

Xyplex Networks Release Notes

Multiprotocol Access Server Software Version 6.0.4, 6.0.3, 6.0.2, 6.0.1, and 6.0

450-0001U

March 1998

Contents

Important Notice	5
Documentation Overview.....	5
Software Overview	6
V6.0.4 Features	7
IPX and XREMOTE Protocol Support Changes	7
Bypassing Capability for LPD Ports Provided.....	7
Disabling of Password Prompt for Port 0 Provided	7
Support Provided for Radius Callback (Dialback)	7
Userdata Support for Telnet Dedicated Service	10
Controlled Port Logout Enhancement	13
Documentation Enhancements	13
V6.0.3 Features	15
MAXserver 1604 and 1608B Terminal Servers.....	15
Figure 3 - MAXserver 1604 Front Panel.....	16
TCP Fast Retransmits	16
APD Port Authentication Command.....	17
Two Syslogd Hosts on Access Server.....	17
SHOW SERVER ALTERNATE STATUS Display	18
RADIUS Accounting Attributes	18
Searching for Available IP Ports.....	18
PPP PAP RADIUS Username and Password.....	19
Get, Set and Trap Parameters	19
Windows 95 TCP-IP PPP Dialup Networking Configuration Option.....	19
Defining Ports Back to Defaults.....	20
Focal Point for the Access Server, Version 1.1.....	20
Stampede™ Remote Office™ Support Discontinued	20
V6.0.2 Features	21
Defining RADIUS Accounting.....	21
RADIUS Accounting Prerequisites	21
Setting Up RADIUS Accounting	21
Defining a UDP Port Number	22
Defining the RADIUS Accounting Logging Attempts Limits	22
Defining RADIUS Accounting for Port Logins and Logouts.....	22
RADIUS Accounting Client Operation.....	23
Accounting Retry and Backoff Timer Process.....	23
Canceling RADIUS Requests	24
Viewing RADIUS Accounting Information	25
RADIUS Accounting Attributes	27
RADIUS Log Messages.....	28
FocalPoint, V.1.1, for the Access Servers.....	30
Miscellaneous V6.0.2 Features.....	30
TN3270 New Features.....	31

Remote Authentication Dial In User Service (RADIUS)	32
Understanding the RADIUS Authentication Process	33
Configuring the RADIUS Server on the Host	34
Configuring RADIUS on the Access Server	35
Defining RADIUS Authentication	37
Access Server Service-Selection	38
RADIUS Server-Selection	40
Displaying RADIUS Server Parameters	41
Configurable Username and Password Prompts	45
Outbound Port Security	45
Login Duration Timer	46
Kerberos Error Messages	46
Privileged Commands in Scripts	47
PPP Port Mapped to Several Internet Addresses	47
PPP Local Address Range	47
TN3270 Enhancements	47
Time Server Enhancement	48
Longer Username Support	49
MIB Support for New Variables	50
Stampede™ Remote Office™ Support	50
Future Support for 1-Megabyte Units	50
Future Support for 2-Megabyte Units	50
Software Kit Changes	51
CD-ROM kits:	51
Print filters and related files no longer distributed:	51
DEC Alpha Workstation Supported for Load/Parameter/Dump Serving	51
1710 TCP/IP-LAT Gateway Software to be No Longer Supported	52
Saving the Parameter File	52
Using the CARDCOPY Command	52
Auto Protocol Detect and Script Logins	53
Flash Cards with Redundant Parameter Areas	53
Note on Using Flash Cards	53
Flash Card Formatting Options	53
Flash Card Vendors	55
Reply Message String Limited to 97 Characters	55
Notes on SNMP	55
SecurID Notes	56
AppleTalk Remote Access (ARAP) Notes	56
CCL Notes (Using Modem-Based Compression)	57
APD Notes	57
Fixed Problems	57
Problems Fixed in V6.0.4	57
Problem Writing to Series II Flashcards with 1608B Terminal Servers	57
Problem Calculating Leap Year	57
define port <i>port-number</i> to defaults Command	58
Problems Fixed in V6.0.3	58

Error Displays	58
PPP Port Logout	58
Line Printer Daemon and AIX Machine	58
IP Address Resolution by DNS Server	58
SNMP BasicPortIndex.....	59
Accounting Log - Invalid Parameter Server Reply Message	59
RADIUS Attributes - Service-Type and Framed-Protocol	59
RADIUS Authentication - Framed Compression	59
Securid - Entering New PIN Mode.....	59
Show Server Securid Display	60
Packet Rejection Message.....	60
Problems Fixed in V6.0.2.....	60
Problems Fixed in V6.0.1.....	62
MX2120 and MX2220 Chassis-Based Access Servers	65
Standalone Access Servers	65

Important Notice

The V6.0.4 parameter files are not backward compatible with parameter files of many previous versions of Multiprotocol Access Server software. Xyplex Networks 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, Xyplex Networks recommends a minimum of one back-up parameter server. Before reformatting a flash card, back up any software images that are on the card to another load server.

Documentation Overview

The following provides a list of the available Access Server documentation.

Table 1 - Available Access Server Documentation

Document Title	Xyplex Networks Part Number
One of the following documents is supplied with your software kit:	
Software Installation Guide, for UNIX Hosts	420-0390
Software Installation Guide, for VMS Hosts	420-0391
Software Installation Guide, for Xyplex Loader Kits	420-0392
All software kits contain the following documents:	
Release Notes	
Software Kit Information	
Multiprotocol Communication Server standard documentation set ¹ :	
Commands Reference Manual	DOC-CS-001
Configuring Access Serving Features	
Configuring Printer Serving Features	
Software Management Guide	
Status and Error Messages Reference Guide	
Using the Multiprotocol Access Server	
Using the ULI Interface	
Using the APGEN Utility	
Advanced Features Guide	
Xyplex Networks supplies the following documentation with the Network 9000 products:	
Getting Started with the Network 9000 Access Server 720	451-0021
Managing Network 9000 Modules and Power Supplies	451-0020
Xyplex Networks supplies the following documentation with other Access Server products:	
MAXserver Hardware Installation Manuals	
MAXserver 1604, 1608A, 1608B, 1620/1640 Access Servers	451-0038
Xyplex Product Release Notes and Hardware Installation and Maintenance Notes²	

¹ Documentation set can be purchased from Xyplex Networks.

² Individual *Product Release Notes* or *Hardware Installation and Maintenance Notes* are available for access server and printer server cards.

Software Overview

These *Release Notes* cover Xyplex Networks Multiprotocol Access Server software, Versions 6.0.4, 6.0.3, 6.0.2, 6.0.1, and 6.0 (hereafter referred to as V6.0.4, V6.0.3, V6.0.2, V6.0.1 and V6.0).

NOTES:

The V6.0 image, the Premium Support Release (as well as V6.0.1 and V6.0.2), supports the xpcsrv20.sys and xpcs00s.sys multi-meg images.

Versions V6.0.3 and V6.0.4 support only Access Servers that load the xpcsrv20.sys image.

