NBase-Xyplex Release Notes

Access Server Software Versions 6.1 and 6.0.4

450-0001V

January 1999

Contents

Important

The V6.1 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.

Before Upgrading - READ ME FIRST!

If you are upgrading from 6.0.4S1-S6 to V6.1 (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 V6.1 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 V6.1

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

Software Overview

These *Release Notes* cover NBase-Xyplex Access Server software, Versions 6.1 and 6.0.4 hereinafter referred to as V6.1 and V6.0.4 in this document.

Access Server Software Version Supported

Image	V 6.1	V6.0.4	V 6.0.3	V6.0.2	V6.0.1	V 6.0
xpcsrv20.sys	X	X	X	X	X	X
xpc00s.sys	—	—	—	X	X	X

Notes:

MAXservers 1604 and 1608B require version V6.0.3 or higher.

The features contained in V6.0.1 through V6.1 require a minimum of 4 MB of memory for the access server.

Contact your local NBase-Xyplex Sales representative or distributor for information about a memory upgrade.

Documentation Update

The following table lists the available Access Server documentation.

PLEASE NOTE THAT VERSION 6.1 includes an updated *Access Server Commands Reference Guide* (which has been revised to include all commands through V6.1), as well as updates to several other manuals. See Table 1 for details.

Table 1 - Access Server Documentation

Document Title	Document Number	Updated for V6.1	Included in CD Software Kit	Available in Hard Copy
Software Kit Information	450-0008	X	X	
Release Notes	450-0001	X	X	X
Software Installation Guides				
For UNIX Hosts	420-0390		X	X
For VMS Hosts	420-0391		X	X
For Xyplex Loader Kits	420-0392		X	X
Access Server Reference Documentation				
Access Server Commands Reference Guide	420-0559	X	X	X
Advanced Configuration Guide	420-0558	X	X	X
Basic Configuration Guide	451-0084	X	X	X
Printer Configuration Guide	451-0112	X	X	X
Error Messages Reference Guide	451-0049		X	X
Getting Started with MAXserver Access Servers Models 1604/1608/1620/1640	451-0038	X	X*	X
Using the ULI Interface	451-0062		X	X
Using the APGEN Utility	451-0065		X	
Network 9000 Reference Documentation				
Getting Started with the Network 9000 Access Server 720	451-0021		X*	X
Managing Network 9000 Modules and Power Supplies	451-0020		X	

*Also ships with unit.

New Features in Version 6.1

The following new features and enhancements have been added to the Access Server software for Version 6.1

Server Enhancements

Autodiscovery

Use this command to allow the server to acquire its working IP address in a non-standard method. Use the SHOW/LIST SERVER IP CHARACTERISTICS command to display the new parameter. If you enable auto discovery, the server will be able to obtain its working IP address even if loading is done using non-standard methods. See the *Access Server Commands Reference Guide* for details.

> ***Note:*** *This command is not available on Network 9000/720 Access Servers. Use the DEFINE CHASSIS SLOT [FACTORY] DEFAULTS command.*

Syntax

```
DEFINE SERVER IP ADDRESS AUTODISCOVERY [ENABLED/DISABLED]
```

SHOW PORT and SHOW SERVER Date and timestamp

The date and timestamp field has been added to the SHOW PORT STATUS screen and all of the SHOW SERVER screens.

Increased packet buffer count

The maximum number of incoming and outgoing packets. For load images that require at least 2MB of memory to run, valid values are 80 to 4088. For load images that can be used with less memory, valid values are 80 to 160. The default value is 80. This command is memory managed. If the memory needed exceeds the value that has been defined, the proper error messages will be displayed.

Prior to this release the maximum packet count was 1088. All original memory requirements and restraints are still in place.

```
DEFINE SERVER PACKET COUNT [packet-buffers]
```

Nested Menu Reload Attempts

The timeout for nested menus mode has been increased to a total of 5 polls in 7 minutes for each entry in the script server list before a TFTP timeout occurs and no Nested Menus are loaded into the Access Server.

RADIUS - RLOGIN Enhancement

V6.1 supports the Radius “Login-Service=Rlogin” attribute.

The following example shows a typical entry in the User's file (Livingston Radius):

smith Password = “password”

Service-Type= Login-user,

Login-IP-Host=1.2.3.4,

Login-Service=Rlogin

Radius will then authenticate the user and open an Rlogin session with the specified host. At this point, the connection is considered a dedicated session with the host.

NOTE: The Radius password is NOT THE SAME password used on the host.

