6
Nbstat.....	7-7
DHCP and DNS.....	7-8
IP Addressing.....	7-9
Static and Dynamic IP addresses.....	7-9
Private IP addresses.....	7-9
MAC Addressing.....	7-10

1

Overview of the ITF Software Solutions

In this chapter...

- [Overview](#), 1-2
- [Architecture of the Intelligent Test Framework 3.1](#), 1-3
- [ITF Server and System Administration](#), 1-8
- [ITF Software Applications](#), 1-9

Overview

This chapter provides you with an overview of the ITF Software Solutions architecture and components.

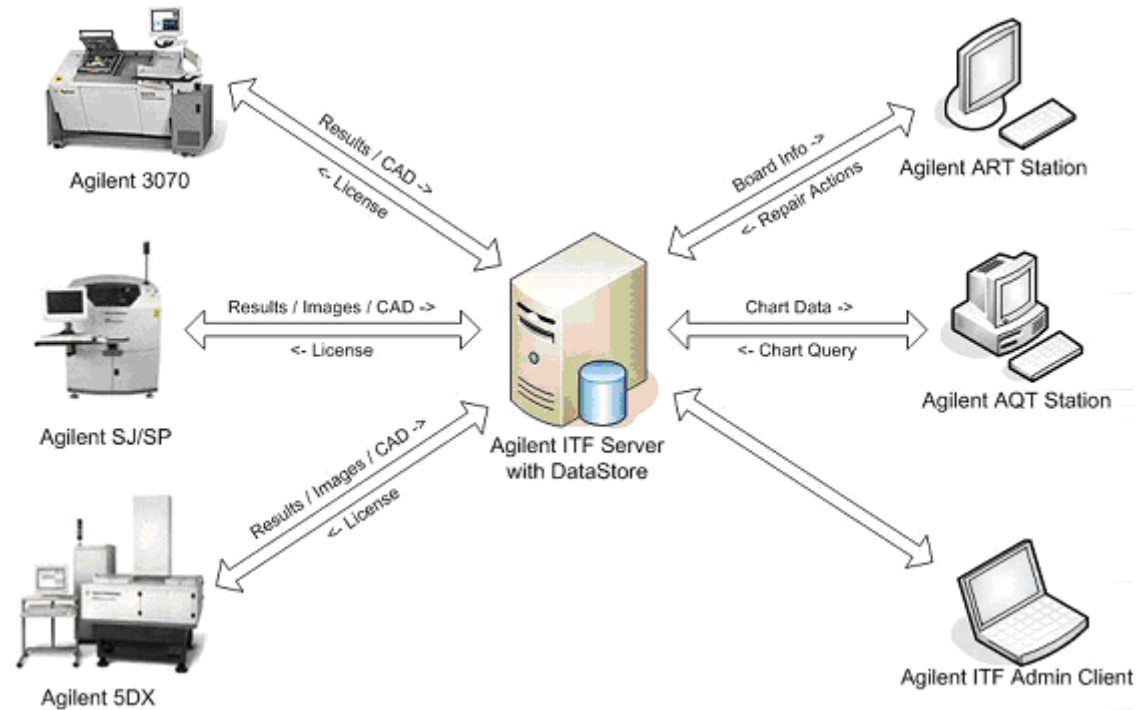
The framework that the ITF architecture provides for communication between the testers and the ITF server is discussed.

You will also gain an understanding of how the software components function in this framework to provide a comprehensive solution for managing your testers.

Architecture of the Intelligent Test Framework 3.1

Figure 1-1 shows a high-level view of the ITF 3.1 architecture.

Figure 1-1 High-Level View of ITF 3.1 Architecture



Key Features of ITF 3.1 Architecture

The following are the key features of the ITF 3.1 architecture:

- Software version of ITF server
- Introduction of Agent framework on both ITF server and testers
- More testers supported by a single ITF server
- Reliable and efficient transmission of test results from testers to ITF server
- Improvement in performance of ART and AQT
- Improved Lifetime Management Engine
- No breaking of file even if network fails
- Improved database design
- Fine-tuned AQT queries

ITF 3.1 Server and Tester Communication

Figure 1-2 shows us the flow of communication between the ITF Server and the various testers.

In each type of testers, there are two processes running and one directory for the temporary stage of test result files.

The temporary directory will guarantee that test results are safely stored before it is sent to ITF server.

Native processes (gc3070, BoardSend, TRCmdPro) will send the test result to some directory when a test or inspection is done.

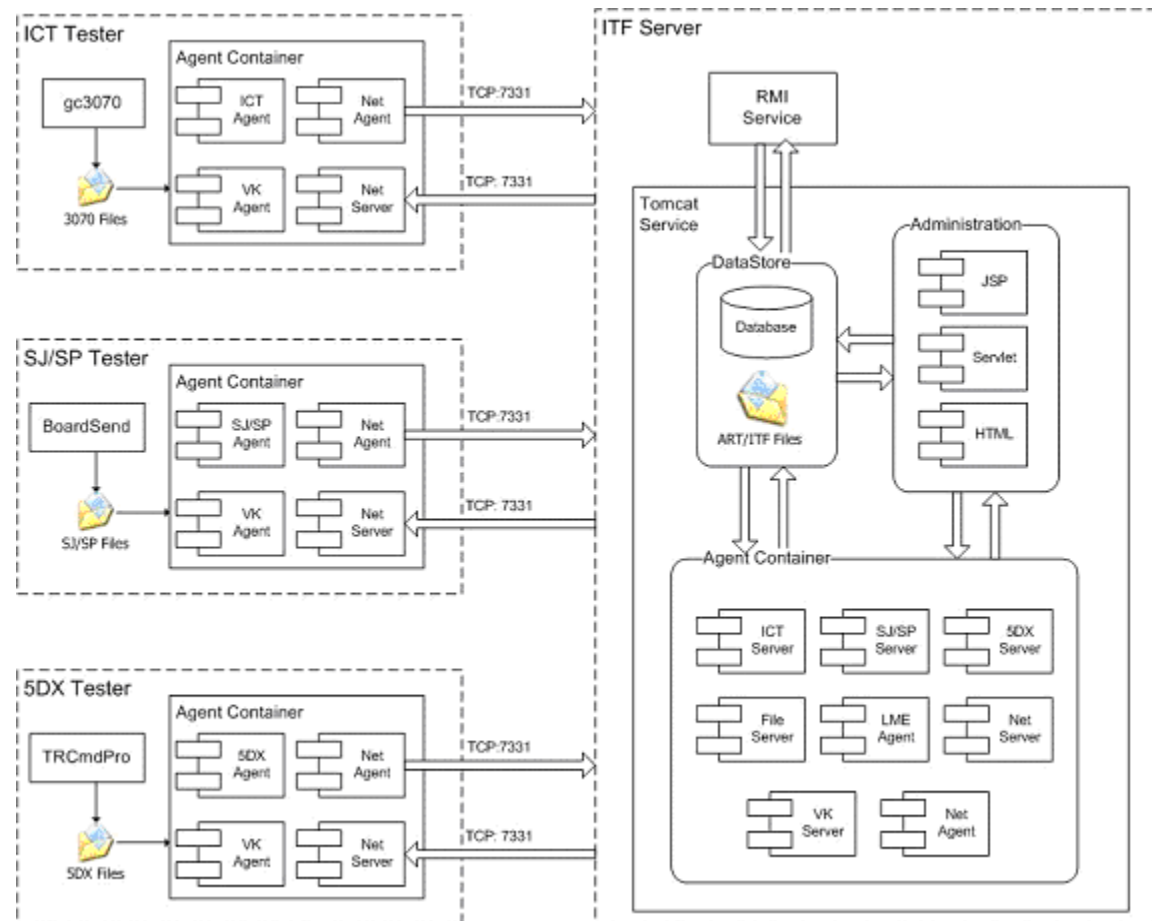
The ITF Agent process, which contains all agents, will collect test results from the directory and send it to ITF server. If the network fails or if the ITF server is down, the Agent process will try to resend the test results until it is successful.

The ITF Agent will connect the ITF server using port 7331. The user can change the port number by setting some configuration files.

The ITF Agent also opens port 7331 on the tester to service requests. Similarly, you can change this port number by setting configuration files.

The communication between the ITF Agent and the ITF Server is two-way.

Figure 1-2 Communication between ITF Server and the Testers



ITF 3.1 Server and ART/AQT Communication

Figure 1-3 shows us the flow of communication between the ITF Server, ART and AQT.