The new MAXserver 1604 and 1608B require version V6.0.3 or higher.

The V6.0 image, the Premium Customer Support release, runs on all the aforementioned units, except where noted. If you need the new features contained in V6.0.1 and V6.0.2, V6.0.3, V6.0.4 you need a minimum of 4 megs of memory for the access server.

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

Caution

V6.0.4 parameter files are not backward compatible with parameter files of many previous versions of Multiprotocol Access Server software. Xyplex Networks recommends that you save a renamed copy of your parameter file on the network or on separate media, before you upgrade.

V6.0.4 Features

This section describes enhancements and problem fixes for V6.0.4 software.

IPX and XREMOTE Protocol Support Changes

As of V6.0.4, 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 [enable/disable]
```

To enable or disable XREMOTE, enter:

```
define server protocol xremote [enable/disable]
```

Bypassing Capability for LPD Ports Provided

V6.0.4 now provides the ability to 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 other ports configured with the same queue name and are operational.

Use the following command to bypass 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.

V6.0.4. 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.

Support Provided for Radius Callback (Dialback)

Radius Callback (Dialback) provides automatic dialback capability to users logging into a Xyplex port. The following actions occur during a typical callback (Dialback) sequence:

1. The user dials into the Xyplex port and enters the Radius username and password information.
2. If the username/password are authenticated by the Radius host, the connecting modems hang up.

3. The Dialback process calls the originating modem.
4. The Radius username prompt appears again.
5. You must re-enter the same username. If the usernames match, the connection continues.

If the user enters a username that does not match the first one, the port is automatically logged out.

Callback Modes

V6.0.4 provides support for Radius Callback (Dialback) in the following modes:

- **Callback-Login** - consists of a dialback followed by a connection to a dedicated host specified in the Radius `users` file.
- **Callback-Framed-User** - consists of a dialback followed by PPP negotiation with the Xyplex Access Server.

Callback-Login Parameters

Parameters for Callback-login are specified in the Radius `users` file. The following shows a typical Callback-Login entry in the `users` file.

```
bob Password = "secret"
    Service-Type = Callback-Login-User,
    Login-IP-Host = 140.210.211.99,
    Login-Service = Telnet
```

In this example, `bob` is the username, `secret` is the password. The Service-Type is `Callback-Login-User`. The Login-IP-Host is IP address for the host machine. The Login-service is `Telnet`.

NOTE: The Service-Type must be `Callback-Login-User` for Livingston Radius implementations (as opposed to `Login-User` for non-dialback logins). For Merit Radius implementations `Callback-Login` is used for dialback and `Login` is used for non-dialback logins. Refer to the radius dictionary file for specific information.

Callback-Framed User Mode

Parameters for Callback-Framed User Mode are specified in the Radius `users` file. The following shows a typical Callback-Framed User entry in the `users` file.

```
sue Password = "secret"
    Service-Type = Callback-Framed-User,
    Framed-Protocol = PPP
    Framed-IP-Address = 140.210.211.99,
    Framed-Compression = Van-Jacobson-TCP-IP
```


In this example, `sue` is the username, `secret` is the password. The Service-Type is `Callback-Framed-User`. The Framed-Protocol is `PPP`. The IP Address to use remotely for PPP is `140.210.211.99`. The Framed-Compression type is `Van-Jacobson-TCP-IP`.

NOTE: The Service-Type must be `Callback-Framed-User` for Livingston Radius implementations (as opposed to `Framed-User` for non-dialback logins). For Merit Radius implementations `Callback-Framed` is used for dialback and `Framed` is used for non-dialback logins. Refer to the radius dictionary file for specific information.

Configuration Tips

Follow these tips and guidelines to configure Radius Callback:

- Dialback provides you with two configuration choices. You can
 - define dialback on the port along with Radius and then limit the users who connect to this port to do Radius and dialback
 - just define Radius on the port.

The Radius callback software automatically enables dialback on the port, for that login session only, upon seeing the "Callback" string in the radius users file. If you choose to configure this way, the port is still available for regular Radius interactive users (Note: The Radius Spec does not provide for support of Callback (Dialback) for interactive users).

- The port must be set to access "dynamic".
- The Dialback process connects to the originating modem. In testing, it has taken up to 25 seconds for the reconnection to occur, once the re-dial has taken place. By default the dialback timeout is set at 20 seconds. Xyplex Networks suggests that you reset it to at least 25 seconds.

To reset the dialback timeout, enter

```
define port port-number dialback timeout 25
```

- The dialback login script should include the `#pause 5`. This line must appear before the line `#atdt`.
- To display Dialback-Login or Dialback-Framed User login information, set the accounting log to verbose priority 7.
- The modem attached to the COM port of the PC must be set to answer mode. Most modems from the factory have auto-answer disabled. This means that the modem will not answer an incoming call.

To enable auto-answer (on most Hayes compatible modems), you need to issue an `ats0=1` (or higher). This sets the modem to answer after 1 ring. Save the configuration on the modem. For additional information refer to the documentation that accompanied your modem.

Supported Platforms

Radius Callback (Dialback) is supported on:

- Chameleon, V4.6
- Stampede Remote Office ,V2.0, with Connect dialog box enabled (although Xyplex Networks has officially ended its support for Stampede Remote Office as of V6.0.3).

These platforms provides a terminal(tty) window that stays active after the first dialback hangup occurs thereby allowing the login user to be prompted for the second `Enter username` prompt.

Unsupported Platforms

Radius Callback (Dialback) is not supported on:

- Windows' 95 Dial-Up Networking
- FTP Software OnNet2.0

Windows' 95 Dial-Up Networking and FTP Software OnNet2.0 do not keep a terminal(tty)window active, and there is no apparent option to keep it active, after the modem hangs up to perform dialback. Windows 95 and OnNet 2.0 consider this a disconnection and end the session. This prevents the login user from receiving the second `Enter username` prompt.

Unsupported Attributes

The Radius CallBack (Dialback) software included in V6.0.4 upgrade does not support

- Callback-Number
- Callback-ID.
- SLIP Connections

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.

Adding A Userdata String

Enter the following to define a userdata string for a dedicated port:

```
define port port-number telnet dedicated [service] [ip-address/domain  
name] userdata "userdata_string"
```

The keyword "telnet" is required. If it is omitted, the user will be unable to enter the "userdata" string.

Deleting a Userdata String

You can keep the service and delete the userdata string, or you can delete both the service and the string:

To keep the service and delete the userdata string:

```
define port port-number telnet dedicated [service] [ip-address/domain  
name] userdata " "
```

To delete the service and the userdata string:

```
define port port-number dedicated none
```

Modifying a Userdata String

To modify a userdata string, you must redefine the service as well.

Using Userdata Strings Characters

The following guidelines apply to the characters within a userdata character string.

1. The string, when computed can store up to 16 characters.
2. The range is as follows:
 - All printable ascii characters.
 - Special escaped ascii characters, including:
 - \b - backspace
 - \t - tab
 - \n - linefeed
 - \f - form feed
 - \v - vertical tab
 - \r - carriage return
 - \\ - backslash
3. All non-printable ascii characters in the form of \000 - \377 octal(hex 00 - FF).

4. The leading backslash (\) is required for the special escaped and octal characters to be interpreted correctly. In fact, if entering an octal, you will receive an error message if you do not use a value in the range of \000 - \377.

The above covers the entire ascii chart from 0-255.

Displaying the Userdata String

The userdata string displays underneath the Dedicated Service display on the Show Port screen. The screen displays characters just as you entered them, with the following minor exceptions:

- If an octal equivalent of a printable character or a special escape character is entered, then that printable or special escape character will be displayed.
- If an octal \377(hex FF) is entered, then it will be doubled. (Telnet interprets the FF has an IAC.)
- If spaces (spacebar) are imbedded in the string, they will be interpreted as a hex 20 and sent up to the connection partner. Do not enter spaces within the string unless you want to pass them to the connection partner.

Sample Userdata Strings

The following examples show how userdata strings convert and display.

Example 1

The user enters `xyp\lex\r\n`, as the userdata string. The string is displayed as is, and computes down to a total of 8 characters. The `\r` is a carriage return(hex 0D)and the `\n`, a linefeed(hex 0A).

The hex equivalent of the above string `78 79 70 6c 65 78 0d 0a` is sent to the connection partner.

NOTE: Keep in mind that all the rules regarding `telnet newline` still apply. If a `\r` (carriage return) is part of the entered string, either a null, linefeed, or nothing will be appended to it, depending on the setting of the `telnet newline` characteristic.

Example 2

A user enters the string `\141\142\143\015\012\000`. The string is displayed as `abc\r\n\000`. The string is sent with Telnet as hex `61 62 63 0d 0a 00`.

Note that, although 4 keystrokes were entered for `\141`, only one character , a, was stored and sent.

Controlled Port Logout Enhancement

In the previous version of Multiprotocol Access Server software the `controlled port logout` command worked only with ports that had access set to `local`. The V6.0.4 software is enhanced, and now allows you to 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`.

Documentation Enhancements

To increase usability, Access Server software documentation for various books published in versions 5.x and greater have been reorganized. The *Software Management Guide* is now discontinued. A new document, the *Advanced Features Guide*, has been added.

Cross references to the discontinued *Software Management Guide* in some Access Server documents have not been updated. Please note the following corrections:

Error Message Reference Guide

For Information About...	Refer to Chapter...	In...
Server memory resources	Chapter 2: Managing Server Resources	<i>Advanced Features Guide</i>
Selecting server protocols and features	Chapter 1: Setting Up the Access Server	<i>Advanced Features Guide</i>

Using the TCP/IP LAT Terminal Server

For Information About...	Refer to Chapter...	In...
Script commands and operations	Chapter 7: Using Scripts	<i>Advanced Features Guide</i>

Configuring Printer Serving Features

For Information About...	Refer to Chapter...	In...
Internet operations	Chapter 3: Using TCP/IP Features	<i>Advanced Features Guide</i>
Selecting protocols and features	Chapter 1: Setting Up the Access Server	<i>Advanced Features Guide</i>

Configuring Access Server Features

For Information About...	Refer to Chapter...	In...
Internet operations	Chapter 3: Using TCP/IP Features	<i>Advanced Features Guide</i>
Selecting protocols and features	Chapter 1: Setting Up the Access Server	<i>Advanced Features Guide</i>
Using Scripts	Chapter 7: Using Scripts	<i>Advanced Features Guide</i>

