Table of Contents

Appendix E - Extra Features/Additional Information

Overview

This appendix provides information about additional features available with the M205/M206.

Key Features

- Detailed overview of print server architecture - *Print Server Architecture* on page E-2
- How to use the M205/M206's built-in security features as well as taking advantage of your Network's security features - *M205/M206 Security* on page E-7
- How to monitor your printer's performance - *Printer Monitoring and Logging* on page E-10
- Using SNMP, including creating custom MIB's - *Managing with SNMP* on page E-19

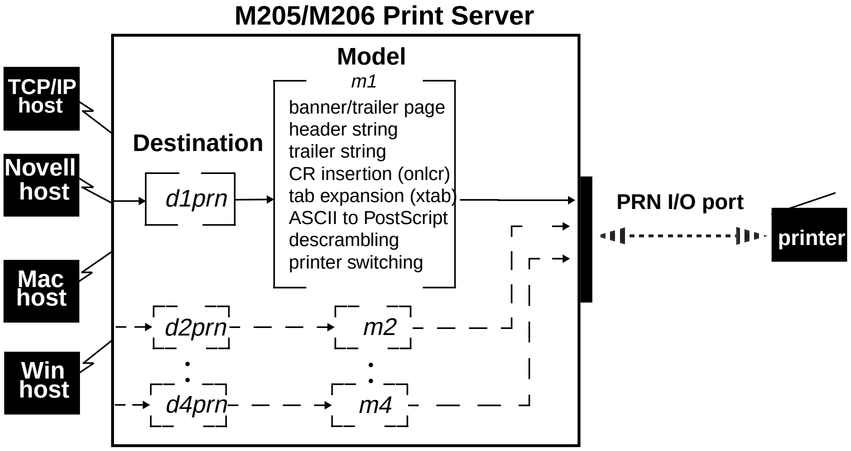
Print Server Architecture

Overview

This section will provide a more detailed description of the internal operating architecture of the M205/M206 including: destinations, models, variables, logpaths, and the I/O port.

When you send a print job to the Print Server, the print job doesn't go directly to the I/O port but first goes to a ***destination***. A destination can be thought of as *logical* place on the Print Server to send print jobs. Each destination has an ***I/O port*** and a ***model*** (see below) associated with it. Since their is only one I/O port on the unit, the I/O port is always the parallel port called **prn**. The purpose of our ***destinations*** is to allow you the ability to configure a number of different print setups on the Print Server.

Figure 1: Print Server Operating Logic



This example follows a print job sent to destination *d1prn. d1prn* is associated with model *m1* and the I/O port *prn.*

When the data is passed through the associated model, any job processing specified by the model is performed on the data.

Destinations

The M205/M206 provides four printer destinations that are used by all hosts. Destinations map a name, with a nine-character maximum, to the I/O port PRN. The I/O port has four destinations mapped to it. The **default destination** names are: d1prn, d2prn, d3prn, and d4prn. If you like, any of these destination names can be changed to be something more meaningful.

Each destination uses one of the defined models for processing. The destination list is limited to a maximum of four entries, and is configured through the **npsh** interface on the Print Server. Default destination names can also be changed to something more meaningful.

Destination definitions include: name, I/O port, model used, logpath, state, and service(s) supported

See also: *list des*t on page G-5**,** *set dest* on page G-6, and *Manipulating the M205/M206's Services* on page E-6.

Models

Each destination on the M205/M206 also has a ***model*** associated with it. The four models (one per destination) can be thought of as a series of mini-filters that can do special processing with the print job data. For example, a model can be set up to do such things as ASCII to PostScript conversion (a2ps) or carriage return insertion (onlcr).

These processing options include:

- banner page generation,
- header string insertion,
- trailer string insertion,
- tab expansion (**xtab**),
- carriage return insertion (**onlcr**),
- ASCII to PostScript conversion (**a2ps**),
- print job descrambling.

The default model names are *m1* to *m4* and each comes mapped to a particular destination. By default, the model settings are **raw**, that is, they simply pass data through to the I/O port untouched. This provides a clean slate to begin your configuration. Model names can be changed to be something more meaningful. Models only need to be reconfigured when you want to do special processing to all the print jobs that are sent to a particular destination.

Note: The models are *not* capable of multiple copies and throughput may decrease if **onlcr** or **a2ps** is enabled.

Each **model definition** includes: name, type, and some of these processing parameters, if any.