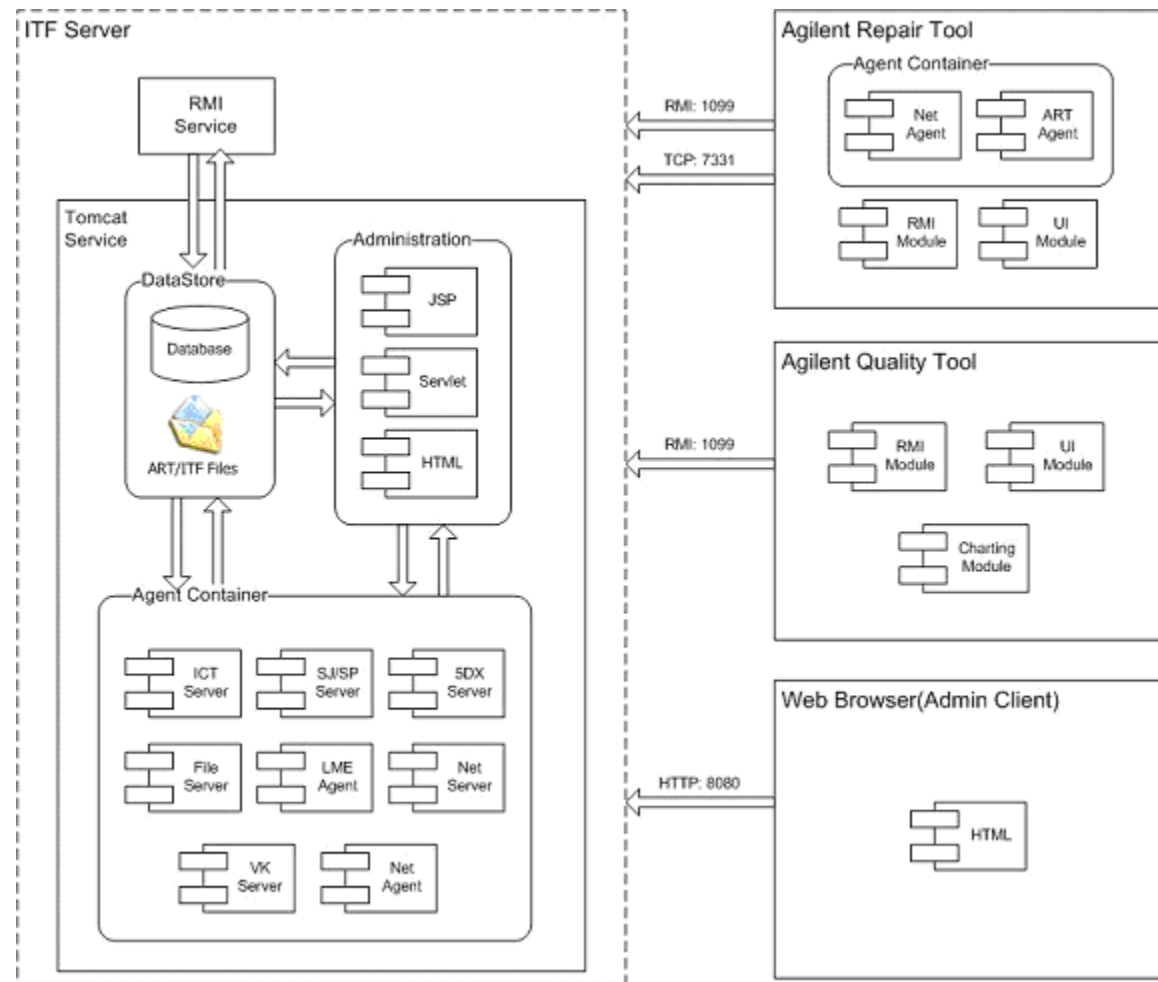
The ART and AQT applications will continue communication with ITF in RMI protocol using port 1099.

ART will download ART files, Cad Files and Images files in row TCP/IP socket. ART will download files by the ITF Agent using port 7331.

There is no change in the communication from AQT to ITF.

The System Administration Client module can still be assessed by web browser on port 8080. The user can change this port number by following the procedure found in [Changing the Web Application Port Number of the ITF Server](#).

Figure 1-3 Communication between the ITF Server and ART/AQT applications



ITF Server and System Administration

The ITF Administration System is a browser-based application used to configure system properties, such as user access, repair configurations and framework services, within the Agilent Repair Tool, the Agilent Quality Tool, and other ITF applications.

The purpose of the ITF Administration System is to provide security and control functionality for the following items:

- Users
- Agilent Repair Tool
- Agilent Quality Tool
- Agilent Intelligent Test Framework

The ITF Administration System Help files allow you to quickly and easily find information about the ITF Administration System. Click any topic in the Help Table of Contents for information on that topic.

NOTE

The ITF Administration System can only be run from the ITF Server or a Client PC.

ITF Software Applications

The following subsections provide a brief introduction to the applications found in the ITF Software Solutions.

Agilent Repair Tool

The Agilent Repair Tool (ART) is a printed circuit board repair tool that supports a common graphical user interface for all three types of Agilent Technologies automated inspection systems: X-ray (AXI), Optical (AOI), and in-circuit test (ICT).

With this tool, operators can leverage skills, knowledge, and training across AXI, AOI and ICT repair loops. This increases the efficiency of repair and provides a more consistent method for reporting repair efforts.

Agilent Quality Tool

The Agilent Quality Tool is a statistical process control and quality control (SPC/SQC) tool for the Agilent 5DX and Agilent SJ Series test systems. The Agilent Quality Tool provides quick and easy access to actionable information on quality, line throughput, and false calls.

When the Agilent Quality Tool is used in conjunction with the Agilent Repair Tool and Agilent test and inspection systems, you can apply SPC and SQC methods to improve assembly and test processes. These process improvements can help you meet your company's targeted quality levels.

2

Changing Preset Values

In this chapter...

- [Overview](#), 2-2
- [Changing the Port Number of the ITF Server](#), 2-3
- [Changing the Web Application Port Number of the ITF Server](#), 2-4
- [Changing the ITF Server Name and Port Number stored on the Tester Controller](#), 2-5
- [Changing the Port Number of the Agent on the Tester Controller](#), 2-6

Overview

The ITF setup programs provide default values for various network settings. This chapter provides you with the instructions for modifying these default values should you find the need to do so.

Changing the Port Number of the ITF Server

The ITF port number is used to enable communication between the ITF Server and tester controllers. The default value of the ITF port number is 7331.

If you need to change this value, do the following.

NOTE

Make sure you update the tester controller to connect to the new port. For instructions, see [Changing the ITF Server Name and Port Number stored on the Tester Controller](#).

- 1 Stop the ITF services on the ITF server.
 - a Browse to the installed ITF folder on the ITF server.
 - b Go to the `bin` subfolder.
 - c Double-click the file, `StopServices.bat`.
- 2 Go to the `storage\AgentContainerRoot\agent\AgentNetServer` within the ITF folder.
- 3 Open the file, `config.properties`, with a text editor.
- 4 Search for the text string, `port=<nnnn>`, where `<nnnn>` represents the current port number in use. For example, `port=7331`.
- 5 Modify the value for the port number to your desired setting.
- 6 Save and close the file.
- 7 Restart the ITF services.
 - a Browse to the installed ITF folder on the ITF server.
 - b Go to the `bin` subfolder.
 - c Double-click the file, `StartServices.bat`.

Changing the Web Application Port Number of the ITF Server

The web application port number is the access port for the Administration System.

If you need to change the web application port number, do the following.

- 1 Stop the ITF services on the ITF server.
 - a Browse to the installed ITF folder on the ITF server.
 - b Go to the `bin` subfolder.
 - c Double-click the file, `StopServices.bat`.
- 2 Go to the `C:\Agilent\ITFSS3.1\ITF\tomcat\jakarta-tomcat-5.0.28\conf` folder.
- 3 Open the file, `server.xml`, with a text editor.
- 4 Search for the text string, `port="<nn>"`, where `<nn>` represents the current port number in use. For example, `port="80"`.
- 5 Modify the value for the port number to your desired setting.
- 6 Save and close the file.
- 7 Restart the ITF services.
 - a Browse to the installed ITF folder on the ITF server.
 - b Go to the `bin` subfolder.
 - c Double-click the file, `StartServices.bat`.

Changing the ITF Server Name and Port Number stored on the Tester Controller

To enable the tester controller to recognize the ITF Server, the tester controller stores the values of the ITF Server name and port number in the `config.properties` file.

