

Data Acquisition Processor Service

Note: Windows refers to Windows 2000, Windows XP, Windows Vista, and Windows 7.

The Data Acquisition Processor service is a Windows Control Panel extension program. It manages and configures DAPcell/DAPcell Local/DAPcell Basic servers for communication between applications and Data Acquisition Processors. The Data Acquisition Processor service is installed by the `SETUP.EXE` installation program and can be started by opening the Windows Control Panel and double-clicking on the Data Acquisition Processor icon. For more information about DAPcell servers, refer to the Microstar Laboratories DAPcell documents.

Working with the Data Acquisition Processor Service

This document describes how to use the Data Acquisition Processor service.

Context-sensitive help is available for most service topics. To get help on a topic, select the question mark button located at the top right corner of the main screen of the service. When the mouse pointer changes to a question mark, place the pointer over any topic and press the mouse button again to display help on that topic. Help may also be found by simply pressing the F1 key while the topic of interest is selected.

To access a complete online help file for the Data Acquisition Processor service, press the Help button at the bottom of the main screen.

The main screen of the Data Acquisition Processor service consists of five sub-screens accessible via named tabs:

- [Control Screen](#)
- [Browser Screen](#)
- [Disk I/O Screen](#)
- [Modules Screen](#)
- [Mapping Screen](#)

The Data Acquisition Processor service can be in one of two modes: server mode or client mode. The service is in client mode if only DAPcell client software is installed.

In server mode, all five screens are accessible. In client mode, only [Browser Screen](#) and [Mapping Screen](#) are available.

Control Screen

The **Control Screen** is used to configure, to start, or to stop the local DAPcell service. The screen is divided into two sections: **Service Status** and **Service Configurations**.

Service Status

A single button in this section controls the status of the DAPcell service.

Start/Stop

Toggles to start or stop the DAPcell service.

Note: The DAPcell service should only be stopped and restarted if reinitializing the Data Acquisition Processor system is necessary. When the DAPcell service starts, the PCI Data Acquisition Processor's service controls are reset by default. A PCI Data Acquisition Processor that has already been functioning is reinitialized with a fresh copy of the DAPL operating system. Programs and data running on the Data Acquisition Processor are permanently lost.

Service Configuration

This section consists of two sub-sections: Startup and Security.

Startup

The Startup sub-section controls the startup configuration of the DAPcell server service. Click the "Change" button to view or edit startup configurations.

Startup Type

Startup Type determines when and how the server service starts:

- When "Automatic" is selected, the server service starts automatically each time Windows starts. The server service remains active across sessions until Windows shuts down.
- When "Manual" is selected, the server service will not begin until a user chooses to start it.

Priority

Service Priority configures the service execution priority and remote server control options.

Windows determines the program to run next on a PC by using scheduling priorities. A running program's scheduling priority is determined by the combination of its **priority class** and its **priority level** within a priority class. By default, all user programs use a base priority at the "normal" level within the "normal" priority class. The DAPcell service runs at this default priority.

Service Priority Class

The [service priority class](#) of a program dictates how much time or priority will be scheduled for the service. The four service priority classes are:

Low

- The lowest priority class. A program in the "low" priority class runs only when the system is otherwise idle.

Normal

- The default priority class. This class is acceptable for most programs.

High

- A program in the "high" priority class runs before programs in the "normal" or "low" classes. The "high" priority class is for programs that perform time-critical tasks.

Realtime

- The highest priority class. This priority class should almost never be used as it can cause the system to behave erratically.

Service Priority Level

The [service priority level](#) of a program dictates the priority the service will be given within a particular [service priority class](#). If two programs are in the same priority class, the priority level determines the one that runs next. Modifying this parameter will raise or lower a service's priority status within a class, but will have no effect between classes. The six service priority levels are:

Lowest

- The lowest priority level. A program in the "lowest" priority level runs only when all other tasks are suspended.

Below Normal

- This priority level is one level higher than the "lowest" level.

Normal

- The default priority level. This level is acceptable for most programs.