All of the normal RLOGIN session rules still apply, such as:

- The normal timeouts are still in effect.
- If you are “trusted” on the host, you can connect to the host without entering a login or password.
- If you are not “trusted” then you will be denied access to the host and will be prompted for a password.
- If you enter an invalid (or no password) at the password prompt, the login prompt will then appear. However, if you have another account on that host, you can enter that account and access will be allowed.

NOTE: If you enter through another account, all accounting information will still be displayed as the user “smith.”

PPP Enhancement

V6.1 supports NOT sending the ACCM (character map) if an LCP Config NAK not to send is received. This enhancement works the same as an LCP Reject for the same situation.

Telnet Enhancements

KICKSTART Feature

The new Kickstart option lets you define a string that can be used to provide a connection to a dedicated service when the input from the serial port matches the defined string.

`DEFINE PORT TELNET DEDICATED[SERVICE][`*`ip-address/domain-name`*`]KICKSTART <`*`string`*`>`

Example

```
DEFINE PORT 3 TELNET DEDICATED SERVICE 140.179.244.100 KICKSTART “ALERT”
```

See the *Access Server Commands Reference Guide* for details.

TN3270 Numeric Override Keymap

Use this command to specify a key to allow alphanumeric data to be entered in a numeric-only field. This command follows all of the standard rules for defining a TN3270 device key.

When the NUM_OVERRIDE is defined, users can toggle this key OFF and ON. It is OFF at the start of any TN3270 session. When the key is ON, the user can enter alpha characters into a numeric-only field. If the status line is activated, the following message displays on the status line: X NUM_OVERRIDE.

Use the SHOW SERVER TN3270 DEVICE command to display the current keymap settings.

`DEFINE SERVER TN3270 DEVICE [`*`device-name`*`] KEYMAP NUM_OVERRIDE [`*`key-sequence`*`] "`*`description`*`"`

See the *Access Server Commands Reference Guide* for details.

Telnet Break Length

Privileged users can now set the length of a break sent out the serial port in response to a Telnet Break (this feature is not supported for LAT). The valid settings are 250ms, 500ms, or 750 ms. See the *Access Server Commands Reference Guide* for details.

Telnet Interrupts as Break

Privileged users can now define a port to interpret a Telnet Interrupt from the LAN as a Telnet Break and send the break out the serial port.

```
DEFINE PORT [port-list] TELNET INTERRUPTS AS BREAK [ENABLED/DISABLED]
```

If this feature is Enabled, it displays on the SHOW/LIST PORT TELNET CHARACTERISITCS screen. See the *Access Server Commands Reference Guide* for details.

Telnet 8 bits, Even Parity Port Setting

You can now define a port to allow 8 bit, even parity to be passed on a port from a serial device during a Telnet session. The command is as follows:

DEFINE/SET PORT TELNET PASS8D ENABLED/DISABLED

See the *Access Server Commands Reference Guide* for details.

Telnet USERDATA Delay

The supported userdata delay values have been increased from 0 – 2.55 seconds to 0 – 30 seconds.

COMPORT Control Feature

Use this command to enable the use of RFC2217(Telnet Com Port Control Options) as described in this section. Use the SHOW/LIST PORT TELNET COMPORTCONTROL CHARACTERISTICS command to display the current settings.

Note: *There is no SET command for this feature. You must log out from the port before the changes can take effect.*

Syntax

```
DEFINE PORT port-list TELNET COMPORTCONTROL [CLIENT] [DISABLED]
                                            [SERVER] [ENABLED]
DEFINE PORT port-list TELNET COMPORTCONTROL[CLIENT TOGGLES DTR][DISABLED]
                                          [SERVER RAISES DTR] [ENABLED]
```

The Comport Control feature has been implemented according to RFC2217. Here is a brief excerpt from RFC2217:

The Telnet protocol defines an interactive, character-oriented communications session. It was originally designed to establish a session between a client and a remote login service running on a host. Many new business functions require a person to connect to remote services to retrieve or deposit information. By in large, these remote services are accessed via an asynchronous dial-up connection. This new class of functions include:

- Dial-up connections to the Internet
- Connecting to bulletin boards
- Connecting to internal and external databases
- Sending and receiving faxes.

The general nature of this new class of function requires an interactive, character-oriented communications session via an asynchronous modem. This is typically known as *outbound modem dialing.*

To help defer the cost of installing and maintaining additional phone lines which may be used very little per person, many equipment manufacturers have added the ability to establish a Telnet session directly to the outbound ports on many of the most popular access servers and routers, here after referred to as access servers.