If you want to connect the tester controller to a different ITF Server, you need to update these values. To do so:

- 1 Log on to the tester controller with Administrator privileges.
- 2 Stop the Agent service.
 - a Browse to the installed Agent folder on the tester controller. The default path is `C:\Agilent\ITFSS3.1\Agent`.
 - b Go to the `bin` subfolder.
 - c Double-click the file, `StopServices.bat`.
- 3 Browse back to the Agent folder.
- 4 Go to the `storage\AgentContainerRoot\agent_Proxy` folder within the Agent folder.
- 5 Open the file, `config.properties`, with a text editor.
- 6 To edit the ITF server name, search for the text string, `server=<aaa>` where `<aaa>` represents the current server name in use. For example, `server=ITF1`.

Modify the server name to your desired setting.

- 7 To edit the ITF server port number, search for the text string, `port=<nnnn>` where `<nn>` represents the current port number in use. For example, `port=7331`.
Modify the value for the port number to your desired setting.
- 8 Save and close the file.
- 9 Restart the Agent services.
 - a Browse back to the Agent folder.
 - b Go to the `bin` subfolder.
 - c Double-click the file, `StartServices.bat`.

Changing the Port Number of the Agent on the Tester Controller

NOTE

This section does not apply to Agilent ICT UX tester controllers.

The port number of the tester agent is used to enable communication between the tester controller and the ITF Server. The default value of this port number is 7331.

If you need to change the port number of the tester agent, do the following.

- 1 Log on to the tester controller with Administrator privileges.
- 2 Stop the Agent service.
 - a Browse to the installed Agent folder on the tester controller. The default path is `C:\Agilent\ITFSS3.1\Agent`.
 - b Go to the `bin` subfolder.
 - c Double-click the file, `StopServices.bat`.
- 3 Browse back to the Agent folder.
- 4 Go to the `storage\AgentContainerRoot\agent\AgentNetServer` folder within the Agent folder.
- 5 Open the file, `config.properties`, with a text editor.
- 6 Search for the text string, `port=<nnnn>` where `<nn>` represents the current port number in use. For example, `port=7331`.

- 7 Modify the value for the port number to your desired setting.
- 8 Save and close the file.
- 9 Restart the Agent services.
 - a Browse back to the Agent folder.
 - b Go to the `bin` subfolder.
 - c Double-click the file, `StartServices.bat`.

3

Changing Log Levels for Logging

In this chapter...

- [Overview](#), 3-2
- [Changing the Log Level](#), 3-3
- [Special Case for ITF Server](#), 3-4

Overview

The log files for ITF Server, ITF agent and ART are generated and placed in their respective log directories. All of them use the same log4j logging mechanism.

This logging mechanism provides four available log levels: **debug**, **info**, **warn**, and **error**.

debug

This level generates huge amounts of logging statements that, most of the time, are useful only to the developer.

info

This level writes a lot of useful information that is more easily understood and helpful to a non-technical person. It, however, also creates a lot of unnecessary information. Thus, turning it on may result in a drop in software performance.

warn

This level will be more effective in striking a balance between logging and performance, where messages are logged only when situations that require attention are encountered.

error

At this level, logging takes place only when errors occur.

Changing the Log Level

The default log level set in ITF Software Solutions is **warn**. In the case where more information is required when a situation arises, you will have to change the log level to **debug**.

To change the log level from **warn** to **debug**, you have to:

- 1 Stop the respective services for ITF server or ITF Agent. Alternatively, close the ART application.
- 2 Locate the file, `log4j.xml`.
- 3 Open it with a text editor.
- 4 Look out for the phrase `<level value="warn"/>`.
- 5 Change the level value from "warn" to "debug".
- 6 Save the file.
- 7 Restart the services, or reopen the ART application.

The following list shows the location where each `log4j.xml` file resides.

- ITF Server
`<ITF>\tomcat\jakarta-tomcat-5.0.28\webapps\adminclient\WEB-INF\classes`
- ITF Agent (Tester Components)
`<Agent>\lib`
- ART
`<ART>\bin\logconf`

Special Case for ITF Server

When you set a different log level in the ITF Server, you need to look further at the type of log file you are changing, unlike the log levels for the ITF Agent and the ART application, where all occurrences of `<level value="warn"/>` can be changed.

Please see the ITF server's `log4j.xml` extract in [Figure 3-1](#) on page 3-5.

Figure 3-1 Code extract from log4j.xml

<pre><logger name="net"> <level value="error"/> <appender-ref ref="Console"/> </logger></pre>	<p>Block 1</p> <p>Block 1 is to be permanent. You should <i>not</i>, at any time, change the log level of this block to any others.</p>
<pre><root> <level value="warn"/> <appender-ref ref="ITFMonthlyLog"/> </root></pre>	<p>Block 2</p>
<pre><logger name="RepairLogger"> <level value="warn"/> <appender-ref ref="RepairLog"/> </logger></pre>	<p>Block 3</p> <p>Blocks 2 and 3 are interchangeable. You should change them when you are investigating a problem.</p>
<pre><logger name="Migration30to31"> <level value="warn"/> <appender-ref ref="Migration30to31Log"/> </logger></pre>	<p>Block 4</p> <p>Block 4 is only applicable to the migration process. Change it when you need more information during data migration.</p>

NOTE

Remember to change the log level back to **warn** once you are done with your investigations.

4

Backing up and Restoring ITF Data

In this chapter...

- [Overview](#), 4-2
- [Stopping the ITF and SQL Services](#), 4-3
- [Phase 1: Backing up ITF Data](#), 4-4
- [Phase 2: Restoring ITF Data](#), 4-10
- [Starting the ITF and SQL Services](#), 4-13

Overview

This chapter explains how to backup and restore Intelligent Test Framework (ITF) files to and from tape media using the Backup utility in Windows 2000 Server.

The following is the list of ITF files that need to be backup or restored:

- Board Test, Image and CAD files
(available in <Drive:>\Agilent\ITFSS\DataStore where the path represents the location of the data store.)
- Intelligent Test Framework (ITF) database
(available in <Drive:>\Program Files\Microsoft SQL Server\MSSQL\Data where the path represents the location of the database.)

NOTE

The backup and restore processes require the ITF services and the SQL Server Service Manager to be stopped. As such, ART and AQT will not be available during the backup and restore processes.


Stopping the ITF and SQL Services

Before you backup or restore ITF data, you need to stop ITF and SQL services.

To stop the ITF services

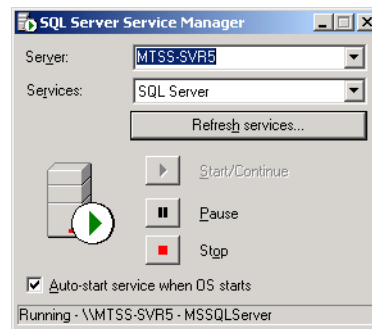
- 1 Browse to the installed ITF folder on the ITF server.
- 2 Go to the `bin` subfolder.
- 3 Double-click the file, `StopServices.bat`.

To stop the SQL services



- 1 Double-click the **SQL Server Service Manager** icon  on the Windows system tray.

The **SQL Server Service Manager** dialog box appears.

Figure 4-1 SQL Server Service Manager dialog box



- 2 Click **Stop** and wait for the SQL server to stop.

When the icon changes from  to , it means that the SQL server has been stopped.

Phase 1: Backing up ITF Data

This section provides you with the procedure for backing up board test files, image files and Intelligent Test Framework (ITF) database.

Preparing Backup data (Optional)

The following procedure allows you to minimize disruption to production while backing up ITF data.

1 Browse to the SQL database directory:

The default location is `<Root drive of system>:\Program Files\Microsoft SQL Server\MSSQL\Data`. `E:\` is the default root drive.

2 Rename the following files:

- `itf_Data.MDF`
- `itf_Log.LDF`

The recommended formats for the new names are:

- `itf_Data_dd_mm_yy.MDF`
- `itf_Log_dd_mm_yy.LDF`

If possible, use the current date.

3 Rename the data directory, DataStore:

The default location is `<Drive:>\Agilent\ITFSS\DataStore`. `E:\` is the default drive.

Recommended format:

`<Drive:>\Agilent\ITFSS\DataStore ddmmyy to ddmmyy` where the first `ddmmyy` represents the date when the first record was created, and the second

`ddmmyy` represents the date when the last record was created.