Above Normal

- This priority level is one level higher than the "normal" level.

Highest

- A program in the "highest" priority level runs before all programs in a particular priority class except those in the "time critical" level.

Time Critical

- The highest priority level. The "time critical" level sets the level to the "highest" priority within the "high" priority class for "low," "normal," and "high" classes. It sets the level to the highest priority possible for the "realtime" class. This priority level can interfere with the normal operation of the operating system and should generally be avoided.

Security

The *Security* sub-section grants or revokes permission for a remote client to control the server service in various ways. Allowing a remote client to control the service is usually dangerous and should be handled with great care. (To view a list of control options, right-click on the server icon in the Browser screen.) To view or edit the security settings, click the “Settings” button.

Remote Server Control

A DAPcell server service can be configured to accept [restart/shutdown](#) requests from remote clients. This option affects the security of the service and should be used with great care. Changing the server control option requires the administrator privilege. The three control options are:

Disabled

- Allows no remote server control.

Restart

- Allows remote clients to restart the service. This is the default.

Restart/Shutdown

- Allows remote clients to restart the service or to shut down or reboot the server machine.

Remote DAP Default Name Reorder

The DAPcell service configures all local Data Acquisition Processors in a way to make it easy for a client to address a Data Acquisition Processor (DAP) by name. By default, DAPs are named `Dap0`, `Dap1`, ..., to `DapN` where `N+1` is the number of DAPs on the local system. For the numbering of DAP names, refer to the topic [UNC Pipe Names](#). Once configured, these names stay with their associated DAPs even after adding or removing DAPs has altered the configuration. A new default name order will not be established until the service is reinstalled or until a request comes to reorder the default names. A local client can always make such a request, however, a remote client can do so only if the service is configured to allow it. Enabling this remote control could potentially cause the service configuration to be inadvertently altered and, thus, should be used with care.

Disabled

- Allows no remote request.

Enabled

- Allows remote clients to restore the server default configuration.

Caution: The default settings for the server configurations are generally acceptable for the service. Changing these settings may affect time-critical programs or cause the system to behave erratically.

Three buttons at the bottom of each of the two subsections control the configurations:

Ok

Saves the modified configurations. A change to the remote server control takes effect immediately even if it is not saved. Changes to the service priorities will not take effect until they are saved and the service is restarted.

Default

Restores the default service configurations.

Cancel

Cancel the configuration modifications.