See also: *list model on page G-5, set model on page G-9,*and *Setting Up Special Job Processing* on page E-6.

Table 1: Model Types

Setting	Inclusions
raw	No content sensing. Jobs are assumed to match the printer type, or else the printer does the autosensing and switching.

Table 1: Model Types

Setting	Inclusions
pcl-ps	For printers that *cannot* autosense the print job format and switch modes by themselves. Precedes each job with a string to switch from PostScript to PCL, or vice versa, depending on job content. These strings must be specified in the setup command.
a2ps	Convert ASCII jobs to PostScript or pass PostScript jobs directly to PostScript printers.

Variables

Variables are actually utilized within the M205/M206's *models* and are useful for defining lengthy header or trailer strings. This might be necessary for certain printer switch strings, for example. Each variable consists of a combination of escape codes and text for this printer control.

Variables are used to make efficient use of the limited space in these header and trailer strings. Only nine elements can be included in these strings. Each element can be one of the following:

letter	**a**
code	**0x40**
variable	**$FF**

Therefore, you could make up a series of variables and specify each of these (up to nine) in the header or trailer string. Each variable could then contain up to 14 elements of its own.

Commands are described in detail in Appendix G. See also: *list var* on page G-6, *set var* on page G-15, *list model* on page G-5, and *set model* on page G-9.

Logpaths

The term *logpath* comes from the UNIX **syslog** logging system. With the M205/M206, each destination can report statistics on: user, page count, job name, and printer errors. In addition, a checksum calculation can be obtained to confirm data integrity when a job is sent to the printer.

Logging occurs either through a printer or terminal connected to the I/O port, or through a Telnet session to a particular TCP port. A logpath can also be configured to report statistics via email to a particular user. This can then be saved to a file if desired. In addition, messages can be logged to SYSLOGD on a particular TCP/IP host.

Each logpath is associated with a particular destination and the four default logpath names range from *l1* to *l4***.** Logpath names can be changed to be something more meaningful.

Logpath definitions include: name, log port, and log type.

See also: *list logpath* on page G-5, see *set logpath* on page G-8, *Controlling the Frame Types Used by the M205/M206* on page E-7.

I/O Port

The M205/M206 comes with one IEEE 1284-I compliant four-speed parallel port which attaches directly to the parallel port of the printer. The I/O port has an internal queuing mechanism that automatically queues print jobs on a first-come, first-serve basis even if the print jobs come from different network environments (e.g. Novell and TCP/IP).

The port has several parameters that can be manipulated to best suit your attached peripherals. These parameters are configured using the **set** commands while **list** commands display the port's settings.

Please refer to the following commands for the indicated information:

- To learn more about the I/O port's parameters, please see *Parallel Port (PRN)* on page F-3.
- To look at current the I/O port settings, please see *list prn* on page G-5.
- To change the I/O port settings, please see *set prn* on page G-11.

General Options

Using Different Naming Schemes

By default, the M205/M206 is named **M_xxxxxx** where ***xxxxxx*** is the last six digits of the Ethernet address as found on the bottom of the unit. This name affects a Novell, AppleTalk, and NetBIOS setup. To change this name to something more suitable for your printing environment, please see *store pserver* on page G-17.

If you decide to reconfigure the default name and you are using a CONFIG file to set M205/M206 parameters with your Novell setup, you must remember to rename the directory containing this file.

Manipulating the M205/M206's UTP Interface

If using UTP on your network, you have some control over the UTP interface and its properties on the M205/M206.

By default, link integrity is turned on but this can be turned off using the Number 3 dipswitch on the back of the unit. Please see *Back to Factory Defaults* on page 55 of the M205/M206 Quick Reference and Installation Guide for more information.

(Applies to M205 only) - you can increase the sensitivity of the 10Base-T receiver for implementations where line lengths exceed the recommended 10Base-T maximum of 100 meters. However, this increases the receiver's vulnerability to noise and should only be used in installations with 2-pair cable. Factory default for this setting is *off*.

To see the current UTP interface settings for a particular network interface, please see *list ifc* on page G-5 To manipulate the UTP interface, please see *store ifc* on page G-16

Setting Up Special Job Processing

Printing with the M205/M206 adds a lot of extra job processing options to your current print setup. No matter the environment, you now have the choice of several helpful features including:

- ASCII to PostScript conversion (**a2ps**),
- carriage return insertion (**onlcr**),
- tab expansion (**xtab**),
- banner page generation,
- printer mode switching and general printer manipulation.