4 Move the renamed SQL database file to the renamed data directory.

Estimated Speed of the Backup Process

The following is the estimated speed of the backup process:

- Backing up the SQL database directory

The default location is `E:\Program Files\Microsoft SQL Server\MSSQL\Data`.

For SQL database, the speed is estimated as 200 to 300 MB/min.

- Backing up your data directory

The default location is `E:\Agilent\ITFSS\DataStore`.

For Images and Board Test files, the speed is estimated as 100 to 150 MB/min.

NOTE

This is just an estimation. The values may vary from one environment to another environment.

Creating Backup Files on Tape

To back up ITF data:

CAUTION



Make sure you have stopped the ITF and SQL services. For detailed instructions, see [Stopping the ITF and SQL Services](#).

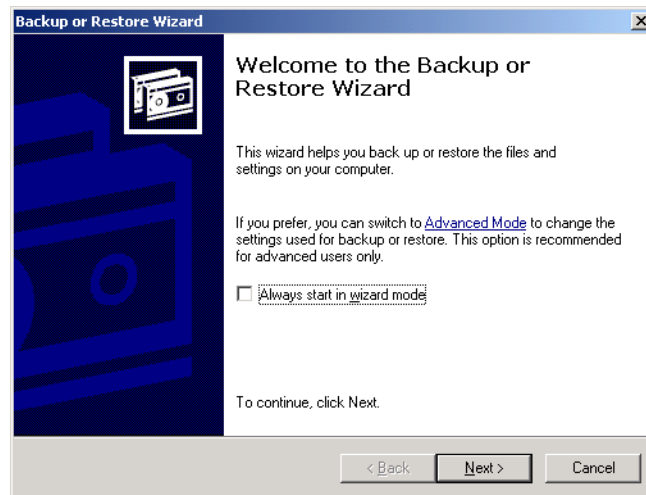
- 1 Click **Start > Programs > Accessories > System Tools > Backup** to start the Backup utility.

The **Backup or Restore Wizard** screen appears.

NOTE

When Backup is started, it will ask you if you want to run the wizards. Choose the Backup Wizard to guide you through.

Figure 4-2 Backup or Restore Wizard screen

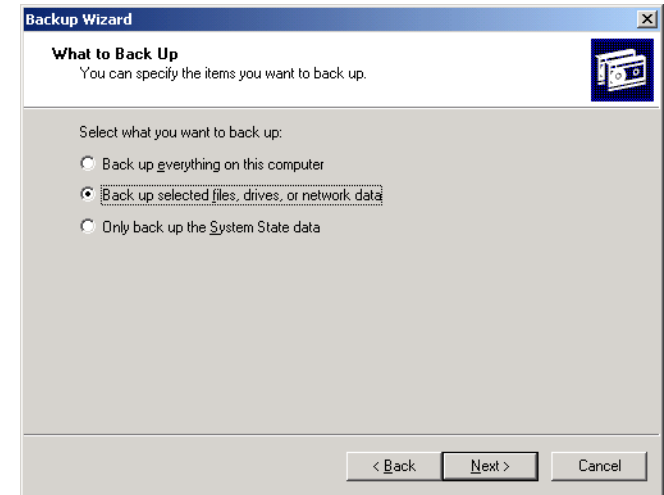


2 Place the tape into the 4mm tape drive and allocate the tape to Backup once detected.

3 Click **Next**.

The **What to Back Up** dialog box appears.

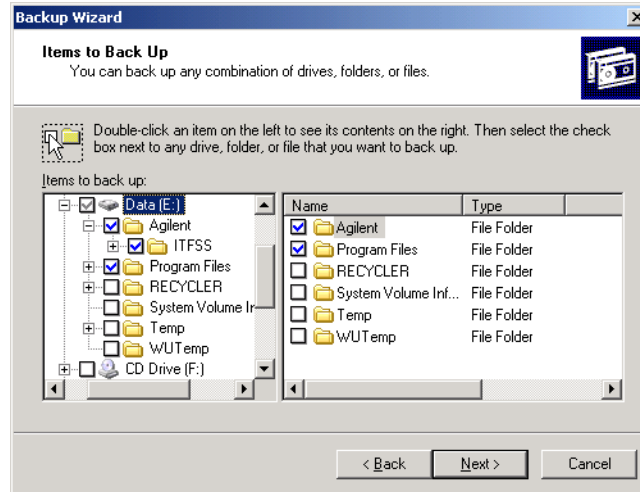
Figure 4-3 SQL Server Service Manager dialog box



4 Click the **Back up selected files, drives, or network data** option button and then click **Next**.

The following **Items to Back up** dialog box appears.

Figure 4-4 Selecting items for backup



5 If you did not carry out the optional procedure described in **Preparing Backup data (Optional)**, ensure that the following items are selected.

- **My Computer > <Drive:> > Agilent > ITFSS > DataStore**

This folder contains the following.

- BoardTest folder
This folder contains board test files and Image folder contains the defect images.
- CAD folder
This folder contains the CAD files associated with the board test files.

- **My Computer > <Drive:> > Program Files**

This folder contains Intelligent Test Framework (ITF) database files.

If you have carried out the optional procedure, ensure that *only* the following item is selected:

- **My Computer > <Drive:> > Agilent > ITFSS > DataStore <ddmmyy to ddmmyy>**

where the first <ddmmyy> represents the date when the first record was created, and the second <ddmmyy> represents the date when the last record was created.

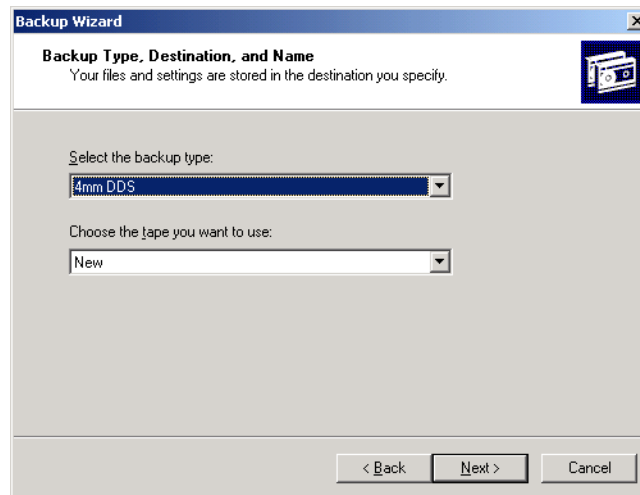
This folder contains the following:

- BoardTest folder
- CAD folder
- ITF_Data_dd_mm_yy.MDF and ITF_Log_dd_mm_yy.LDF are the related database files.

6 Click **Next**.

The **Where to Store the Backup** dialog box appears.

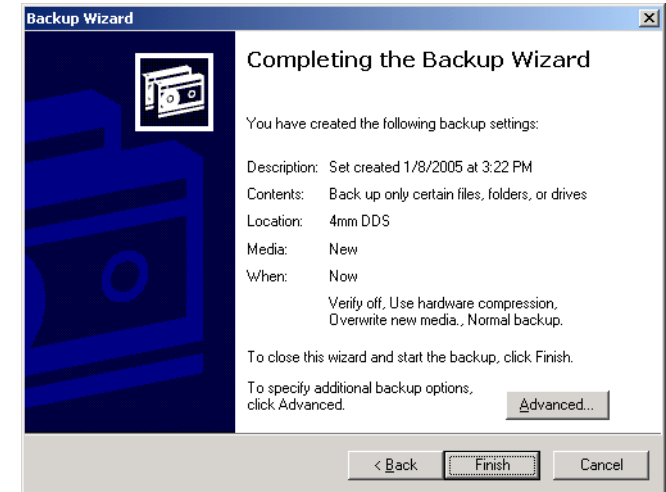
Figure 4-5 Specifying backup media



- 7 Select the media type as **4mm DDS** for the **Backup media type** and click **Next** to continue.

The backup method and settings are displayed.

Figure 4-6 Completing the backup procedure



- **Media: New Media**

This means the media is treated as new media. If it contains data, the data will be overwritten.

- **When: Now**

This means that the backup process will start immediately when the Finish button is clicked. The alternative option is to set a schedule for the backup.

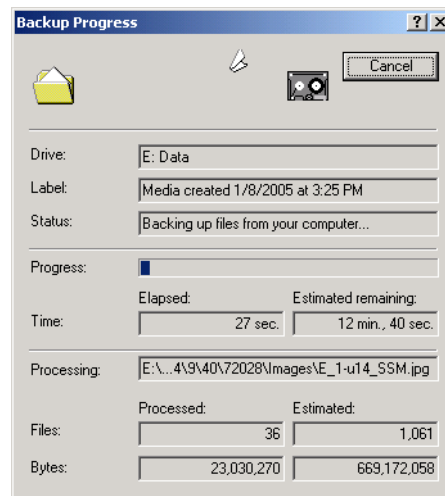
- **How: Verify off, Use hardware compression, Overwrite new media**

Verify Off means that data verification will not be performed after the backup is completed successfully.