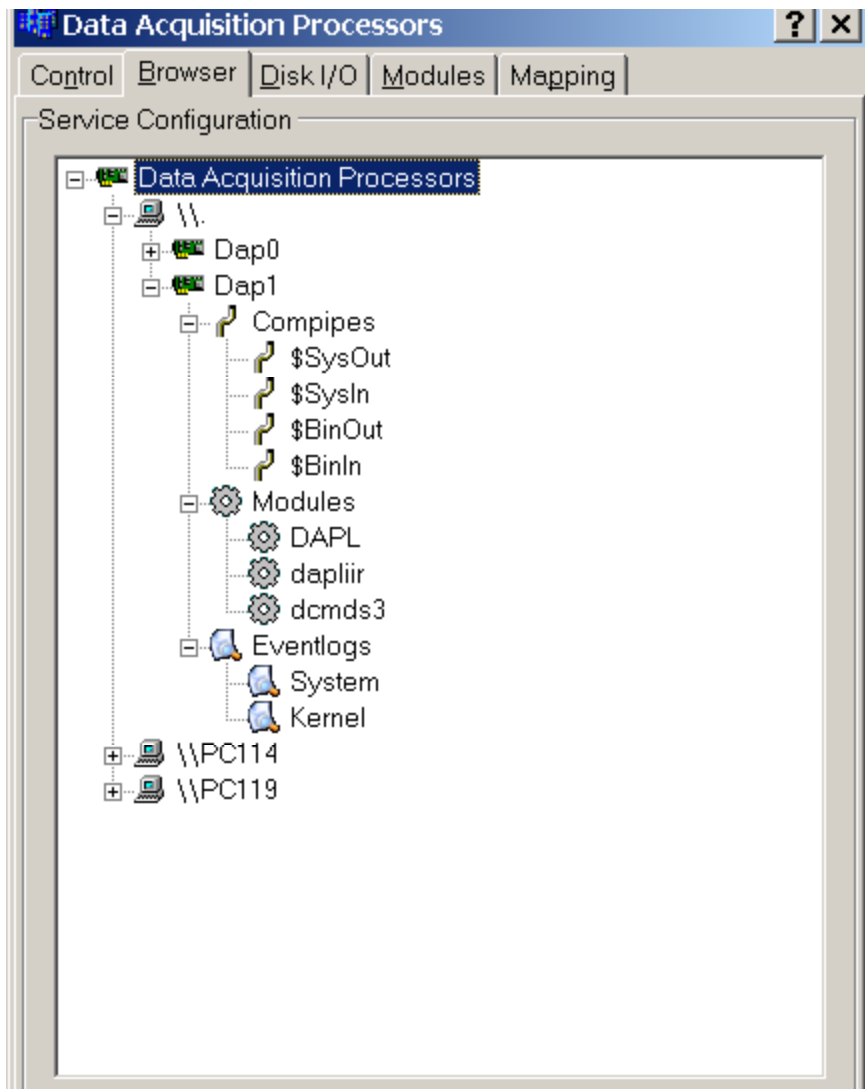
Browser Screen

The [Browser Screen](#) allows users to display and search for installed DAPcell servers and DAPs on a local machine or over the network. The screen contains a [Service Configuration](#) section that gives both textual and graphical descriptions of the installed DAPcell servers and the DAPs they control.

Service Configuration Tree View

A display box in the [Service Configuration](#) section of the [Browser Screen](#) shows the search result of the DAPcell servers and DAPs installed on the local machine or over the network. The servers and DAPs are displayed as icons arranged in a graphical tree structure. Double-clicking on the selected icon in the display moves down one level in the search tree.

The following diagram displays an example Data Acquisition Processor configuration:



At the very top is the Data Acquisition Processor icon, representing the network search level. The three servers connected to the network are `\\.`, `\\PC114`, and `\\PC119`. The servers are identified by computer icons and are designated as `\\` followed by PC names.

Right-clicking on a server node brings up a server control menu that provides six control functions: *Restart the DAP service*, *Shutdown the server*, *Force the server to shutdown*, *Reboot the server*, *Force the server to reboot*, and *Reorder DAP default names*. For a remote server, such an operation succeeds only when the server is configured to do so.

The next level down in the search tree displays the DAPs attached to each server: `Dap0`, `Dap1`, ..., and `Dap(N-1)` where `N` is the number of DAPs attached to each server. Each DAP is identified by a DAP icon.

Selecting one of the DAPs moves down to the next level, which typically displays three categories of DAPL objects: `Compipes`, `Modules`, and `Eventlogs`. The `Compipes` category includes communication channels defined between the PC and the DAP. The `Modules` category includes software `Modules` installed on the DAP. And the `Eventlogs` category allows viewing the contents of eventlogs on the DAP, if the DAP supports it.

Right-clicking on the `Compipes` node brings up a menu for creating a custom communication channel between the PC and the DAP.

Selecting `Compipes` moves down to the lowest level in that category, and displays the communication channels defined for the DAP: `$SysOut`, `$SysIn`, `$BinOut`, and `$BinIn`, and custom-created communication channels if any. Additional information can be found under the topic [UNC Pipe Names](#).

Right-clicking on a channel node brings up a menu for deleting the communication channel.

Selecting `Modules` displays a list of software modules installed on the DAP. It could be empty if no other downloadable software modules are installed besides the DAPL operating system.

Clicking on one of the items under `Eventlogs` brings up the contents of that eventlog.

