Release Notes

MRV Communications (NBase-Xyplex) Access Server Software Versions 6.3 and 6.1.1*
450-0130A

Contents

IMPORTANT

The V6.3 parameter files are not backward compatible with parameter files of many previous versions of Multiprotocol Access Server software. NBase-Xyplex recommends that you save a renamed copy of your parameter file on the network or on a separate media, before you upgrade.

If you are using a flash card as a parameter server, NBase-Xyplex recommends a minimum of one backup parameter server. Before reformatting a flash card, back up any software images that are on the card to another load server.

* Version 6.1.1 was a product-specific release to support the Integrated Access Server (IAS) PIM in the Network 3000.

Before Upgrading – READ ME FIRST!

If you are upgrading from 6.0.4S1-S6 to V6.3 (on the standalone units only) follow these steps to avoid going back to default settings:

Issue the following command:

DEFINE SERVER USE DEFAULT PARAMETERS ENABLED

This command was developed to allow the standalone servers to have their parameters defaulted via a software command. (See the *Access Server Commands Reference Guide* for more details about this command.)

An issue arose in V6.0.4S1-S6 in which an upgrade to a higher revision would cause the server to reset to defaults, even when this setting was Disabled. Follow the instructions above so that the server's parameters will not be defaulted. The bit that controls this parameter was erroneously flipped in V604S1-S6, so if you enable this parameter when upgrading to V6.3 from those revisions, the server, upon the next reboot (to a higher revision), will NOT be defaulted.

Have your load host set up to offer V6.3

Wait for the parameters to write out successfully. When finished, use the INITIALIZE DELAY 0 command to reboot the server.

Software Versions

These *Release Notes* cover NBase-Xyplex Access Server software, Versions 6.1.1 and 6.3 hereinafter referred to as V6.1.1 and V6.3.

New Features in Version 6.3

The following new features and enhancements have been added to the Access Server software for Version 6.3.

Telnet Enhancements

LF_TO_CRLF parameter

The LF_TO_CRLF parameter is a Telnet newline filter for specific ports during a Telnet connection. When LF_TO_CRLF is enabled on a port, any linefeed received from the host is converted into a "Carriage return/Linefeed" (CR/LF) before it is sent out the serial port.

Telnet Session to Port 0

Telnet sessions to port 0 were not disconnecting after the password limit was reached.

This problem was corrected by the new port option, DISCONNECT ENABLED/DISABLED, which disconnects the session when the password limit is reached.

Syntax

```
    DEFINE/SET PORT 0 DISCONNECT [ENABLED/DISABLED]
```

Where	**Means**
ENABLED	The Telnet session to port 0 will be disconnected when the password limit is reached.
DISABLED	The Telnet session to port 0 will continue when the password limit is reached. This is the default setting.

SNMP Enhancement

Authenticate Always Option for SNMP Requests

Use this command to require community-string authentication for each Get, Set, or Getnext request from an SNMP Management Station. If Authenticate Always is enabled, the SNMP Management Station must provide a matching community string to the Access Server in each Get, Set, or Getnext request. If Authenticate Always is *disabled*, the SNMP Management Station is required to provide a matching community string in the first Get, Set, or Getnext request. In this case, a matching community string will only be required for subsequent Get, Set, or Getnext requests if another SNMP Management station interrupts with its own SNMP request.

Use the SHOW/LIST SERVER IP SNMP CHARACTERISTICS command to display the current setting of Authenticate Always.

Syntax

```
DEFINE/SET SERVER IP SNMP COMMUNITY AUTHENTICATE ALWAYS [ENABLED/DISABLED]
```

Where	Means
ENABLED	The SNMP Management Station must provide a matching community string to the Access Server in each Get, Set, or Getnext request. This is the default.
DISABLED	The SNMP Management Station is required to provide a matching community string in the first Get, Set, or Getnext request. In this case, a matching community string will only be required for subsequent Get, Set, or Getnext requests if another SNMP Management station interrupts with its own SNMP request.

PPP Enhancement

WINS Address Negotiation

Use this command to implement options 130 and 132 of the Point-to-Point Protocol.