These are just some of the many features provided and with each of these, you may set them on the host within an interface file, **nprbsd.if** or **nprsysv.if**, or on the Print Server itself.

You are automatically given the choice between four different **destinations** on the M205/M206 allowing for four different possible print setups; each of these print setups is defined by the extra processing specified by it's associated **model**. It is the model that defines most of these extra processing options.

To make use of these special job processing features, please read over the appropriate host configuration section or the full list of extra job processing options documented in *set model* on page G-9.

Manipulating the M205/M206's Services

The M205/M206 provides many different functions; however, the more features it has, the more memory it requires. Therefore, it is possible to control the number of features enabled.

If you are not utilizing all of the protocols provided on the M205/M206, you can disable the unused ones providing more memory for the protocol(s) in use. Please see *set sysinfo module* on page G-14 for the command details.

In addition to disabling certain modules, you can also disable destination services. Not every destination on the M205/M206 needs to have the same functionality and in the case of an AppleTalk setup, you probably don't want every destination appearing in the Chooser. Please see *set dest* on page G-7.

Controlling the Frame Types Used by the M205/M206

Various frame types can be used by the Print Server at any given time but each supported protocol's frame type configuration is completely separate from another protocol's. This frame type support is configurable.

Novell and TCP/IP are really the only protocols that offer this configuration. The M205/M206 provides simultaneous support of multiple Novell frame types. Please see *store pserver* on page G-17 and *store tcpip* on page G-19 to find out which frame types are offered in each environment.

Remotely Managing the M205/M206

In a TCP/IP environment, various methods are available for remotely monitoring the Print Server. These include:

- a Telnet session,
- using **rsh/rcmd/remsh** and a command from the unit's command set,
- using **ezsetup**'s *Detailed Configuration Options Sub-Menu*,
- using the FTP Daemon,
- through an SNMP manager.

M205/M206 Security

The M205/M206 Quick Reference and Installation Guide touches upon the most popular built-in security feature - permission levels and passwords. Setting passwords and assigning a permission level to users makes it difficult for unauthorized users to gain access to the M205/M206's command set and manipulating the settings.

However, the print server also uses TCP access lists to restrict host connections with the device and allows scrambling/descrambling of print jobs.

Users and Passwords

The M205/M206 supports two user types:

root Access to everything within the print server including all configurable settings.

guest Ability to list settings but not configure them.

For each user type, passwords can be set. However, you would normally only set a password for the root user to protect the M205/M206's configuration. Guest users cannot alter the print server's configuration in any way.

To configure a root password on your M205/M206, you will need to:

1 Start a Telnet session with the M205/M206. Type:
`telnet` ***`M205/M206IPaddress`***

2 Login to the M205/M206 through an **npsh** session as a root user.

Note: If prompted for a "User ID" and password first, type in "**`root`**" for the ID and press ENTER at the password prompt since there's no password by default.

3 At the **npsh** prompt, follow this syntax:
`set user passwd` ***`username password`***

For example, to set the root password to "mplex1" type:

```
set user passwd root mplex1

save
```

From this point on, anytime you log in to the M205/M206 as "**`root`**", you will need to specify this password or else your login attempt will fail.

Note: To clear this password or change it, follow the same instructions. Just enter the appropriate "Old" password and put in the new one (or nothing if you don't want a root password any longer). The commands syntax is:

```
set user from default

save
```

TCP Access Lists

Within TCP/IP environments, the M205/M206 can restrict host access to destinations/queues and remote command (i.e. rsh, rcmd, remsh and telnet) execution services. This is done using an access list similar in function to the Unix.rhosts file.

To view the current access list on the print server, you will need to:

1 Start a Telnet session with the M205/M206.
`telnet` ***`M205/M206IPaddress`***

2 Log in as "**`root`**" and press ENTER at the password prompt since there is no password by default.

3 List the current access list.
`list tcpip`

If the list is empty, all hosts have access to the M205/M206's services. If there are entries in the list, only those hosts specified have access to printing and remote command execution.

Note: Only users that have **root** permission can configure the remote access entries. Users with **guest** permission can only display them.

To add and delete access list entries, the commands are:

```
store tcpip tcp access add|del hostIPaddress|networkaddress

reset
```

where ***hostIPaddress*** is the IP address of a TCP/IP host on your network and ***networkaddress*** is the address of a subnet on your network. For example:

```
store tcpip tcp access add 192.75.11.25

store tcpip tcp access add 192.75.12.0

store tcpip tcp access del 192.75.11.25

reset
```

Note: Although the maximum number of entries in the access list is 10, each entry can refer to a network rather than a specific host. This allows all hosts on that specified network to have access plus any individual hosts specified in the list.