TCP/IP LAT Commands Reference Guide

For Information About...	Refer to Chapter..	In...
Using scripts	Chapter 7: Using Scripts	<i>Advanced Features Guide</i>
Configuring domain name serving	Chapter 3: Using TCP/IP Features	<i>Advanced Features Guide</i>
TN3270 operations	Chapter 4: Setting Up TN3270 Terminals	<i>Advanced Features Guide</i>
LAT services, concepts	Chapter 2: Managing Server Resources	<i>Advanced Features Guide</i>
Setting up modems	Chapter 3: Setting Up Basic Modem Operations	<i>Configuring Access Server Features</i>
Flow control (XON,XOFF, DCD,DTR, RTS/CTS)	Appendix A: Modem and Flow Control Operations	<i>Configuring Access Server Feature</i>
SLIP concepts	Chapter 1: Introducing the Communications Server	<i>Configuring Access Server Features</i>
SLIP Operations	Chapter 5: Serial Line Internet Protocol	<i>Configuring Access Server Features</i>
Managing server sessions	Chapter 2: Managing Server Resources	<i>Advanced Features Guide</i>
Accounting operations	Chapter 8: Using the Accounting Feature	<i>Advanced Features Guide</i>
Managing server memory	Chapter 2: Managing Server Resources	<i>Advanced Features Guide</i>
TCP/IP operations	Chapter 3: Using TCP/IP Features	<i>Advanced Features Guide</i>
Creating a rotary	Chapter 3: Using TCP/IP Features	<i>Advanced Features Guide</i>
SNMP operations	Chapter 3: Using TCP/IP Features	<i>Advanced Features Guide</i>
Defining an internet route	Chapter 3: Using TCP/IP Features	<i>Advanced Features Guide</i>
Defining a server node limit	Chapter 2: Managing Server Resources	<i>Advanced Features Guide</i>
Defining a server packet count	Chapter 2: Managing Server Resources	<i>Advanced Features Guide</i>
Rlogin operations	Chapter 2: Managing Server Resources	<i>Advanced Features Guide</i>
Defining a server session limit	Chapter 2: Managing Server Resources	<i>Advanced Features Guide</i>
Defining a server textpool limit	Chapter 2: Managing Server Resources	<i>Advanced Features Guide</i>
Configuring Novell printing	Chapter 5: Configuring Print Services for Novell Users	<i>Configuring Printer Server Features</i>
Configuring IP routes	Chapter 3: Using TCP/IP Features	<i>Advanced Features Guide</i>
Defining server daemons (lpd, routed, rwhod)	Chapter 5: Setting Up UNIX Daemons	<i>Advanced Features Guide</i>
Defining server daemons (syslogd)	Chapter 8: Using the Accounting Feature	<i>Advanced Features Guide</i>
Defining the lpd queue	Chapter 3: Setting Up Printers Using the lpd Daemon	<i>Configuring Printer Server Features</i>
ARAP concepts and operations	Chapter 6: Setting Up ARAP	<i>Configuring Server Access Features</i>

V6.0.3 Features

This section describes the new features as well as enhancements and problem fixes for V6.0.3. For more information about Access Server features, refer to Xyplex Networks' World Wide Web page located at www.xyplex.com.

Features in V6.0.3 provide the addition of the MAXserver 1604 and 1608B Terminal Servers as well as enhancements and problem fixes for V6.0.3. Version 6.0.3 also provides all the features of V6.0, V6.0.1 and V6.0.2. For a list of problem fixes, refer to the [Fixed Problems](#) section.

MAXserver 1604 and 1608B Terminal Servers

The MAXserver 1604 and 1608B are the newest additions to the MAXserver Access Server product line with V6.0.3. The front panels of the MAXserver 1604 and 1608B terminal servers are identical except for the model designation. Figures 2 through 4 illustrate the MAXserver 1604 and 1608B.

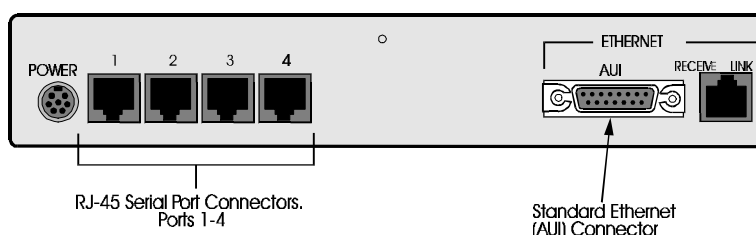


Figure 1 - MAXserver 1604 Rear Panel

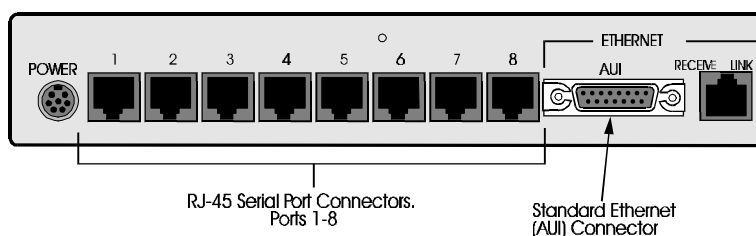


Figure 2 - MAXserver 1608B Rear Panel

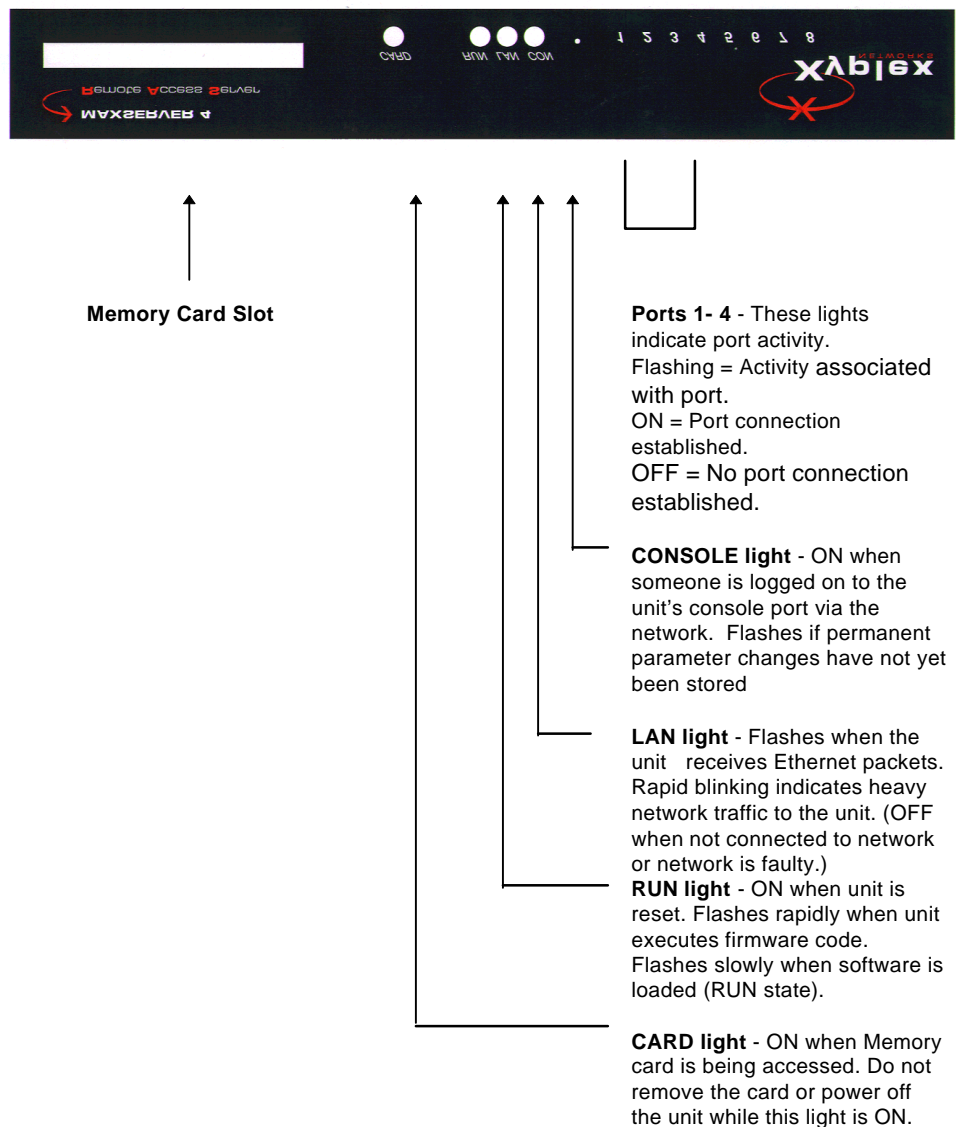


Figure 3 - MAXserver 1604 Front Panel

TCP Fast Retransmits

TCP now performs retransmission of missing segments without waiting for a retransmission timer to expire. Previously, because TCP did not know whether a duplicate Acknowledgment (ACK) was caused by a lost segment or just a reordering of segments, it waited for a small number of duplicate ACKs to be received.

APD Port Authentication Command

When a new switch is enabled, users accessing through an APD port using PPP or SLIP will be authenticated if either PAP or CHAP is enabled on the port. Interactive users will be prompted after the APD message displays and continue to use RADIUS or KERBEROS authentication.

Use the following new command to enable authentication and interactive mode for an APD port:

```
DEFINE PORT number APD AUTHENTICATION
INTERACTIVE [ONLY] ENABLE/DISABLE
```

If you disable interactive mode, authentication will be performed as previously.

NOTE: When you enable interactive mode also enable PAP or CHAP for users accessing through PPP or SLIP. Otherwise, users will have access without needing authentication.

Two Syslogd Hosts on Access Server

You can now define up to two Syslogd hosts for logging of information. Please note the following whenever you define a Syslog host:

- Host 1 must be defined first
- A unique IP address must be defined for each Syslogd host
- Syslog messages for both hosts must be logged at the same Log Facility
- To delete a Syslogd host, you must first disable Host 2

Use the following command to define the Syslog hosts:

For Host 1, use:

```
DEFINE SERVER DAEMON SYSLOGD ENABLED HOST1<ip-address-syslogd-host1>
```

For Host 2, use:

```
DEFINE SERVER DAEMON SYSLOGD ENABLED HOST2 <ip-address-of-syslogd-
host2>
```

To display Syslogd host, use the following command:

```
SHOW UNIT
```

Both Syslogd hosts display if they have been previously defined.

NOTE: If you are upgrading from an earlier revision and already have a Syslogd host defined, then the SHOW UNIT display will now show that host as "Host1" as opposed to "Host."

SHOW SERVER ALTERNATE STATUS Display

The Syslogd host and Log Facility information is no longer present on the SHOW SERVER ALTERNATE STATUS screen. Use the SHOW UNIT command to display this information.

RADIUS Accounting Attributes

V6.0.3 supports the following attributes for a “Framed” user (such as PPP):

ID#	Attribute Name	Type
47	Acct-Input-Packets	Integer
48	Acct-Output-Packets	Integer

These attributes log the number of IP input/output packets that occurred during a session to the accounting log file.

NOTE: Merit has already defined these attributes in their dictionary, so no configuration is needed for Merit users. Livingston V1.16 and V2.0 do not have these attributes defined in their dictionary files. Therefore, Livingston users must insert these two attributes into the file.

Searching for Available IP Ports

Previously, the only way to search for available IP ports was the Roundrobin method, which meant the next available port was chosen from the IP Rotary List. This method did not always find the lowest available port, because as ports are connected and disconnected, the next session created picked the next ascending available port.

V6.0.3 provides another method to search for available IP Ports. This new feature manipulates the chain of sessions so that the disconnected session is put back into its original place and not at the end of the list (if Roundrobin is disabled). This means that now when you search for available IP ports the search always begins at the lowest port in the Rotary list.

Use the following command (in privileged mode) to search for the lowest available IP port:

```
DEFINE SERVER ROTARY ROUNDROBIN [ENABLED/DISABLED]
```

The default is Roundrobin enabled. With Roundrobin disabled, the search for an available port mapped to an IP Rotary will always begin at the first port in the Rotary list. Use the following command to display which search method is in use:

```
SHOW SERVER IP ROTARY
```

This screen now displays one of the following search methods:

Round Robin search: ENABLED

or

Round Robin search: DISABLED, Search by first available

PPP PAP RADIUS Username and Password

Problem: Previous versions of RADIUS only allowed a user one attempt at entering their username and password correctly before being logged out.

Solution: Users now have up to three tries to enter their correct username and password before RADIUS logs the port out.

NOTE: This enhancement works with Windows 95 Dialup Networking and MacTCP.

Other systems may have stacks that will, when seeing a PAP authorization not accepted, send a ATH command and disconnect the phone link.

Get, Set and Trap Parameters

This enhancement to the Get, Set and Trap parameters now allows for an additional 8 Get, Set and Trap clients to be added to the Terminal Server for a total of 12 clients each.

NOTE: Because the number of clients supported has now increased, the SHOW SERVER IP SNMP CHARACTERISTICS display will scroll off the screen. To solve this problem, enable "Pause" on the port to display one screen at a time.

Windows 95 TCP-IP PPP Dialup Networking Configuration Option

This Configuration Option defines a method for negotiating with the remote peer(Xyplex Access server) the address of the primary and secondary DNS server to be used on the local end of the link. If the local peer(local is the device on one of our serial ports) requests these options, the remote peer(Xyplex Access server) specifies the Xyplex defined DNS address(s) by NAKing this option, and returning the IP address(s) of the valid DNS server(s).

V6.0.3 supports RFC1877. An abstract of RFC1877 follows:

Abstract:

The Point-to-Point Protocol (PPP) [1] provides a standard method for transporting multi-protocol datagrams over point-to-point links. PPP defines an extensible Link Control Protocol and a family of Network Control Protocols (NCPs) for establishing and configuring different network-layer protocols.

This document extends the NCP for establishing and configuring the Internet Protocol over PPP [2], defining the negotiation of primary and secondary Domain Name System (DNS) [3] addresses.

The two name server address configurations that Xyplex now supports are options 129 and 131. These provide a method of obtaining the addresses of Domain Name System (DNS) servers on the remote network.

NOTE: This new feature only includes support for the Primary and Secondary DNS addresses (Options 129 and 131). We will NOT be supporting the Primary and Secondary NetBIOS Name server nodes (Options 130 and 132).

Defining Ports Back to Defaults

V6.0.3 now allows a privileged user to define ports back to factory default settings. Use the following command:

```
DEFINE PORT <port-number-or port-list> TO DEFAULTS
```

Example:

```
DEFINE PORT PORT 1-20 TO DEFAULTS
```

The system prompts you for verification on each port (1 through 20) in succession.

Press Return to reset the factory defaults for that port or press any other key to terminate the process. Pressing any other key terminates the process from that port on. However, the ports that have already been returned to factory defaults will stay defaulted. The ports must be logged out in order for the changes to take effect.

The following parameters are not changed (if defined) when the ports are reset to defaults:

- Internet security
- IP filters
- IPX filters

Focal Point for the Access Server, Version 1.1

Version 6.03 bundles FocalPoint for the Access Servers, Version 1.1, which enables easy Access Server configuration using a Graphical User Interface (GUI) that steps users through the configuration process. For more information, refer to the [Focal Point, v. 1.1. for the Access Servers section](#).

Focal Point for the Access Servers, V1.1 is provided on the Kit 15 CD.

Stampede™ Remote Office™ Support Discontinued

Stampede™ Remote Office™ support and the demonstration version of it are dropped in V6.0.3.

V6.0.2 Features

This section describes some of the new features provided by V6.0.2. For more information about Access Server features, refer to Xyplex Network's World Wide Web page located at www.xyplex.com.

V6.0.2 provides the RADIUS Accounting feature. V6.0.2 also provides all the features of V6.0.1 and V6.0. For a list of problem fixes, refer to the [Fixed Problems section](#).

Defining RADIUS Accounting

This section describes the new remote access user accounting feature, called RADIUS Accounting. RADIUS Accounting is a client/server account logging scheme that allows you to log user account information to a remote server in a per client file. The file or record can contain information such as the user who logged in, the duration of the session, and the number of bytes/packets that were processed by the Access Server.

The use of RADIUS Accounting solves the problems associated with local storage of large numbers of records. It also provides a method for billing customers for account usage.

NOTE: RADIUS Accounting is a developing standard that is *vendor extensible by design*, including a provision for vendor specific extensions. This allows for greater expandability of accounting information in the future.

For further information about RADIUS Accounting, refer to IETF Draft: RADIUS Accounting, July 1996, RADIUS Working Group.

RADIUS Accounting Prerequisites

To use RADIUS Accounting on an access server, you need the following:

- Support for Internet Draft RADIUS Accounting on a RADIUS Authentication Server in the network. (This is usually done with portable code for the RADIUS Accounting feature installed on the RADIUS Authentication Server.)
- Interoperation with a RADIUS server, such as a Merit RADIUS server.
- Minimum of 3 MB of memory.

Setting Up RADIUS Accounting

To setup RADIUS Accounting on your access server:

1. Make a copy of your parameter file. Xyplex Networks recommends that you copy the existing file to a file with an ".old" extension.
2. Insert the flash card containing the load image and reboot the access server.
3. Enable RADIUS on the access server, using the following command:

```
define server radius enabled
```

4. Enable Xyplex Accounting at a priority level 7, using the following commands:

```
define server accounting entries 255
init delay 0
define server verbose accounting enabled
define server verbose priority 7
define server radius logging enabled
```

Xyplex Accounting is independent of RADIUS Accounting and therefore able to log all events including failures. This allows you to troubleshoot RADIUS authentication and RADIUS accounting problems.

5. Verify that the parameter state has gone to “current,” using the following command:

```
monitor parameter server
```

6. Reboot the access server.