This command specifies a WINS Primary Address, or WINS Secondary Address, that is sent by the Access Server to the local peer. The local peer can respond by requesting a different WINS address. In turn, the remote host (Access Server) will do the following:

- refuse the request from the local peer by NAKing the packet in which it was sent, and
- return the defined WINS address to the local peer.

Use the SHOW/LIST SERVER IP command to display the Primary WINS Address and Secondary WINS Address that are currently specified with this command.

Syntax

```
DEFINE/SET SERVER IP PRIMARY WINS ADDRESS internet-address
DEFINE/SET SERVER IP SECONDARY WINS ADDRESS internet-address
```

Where	Means
internet-address	The WINS Primary Address, or WINS Secondary Address, that is sent by the Access Server to the local peer.

Port Settings

Inactivity Timer

This feature enables users to control idle timeouts so that a port can be logged out from inactivity coming from the LAN side direction or inactivity coming from the attached serial device. Users can now specify the port timeout if the Telnet user activity to or from that serial port ceases for the defined timeout period.

Syntax

```
DEFINE/SET PORT port-number IDLE TIMEOUT RECEIVE MODE [ENABLED/DISABLED]
```

Where **Means**

ENABLED Data coming into the port from the attached serial device will not be viewed as activity and the Port Idle Timeout (if set as non-zero) will log out the session after the idle time has expired provided there is no data being transmitted out the port at that time. (The Port Idle Timeout *must* be set to a non-zero value for this setting to have any effect. The Port Idle Timeout is set with the DEFINE/SET PORT IDLE TIMEOUT command.)

DISABLED The session will not be logged out as a result of data not being transmitted from the port before the expiration of the Port Idle Timeout. This is the default.

Syntax

```
DEFINE/SET PORT port-number IDLE TIMEOUT TRANSMIT MODE [ENABLED/DISABLED]
```

Where **Means**

ENABLED Data coming from the network to the serial port will not be viewed as activity and the Port Idle Time (if set as non-zero) will log out the session after the idle time has expired provided there is no data being received into the port at that time.

DISABLED The session will not be logged out as a result of data not being received into the port before the expiration of the Port Idle Timeout. This is the default.

NOTE: If you enable both RECEIVE AND TRANSMIT modes, the session will be logged out (if the idle time is non-zero) regardless of data activity.

Setting the Port Signal Level

This command is used to set the Ready To Send (RTS) and Data Terminal Ready (DTR) signals for a specific port.

Syntax

```
SET PORT port-number RTS [ENABLED/DISABLED] DTR [ENABLED/DISABLED]
```

Where **Means**

ENABLED The specified signal is set high.

DISABLED The specified signal is set low.

NOTE: SET is the only command verb that can be used in this syntax. If you use the DEFINE command verb in this syntax (for example, DEFINE PORT # RTS ENABLED DTR ENABLED), error code 736 will be returned.

From the time the SET PORT *port-number* RTS DTR command is entered, it will be between 20 and 50 milliseconds before the port signals are modified. If the requested state of the signal is the current state of the signal, no action is taken.

Examples

You would use the following command to set the RTS and DTR signals on port 7 to high:

```
SET PORT 7 RTS ENABLED DTR ENABLED
```

You would use the following command to set the RTS signal on port 7 to high and the DTR signal on port 7 to low:

```
SET PORT 7 RTS ENABLED DTR DISABLED
```

Server Enhancement

Nested Menus

The following enhancements were added for Nested Menus:

- Nested Menus is supported on Port 0.
- There are two new ways to define file names for Nested Menus.

Use the following commands to define file names for Nested Menus.

Syntax

DEFINE SERVER NESTED MENU SYSNAME [ENABLED/**DISABLED**]

Where	Means
ENABLED	The unit's server name (with the suffix **.txt**) is used as the file name for Nested Menus. Note: Except for the **.txt** suffix, all letters in the filename are in uppercase.
DISABLED	Under this option, the file name for Nested Menus will be as specified in the DEFINE SERVER NESTED MENU NAME command or the DEFINE SERVER NESTED MENU ETHERNET command. If neither the DEFINE SERVER NESTED MENU NAME nor the DEFINE SERVER NESTED MENU ETHERNET command were executed, there will be no file name for Nested Menus. See the *Access Server Commands Reference Guide* for more information. This is the default.