Scrambling/Descrambling

Another method of security is provided through data scrambling and descrambling. This TCP /IP security method protects user's print data as it is sent across the network the M205/M206 for printing. Microplex provides a binary on the host which scrambles the print job, **npscramble**. When the job reaches the print server it is desrambled for printing.

Note: This scrambling method will protect against casual viewing with network analyzers. However, it is *not* encrypted and *cannot* be considered safe from cryptographic attack.

To utilize this feature, you need to:

1 Look into the npscramble.c source code fora variable called SR_KEY. This contains a four digit hexadecimal value to be used as the descrambling key on the M205/M206.

2 Log into the printer server as **root** user and set this value as key. Type:
```
set sysinfo descramblekey key
```

3 Set descrambling on the model you are utilizing. Type
```
set model modelname stty descramble
```

4 Save these settings.

```
save
```

5 Incorporate **npscramble** into your print setup on your host. Scrambling can be set within npr.if or added to the command line when printing. For example:

```
cat test.txt | npscramble | rsh spike lp -d d1prn
```

where **test.txt** is piped through **npscramble** for scrambling and then sent for printing on the M205/M206 **spike** destination **d1prn**.

Setting Novell Password Security

Besides the general security measures described above, a Novell setup provides further password security. Please refer to *Appendix C - More on Novell*.

SNMP Security

SNMP does not include any formal type of security definition. However, security can be accomplished using *communities*. A *community* is a string that is sent with every SNMP request and is used to define a certain view of the MIB. By doing this, you can control what parts of the MIB are accessed by SNMP manager.

To access the M205/M206's custom MIB, the public *community* string can be use to read any variables that have access. To restrict **write** access, there is an additional security step, involving defining a user named **snmp** on the M205/M206 with **root** privileges. The password defined for this **snmp** user will then be used as the *community* string which allows **write** access.

Note: If no **snmp** user is defined with **root** privileges, no **write** requests will be accepted by the M205/M206.

Printer Monitoring and Logging

One of the key aspects of maintaining a computing environment is monitoring printer status and logging this information to useful places. The destination of this information is controlled through logpaths. In addition, the Print Server's **lp**stat command provides parallel port printer status and job information as a user sends a job.

Printer and Print Job Monitoring

To view the current status of the I/O port on the M205/M206, two methods are available:

1 Login to the print server as either **guest** or **root**.

2 Type the "**`lpstat`**" to get a description of the I/O port's status and a list of queued jobs. *Table 1* describes some of the common terms you may come across when viewing this status.

Table 1: Key Printer Logging Terms

Term	Description
"`idle`"	There is no job queued for the M205/M206's I/O port.
"`blocked`"	The printer is not allowing the M205/M206 to send data to it. Check that there isn't a printer error and it's on-line and ready to go.
"`waiting`"	The M205/M206 knows about a print job but is waiting for the host to send more data or to send an expected packet.

Printer Logging Through Logpaths

Within the M205/M206 Quick Reference and Installation Guide, destinations are described as logical queues with associated models and logpaths. Models determine if any extra processing is needed with the print jobs passing through and logpaths determine whether any logging is needed for each job. With the M205/M206, destinations can report statistics on a checksum calculation can be obtained to confirm data integrity when a job is sent to a printer.

Logging occurs either through a printer connected to the I/O port or through a telnet session to the TCP port. A logpath can also be configured to report statistics via e-mail to a particular user. This can then be saved to a file if desired. Messages can also be logged to SYSLOGD on a particular TCP/IP host.

Each logpath is associated with a particular destination and the four default logpath names range from 11 to 14. Logpath names can be changed to something more meaningful.

Each logpath on the M205/M206 consists of two parts:

Type The type of log information to be captured. The choices are "**`job`**" for job ID and username, "**`user`**" for user ID (and three messages per job), "**`pgcnt`**" for total pages printed in a job, "**`cksum`**" for file checksums, "**`printer`**" for special printer feedback, and "**`ioport`**" for parallel printer status messages.

Port Where this log information will be sent to. The choices are a **TCP port number** (e.g. 4400), an **e-mail address** (including an alias), and a central host running a **SYSLOG daemon**.