```
init delay 0
```

7. Enable RADIUS logging, using the following command:

```
define server radius logging enabled
```

This logs entries about the RADIUS protocol to the Xyplex accounting log.

Defining a UDP Port Number

To define a UDP port number used by the RADIUS client and server for communication, use the following command:

```
DEFINE/SET [SERVER] RADIUS ACCOUNTING PORT n
```

The default value is 1646.

Defining the RADIUS Accounting Logging Attempts Limits

To define the number of times that the access server attempts to log the accounting record to both the primary and secondary servers before giving up and failing, use the following command:

```
DEFINE/SET [SERVER] RADIUS ACCOUNTING ATTEMPTS n
```

A backoff algorithm is implemented to delay for a period of time between these attempts. The default value is 5 attempts.

Defining RADIUS Accounting for Port Logins and Logouts

To enable RADIUS Accounting for port logins and logouts, use the following command:

```
DEFINE/SET PORT n RADIUS ACCOUNTING {ENABLED|DISABLED}
LOG PORT n
```

Note that even though it is enabled, nothing is logged until an authentication protocol is enabled.

RADIUS Accounting Client Operation

During the authentication process, when RADIUS Accounting is enabled on an appropriate port, an accounting request (a start request) is sent before login to the RADIUS Accounting process begins. As a result of the start request, a start record containing the following is created for each user session:

- User-name
- NAS-Identifier
- NAS-IP-Address
- NAS-Port
- NAS-Port-Type
- Service-Type
- Acct-Status-Type
- Acct-Delay-Time
- Acct-Session-Id
- Acct-Authentication

The majority of the accounting record information appears in the *stop* record. The stop record is created when the port is logged out, provided that a matching start record was previously sent. The information in the stop record includes everything in the start record, and additional information, such as session time and bytes/packets transferred.

There are two special records that are logged for RADIUS Accounting.

- Accounting-on. This record is logged when the access server is first booted.
- Accounting-off. This record is logged, if possible, when the access server is shutdown.

These records only contain the Session-Id, Acct-Status-Type, and NAS-IP-Address. Since these accounting requests only relate to the access server using the protocol and not to accounting on a specific port, they are only attempted if the RADIUS protocol is enabled.

Accounting Retry and Backoff Timer Process

RADIUS Accounting has built-in timeout and retry capabilities. The RADIUS Accounting feature logs the record to the remote server, when possible. However, sending requests constantly and continually trying to process them should be avoided. Therefore, this implementation of RADIUS Accounting uses a two-part retry and backoff algorithm based on the following configurable controls:

- The first part of the retry mechanism directly affects the communication between the RADIUS client on the NAS and each RADIUS server. It is the same retry functionality that RADIUS authentication uses. The NAS client waits a configurable amount of time (*Request Timeout* in seconds) for an acknowledgment after it sends an accounting request to a server. If the timeout period occurs, it retries the server again. After three retries, it proceeds to the next (secondary) server in the list. The secondary server is then tried in the same way, provided that the servers are configured. RADIUS Servers configured on the NAS with the default value 0.0.0.0 are not used.
- The second piece of the retry mechanism involves the available primary and secondary RADIUS servers. After sending requests to all the configured servers and failing to get a timely response, the request waits a period of time before starting over with the first server in the list and re-sending the request. The period of time that it waits is based on the configurable *request timeout* and the number of attempts that have been made to send this request to all the servers.

This delay period starts with a value based on the request timeout (*start delay* = *request timeout*) and increases with each successive attempt by an exponential factor (*new delay* = *previous delay* * 2^(attempt #)) up to a maximum backoff factor of 16 or 2^(4th attempt). This delay value remains for all remaining log attempts. The maximum number of log attempts (*Attempts to Log Record*), or number of times all the servers are tried, is also configurable.

The following table provides an example of the retry and delay time process. In this example, the NAS client uses a timeout value of 5 seconds, an attempt limit of 6, and both primary and secondary servers. With these values the delay between attempts is:

Log Attempt	Total of all Timeouts for Both Servers	Delay Time After This Log Attempt	Total Wait Time Before Next Log Attempt
1	30 secs = 2 * 3 * 5 secs	10 secs	40 secs = 30 + 10
2	30 secs = 2 * 3 * 5 secs	40 secs	70 secs = 30 + 40
3	30 secs = 2 * 3 * 5 secs	5.33 mins \cong 320 secs	5.83 mins \cong 350 secs = 30 + 320
4	30 secs = 2 * 3 * 5 secs	1.4222 hrs \cong 5120 secs	1.431 hrs \cong 5150 secs = 30 + 5120
5	30 secs = 2 * 3 * 5 secs	1.4222 hrs \cong 5120 secs	1.431 hrs \cong 5150 secs = 30 + 5120
6	30 secs = 2 * 3 * 5 secs	No delay after last attempt	Only waits (30 secs) on last attempt

Canceling RADIUS Requests

Once a RADIUS request is added to a respective process queues, you may want to “cancel” the request and prevent the RADIUS client from retrying a server that cannot or does not respond. To do this use the following command:

```
CLEAR/PURGE SERVER RADIUS {AUTHENTICATION|ACCOUNTING} {n|ALL}
```

The request id, 'n', is obtained by viewing information in the server accounting log on the access server, provided that server accounting and RADIUS logging (not RADIUS account logging) are enabled. All outstanding requests may be eliminated if 'ALL' is specified.

Viewing RADIUS Accounting Information

To display the access server's RADIUS server and accounting information, use the following command:

Show Server RADIUS Accounting

```
Xyplex>> show server RADIUS accounting

MX1620 V6.0.2  Rom 480000 HW 00.00.00 Lat Protocol V5.2 Uptime: 0 00:00:49
                                     11 Apr 1996  16:11:44

RADIUS Primary Server:      KAB
Resolved Address:           140.179.100.200      Secret:  CONFIGURED

RADIUS Secondary Server:    NONE
Resolved Address:           0.0.0.0              Secret:  DEFAULT

Accounting Port Number:     1646                  Request Timeout (sec):      5
Next Available Session #:   2d000002              Attempts to Log Record:     3
RADIUS Server Retries:      3
RADIUS Acct Ports Enabled:  16, 18-19

Successful Acct Entries:    2                      Failed Acct Entries:        0
Requests Waiting:           0