However, the current Telnet protocol definitions are not sufficient to fully support this new use. There are three new areas of functionality which need to be added to the Telnet protocol to successfully support the needs of outbound modem dialing. These are:

- The ability for the client to send com port configuration information to the access server which is connected to the outbound modem. This is needed to ensure the data being transmitted and received by the modem is formatted correctly at the byte level.
- The ability for the access server to inform the client of any modem line or signal changes such as RLSD changes (carrier detect). This information is vital, since many client software packages use this information to determine if a session with the remote service has been established.

- The ability to manage flow control between the client and the access server which does not interfere with the flow control mechanisms used by the session between the client and the remote service.

How NBase-Xyplex Implemented this New Functionality

We have implemented the three new areas of functionality, as follows:

- A "limited" client (explained under Client Side Particulars).
- A "server side"(explained under Server Side Particulars and Restrictions. See below and the RFC for more detail).
- Flow control has been implemented from the client (not ours) to server. For example, the server side (NBase-Xyplex Access Server) will respond to flow control "suspends" and "resumes" from the client.

Server Side Particulars and Restrictions

We will accept all of the client's request and respond to them(see the RFC for more) except:

- If the client sends us a "SIGNATURE" sub packet with text included, we(as the server side) will not respond to or act on it unless there is no text, then we will follow the spec and send back what our signature is. At this time, it is hardcoded as an uppercase "X".
- If the server side sees a "SET-CONTROL" sub packet from the client for inbound flow control requests, we will just respond with the flow control that we are doing on the port at that time. We have no plans to separate our flow control into inbound and outbound.
- There is no support in this release for the "PURGE-DATA" sub packet from the client. We will ignore any requests in this manner from the client.

Client Side Particulars:

We have implemented a "limited" client side to our software. The following quote from RFC2217 is included for clarity:

"As initially proposed, com port configuration commands are only sent from the client to the access server. There is no current vision that the access server would initiate the use of a com port configuration command, only the notify commands."

Basically, our client will only do the following:

1. Send the Com Port Control option protocol negotiation.

2. Send a hardcoded "SET-MODEMSTATE-MASK" sub packet to the server side with a value of 255. The value of 255 means that we will allow the server side to send any modem state changes that occur on the server side's port via the sub packet route to the client. This is done only once per telnet connection.

3. Send a hardcoded "SET-LINESTATE-MASK" sub packet to the server side with a value of 0. 0 means that we will NOT allow the server side to send any line state changes that occur on the server side's port via the sub packet route to the client. This is done only once per telnet connection.

4. If the server side sends us a NOTIFY-MODEMSTATE sub packet informing us that DCD has come high(or low), we as the client can raise(or lower DTR) accordingly on our port when this feature is enabled.

5. Upon a telnet connection, we as the client can send a "SET-CONTROL" sub packet requesting that the server side raise its DTR signal on the port when this feature is enabled.

Port Settings

HDLC Discards Counter

An HDLC discards counter field has been added to the SHOW PORT PPP COUNTERS screen. This counter tracks the following information

HDLC Discards Received - The number of broadcast packets received that were discarded for reasons other than framing errors, incorrect checksums or insufficient resources.

HDLC Discards Transmitted - The number of broadcast packets that were attempted to be transmitted out the port, but could not because the PPP QUEUE LIMIT has been reached.

This counter can only be incremented when PPP IP BROADCAST is enabled on the port in question.

PPP IPCP Interpreted Logging

The PPP IPCP log message is now more descriptive.

Banner Display before Authentication

Privileged users can enable this command on specified port(s) to display the Welcome banner before the user is prompted for the Radius, Kerberos or SecurID username and password. If enabled, "Welcome Before Authentication" text displays under Enabled Characteristics on the SHOW PORT CHARACTERISTICS display.

Notes: This is a DEFINE only command for this feature. The port(s) must be logged out for this command to take effect. This feature cannot be enabled on Port 0. If you are using APD, you must enable the DEFINE PORT APD AUTHENTICATION INTERACTIVE command to have the Welcome banner print out first.

```
DEFINE PORT WELCOME BEFORE AUTHENTICATION [ENABLED/DISABLED]
```

Controlled Port Logout command

Before this release, only ports defined as LOCAL access types could use this command. This release allows REMOTE and DYNAMIC ports to use this feature. See the DEFINE/SET PORT CONTROLLED PORT command in the *Access Server Commands Reference Guide* for details.

IPX and XREMOTE Protocol Support Changes

You no longer need a password, nor are you prompted for one, when you enable or disable the IPX or XREMOTE protocols.