Syntax

DEFINE SERVER NESTED MENU ETHERNET [ENABLED/**DISABLED**]

Where	**Means**
ENABLED	The unit's 12-digit Ethernet address (with the suffix **.txt**) is used as the file name for Nested Menus; for example, 080087AJ1539.txt. Note: All letters in the filename, except for the suffix **.txt**, are in uppercase.
DISABLED	Under this option, the file name for Nested Menus will be as specified in the DEFINE SERVER NESTED MENU NAME command or the DEFINE SERVER NESTED MENU SYSNAME command. If neither the DEFINE SERVER NESTED MENU NAME nor the DEFINE SERVER NESTED MENU SYSNAME command were executed, there will be no file name for Nested Menus. See the *Access Server Commands Reference Guide* for more information. This is the default.

NOTE: Only one of these options can be enabled at a time. You must reboot the unit before these changes to the Menu file can take effect.

Virtual Management Ports

Eight virtual management ports have been added in this release. The new virtual management ports mirror port 0 in the way they operate and are configured.

The new virtual management ports start at the maximum physical port, plus 2. The reason for skipping a port (i.e., not starting at maximum physical port, plus 1) is that the server uses the next non-physical port for SNMP.

Example

On a 1620, the new virtual management ports would be ports 22 – 29 with remote ports of 4200 – 4900. The virtual management ports can be configured the same way as port 0. (This means that PPP can not be enabled on the virtual ports.)

Autodiscovery of the Gateway Address

If the gateway address is not defined in the parameter file, the server will attempt to get the gateway address from the bootp server at system boot-up.

Autodiscovery of the Subnet Mask

If the subnet mask is not defined in the parameter file *and* IP SUBNET MASK AUTOCONFIGURE is disabled, the server will attempt to get the subnet mask from the bootp server at system boot-up.

NOTE: If IP SUBNET MASK AUTOCONFIGURE is *enabled*, the server calculates the subnet mask automatically. For more information, see the documentation of DEFINE/SET SERVER IP SUBNET MASK AUTOCONFIGURE in the *Access Server Software Commands Reference Guide*.

Autodiscovery of the IP Address

If the IP address is not defined in the parameter file, the server will attempt to get the IP address from the bootp server at system boot-up.

TFTP put and get Commands

Access Server V6.3 provides a Trivial File Transfer Protocol (TFTP) server capability, as defined by IETF RFC 1350. This capability enables you to use get and put commands to move files from one location to another, using utilities such as Sun™ UNIX TFTP. The get command obtains a file from a server, such as a Xyplex Access Server, and stores it on a client, such as a UNIX host. The put command sends a file from the client to a destination server; for example, a Xyplex Access Server.

You can use the get and put commands to obtain a new version of the Access Server load image, and send it to an Access Server unit on the network. You can use these commands to replace a file on either a diskette or memory card. This section describes TFTP client/server operations, using Sun UNIX TFTP in the examples.

Figure 1 shows a network with two Xyplex Networks units that act as TFTP servers and UNIX host that acts as a TFTP client.

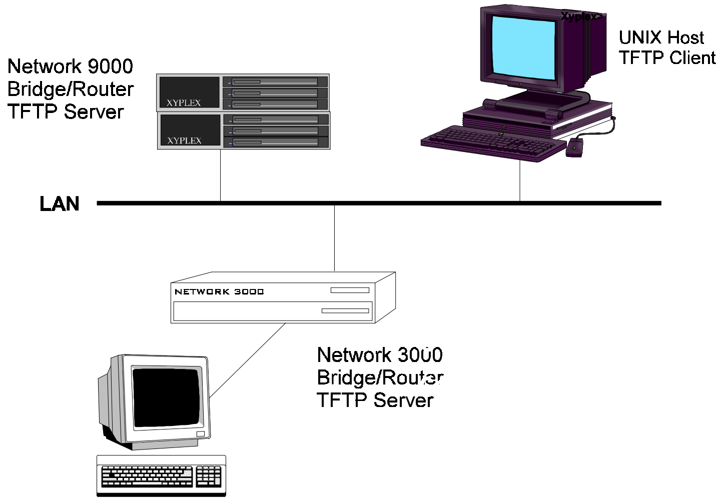

Figure 1 - TFTP Clients and Servers

Follow these steps to start TFTP on the client and use the get or put commands to move a file between the server and a Xyplex Access Server:

- Move (cd) to the directory on the server where the file resides, or to the directory where you will place the file:

```
{jma}/usr/jma: cd temp
```

- Start up TFTP on the client:

```
{jma}/usr/jma/temp: tftp
```

When you start TFTP, you can obtain help with the ? command. You can exit from TFTP with the quit command.