Descriptions

The Description area below the display box provides the following information about the selected search tree node:

At the Network level:

- Client version
- Number of servers found
- Number of DAPs found

At the Server level:

- Server Name
- Server Version
- Server OS
- Connection Protocol

At the DAP level:

- DAP Model
- Serial Number
- Interrupt Level (present when relevant)
- Location (format is hardware interface dependent)

At the pipe level:

- Direction
- Width
- Buffer Size

At the module level:

- Description
- Versions
- Copyright
- Location

Find Server

A [Find server](#) edit box takes a UNC server path and tries to find the remote DAPcell server over the network. If found, the server is displayed in the tree-view box. This is a faster way to search for a server if the path of the server is known.

Network Transport

A [Network transport](#) drop-down box at the bottom of the [Browser Screen](#) provides the capability to search the entire network or to customize the search using either the Local, All, NetBEUI, SPX/IPX, TCP/IP, or NamedPipe network transports:

- Selecting the Local transport and the [Refresh](#) button will search DAP servers only on the local machine.
- Selecting one of the other network transports and the [Refresh](#) button will search over the network using that transport. If All is selected, the DAP Service will search the network using all network transports that the local system supports.

Include Cache

Once a server is found, it is cached. The [Include cache](#) check box is used to instruct the refresh operation whether to include cached servers or not.

Refresh

The [Refresh](#) button at the bottom of the screen toggles to "Abort" once it is clicked to start a refreshing session, and toggles back to [Refresh](#) when the session is done. It either refreshes the [Service Configuration](#) tree view using the transport selected in the network transport drop-down box or aborts the refresh operation if one is going on.

Disk I/O Screen

The **Disk I/O Screen** is used to specify default data paths and access permission for direct disk I/O performed on the server side. The settings do not affect disk I/O performed on the client side.

DAPcell Service and DAPcell Local Service both support direct disk I/O through the `DapPipeDiskLog` and `DapPipeDiskFeed` functions. Direct disk I/O is not available in DAPcell Basic Service. When direct disk I/O is not supported, the **Disk I/O Screen** is disabled (with all the options grayed).

The **Disk I/O Screen** is divided into two sections: Disk Logging and Disk Feeding. Each section contains a **Default Path** subsection and a **Permission** subsection. The screen also provides a Save button and a Cancel button.

Default Path

The **Default Path** section displays the current default paths to the target disk files if there are any previously registered. New paths can be entered to replace the existing ones. New paths will not take effect until after they are saved using the Save button.

To enter new default paths, click the Edit button. This brings up an edit dialog box. The edit dialog has two check boxes, labeled Create Share and Automatic; a Default Path edit box; and a Default Shares edit box.

Checking the Create Share box allows creating a network Share name for each path entered. That way, any PC on the network can access the path using the share name. If the Automatic box is also checked, a share name is automatically created for each path entered.

Default Path is a list of absolute directory paths, each starting with a drive letter, separated by a semicolon. For example, `c:\Data;d:\Data\Backup` is a valid default path list while `e \Data;Backup` is not.

Default Shares is a list of network share names, also separated by semicolons. A share name must be unique on the host system. If automatic share names are used, they follow a predefined naming convention of `DAPcellDataL<n>` for disk logging and `DAPcellDataF<n>` for disk feeding, where `<n>` is a zero-based integer.

Each item in the Default Shares edit box corresponds to the item listed in the same order in the Default Path edit box. There can be one share name for each path in the **Default Path** edit box. In other words, the first Share listed is the name used for the first Path listed, the second Share is the name used for the second Path, and so on.

Permission

The **Permission** section displays the current disk I/O access permission level. Clicking on the desired radio button changes the permission level. The new level will not take effect until after it is saved using the Save button.

Three permission levels are available to control the disk I/O access:

Not allowed

- Allows no disk I/O.

Restricted

- Allows disk I/O only if the target file resides in one of the directories specified by the Default Path, or in one of its subdirectories; otherwise, disk I/O requests will be rejected. If a disk write request is allowed and the target subdirectory does not exist, the directory will be created.

Normal

- In addition to what the [Restricted](#) level allows, this permission level allows direct disk I/O to perform in any reachable directories as long as they exist. However, it will not create any new directory beyond what the [Restricted](#) level allows.