Use Hardware Compression means the standard compression available for the selected media type will be used. Depending on the media type used, the 4mm tape has a standard compression for its use.

- 8 If you want to change any of these default settings, click **Advanced**, make the desired changes and then return to the **Completing the Backup Wizard** dialog box.
- 9 To complete the backup procedure, click **Finish**.
The **Backup Progress** dialog box appears.

Figure 4-7 Backup progress



NOTE

If you have carried out the procedure described in **Preparing Backup data (Optional)**, you can restart the ITF and SQL services now. For detailed instructions, see **Starting the ITF and SQL Services**. After restarting the services, do the following:

- 1) Browse to the C:\Agilent\ITFSS3.1\ITF\db folder.
- 2) Double-click the MakeDB.bat file.

This creates a new ITF database.

If you did not carry out the optional procedure, restart the services *after* the entire backup process is completed.

You will be prompted to insert a new tape if the capacity of the tape is not big enough to store all the files you plan to backup.

- 10 After the backup is completed, remove the tape from the tape drive.

NOTE

If you have not yet restarted the ITF and SQL services, remember to do so. See **Starting the ITF and SQL Services**.

Phase 2: Restoring ITF Data

You may want to view ITF data which you have archived previously. To do so, you need to restore ITF data back to the ITF server.

To restore ITF data:

CAUTION



Make sure you have stopped the ITF and SQL services. For detailed instructions, see [Stopping the ITF and SQL Services](#).

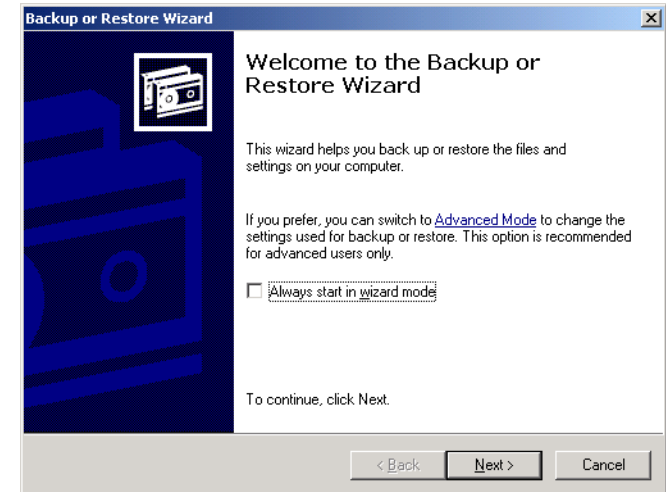
- 1 Click **Start > Programs > Accessories > System Tools > Backup** to start the Backup utility.

The **Backup or Restore Wizard** screen appears.

NOTE

When Backup is started, it will ask you if you want to run the wizards. Choose the **Restore Wizard** to guide you through.

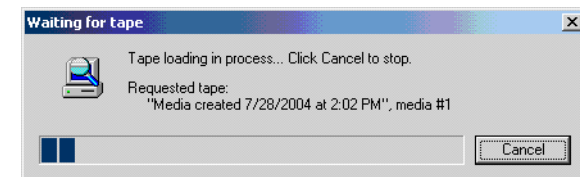
Figure 4-8 Backup or Restore Wizard screen



- 2 Place the backup tape into the 4mm tape drive and select the folders in the tape media that you want to restore to the ITF server.
- 3 Click **Next** to continue.

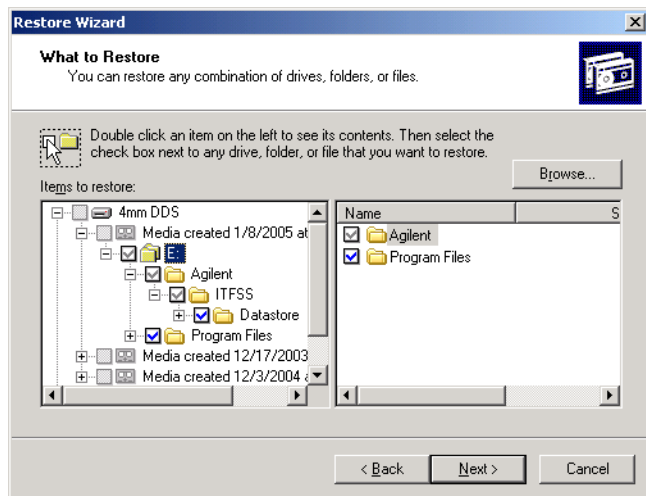
The **Waiting for tape** dialog box appears.

Figure 4-9 Tape loading



After the tape is loaded, the **What to Restore** dialog box appears.

Figure 4-10 Selecting items to restore



NOTE

The ITF server may take some time to read the information from the tape when you first select “4mm DDS” to display the directory structure.

- 4 If you did not carry out the optional procedure, ensure that the following items are selected:
 - **My Computer > <Drive:> > Agilent > ITFSS > DataStore**
 - **My Computer > <Drive:> > Program Files**

If you have carried out the optional procedure, ensure that *only* the following item is selected:

- **My Computer > <Drive:> > Agilent > ITFSS > DataStore <ddmmy to ddmmy>**

- 5 Click **OK**.

The restore method and settings are displayed.

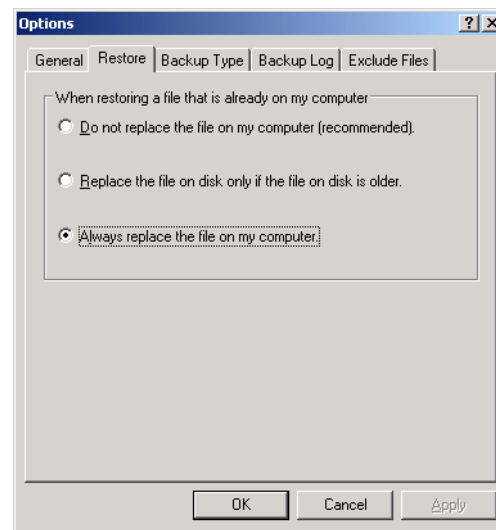
Figure 4-11 Completing the Restore procedure



- 6 Make sure **Always replace** is the selected setting for **Existing files**. This ensures that files from the tape will be copied back to the original location on the ITF Server where the files were backed up from.

If this setting is not selected, click **Cancel** to return to **Restore** menu. Then, click **Tools > Options** to select **Always replace the file on my computer**.

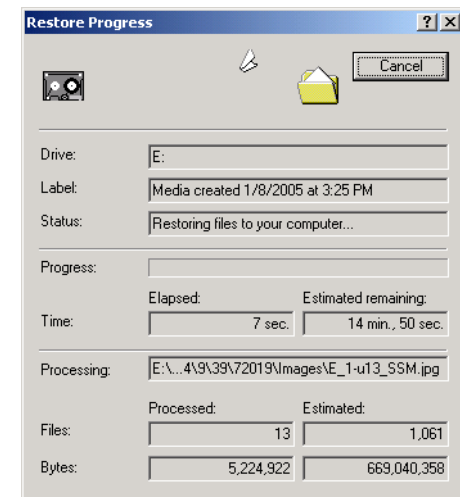
Figure 4-12 Options dialog box



7 After you have verified all the restore settings required, click **Finish**.

The **Restore Progress** dialog box appears.

Figure 4-13 Restore in progress



8 After the backup is completed, remove the tape from the tape drive.

NOTE

Remember to restart the ITF and SQL services. For detailed instructions, see [Starting the ITF and SQL Services](#).

Starting the ITF and SQL Services

After you complete the backup or restore procedure, you need to restart the SQL services *first*, followed by the ITF services.

To start the SQL services

- 1 Double-click the **SQL Server Service Manager** icon on the Windows system tray.
- 2 Click **Start** and wait for the SQL server to restart.

To start the ITF services

- 1 Browse to the installed ITF folder on the ITF server.
- 2 Go to the `bin` subfolder.
- 3 Double-click the file, `StartServices.bat`.

5

Understanding Drives and Drive Arrays

In this chapter...