To view the current logpath settings on the print server, you will need to:

1 Start a Telnet session with the M205/M206.
```
telnet M205/M206IPaddress
```

2 Log in as "**`root`**" and either type the password or press ENTER at the password prompt since there is no password by default.

3 The command to view the logpath settings is:
```
list logpath
```

At this point, you can alter any of these settings by using the **`set logpath`** commands. For further information, please refer to *set logpath from default* on page G-8 of *Appendix G - More on Commands*.

lp Method

The M205/M206 provides its own version of the **lp** print command. This is used in conjunction with **rsh/rcmd/remsh** within an interface script or directly from the command line on the host. By default, it provides parallel port printer status and can also be configured to report incremental byte counts as the job prints and the job's position in the M205/M206's queue.

Note: Using **lp** will provide printer error messages as well as job status.

If **lp** is used from the command line, any printer status will come right back to the screen. If used within an interface script, the messages will go to the log file located in the spooling directory.

Note: Since **lp** must be used with **rsh/rcmd/remsh** only, this feature is only offered with a print setup utilizing an interface script or with a **rsh/rcmd/remsh** command from the command line on the host.

Please see *lp options -d destname* on page G-22 and *rsh/rcmd/remsh* on page B-9 for further details.

FTP Daemon

The FTP Daemon provides an additional method to access the M205/M206. Using the FTP Daemon, users are able to submit print jobs, cancel print jobs, monitor the print queue, and upload/download M205/M206 configuration files. Users FTP to the M205/M206 as if it were any other computer on the network.

For the purposes of FTP, a pseudo file system has been defined on the M205/M206 to allow access to the unit's functions. Three types of users can access this file system: **root**, **guest**, and **anonymous**. **Root** and **guest** correspond to the entries in the M205/M206's user list; **anonymous** is a special type that does not require a password. For each directory or file within this file system, there are access restrictions according to the type of user logged in.

M205/M206 FTP File System

The M205/M206 FTP file system is where you execute all **ftp** commands on the unit. Please see the examples on the following pages for a complete description of the commands and how they are executed.

The following is the structure of the file system you will see when you **ftp** to the unit:

/queue

Contains one file with information pertaining to the print queue associated with the M205/M206's parallel port. This file allow you to view the current status of the queue.

/dest

Contains four subdirectories, one for each of the four print destination on the M205/M206. Please see *Print Path* on page 4 of the manual to better understand destinations and printing. These directories are where files are **put** in order to print.

/jobs

Contains files representing all the print jobs currently queued. The only command available for these files is **del**, which cancels the job.

/config

Contains three subdirectories: **current**, **stored**, and **default**. Each of the files in these subdirectory represents one data structure of the M205/M206. The files in the **current** directory reflect the current configuration, files in the **stored** directory reflect the stored configuration, and files in the **default** directory reflect the default configuration. These files are in binary format.

/exec

This directory is used as a command interpreter directory. Any file with M205/M206 configuration commands that is **put** to this directory will be interpreted as a series of **npsh** commands.

Printing A File Using FTP Daemon

The following example shows how to print a file using FTP:

1 Change to the local directory where the file to print resides.

2 Login to the M205/M206 using **ftp**.
```
ftp ipname
```

3 Login as **guest**, **root,** or **anonymous**.

Note: **Guest** and **root** users require the use of passwords as configured in the unit's user list. **Anonymous** is a special login that does not require a password.

4 Change to the **/dest** directory that you want to print to.
```
cd dest/destinationname
```

5 List the contents of this directory using the "**`dir`**" command and determine which destination/queue you'd like to send the print job through. Most likely you will select "**`d1prn`**" for the PRN port.

6 Change to this destination directory. For example:
```
cd d1prn
```

7 Change the mode to correspond to the type of file to be printed. Choose binary mode if the file to be printed contains both text and graphics and ASCII mode if the file is text only. The default mode is always ASCII.
```
bin
```

8 Copy the file you want to print to this directory.
```
put filename
```

The file is spooled and printed.

9 Logout of the FTP session.
```
quit
```

Removing a Print Job Using FTP

The following example shows how to remove a print job using FTP:

1 Login to the M205/M206 using **ftp**.
```
ftp ipname
```

2 Login as **guest**, **root** or **anonymous**.

3 Change to the **/jobs** directory
```
cd jobs
```

4 Display a list of current print jobs.
```
ls
```

Displays listing of all queued print jobs by their ID number.