Server access attempts:
      Primary      Secondary
Successful:        3              0
Failed:            0              0

Xyplex>>
```

The following list describes the individual fields in the Show Server window.

RADIUS Primary Server	The server that is tried first for each authentication attempt. Valid values are text strings up to 51 ASCII characters specifying a DNS host name or a valid IP address. The default is no configured primary server or the null string "".
Primary Resolved Address	The IP address associated with the DNS name used for the Primary RADIUS server. The default value is the address 0.0.0.0.
RADIUS Secondary Server	The DNS name of the RADIUS server used when the primary RADIUS server is unavailable. The default value is "".
Secondary Resolved Address	The IP address associated with the DNS name used for the Secondary RADIUS server. The default value is the address 0.0.0.0.

Accounting Port Number	The UDP port that the RADIUS Accounting requests are transmitted and received from. The default value is 1646.
Request Timeout	The period of time between RADIUS client retransmissions to the server when trying to log an accounting record. It is the time that the access server waits for a reply from the RADIUS server. The default value is 5 seconds.
Next Available Session #	The next available session number used in the log record for the next port login.
Attempts to Log Record	The number of times that the access server attempts to log the accounting record to both the primary and secondary servers before giving up and failing. The default is 5 attempts.
RADIUS Server Retries	The number of times a particular server is tried. These tries are in succession for RADIUS accounting. The default value is 3.
RADIUS Acct Ports Enabled	A list of actual port numbers indicating the ports on the access server that have RADIUS Accounting enabled.
Successful Acct Entries	The number of successful log entries made to the RADIUS server.
Failed Acct Entries	The number of unsuccessful log entries made to the RADIUS server. The number of allowable log attempts has been exceeded and the access server has stopped trying to log the record.
Requests Waiting	The number of requests that are queued up at a given time waiting for a reply from the RADIUS server. Up to 300 of these outstanding requests can be buffered before records are lost.
Primary Server Access Successes	The number of times the primary RADIUS server and the client successfully exchanged messages.
Secondary Server Access Successes	The number of times the secondary RADIUS server and the client successfully exchanged messages.
Primary Server Access Failures	The number of times the primary RADIUS server and the client failed to exchange messages.
Secondary Server Access Failures	The number of times the secondary RADIUS server and the client failed to exchange messages.

To display the access server's port characteristics, use the following command:

Show Port ALT Characteristics

```
Xyplex>> show port alt char
```

```
Port 2:  rhw                                05 Jan 1997   09:54:04

Resolve Service:      Any_Lat                DTR wait:      Disabled
Idle Timeout:         0                      Typeahead Size: 128
SLIP Address:         N/A                    SLIP Mask:     N/A
Remote SLIP Addr:     N/A                    Default Session Mode: Interactive
TCP Window Size:      256                    Prompt:        X021812
DCD Timeout:          N/A                    Dialback Timeout: N/A
Stop Bits:            N/A                    Script Login:   Disabled
TCP Keepalive Timer:  N/A                    Username Filtering: None
Nested Menu:          Disabled                Nested Menu Top Level: 0
Command Size:         132                    Clear Security Entries: Disabled
Rlogin Transparent Mode: N/A                  Login Duration: 0
Xon Send Timer:       N/A                    TCP Outbound Address: 0.0.0.0
SLIP AutoSend:        N/A                    RADIUS Accounting: Enabled
APD Autobaud:         Enabled