To enable or disable IPX, enter:

```
DEFINE SERVER PROTOCOL IPX [ENABLED/DISABLED]
```

To enable or disable XREMOTE, enter:

```
DEFINE SERVER PROTOCOL XREMOTE [ENABLE/DISABLE]
```

Bypassing Capability for LPD Ports Provided

You can now bypass LPD ports that are in the XOFF state. With "bypass" enabled, if the LPD port is Xoff'd, then all subsequent print jobs are sent to the next LPD port. The LPD port must be configured with the same queue name.

You should only bypass LPD ports that have other ports configured with the same queue name and are operational.

Use the following command to bypass on a specific queue:

```
DEFINE LPD QUEUE [queue-name] BYPASS ENABLE
```

Disabling of Password Prompt for Port 0 Provided

Previous versions of Access Server require you to enter a password to access port 0.

V6.1 software allows you to disable the password prompt for port 0. To disable the password prompt, use the `following command:`

```
DEFINE PORT 0 PASSWORD [ENABLE/DISABLE]
```

Note: *Disabling the password leaves port 0 with no default security.*

Userdata Support for Telnet Dedicated Service

V6.0.4 enhances the Telnet Dedicated Service by adding support for userdata string functions. Userdata string functions provide you with a way to add a userdata string to a Telnet dedicated service. The userdata string is passed to the network partner upon connection. The new commands are:

Adding A Userdata String - lets you define a userdata string for a dedicated port:

```
DEFINE PORT [port-number] TELNET DEDICATED SERVICE [ip-address/domain name]
USERDATA "userdata_string"
```

Deleting a Userdata String - lets you keep the service and delete the userdata string, or you can delete both the service and the string:

```
DEFINE PORT [port-number] TELNET DEDICATED SERVICE [ip-address/domain name]
USERDATA ""
```

```
DEFINE PORT [port-number] DEDICATED NONE
```

See the *Access Server Commands Reference Guide* for detailed descriptions of the userdata commands.

Controlled Port Logout Enhancement

In the previous version of Access Server software the `CONTROLLED PORT LOGOUT` command worked only with ports that had ACCESS set to `local.` You can now apply this function to a port whose access is set to `REMOTE or DYNAMIC`.

Note that all rules and limitations that apply to `CONTROLLED PORT LOGOUT` on a local port also apply when the port is set to remote or `dynamic`.

Series 2 Flash Cards

Series 2 Flash Cards are supported in V6.1

Fixed Problems in 6.1

UDP

UDP would not send an SNMP reply back to a network management station that was doing an SNMP set of a Primary Gateway Address.

DEFINE PORT TO DEFAULTS Command

When this command was used to define a port back to defaults, if PPP was not enabled on the Access Server, the server would crash.

Telnet Dedicated Service and Userdata

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

```
DEFINE SERVER IP NAME NONE
XDM HOST NONE
RLOGIN NONE
DEFINE PORT RLOGIN DEDICATED SERVICE NONE
DEFINE PORT RLOGIN PREFERRED SERVICE NONE
DEFINE PORT TELNET PREFERRED SERVICE NONE
USER DATA STRING
```

LPD Queue Bypass Feature

Bypass is now disabled by default

You can now display each defined LPD queue on both the LIST and SHOW LPD QUEUE displays. Each defined queue is separated by a blank line for clarity.

LPD Signal check

If signal check was enabled on a port and no DSR observed and the queue limit was set to one less than the number of print jobs, the user would clean the LPD jobs from the host and then attempt to clean the queue. This would cause a crash.

Reliable Accounting and Logging

Using reliable accounting and logging PPP interpreted messages could cause the Access Server to crash with a code of 004A0002.

The PPP IPCP message was longer than the defined length. In the future if the message exceeds the field length it will be truncated rather than cause a crash.

PAP and CHAP Authentication

When PPP, PAP Radius and the Framed-Filter-ID attribute was used the only valid filename for scripts was “login.” You can now use any name as the script file name.

Problem: When using PPP/PAP-Radius, Radius attribute "Framed-Filter-Id"(TFTP scripting function), dynamic access, and Noloss. After dialing in and establishing a PPP connection, the connection would time out after 2 minutes if there was a privileged command in the script, or if there was no script.

Solution: The code has been changed so that the above will no longer occur.

Problem: Same configuration as above. If the script failed for any reason, NBase-Xyplex would still allow the PPP connection to be formed. This should not have occurred.

Solution: The code has been changed so that if the script fails for any reason(including syntax errors and/or privileged commands without the #privileged entry), then the link will be torn down and the port logged out.