5 Remove desired print job from the list.
```
del jobname
```

6 Logout of the FTP session.
```
quit
```

Monitoring a Print Queue Using FTP

The following example shows how to monitor a print queue using FTP:

1 Login to the M205/M206 using **ftp**.
```
ftp ipname
```

2 Login as **guest**, **root** or **anonymous**.

3 Change to the **/queue** directory
```
cd queue
```

4 Turn interactive mode off.
```
prompt
```

This enables you to copy a number of files without having to respond to prompts by the M205/M206.

5 Download the file in the print queue directory.
```
mget *
```

The file prn is downloaded to the users local directory.

6 Logout of the FTP session.
```
quit
```

7 View file with information pertaining to print queue status.
```
cat prn
```

Note: This command gives you the same information as a **lpstat** in **npsh**. **cat** is a UNIX command; with DOS, use the **type** command.

Configuring M205/M206 Parameters Using FTP

Users have two ways of configuring the M205/M206's parameters using FTPD. The first is by uploading binary files to the /**config** directory and the second is by uploading text configuration files to the /**exec** director**y**. We discuss each method and give appropriate examples below.

A. /config Directory

The /**config** directory is divided into three subdirectories; **current**, **stored**, and **default**. Each of the files in these sub-directories represent one data structure regarding the configuration of the unit. These files can be used to make a backup copy of the unit's configuration parameters or to copy configuration parameters from one unit to another.

Note: The configuration files are in binary form and their format may differ between firmware versions. Users may not be able to upload a configuration file that was downloaded from a previous version.

Copying a Configuration Using FTP

The following example shows how to copy a configuration file using FTP:

1 Login to the M205/M206 using **ftp**.

```
ftp ipname
```

2 Login as root.

You must be a **root** user in order to copy a configuration file.

3 Change to the **config/stored** directory.

```
cd config/stored
```

4 Set mode to binary.

```
bin
```

5 Turn off the interactive mode.

```
prompt
```

6 Download all the files in this directory.

```
mget *
```

Downloads a copy of all files in the **config/stored** directory to the user's local directory on their host.

7 Logout of the FTP session.

```
quit
```

Now you have a copy of the M205/M206's stored configuration parameters. These files can be saved for archival purposes, used to reconfigure the unit to a previous setting, or used to set a number of units to the same configuration.

Note: It is only necessary to save the files from the **stored directory**. Files from the default and current directory are not required in order to restore a unit's configuration.

Restoring a Configuration Using FTP

FTP can be used to restore a configuration saved from the unit or restore a configuration saved from another unit.

Note: If you are restoring a configuration saved from another unit, the configuration must be of the same version as the unit receiving the configuration.

1 Change to the local directory on the host where the saved configuration files reside.

2 Login to the M205/M206 using **ftp**.

```
ftp ipname
```

3 Login as **root**.

Note: You must be a **root** user in order to FTP files to the /**config** directory.

4 Change to the **config/stored** directory.

```
cd config/stored
```

5 Set mode to binary. Configuration files are always in binary form.

```
bin
```

6 Turn off the interactive mode.

```
prompt
```

7 Upload all the files from the user's local directory.

```
put *
```

Copies all files from the local directory to the **config/stored** directory.

8 Logout of the FTP session.

```
quit
```

Note: It will be necessary to **reset** the M205/M206 for the changes to take effect.

B. /exec directory

Using the /**exec** directory, users can upload a text file that includes a number of configuration commands. When this file is placed in the /**exec** directory, the commands contained in it are executed as if they were commands entered sequentially from a telnet session using **npsh**. This feature enables the user to create a single text configuration file that can be used to quickly and easily configure a number of M205/M206s.

Note: The command syntax for the text configuration file is exactly the same as if you were entering individual commands with **npsh** through a telnet session. See "Command Shell Overview" on page G-2for details regarding the commands and their syntax.

The configuration file can be seen as simply a user-defined script that includes a number of configuration commands to be executed. Comments describing the configuration can also be included in this file provided they follow the correct syntax.

The following is an example of a simple configuration file:

```
; These are comments for the example config file.
; Note that comments have to start at the beginning
of a
```

```
; line and be preceded by an ‘;’
;
version 5.6
; If this command is found and the current version
does not
; correspond to the command parameter, the file
execution
; will abort.
;
redirect prn
load default
set dest d1prn name newdest
set dest d2prn name another
set model m1 name newmod
set prn slowmode
save
```

Note: The above example includes a line for the **version number**. Because the commands and/or syntax **may** change from one firmware version to another, an old configuration file may be incompatible with the current version. By entering a version number, the transfer will be aborted and the user notified to check if the commands are compatible with the current firmware version if the version numbers do not match.