- [Overview](#), 5-2
- [Drive Array](#), 5-3
- [Array Controller](#), 5-4
- [Fault Tolerance](#), 5-5
- [RAID 1](#), 5-6
- [RAID 5 - Distributed Data Guarding \(Distributed Parity Blocks\)](#), 5-7
- [LED Patterns on the Hard Drive](#), 5-8

Overview

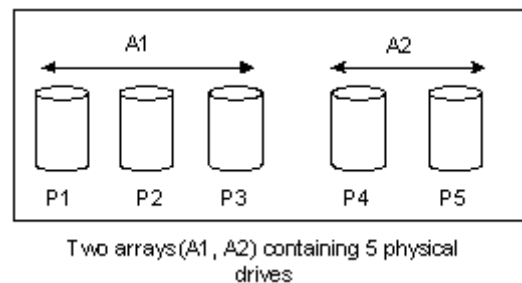
This chapter provides you with a brief introduction to the drive arrays, array controllers and different RAID configuration used in the ITF server.

A list of LED illumination patterns and their meanings is also provided for your reference.

Drive Array

A drive array is defined as a storage system composed of several hard disks. Data is divided among the different drives for greater speed and higher reliability. It is in fact a set of disk drives that are managed as if they were a single storage device.

Figure 5-1 A drive array



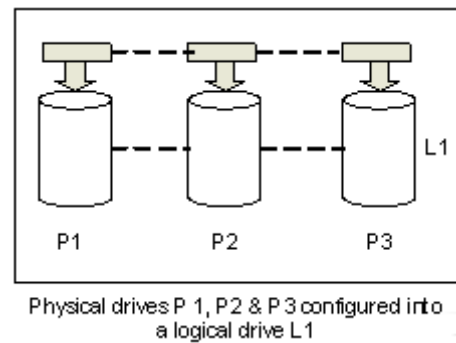
Array Controller

When an array controller is installed in the system, capacity of several physical drives can be combined into 1 or more virtual units called logical drives.

The read/write heads of all of these physical drives are active simultaneously, reducing the total time required for data transfer.

Because the read/write heads are active simultaneously, the same amount of data is written to each drive during any give time interval. Each unit of data is called a block, and over all the physical drives in a logical drive the blocks form a set of data stripes.

Figure 5-2 An array controller



Fault Tolerance

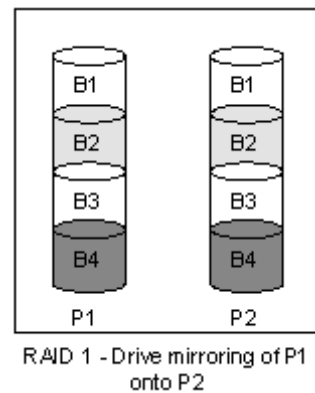
To protect against data loss due to physical drive failure, logical drives are configured with fault tolerance. The ITF server's hard disk is configured as follows:

- RAID 1 (C drive)
- RAID 5 (E drive)

RAID 1

When implementing RAID 1, data is duplicated onto a second drive. This method is useful when high performance and data protection are more important than the cost of physical drives. This is also commonly known as drive mirroring when only two hard disks are used.

Figure 5-3 RAID 1



Advantages

The following are the advantages of implementing RAID 1:

- Highest read and write performance of any fault-tolerant configuration, and
- No loss of data as long as none of failed drives are mirrored to another failed drive (up to half of the physical drives in the array can fail).

Disadvantage

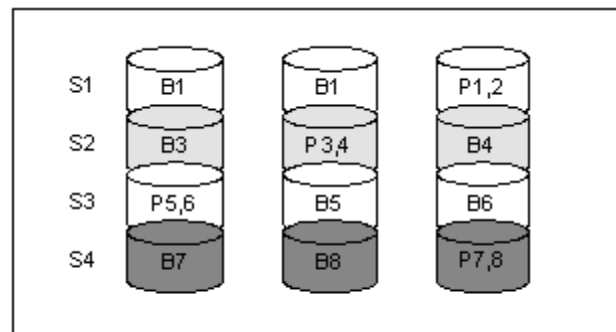
The following is the disadvantage of implementing RAID 1:

- Only 50% of total drive capacity usable for data storage.

RAID 5 - Distributed Data Guarding (Distributed Parity Blocks)

For implementing RAID 5 - Distributed Data Guarding, a block of parity data is calculated for each stripe from the data that is in all other blocks within that stripe.

Figure 5-4 RAID 5



RAID 5 - Parity Information (P×,y)

The blocks of parity data are distributed over every physical drive within the logical drive. When a physical drive fails, data that was on the failed drive can be calculated from the user data on the remaining drives and the parity data. This recovered data is usually written to an online spare in a process called a rebuild.

This method is useful when cost, performance and data availability are equally important.

Advantages

The following are the advantages of implementing RAID 5:

- High read performance,
- No loss of data if one physical drive fails, and
- More drive capacity usable than implementing RAID 1.

Disadvantages

The following are the disadvantages of implementing RAID 5.

- Relatively low write performance, and
- Loss of data if a second drive fails before data from the first failed drive is rebuilt.




LED Patterns on the Hard Drive

The LEDs in front of each hard drive are visible through the front panel of server or external storage unit.

When a drive is configured as a part of an array and attached to a controller, the status of the drive can be determined from the illumination pattern of these LEDs.

Table 5-1 lists the possible LED patterns that may be displayed on the hard drive’s LED panel, and their meanings.

Table 5-1 Hard Drive Status from LED Illumination Patterns

Activity 	Online 	Fault 	Meaning
On, off, or flashing	On or off	Flashing	A predictive failure alert has been received for this drive. Replace the drive as soon as possible.
On, off or flashing	On	Off	OK to replace the drive online if the array is configured for fault tolerance and all other drives in the array are online.
On	Flashing	Off	Do not remove the drive. Removing drive during this process may terminate the current operation and cause data loss.
On	Off	Off	Do not remove the drive. Removing drive during this process may cause data loss.
Flashing	Flashing	Flashing	Do not remove the drive. Removing drive during this process can cause data loss in non-fault-tolerant configurations.
Off	Off	On	OK to replace the drive online.
Off	Off	Off	OK to replace the drive online if the array is configured for fault tolerance and all other drives in the array are online.

If you need more information on the hard drive or drive array controller, refer to the documentation that came with it.

Gathering Information for Technical Support

Before escalating to the next level of technical support, application engineers need to prepare the following information:

- Screen captures of issues
- Board test result set
 - For AXI: .res, .cx, and .log files and Image folder
 - For AOI: .rep, .plx, .pls, and .dat files and Image folder
 - For ICT: GENCAM .gcm files and .log files

- ITF log files

The following are the log files for each software and their locations.

- ITF

Location: <ITF>\storage\clients\logs
where <ITF> represents the directory where ITF is installed.

- AQT

Location: <AQT>\clients\logs and
<AQT>\clients\Views where <AQT>
represents the directory where AQT is installed.

- ART

Location: <ART>\clients\logs where <ART> represents the directory where ART is installed.

- Windows event log on ITF Server

- Application
- Security
- System

Saving the Windows event log file

- 1 Click **Start > Control Panel**.
- 2 Double-click **Administration Tools** followed by **Event Viewer**.
- 3 In the tree console on the left pane, select **Application**.
- 4 On the **Action** menu, click **Save Log File As**.
- 5 In the **Save “Application” As** dialog box, browse to the folder where you want to save the log file and enter a name for the file.
- 6 Click **Save**.
- 7 Repeat steps 3 through 6 for the rest of the entries in the tree console:
 - **Security**
 - **System**
- 8 Close the **Event Viewer** window.

7

Useful Network Utilities

In this chapter...

- [Overview](#), 7-2
- [Ipconfig](#), 7-3
- [Ping](#), 7-4
- [Traceroute](#), 7-5
- [Netstat](#), 7-6
- [Nbstat](#), 7-7
- [DHCP and DNS](#), 7-8
- [IP Addressing](#), 7-9
- [MAC Addressing](#), 7-10

Overview

This chapter contains some information on several useful network utilities that application engineers may need to use during their course of work.

- **Ipconfig**
- **Ping**
- **Traceroute**
- **Netstat**
- **Nbstat**
- **DHCP and DNS**
- **IP Addressing**
- **MAC Addressing**

Ipconfig

Ipconfig is a command which display the current network setting assigned by the DHCP server. It also verifies the network connection.