Modules Screen

The [Modules Screen](#) is used to configure the Data Acquisition Processor service for DAPL module installation. This includes configuring remote module installation permission and module management options.

The [Modules Screen](#) is divided into two sections: [Permission](#) and [Installed Modules](#). The [Installed Modules](#) section consists of a tree view of installed modules and a module description block. At the bottom of the screen, four buttons are available for module management operations: [Add](#), [Delete](#), [Setting](#), and [Reload](#).

Permission

A selected radio button in the [Permission](#) section shows the current permission for remote module installation. To change the permission, click the desired button and the change takes effect immediately.

Installed Modules

A tree view displays all the modules currently installed for designated DAPL operating systems on this server. Selecting one of the nodes in the tree view makes the module that the node represents the active target. Then [Delete](#), [Setting](#), and [Reload](#) buttons will all operate on this active target. The [Description](#) block will show a list of information items about the selected module, such as the module description, version, copyright, and location, if they are available.

The root of the tree does not represent any specific modules. Selecting the root node enables the [Add](#) button only.

DAPL operating system modules are shown in the tree view as the parent nodes of all other modules installed for the operating systems. They are named `DAPL2000` and `DAPL3000` representing DAPL 2000 and DAPL 3000 operating systems respectively. When one of them is selected, only the [Add](#) button and the [Reload](#) button are active. The [Add](#) button adds modules under the selected operating system and the [Reload](#) button reloads the operating system to a selected set of Data Acquisition Processors. When the DAPL module is reloaded, all modules installed for each selected DAP are reloaded as well.

Selecting a child node under an operating system node enables all four buttons. The complete set of module management options is available for the selected module.

The module tree view does not include ROM-based modules, that are available on some Data Acquisition Processors.

Add

The [Add](#) button allows installing a module and optionally loading it to the Data Acquisition Processors on the system at the same time.

Clicking the [Add](#) button brings up an `Adding a module` dialog box. The first thing to do is to select the DAPL operating system(s) the new module is to be installed to. Selecting `DAPL3000` or `DAPL2000` will install a new module only to the corresponding operating system. Selecting `Both` will install the module to both operating systems.

Next, enter the complete path of the target module and click `OK` to install. There are two ways to enter the path: (1) type the path directly into the edit box or (2) click the `Browse` button to bring up an `Open` box, navigate to find and select the target module, and click `Open` to automatically enter the path. Once a module is installed, it persists until it is uninstalled.

The `Adding a module` dialog box has an `Options` section with four options.

`Copy`

Copy the module binary from the user-specified directory to the default directory the `SETUP` program created. The `Data Acquisition Processor` service then uses the copy from the default directory whenever it is needed. If `Copy` is not selected, the `Data Acquisition Processor` service uses the copy from the user-specified directory.

`Load`

Load the module binary to the `Data Acquisition Processors` with the installation so that the module is immediately available for use.

`Replace`

Replace the module with the new binary if it is already installed.

`Force`

Force the module installation, ignoring any resources the module may need in order to be installed, such as the existence of an installed module it depends on. This option should be used with caution because it can create an inconsistent configuration.

The default `Add` option configuration is `Copy`, `Load`, and `Replace`.

The `Adding a module` dialog box also has a list of check boxes for all the `Data Acquisition Processors` on the system. Unchecking a `Data Acquisition Processor` will disable the module installation to that particular `Data Acquisition Processor`.

Delete

The `Delete` button allows uninstalling a module from the system and optionally removing the module from the `Data Acquisition Processors` at the same time.

Clicking the `Delete` button brings up a `Deleting a module` dialog box.

The `Deleting a module` dialog box has an `Options` section with three options.

`Force`

Force the removal of the target module even if it is being used.

`Unload`

Unload the module from the `Data Acquisition Processors` with uninstallation. If this option is not selected, the module is uninstalled from the system but stays loaded on the `Data Acquisition Processors` until the `DAPL` operating system is reloaded.

`Remove Dependents`

Uninstall the module and all modules that depend on this module as well.

The default `Delete` option configuration is `Unload` only.