Note: The above example includes the **load default** command. This is optional. Including **load default** ensures that you always begin a

Note: It is not possible to generate a text configuration file from an existing binary configuration file in the **/config** directory.

Executing a Configuration File Using FTP

The following example shows how to execute a configuration file using FTP:

1 Change to the local directory where the text configuration file resides.

2 Login to the M205/M206 using **ftp**.

`ftp` ***`ipname`***

3 Login as **root**.

Note: You must be a root user in order to FTP files to the /**exec** directory.

4 Change to the /**exec** directory.

`cd exec`

5 Copy the text configuration file to the **exec directory**.

`put` ***`filename`***

The M205/M206's parameters are now set according to the commands in the configuration file.

Note: Depending on the specific commands in the configuration file, it may be necessary to **reset** the M205/M206 for the commands to take effect. Basically, the same rules apply whether you are using **npsh** to issue commands or a configuration file to issue commands. See "Command Shell Overview" on page G-2 for more information on the rules regarding configuration commands and options.

6 Logout of the FTP session.

```
quit
```

Note: If two FTP clients try to send configuration files to the exec directory at the same time, the second file will fail.

Managing with SNMP

SNMP (Simple Network Management Protocol) is a protocol for internetwork management services. This protocol provides a means for computers (or *agents*) to be managed remotely by *managers*. The level of management depends on the manager and agent and can go from providing information such as statistics to providing full management capabilities of the agent.

MIB (Management Information Base) files are a description of managed objects available in an agent. MIB files provide the data for the manager so they can remotely manage the agent. A MIB file is simply a formal description of the way an agent can be accessed using SNMP and what functions can be managed.

The M205/M206 is a fully manageable SNMP agent that supports MIB-II, custom MIB's and traps.

MIB II Support

The M205/M206 is MIB II compliant allowing SNMP managers to monitor protocol, network, and routing statistics.

Custom MIBs and Traps

The M205/M206 provides a custom MIB definition file which consists of 150 variables and three traps. This MIB file allows you to monitor and configure the Print Server directly. In fact, the MIB file represents all of the possible configuration options such as destination settings, network configurations, print queue status, loading of defaults, etc.

The M205/M206's custom MIB definition file is included on the host software disk in a file called **m205mib.txt**. This file can also be downloaded from the Microplex FTP site (**ftp.microplex.com: support/m205/ misc/m205mib.txt**) or can be accessed via the Microplex Web site (**http:/ /www.microplex.com/microplex/support.html/**).

Custom MIB Variables

The variables found within the custom MIB definition file describe every type of internal information that can be accessed on the M205/M206 by an SNMP manager. These variables can be divided into two groups: system variables and product variables.

System Variables

The first grouping of variables contains general information about the Print Server such as firmware version, serial number, etc. In addition to these, it includes a trap table which defines what SNMP managers will receive the traps generated by the M205/M206. The trap table can have up to ten entries, but only the first entry is saved to EEPROM.

Product Variables

The second grouping of variables contains information defining all of the remaining functionality of the Print Server. The product variables are divided into:

config group All configuration components such as models, destinations, logpaths, and users.

status group All dynamic monitoring components such as print queues, user logins, and RPRINTER configurations.

command group This includes the commands save, load, and reset.

Note: These variables can have read, write, or read-write permissions. Along with these permissions there are other elements that can limit the write access to these variables. Please see *SNMP Security* on page E-10 and *Users and Passwords* on page E-7 for more information.

Custom MIB Traps

A trap is an event generated by an agent to indicate a significant event to the manager. The M205/M206 continuously generates three traps:

coldstart A generic trap generated every time the M205/M206 is powered on or reset

authenticationFailure A generic trap generated whenever a disallowed access is attempted

lpqIOStatusChanged The only custom trap. This trap is generated whenever the I/O port's status changes.

Note: No trap is generated on a CTS change on the serial ports. Only DCD changes will trigger this.

Adding an SNMP User

To add a user named **snmp** with **root** privileges, please follow the steps below:

1 Login to the M205/M206 as a **root** user.

2 Add a user named **snmp**.
```
set user add snmp
```

3 Set the user type to **root**.
```
set user type snmp root
```

4 Set the password for the **snmp** user.
```
set user passwd snmp snmppassword
```

5 Save the changes.
```
save
```

The user **snmp** is now created and *snmppassword* is the only community string which will allow **write** access.