- Enable binary mode, also known as "octet" mode, if necessary.

The TFTP server supports only "octet" mode, not ASCII mode. ASCII mode is the default mode for SUN UNIX, so you must enable binary mode. This is not a limitation, because only binary files reside on the Xyplex Access Server. (You can transfer an ASCII file as a binary file, if this is necessary.)

To set binary mode in Sun UNIX TFTP, use the binary command:

```
tftp> binary
```

At this point you might want to enable verbose mode in TFTP. While it is not necessary to complete a get or put procedure, verbose mode causes TFTP to display status messages on the screen that can be helpful. To enable verbose mode, enter the verbose command:

```
tftp> verbose

Verbose mode on.
```

- Establish a connection with the TFTP server. This can be the unit where you want to send a file with the put command, or the unit where you want to obtain a file with the get command. If you skip this step, you will need to include an IP address along with a complete path name. This example uses 172.19.227.32 as the Internet address of the target unit.

  ```
  tftp> connect 172.19.227.32
  ```

- Enter the get or put command to move the file you specify. Include the system password of the remote system as a suffix to the filename. This enforces security on the remote system. The format for the suffix is _system-password. The syntax for these commands follows:

  ```
  get  /remotepathname/filename_system-password  localfilename

  put  localfilename  /remotepathname/filename_system-password
  ```

Examples

This put command sends a load image from the TFTP client to the MEMORY CARD of a TFTP server, which is an Access Server unit. The system password in this example is "syspass."

```
tftp> put xpcsrv20.sys /MC/SYSTEM/AREA2/xpcsrv20.sys_syspass
```

This get command obtains a load image from an Access Server on the network and stores it on the TFTP client. The system password in this example is "syspass."

```
tftp> get /MC/SYSTEM/xpcsrv20.sys_syspass xpcsrv20.sys
```

About Access Server Devices and Directories

You must specify all directories and filenames using capital letters. The filename is a maximum of 8 characters and the extension is a maximum of 3 characters.

The directories on the memory card are as follows:

```
/MC/SYSTEM
/MC/PARAM
```

Use this directory for writing a file to the `/SYSTEM` directory, Area *x*:

```
/MC/SYSTEM/AREAx/
```

Use this directory for reading a file from the `/SYSTEM` directory:

```
/MC/SYSTEM/
```

Use this directory or reading or writing a file to the /PARAM directory:

```
/MC/PARAM/
```

All file system parameters MUST be in uppercase letters. Note that when putting files into the `/`*`device`*`/SYSTEM` directory, the old file is erased before the transfer starts. Consequently, the old file is erased if a transfer is aborted.

A TFTP put command to the `/`*`device`*`/SYSTEM` directory has the same effect as the GET CARD LOAD FILE command. TFTP does not do the initial file checking that the GET CARD LOAD FILE does. Therefore, it is possible to put a non-executable file into the `/`*`device`*`/SYSTEM` directory.

Troubleshooting

If a TFTP timeout error occurs during the file transfer, you might need to increase the TFTP timeout values to allow more time. The rexmt command specifies the per-packet retransmission timeout in seconds. The timeout command specifies the total retransmission timeout, in seconds.

The following example shows the sequence of commands necessary to use put command, along with the rexmt and timeout commands.

Example

```
tftp> connect 172.17.0.1
tftp> verbose
tftp> binary
tftp> timeout 300
tftp> rexmt 20
tftp> put xpcsrv20.sys /MC/SYSTEM/AREAx/xpcsrv20.sys_syspass
tftp> quit
```

Support for the Integrated Access Server Module

Access Server V6.3 supports the NBase-Xyplex Integrated Access Server (IAS) Module. The IAS Module provides a low-cost, reliable means for users at branch offices or small central sites to connect local users to the LAN and to modems and printers.