Setting

The **Setting** button allows reconfiguring the system so that the target module is installed for the selected Data Acquisition Processors only.

Clicking the **Setting** button brings up a `Configuring a module` dialog box. Check the Data Acquisition Processors that need the module and uncheck those that do not. The new configuration will not take effect until the DAPL operating system is reloaded.

For DAPs that have ROM-based modules, this screen should be used to selectively skip the installation of a module to those DAPs, so that they can keep their ROM version of the module, or to include it, so to override the ROM-based module.

Reload

The **Reload** button allows reloading the selected module to the Data Acquisition Processors.

Clicking the **Reload** button brings up a `Loading a module` dialog box. Check the Data Acquisition Processors that need the module to be reloaded and uncheck those that do not.

The `Loading a module` dialog box has an `Options` section with two options.

Replace

Replace the module with the new module binary if it is already loaded on the Data Acquisition Processors.

Force

Force the reloading even if the module is being used on the Data Acquisition Processors.

See the `DAPI032 Reference Manual` for more information about module installation operations and their options.

Mapping Screen

The [Mapping Screen](#) is used for custom DAP and ACCEL mapping. Two buttons, [DAP Mapping](#) and [ACCEL Mapping](#), each access an additional window where the actual mappings are specified.

The DAP Map and ACCEL Map windows are discussed in greater detail in the following sections. Generally, both windows provide the same drag-and-drop editing mechanism. Select a target in the display box, drag it to the corresponding grid, and drop it. Direct editing may also be done in the grid box. In either window, a user may right-click on the display box to refresh the box.

DAP Mapping

[DAP Mapping](#) is used only for 32-bit applications. It is unnecessary unless an application does not want to use the complete network UNC address of the DAPs. The mapping is between DAP names only and, if done, goes to the Windows registry.

When the [DAP Mapping](#) button is selected, the DAP Map screen appears. From this screen the user can specify custom mapping schemes for DAP names.

The DAP Map screen contains a menu bar at the top with a single menu.

Search Menu

- Allows the user to refresh the DAP Map screen and search a local machine or network for installed DAPs.

By right-clicking on the shaded column in the grid box, a user may select a direct DAP name or a local DAP name to map to. Up to 63 DAP names may be mapped.

ACCEL Mapping

In the DOS and Windows DAP drivers, a communication channel to a Data Acquisition Processor is seen as an ACCEL device, either as a directed ACCEL device or as a numbered ACCEL device. In order for DAPcell to support existing DOS and Windows applications, it is necessary to provide a mechanism to map the ACCEL device names to the corresponding [UNC Pipe Names](#) that DAPcell recognizes.

By default, DAPcell automatically maps ACCEL0 to `\\.\Dap0\$\SysIn` and `\\.\Dap0\$\SysOut` and ACCEL1 to `\\.\Dap0\$\BinIn` and `\\.\Dap0\$\BinOut`. Then it maps ACCEL2 to `\\.\Dap1\$\SysIn` and `\\.\Dap1\$\SysOut` and ACCEL3 to `\\.\Dap1\$\BinIn` and `\\.\Dap1\$\BinOut`. And so on, depending on how many Data Acquisition Processors are installed on the local machine.

[ACCEL Mapping](#) is necessary if a configuration involves remote DAPs or additional communication pipes. A mapping file called ACOM.INI, which resides in the Windows system directory, fulfills the custom mapping. This file specifies a complete set of mappings an application requires. The DAPcell Service creates the ACOM.INI file and then makes the mapping according to the specification.

When the [ACCEL Mapping](#) button is selected, the ACCEL Map screen appears. From this screen the user can specify custom mapping schemes for ACCEL devices to [UNC Pipe Names](#).

The ACCEL Map screen contains a menu bar with three menus:

File Menu

- Provides file operations for the section workspaces.

Search Menu

- Allows the user to refresh the ACCEL Map screen and search a local machine or network for installed DAP servers.

View Menu

- Allows the user to toggle easily between viewing different sections.

Up to 127 ACCEL devices may be mapped.