IP Filter

The DEFINE PORT IP FILTER command could be issued via a NON-privileged user. This has been corrected.

Problem Writing to Series II Flashcards with 1608B Access Servers

Problem: 1608B Access Severs were able to read but unable to write data to certain Series II Flashcards.

Solution: This release has corrected the problem. The 1608B Access Servers can now write to a Series II Flashcard.

Problem Calculating Leap Year (Year 2000)

Problem: Previous software versions did not calculate the leap year 2000 time correctly when receiving it from a time server.

Solution: This release has corrected the problem, and the date correctly advances from February 28 to February 29 in the year 2000.

DEFINE PORT *PORT-NUMBER* TO DEFAULTS Command

Problem: Entering the `define port` *`port-number`* `to defaults` command did not reset the `Noloss` and/or `autoconnect` parameters, if enabled, to a disabled state.

Solution: The problem has been corrected in this release.

Software Kit Changes

NBase-Xyplex has made the following changes to the Access Server software kits.

DEC Alpha Workstation Supported for Load/Parameter/Dump Serving

In Access Server Kit CS12 (Version 6.0), NBase-Xyplex began supplying versions of the XYP_MANAGER.EXE and XYP_SYSTEM.EXE programs that run on DEC Alpha Workstations using the OpenVMS Operating System, Version 6.1, or earlier. This allows Alpha Workstations to be used for parameter serving. The Maintenance Operations Program ("MOP loader"), supplied with the OpenVMS operating system, supports load serving and dump serving. Initially, the only supported media type that supports Alpha Workstations is ISO-9660 compatible CD-ROM format. For more information about these products, contact your local NBase-Xyplex Sales Representative or Distributor.

Flash Card Enhancements

Since V6.0.1, the following flash card enhancements were made:

- **Series 2 Flash Card Support -** V6.0.1 enhances the flash card drivers to be compatible with Intel Series 2 devices. Series 2 flash cards offer all the features of traditional series 1 flash cards, but at a reduced price. With V6.0.1, the following NBase-Xyplex access server products support Series 2 flash cards:
  - MAXserver 1450
  - MAXserver 1600
  - MAXserver 1608
  - MAXserver 1608A
  - MAXserver 1620
  - MAXserver 1640
  - Network 9000 Access Server 720

Notes: *Access Server software versions prior to V6.0.1 do not support Series 2 flash cards.*

Series 1 flash cards are obsolete and as a result are hard to find. Customers who are forced to migrate to Series 2 flash cards must upgrade to at least V6.0.1. This may require additional memory in the unit to accommodate the larger image size.

Refer to the Notes and Restrictions section for information about using the NBase-Xyplex CARDCOPY command to copy information from a traditional flash card to a Series 2 flash card, or between cards of different sizes, such as 2 and 4 Megabyte flash cards.

For the most up-to-date Series 2 information, refer to the NBase-Xyplex home page on the World Wide Web (http://www.xyplex.com) or contact your NBase-Xyplex sales representative or distributor.

4- and 8-Megabyte Formatting Options

V6.0.2 and V6.0.1 supported new options for formatting 4 and 8 MB flash cards. For more information on these options, refer to the section on Flash Card Formatting Options.

Future Support for 1-Megabyte Units

With the shipment of V6.0, the 1-Megabyte images were full and NBase-Xyplex no longer adds new features to the software load images that run on 1-Megabyte access servers. As a result, V6.0 was the last release to contain changes and enhancements to the 1-MB load images.

In addition, NBase-Xyplex only plans to continue distribution of these access server load images on a request basis. However, NBase-Xyplex remains committed to supporting customers who use these images.

Customers who need features not contained in the 1-Megabyte images should contact their local NBase-Xyplex Sales representative or distributor.

Future Support for 2-Megabyte Units

With the shipment of V6.0.1, the 2-Megabyte images were full. NBase-Xyplex no longer adds new features to the software load images that run on 2-Megabyte access servers. As a result, V6.0.1 is the last release to contain new features and enhancements to the 2-Megabyte load images.

NBase-Xyplex remains committed to supporting customers who use these images and distributes maintenance releases on a regular basis. Customers who need features not contained in the 2-Megabyte images should contact their local NBase-Xyplex Sales representative or distributor.

Notes and Restrictions

Using MOP to Load Parameters

NBase-Xyplex Access Servers cannot load from a DEC Info Server or any other device that does not support loading via DEC MOP V3 using all 5 parameters (Including the fifth parameter, which is the Host date/time stamp) for "Parameter Load with Transfer Address" using MOP.