The following section describes features of the IAS Module that were not documented in *Getting Started with Network 3000™ Integrated Access Server Module.*

The “Problems and Restrictions” section on page 13 of these Release Notes describes known problems and restrictions of the IAS Module.

For more information about the IAS Module, refer to *Getting Started with Network 3000™ Integrated Access Server Module* (451-0257A).

Undocumented Features

The commands and features described in this section apply *only* to the IAS Module.

Updating Flash Image

You can use any Network 3000 (including the unit where the IAS Module is currently inserted) as an XMOP load server for the IAS Module.

NOTE: The IAS Module does not boot and load from the Network 3000’s flash card or floppy. The IAS Module boots directly from its internal flash memory.

Use the following command to update the image on the flash part of the IAS Module:

```
  Xyplex> UPDATE IMAGE FLASH <”filename”> ADDRESS <ethernet-address>
                                        IP ADDRESS <ip-address>
```

Field	Description
“filename”	The image’s filename. Enclose the name in quotes (i.e., “xpcsrv20.sys”).
ethernet-address	Specify the Ethernet Address where the source file is stored. Using a NBase-Xyplex Ethernet Address causes XMOP to be used. Using any other type of Ethernet Address causes MOP to be used.
ip-address	Specify the IP Address where the source file is stored. Using an IP Address causes TFTP to be used to retrieve the file.

Examples

```
UPDATE IMAGE FLASH “xpcsrv20.sys” IP ADDRESS 143.182.163.110

UPDATE IMAGE FLASH “xpcsrv20.sys” ADDRESS 08-00-87-0E-3E-E1
```

Displaying Update Status

Use the following command to track the progress of the image update from the source to the flash part:

```
        Xyplex> SHOW/MONITOR IMAGE FLASH STATUS
```

```
Xyplex>> SHOW IMAGE FLASH STATUS

N3AS08  V.6.1.1  Rom 410000  HW 05.00.00 Lat Protocol V5.2 Uptime: 0 00:4:14
Address:   08-00-87-0E-3E-E1    Name:  X0E3EE1          Number:   0
                                                    02 Feb 2000   20:11:10

Update Image Flash File Host: 143.182.163.110

Update Image Flash File Name: xpcsrv20.sys

Update Image Flash Current State:    Idle
Update Image Flash Previous Status:  Image Flash Updated Successfully
```

Update Image Flash…	Description
File Host	The IP address/Ethernet address where the source image is located.
File Name	The name of the file being copied to the flash part from the source.
Current State	Indicates the current state of the operation. DO NOT REBOOT OR POWER OFF THE UNIT DURING AN UPDATE.
Previous Status	Indicates the status of the last flash update.

Configuration Menu Commands

There are differences between the Access Server and the IAS Module Internal Configuration Menus when you want to modify the initialization record located on the IAS Module’s flash memory. The differences are as follows.

```
   Enable ALL methods for image loading? [Y,N] Y
```

When you enter a “Y” at this prompt on the IAS Module you are enabling the protocols that can be used to update the image flash memory. This selection is only utilized when you also enter a “Y” at the following prompt:

```
   Do you wish to update software in Flash?[N,Y] Y
```

If you select Y, the protocols you select for image loading will be used to get the new image. If you do not select “Enable ALL methods for image loading” you must select a load method, as follows:

```
   Toggle (DTFTP,XMOP,MOP,BOOTP, RARP) load methods [X,M,B,R]:
```

When you select a load method you are enabling the load method that can be used to update the image flash memory.

After completing your changes, select X to return to the Terminal Server Configuration Menu.

Select S (Exit saving changes) from this menu. The following prompt displays:

```
Save changes and Exit(Y,N)?[Y]
Changes Saved.
```

Select Y to Exit the Configuration Menu. The following prompt displays.

```
Do you wish to update software in Flash? [N,Y] Y
```

If you select Y, the protocols you selected for image loading will be used to get the new image.

The rest of the selections function the same as the Access Server Configuration Menu.