To use the `ipconfig` command:

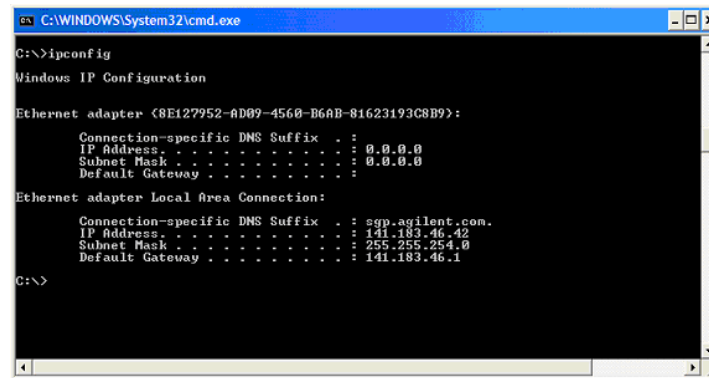
- 1 In Windows, select **Start > Programs > Accessories > Command Prompt**.

The Command Prompt window appears.

- 2 Enter `ipconfig` at the command prompt.

Information similar to that shown **Figure 7-1** appears.

Figure 7-1 ipconfig



```
C:\WINDOWS\System32\cmd.exe
C:\>ipconfig

Windows IP Configuration

Ethernet adapter {8E127952-AD09-4560-B6AB-81623193C8B9}:

    Connection-specific DNS Suffix  . : 
    IP Address . . . . . : 0.0.0.0
    Subnet Mask . . . . . : 0.0.0.0
    Default Gateway . . . . . : 

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : sgp.agilent.com.
    IP Address . . . . . : 141.183.46.42
    Subnet Mask . . . . . : 255.255.254.0
    Default Gateway . . . . . : 141.183.46.1

C:\>
```

If the command return the IP address and subnetmask 0.0.0.0, there could be a problem in your network connection. Check that your network card is installed properly and the DHCP Client service is running.

Ping

Ping is a command which tells you if the connection between your computer and a particular domain is working correctly.

To use the `ping` command:

- 1 In Windows, click **Start > Programs > Accessories > Command Prompt**.

The Command Prompt window appears.

- 2 Enter `ping`, followed by a space character, and then the domain name at the prompt.

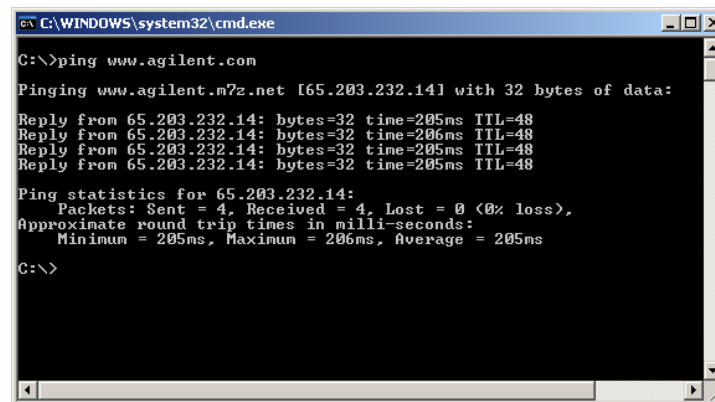
For example, `ping www.agilent.com`

Information similar to that shown [Figure 7-2](#) appears.

If the results show a series of replies, the connection is working. The response time shows you how fast the connection is.

If you see a “Request timed out” error instead of a reply, there is a breakdown in connection somewhere between your computer and the domain.

Figure 7-2 ping



```
C:\WINDOWS\system32\cmd.exe
C:\>ping www.agilent.com
Pinging www.agilent.m7z.net [65.203.232.14] with 32 bytes of data:
Reply from 65.203.232.14: bytes=32 time=205ms TTL=48
Reply from 65.203.232.14: bytes=32 time=206ms TTL=48
Reply from 65.203.232.14: bytes=32 time=205ms TTL=48
Reply from 65.203.232.14: bytes=32 time=205ms TTL=48
Ping statistics for 65.203.232.14:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 205ms, Maximum = 206ms, Average = 205ms
C:\>
```

Traceroute

Traceroute is a command which returns the path a packet of information takes as it travels from your computer to a location you specify. This command lists all the routers the packet passes through until the packet reaches its destination or fails midway and is discarded. In addition, this command tells you how long each ‘hop’ from router to router takes.

To use the `tracert` command:

- 1 In Windows, click **Start > Programs > Accessories > Command Prompt**.

The Command Prompt window appears.

- 2 Enter `tracert`, followed by a space, then the domain name at the prompt.

For example, `tracert www.agilent.com`

Information similar to that shown [Figure 7-3](#) appears.

Figure 7-3 traceroute

```

C:\WINDOWS\system32\cmd.exe
C:\>tracert www.agilent.com
Tracing route to www.agilent.n7z.net [65.203.232.141]
over a maximum of 30 hops:
  0  <1 ms    <1 ms    <1 ms    192.168.2.1
  1  10 ms    22 ms    23 ms    10.52.0.1
  2  8 ms     24 ms    26 ms    172.20.52.129
  3  12 ms    9 ms     13 ms    172.26.52.1
  4  9 ms     21 ms    17 ms    172.20.7.8
  5  15 ms    11 ms    19 ms    61.8.233.161
  6  16 ms    12 ms    25 ms    ge-4-0-a01.sngps101.sg.ra.verio.net [61.8.234.35]
  7
  8  45 ms    42 ms    44 ms    ge-1-0-0.r00.sngps101.sg.bb.verio.net [61.8.234.93]
  9  200 ms   202 ms   198 ms   pl-0-1-2.r00.sttlva01.us.bb.verio.net [129.250.3.181]
 10  201 ms   202 ms   200 ms   pl6-1-1-1.r21.sttlva01.us.bb.verio.net [129.250.3.171]
 11  205 ms   200 ms   215 ms   pl6-2-0-0.r03.sttlva01.us.bb.verio.net [129.250.3.171]
 12  207 ms   199 ms   200 ms   POS1-1.BR2.SEA1.ALTER.NET [204.255.174.245]
 13  203 ms   202 ms   205 ms   0.so-1-2-0.MI2.SEA1.ALTER.NET [152.63.106.61]
 14  222 ms   202 ms   208 ms   0.so-7-0-0.WR2.SEA10.ALTER.NET [152.63.107.137]
 15  *        *        *        Request timed out.
 16  203 ms   203 ms   200 ms   65.203.224.36
 17  202 ms   201 ms   200 ms   65.203.231.57
 18  207 ms   204 ms   203 ms   65.203.232.14
Trace complete.
C:\>

```

This is extremely useful when trying to find out why a web site is unreachable, as you will be able to see where the connection fails.

If you have a web site hosted somewhere, it would be a good idea to do a traceroute to it when it is working. In this way, at times when it fails, you can do another traceroute to it, which will probably time out if the web site is unreachable, and compare the data.

Netstat

Netstat is a useful tool for checking your network configuration and activity.

To use the `netstat` command:

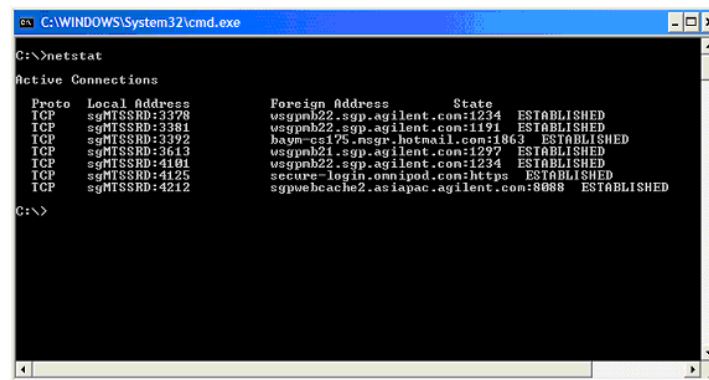
- 1 In Windows, click **Start > Programs > Accessories > Command Prompt**.

The Command Prompt window appears.

- 2 Enter `netstat` at the prompt.

Information similar to that shown [Figure 7-4](#) appears.