Compiling and Monitoring the Custom MIB

For read-only SNMP functionality, please follow the steps below:

1 Copy the M205/M206 MIB definition file from the host software disk in a file called **m205mib.txt**. This file can also be downloaded from the Microplex FTP site (**ftp.microplex.com: support/m205/misc/m205mib.txt**) or can be accessed via the Microplex Web site (**http://www.microplex.com/microplex/support.html/**).

2 Compile this MIB description file to work with your SNMP manager.

3 Using your SNMP manager, view the particular MIB variables that you wish to monitor.

Note: If you are using SunNet Manager, you will need to download a special MIB file (**ftp.microplex.com: support/m205/misc/m205mib.txt.SNM**) from the Microplex FTP site. This file can also be accessed via the Microplex Web site.

Note: If you are using Castle Rock Computing's *SNMPc* package, you will need to rename the MIB variable *UInteger32* to another name such as *U32*.

Writing to the Custom MIB

The following example explains how to use the custom MIB variables to set the M205/M206's parameters. For example, to turn on bbmode and onlcr on the M205/M206's prn port, please follow the steps below:

Note: This example assumes that the snmp password has been defined as *custommib*, that the M205/M206's ipname is *spike*, and that the SNMP manager is the Tricklets package.

1 Set up an **snmp** user with **root** privileges on the M205/M206. Please see *Adding an SNMP User* on page E-21 for details.

2 Issue the following configuration commands using the snmp user's password as the community string.

```
echo “m205IfPrnbbM[1.2]=2” | snmp-set spike custom-
mib

echo “m205IfOnlcr[1.2]=2” | snmp-set spike custom-
mib
```

Setting the M205/M206 to Send Traps to an SNMP Manager

The M205/M206 continuously generates traps but unless the trap table is filled in, no SNMP manager will receive this information. To set the M205/M206 to send traps to a particular SNMP manager, please follow the steps below:

Note: This example assumes that the snmp password has been defined as *custommib*, that the M205/M206's ipname is *spike*, and that the SNMP manager is the Tricklets package.

1 Set up a **snmp** user with **root** privileges on the M205/M206. Please see *Adding an SNMP User* on page E-21 for details.

2 Set the following M205/M206 trap variables using your SNMP manager. The actual syntax of the commands will depend on the particular SNMP manager you are using.

```
echo “trapCommunity[1]=\”building-A\”” | snmp-set
spike custmmib
```

where **building-A** is the string that you want the M205/M206 to send with the trap information. This community string has a 14 character maximum.

```
echo “trapDest[1]=192.75.11.11” | snmp-set spike
custommib
```

where **192.75.11.11** is the IP address of your SNMP manager.

Note: To disable the entry in the trap table, set the IP address to 0.0.0.0

The M205/M206 will now send trap information with the community string *building-A* to the SNMP manager with the IP address *192.75.11.11*. For more information on these trap variables, please see their description in the custom MIB definition file.

Note: The trap table can hold up to ten entries but only the first entry is stored in EEPROM. If you turn the unit off, you will lose the additional entries.

Troubleshooting

Test Pages

To test M205/M206 and printer communications without bringing the network into the picture, a test page feature has been added in **version 5.6.3 and higher**.

To get test pages, you will need to:

1. Unplug the M205/M206.
2. Look to the front of the device and move **Dipswitch 1** and **Dipswitch 2** to the **on** position (i.e. down).
3. Once the M205/M206 is attached to a printer that's ready to print, plug it in to get two automatic test pages.
4. When done, unplug the M205/M206 and move **Dipswitch 1** and **Dipswitch 2** to the **off** position (i.e. up) again for normal operations.

Note: It is very important that the dipswitches be returned to their default states once you are finished with the test pages.

NCSA

NCSA is a freeware package available on the Internet at **zaphod.ncsa.uiuc.edu** in the directory **/PC/Telnet/msdos/contributions.** The file is **tel23bin.zip**. It contains an **lpr** client for DOS that is compatible with the Print Server.

You can send jobs to the M205/M206 with the following command syntax:

```
lpr -Sipname -Pdestname
```

where ***ipname*** is the M205/M206 IP name or IP address and ***destname*** is the name of a M205/M206 destination. For example:

```
lpr -Sspike -Pd1prn
```

sends a print job to **d1prn** on the M205/M206 named **spike**.