Universal Naming Convention (UNC) Pipe Names

A remote machine is represented by its unique network machine name. The local machine is denoted by a period.

The Data Acquisition Processor names are predefined as `Dap0`, `Dap1`, ..., and `Dap(N-1)` where `N` is the number of Data Acquisition Processors installed on the system. The ordering depends on the numeric ordering of the I/O addresses that the Data Acquisition Processors use. The name ordering of PCI Data Acquisition Processors is based first on the PCI bus number and then on the slot number. USB DAPs follow PCI DAPs and are ordered by their port numbers. For example, in a single Data Acquisition Processor system, the name of the DAP is always `Dap0`. In a four-DAP system, the PCI DAP sitting on PCI bus 0 slot 11 is `Dap0`, the PCI DAP sitting on bus 1 slot 5 is `Dap1`, the USB DAP connected to port 1 is `Dap2` and the USB DAP connected to port 4 is `Dap3`. (Note that USB port numbers in Windows may not be unique under certain system configurations; in such cases, port numbers are not the only ordering criteria.)

The pipe names are also predefined. On the Data Acquisition Processor, two communication pipes are associated with one integer number but differ in transfer directions, input or output. `$SysIn` and `$SysOut` are the default input and output pipes with the number zero, while `$BinIn` and `$BinOut` are the default input and output pipes with the number one. DAPcell supports a maximum of 32 sets of input and output communication pipes on each Data Acquisition Processor, therefore the largest number that can be associated with a pipe is 31. Except for the two default sets, all predefined pipe names carry both the pipe number information and the pipe direction information. Following is a list of the 32 supported sets of communication pipes:

<code>\$SysIn</code>		<code>\$SysOut</code>
<code>\$BinIn</code>		<code>\$BinOut</code>
<code>Cp2In</code>		<code>Cp20ut</code>
<code>Cp3In</code>		<code>Cp30ut</code>
<code>Cp4In</code>		<code>Cp40ut</code>
	<code>...</code>	
<code>Cp31In</code>		<code>Cp310ut</code>

Thus, the communication pipe `$SysIn` of the Data Acquisition Processor `Dap0` on the local machine is represented by the UNC name `\\.Dap0\\$SysIn`, and the pipe `$BinOut` of the Data Acquisition Processor `Dap1` on the remote machine `PC101` is referred to as `\\PC101\Dap1\\$BinOut`. For example,

```
\\.DapX\\$SysIn
\\.DapX\\$SysOut
\\.DapX\\$BinIn
\\.DapX\\$BinOut
```

are the four default communication pipes on the Data Acquisition Processor `DapX` on the local machine, and

```
\\PC101\DapX\\$SysIn
\\PC101\DapX\\$SysOut
\\PC101\DapX\\$BinIn
\\PC101\DapX\\$BinOut
```

are the four default communication pipes on the Data Acquisition Processor `DapX` on the remote machine `PC101`.

Copyrights and Trademarks

This document contains proprietary information that is protected by copyright. All rights are reserved. No part of this document may be photocopied, reproduced, or translated to another language without prior written consent of Microstar Laboratories, Inc.

Copyright © 1998 - 2010

Microstar Laboratories, Inc.
2265 116th Avenue N.E.
Bellevue, WA 98004
Tel: (425) 453-2345
Fax: (425) 453-3199
[http:// www.mstarlabs.com](http://www.mstarlabs.com)

Microstar Laboratories, DAPcell, Data Acquisition Processor, DAP, xDAP, DAPL, DAPview, and DAPstudio are trademarks of Microstar Laboratories, Inc.

Microstar Laboratories requires express written approval from its President if any Microstar Laboratories products are to be used in or with systems, devices, or applications in which failure can be expected to endanger human life.

Microsoft, MS, and MS-DOS are registered trademarks of Microsoft Corporation. Windows is a trademark of Microsoft Corporation. IBM is a registered trademark of International Business Machines Corporation. Intel is a registered trademark of Intel Corporation. Other brand and product names are trademarks or registered trademarks of their respective holders.