Figure 7-4 netstat



```
C:\WINDOWS\System32\cmd.exe
C:\>netstat

Active Connections

Proto Local Address           Foreign Address         State
TCP    sgMTSSRD:3378           usgpnb22.sgp.agilent.com:1234 ESTABLISHED
TCP    sgMTSSRD:3381           usgpnb22.sgp.agilent.com:1491 ESTABLISHED
TCP    sgMTSSRD:3392           bayn-cs175.nsgp.hotmail.com:1863 ESTABLISHED
TCP    sgMTSSRD:3613           usgpnb21.sgp.agilent.com:1297 ESTABLISHED
TCP    sgMTSSRD:4101           usgpnb22.sgp.agilent.com:1234 ESTABLISHED
TCP    sgMTSSRD:4125           secure-login-omnipod.com:https ESTABLISHED
TCP    sgMTSSRD:4212           sgpuehcache2.asiapac.agilent.com:8088 ESTABLISHED

C:\>
```

Nbtstat

Nbtstat is a command that displays protocol statistics and current TCP/IP connections using NetBIOS over TCP/IP (NBT).

NBT is defined in RFC 1001 and RFC 1002 and is a protocol that supports NetBIOS services on TCP/IP.

NetBIOS stands for Network Basic Input/Output System. NetBIOS was developed to allow software applications commonly used on IBM-compatible computers communicate with network hardware, allowing data to be transmitted properly over a network. NetBios commonly communicates on ports 137, 138 and 139.

TCP/IP stands for Transmission Control Protocol/Internet Protocol. TCP/IP was developed by the U.S. Department of Defense. TCP/IP is a language governing communications among all computers on the Internet.

TCP/IP uses two separate protocols, TCP and IP, together.

IP, which stands for Internet Protocol, dictates how packets of information are sent out over networks. IP has a packet-addressing method that lets any computer on the Internet forward a packet to another computer that is a step (or more) closer to the packet's recipient.

TCP, which stands for Transmission Control Protocol, ensures the reliability of data transmission across Internet-connected networks. TCP checks packets for errors and submits requests for re-transmissions if errors are found. It will also return the multiple packets of a

message into a proper, original sequence when the message reaches its destination.

To use the nbtstat command:

- 1 In Windows, click **Start > Programs > Accessories > Command Prompt**.

The Command Prompt window appears.

- 2 Enter nbtstat at the prompt.

Information similar to that shown [Figure 7-5](#) appears.

Figure 7-5 nbtstat

```

C:\WINDOWS\System32\cmd.exe
C:\>nbtstat -n
\Device\NbfT_Tcpip_{8E127952-AD09-4560-B6AB-81623193C8B9}:
Node IpAddress: {0.0.0.0} Scope Id: {}

No names in cache

Local Area Connection:
Node IpAddress: {141.183.46.42} Scope Id: {}

NetBIOS Local Name Table

Name                Type                Status
-----
SGHTSSRD             <00> UNIQUE          Registered
SGHTSSRD             <20> UNIQUE          Registered
AGILENT              <00> GROUP           Registered
AGILENT              <1E> GROUP           Registered
AGILENT              <1D> UNIQUE          Registered
...MSBROMSE          <01> GROUP           Registered
SGHTSSRD             <03> UNIQUE          Registered
CHINYONG             <03> UNIQUE          Registered
  
```

DHCP and DNS

DHCP is short for Dynamic Host Configuration Protocol (DHCP) is an Internet protocol for automating the configuration of computers that use TCP/IP. DHCP can be used to automatically assign IP addresses, to deliver TCP/IP stack configuration parameters such as the subnet mask and default router, and to provide other configuration information such as the addresses for printer, time and news servers.

DNS stands for Domain Name System (or Service or Server), an Internet service that translates domain names into IP addresses. It is easier to remember domain names because they are alphabetic. The Internet, however, is really based on IP addresses. Every time you use a domain name, therefore, a DNS service must translate the name into the corresponding IP address.

To check the IP addresses used by the DHCP and DNS servers:

- 1 In Windows, click **Start > Programs > Accessories > Command Prompt**.

The Command Prompt window appears.

- 2 Enter `ipconfig /all` at the prompt.

Information similar to that shown [Figure 7-6](#) appears.

The information in [Figure 7-6](#) tells us that the IP address for the DHCP server is 141.183.12.250. In addition, there are two DNS servers which have the IP address of 141.183.101.250 and 141.183.12.250 respectively.

Figure 7-6 IP addresses of DHCP and DNS servers

```

C:\WINDOWS\System32\cmd.exe
Description . . . . . : Nortel IPSEC3HM Adapter - Packet Scheduler
Physical Address . . . . . : 44-45-53-54-42-00
Dhcp Enabled . . . . . : No
IP Address . . . . . : 0.0.0.0
Subnet Mask . . . . . : 0.0.0.0
Default Gateway . . . . . :

Ethernet adapter Local Area Connection:
Connection-specific DNS Suffix . . . . . : sgp.agilent.com
Description . . . . . : National Semiconductor Corp. DP83815/816 1
PCI Adapter
Physical Address . . . . . : 00-0F-20-C9-B7-6B
Dhcp Enabled . . . . . : Yes
Autconfiguration Enabled . . . . . : Yes
IP Address . . . . . : 141.183.46.42
Subnet Mask . . . . . : 255.255.254.0
Default Gateway . . . . . : 141.183.46.1
DHCP Server . . . . . : 141.183.12.250
DNS Servers . . . . . : 141.183.101.250
                          141.183.12.250
Primary WINS Server . . . . . : 141.183.6.46
Secondary WINS Server . . . . . : 141.183.102.129
Lease Obtained . . . . . : Tuesday, October 19, 2004 8:31:37 AM
Lease Expires . . . . . : Wednesday, October 20, 2004 8:31:37 AM

C:\>

```


IP Addressing

The following subsections provide a brief description of the more commonly used methods of IP addressing.

Static and Dynamic IP addresses

Static IP addresses are the same every time you connect to the network, else dynamic IP addresses may change each time you connect to the network. Dynamic IP would lease an IP Address from the DHCP server. Hence, dynamic IP setting works together with a DHCP server.

Private IP addresses

The Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of the IP address space for private internets (local networks):

- 10.0.0.0 - 10.255.255.255
- 172.16.0.0 - 172.31.255.255
- 192.168.0.0 - 192.168.255.255

In addition, IP addresses in the range of 169.254.0.0 -169.254.255.255 are reserved for Automatic Private IP Addressing, APIPA.

Windows 98/98 SE, Windows ME, Windows 2000, Windows XP, and Windows 2003 Server have an Automatic Private IP Addressing (APIPA) feature that will automatically assign an Internet Protocol address to a computer on which it is installed. This occurs when the TCP/IP protocol is installed, set to obtain its IP address automatically from a Dynamic Host

Configuration Protocol server and when the DHCP server is absent or not available.

The abovementioned IP addresses should not be used on the Internet.

MAC Addressing

MAC is short for Media Access Control address, a hardware address that uniquely identifies each network adapter.

In IEEE 802 networks, the Data Link Control (DLC) layer of the OSI Reference Model is divided into two sublayers: the Logical Link Control (LLC) layer and the Media Access Control (MAC) layer. The MAC layer interfaces directly with the network medium.

To check the MAC address of the network adapter:

- 1 In Windows, click **Start > Programs > Accessories > Command Prompt**.

The Command Prompt window appears.

- 2 Enter `ipconfig /all` at the prompt.

Information similar to that shown [Figure 7-7](#) appears.

The information in [Figure 7-7](#) tells us that the MAC address, also known as the physical address, is 00-0F-20-C9-B7-6B.

Figure 7-7 MAC address

```

C:\WINDOWS\System32\cmd.exe
Description . . . . . : Nortel IPSEC3HM Adapter - Packet Scheduler
Physical Address . . . . . : 44-45-53-54-42-00
Dhcp Enabled . . . . . : No
IP Address . . . . . : 0.0.0.0
Subnet Mask . . . . . : 0.0.0.0
Default Gateway . . . . . :

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix . . . . . : sgp.agilent.com
    Description . . . . . : National Semiconductor Corp. DP83815/816 1
    PCI Adapter
    Physical Address . . . . . : 00-0F-20-C9-B7-6B
    Dhcp Enabled . . . . . : Yes
    Autoconfiguration Enabled . . . . . : Yes
    IP Address . . . . . : 141.183.46.42
    Subnet Mask . . . . . : 255.255.254.0
    Default Gateway . . . . . : 141.183.46.1
    DHCP Server . . . . . : 141.183.12.250
    DNS Servers . . . . . : 141.183.101.250
                            141.183.12.250
    Primary WINS Server . . . . . : 141.183.6.46
    Secondary WINS Server . . . . . : 141.183.102.129
    Lease Obtained . . . . . : Tuesday, October 19, 2004 8:31:37 AM
    Lease Expires . . . . . : Wednesday, October 20, 2004 8:31:37 AM

C:\>

```