Displaying Software Version

Use the SHOW/LIST/MONITOR UNIT command to display the current revision of the image in the flash part. The current Revision number displays in the “Flash Image Revision” field. The Flash Image Revision field displays as “Unavailable” if you issue this command during an update image operation or during a parameter save operation.

```
Xyplex>> SHOW UNIT

Hardware Type:               123
Hardware Revision:           05.00.00
Rom Revision:                410000
Software Type:               Terminal Server Level 4
Software Revision:           V6.1.1
Flash Image Revision:        Unavailable
Protocol Type:               LAT, TELNET, RLOGIN, SNMP
Daemon(s):


Enabled Feature(s):          HELP, ULI
```

Hardware Type

The Hardware ID for the Integrated Access Server Module is 123.

Problems and Restrictions

The problems and restrictions described in this section apply *only* to the IAS Module.

Unit Resetting/Power Loss Advisory

Resetting/powering off the unit or using the user interface CRASH command during an image update or when saving parameters produces the following unfavorable results:

- If the image update does not complete there will be no valid image in the flash and the unit will not boot. To restore the image to the flash you will have to be local to reset the unit, access the firmware configuration menu and update the flash with an image from a load server.
- If parameter saving to the unit’s flash memory does not complete before a reboot the results are unpredictable.

- The Override option of the INITIALIZE DELAY command has been disabled on the IAS Module. This was done to prevent the IAS Module from rebooting during reloading/updating of the image or while saving parameters.

Communicating with other Devices

The IAS Module can only communicate with other network devices if the Network 3000's 10Base-T or AUI port is connected to a network.

Parameter and Software Loading

The IAS Module is identical to other Access Servers except for the following software and parameter loading differences:

Loading Operational Software – The operational software can only be loaded from internal flash memory on the IAS Module. If the software needs to be updated, use either the firmware configuration menu or the UPDATE IMAGE FLASH command which is described in the New Features section of this document.

Loading Parameters – Each time the unit boots, the parameters are read by the runtime software from internal flash memory. The parameter file is written directly into that internal flash memory by the software. Network-based parameter loading is not supported; however, network-based parameter saving is supported to allow backing up parameter files.

FLASH CARD Commands

The IAS Module does not have a Flash Card and does not act as a load or parameter server, therefore all CARD commands are inoperable with this unit.

MANAGER and LOADDUMP Commands

The IAS Module does not act as a load server and cannot be used to load software and parameters to other units, therefore all MANAGER and LOADDUMP commands are inoperable with this unit.

Fixed Problems in Version 6.3

Crash with a 150002 Code

When a user entered any of the following commands, the Access Server would crash with a 150002 code:

```
FORMAT CARD

GET CARD LOAD FILE
```

Radius Reply Message

The Radius Reply message was not being sent back to users when they logged in to a remote access port that had Radius enabled.

The Radius Reply message is now sent back to users when they log in to any port that has Radius enabled.

Radius Username

On remote access ports set for “telnet transmit immediate” and “telnet echo mode character”, the Radius username was not echoed until the user entered a carriage return.

The Radius username now echoes as it is typed; the user no longer needs to enter a carriage return in order to echo the Radius username.

Remote Port Logins

Users logging into a remote access port would not get disconnected when they entered the wrong username or password.

Users are now disconnected when they enter the wrong username or password during a login attempt.

SHOW PORT TELNET CHAR Screen

The SHOW PORT TELNET CHAR screen now displays accurate information for virtual ports.

SnmpGet Command

A user could issue a snmpGet command to get the “set community string”. Once the user had that string, snmpSets could be done to the Access Server. This was considered a security breach.

An snmpGet of the “set community string” now returns a NULL string.

TN3270 Session

TN3270 sessions were being terminated with the following error message:

```
A MF order while not positioned at an FA
```

The error occurred under the following scenario:

- The customer’s application sent a Start Field Extended (SFE) to the Access Server. The SFE did not contain the 3270 field attribute pair (CO xx).
- A Modified Field (MF) was then sent by the customer’s application.

Since the Access Server did not know which attribute was being modified, the session was disconnected.

The code was modified to use the default value for a 3270 field attribute when the Access Server gets an SFE without the 3270 field attribute pair (CO xx).

TN3270 Session Underlining

Underlining was not appearing where it should have appeared on terminal screens. This occurred when a space or a null character was used as a repeated character.