Username Prompt:      Enter username>
Password Prompt:      Enter user password>
```

RADIUS Accounting Attributes

The following table shows the RADIUS attributes that are available for RADIUS Accounting.

Table 2. RADIUS Accounting Attributes

Id #	Attribute Name	Allowed in Request
01	User-Name	0 - 1
04	NAS-IP-Address	0 - 1
05	NAS-Port	0 - 1
06	Service-Type	0 - 1
07	Framed-Protocol	0 - 1
08	Framed-IP-Address	0 - 1
09	Framed-IP-Netmask	0 - 1
11	Filter-Id (only 1)	0+
13	Framed-Compression	0+
14	Login-IP-Host (only 1)	0+
15	Login-Service	0 - 1
16	Login-Port	0 - 1
23	Framed-IPX-Network	0 - 1
25	Class	0+
27	Session-Timeout	0 - 1
28	Idle-Timeout	0 - 1
32	NAS-Identifier	0 - 1
34	Login-LAT-Service	0 - 1
35	Login-LAT-Node	0 - 1
40	Acct-Status-Type	1

41	Acct-Delay-Time	0 - 1
42	Acct-Input-Octets	0 - 1
43	Acct-Output-Octets	0 - 1
44	Acct-Session-Id	1
45	Acct-Authentic	0 - 1
46	Acct-Session-Time	0 - 1
49	Acct-Terminate-Cause	0 - 1
61	NAS-Port-Type	0 - 1

KEY:

- 0 This attribute MUST NOT be present in packet.
- 0+ Zero or more instances of this attribute can be present in packet.
- 0-1 Zero or one instance of this attribute can be present in packet.
- 1 Exactly one instance of this attribute MUST be present in packet.

Allowed in Request - Number of attributes allowed in a request from the RADIUS client (access server, router) to the RADIUS server.

RADIUS Log Messages

The following table lists the RADIUS-related server accounting messages.

Table 3. RADIUS-Related Server Accounting Messages

Log Message Symbol	Log Message Text
RAD_LOG_A_SERVER_FAILURE	"A server was accessed, but others failed"
RAD_LOG_ACCOUNTING_FAILURE	"Failed - No request sent (acct) - NOT LOGGED"
RAD_LOG_ACCT_DISABLED_NO_CLASS	"RADIUS acct is disabled. Attribute ignored."
RAD_LOG_ACCT_NO_MEMORY	"No memory available (acct) - NOT LOGGED"
RAD_LOG_ACCT_NO_MORE_ATTEMPTS	"Exceeded # of attempts to log the record"
RAD_LOG_ACCT_NO_REPLY	"No reply to request (acct) - NOT LOGGED"
RAD_LOG_ACCT_REQ_NOT_ALLOWED	"Accounting request not allowed"
RAD_LOG_ACCT_REQUEST_ID	"Request id (acct): %d"
RAD_LOG_ACCT_REQUEST_TIMEOUT	"Request (acct) timed out - Id: %d"
RAD_LOG_ACCT_RETRY_REQUEST	"Retrying request (acct) - attempt #%d"
RAD_LOG_ACCT_SEND_FAILURE	"Failed to send packet (acct)"
RAD_LOG_ACCT_SEND_SUCCESS	"Sent packet (acct) to %s"
RAD_LOG_ACCT_START_DELAY_TIMER	"Delay timer set for %d seconds"
RAD_LOG_ACCT_START__SEND_SUCCESS	"Sent packet (act-start) to %s"
RAD_LOG_ACCT_STOP__SEND_SUCCESS	"Sent packet (act-stop) to %s"
RAD_LOG_ACCT_WAIT_TO_RETRY	"Waiting to retry request (acct)"
RAD_LOG_ALL_ACCT_IDS_USED	"All RADIUS (acct) ids used - wait to send"
RAD_LOG_ALL_SERVERS_FAIL	"All server accesses failed"
RAD_LOG_ATTRIB_CREATE_ERR	"Error storing an attribute"
RAD_LOG_ATTRIB_FAILED	"Failed on attribute - %d"
RAD_LOG_AUTH_CONTINUE_ON_FAIL	"Trying another server on auth failure"
RAD_LOG_AUTH_FAILED	"Authentication failure - logging out"

RAD_LOG_AUTH_NO_MEMORY	"No memory available (auth) - logging out"
RAD_LOG_AUTH_REQUEST_ID	"Request id (auth): %d"
RAD_LOG_AUTH_REQUEST_TIMEOUT	"Request (auth) timed out - Id: %d"
RAD_LOG_AUTH_SEND_FAILURE	"Failed to send packet (auth)"
RAD_LOG_AUTH_SEND_SUCCESS	"Sent packet (auth) to %s"
RAD_LOG_BAD_ATTRIB_FOR_CONFIG	"Invalid attribute for configuration"
RAD_LOG_BAD_ATTRIB_VAL_LEN	"Invalid attribute length"
RAD_LOG_BAD_ATTRIB_VALUE	"Invalid/unsupported attribute value"
RAD_LOG_CANCEL_ACCT_REQUEST	"Request canceled (acct) - Id: %d"
RAD_LOG_CANCEL_AUTH_REQUEST	"Request canceled (auth) - Id: %d"
RAD_LOG_CHAP_REQUEST	"Challenge Authentication request"
RAD_LOG_CONFIG_FAILED	"Configuration failure - logging out"
RAD_LOG_CONFIG_LIST_ERR	"Failed to build configuration list"
RAD_LOG_GOT_ACCEPT	"Received packet (Accept) from %s"
RAD_LOG_GOT_ACCT_RESPONSE	"Received response (acct) from %s"
RAD_LOG_GOT_ACCT_START_RESPONSE	"Received response (acct_start) from %s"
RAD_LOG_GOT_ACCT_STOP_RESPONSE	"Received response (acct_stop) from %s"
RAD_LOG_GOT_CHALLENGE	"Received packet (challenge) from %s"
RAD_LOG_GOT_REJECT	"Received packet (Reject) from %s"
RAD_LOG_INVALID_AUTH	" Invalid Authenticator - packet code %d"
RAD_LOG_INVALID_AUTH_REJ	" Invalid Authenticator - mismatched secret?"
RAD_LOG_INVALID_PACKET	"Received invalid packet from %s"
RAD_LOG_INVALID_PKT_CODE	" Invalid/unsupported packet code - %d"
RAD_LOG_INVALID_PKT_ID	" Unexpected RADIUS packet id - %d"
RAD_LOG_MISSING_REQ_FRAMED_PROT	"Missing required framed protocol"
RAD_LOG_MISSING_REQ_LAT_PARAMS	"Missing a required LAT parameter"
RAD_LOG_MISSING_REQ_LOGIN_SERVICE	"Missing required login service"
RAD_LOG_MISSING_REQ_SERVICE_TYPE	"Missing required service type"
RAD_LOG_MISSING_REQ_TELNET_PARAMS	"Missing a required TELNET parameter"
RAD_LOG_NO_PACKET_MEM	"No memory for request packet"
RAD_LOG_NO_PASSWORD	" No password specified"
RAD_LOG_NO_REC_BUFF_MEM	"No memory for receive buffer"
RAD_LOG_NO_USERNAME	" No username specified"
RAD_LOG_PAP_REQUEST	" Password Authentication request"
RAD_LOG_POLICY_FAILED	"Policy failure - logging out"
RAD_LOG_SCRIPT_FAILURE	"RADIUS script execution failure"
RAD_LOG_SECRET_CHANGED	"Secret was changed - server %d"
RAD_LOG_SEND_CHAL_REPLY	"Sent packet (response) to %s"
RAD_LOG_SERVICE_HINT_USED	" Service type hint : %s"
RAD_LOG_SERVICE_NOT_CHOSEN	"Service not type chosen"
RAD_LOG_TOO_MANY_PENDING_REQUESTS	"Too many pending requests (acct) - NOT LOGGED"

RAD_LOG_UNKNOWN_COM_ATTR	"Unexpected common attribute - %d"
RAD_LOG_UNKNOWN_RAD_ATTR	"Unexpected RADIUS attribute - %d"

FocalPoint, V.1.1, for the Access Servers

To provide Xyplex Networks customers with an easy-to-use access server configuration tool, Xyplex Networks has created FocalPoint for the Access Server (hereafter referred to as FocalPoint), Version 1.1. FocalPoint allows you to configure your access server using a Graphic User Interface (GUI) that steps you through the configuration process. By doing this, the Command Like Interface (CLI) or UNIX Like Interfaces (ULI) are no longer needed to configure your access server. For additional information, refer to the [FocalPoint for the Access Server Release Notes](#).

Miscellaneous V6.0.2 Features

APD Message Strings

A new command has been added that allows you to create an APD message string. To create a message string, use the following command:

```
DEFINE SERVER APD MESSAGE message-string
```

Boot Time Load Status Messages

The load status messages sent by the boot ROMs to a connected serial device at initialization time can now be enabled/disabled at the command line. To do this, use the following command:

```
DEFINE SERVER LOAD STATUS MESSAGE [ENABLE/DISABLE]
```

To view the current status (enabled or disabled) of the load status message, use the following command:

```
LIST SERVER LOADDUMP CHARACTERISTICS
```

Dedicated Remote Login (RLOGIN)

You can now access a dedicated or preferred service using RLOGIN. To do this, use the following commands:

```
DEFINE PORT port-number RLOGIN DEDICATED service-name
DEFINE PORT port-number RLOGIN DEDICATED SERVICES service-name
```

```
DEFINE PORT port-number RLOGIN PREFERRED service-name
DEFINE PORT port-number RLOGIN PREFERRED SERVICES service-name
```

The dedicated or preferred services can be viewed using the following command:

```
SHOW PORT port-number
```

The DEFINED port USERNAME is used for DEDICATED RLOGIN SERVICES and the port login USERNAME is used with a RLOGIN PREFERRED SERVICE.

NOTE: The following RLOGIN features are not supported:

- The ability to specify a RLOGIN USERNAME other than the defined port username with a dedicated rlogin service.
- The following commands are only supported for LAT and TELNET:

```
DEFINE PORT port-number DEDICATED SERVICES service-name  
SET PORT port-number PREFERRED SERVICES service-name
```

SLIP Autosend

The following new command has been added to SLIP:

```
DEFINE/SET PORT port-list INTERNET SLIP AUTOSEND [ENABLED/DISABLED]
```

With this command enabled, the following addresses are returned when a user issues the SET PORT IP SLIP ENABLE command:

- SLIP remote address
- SLIP local address
- SLIP Mask address

To see the setting of SLIP AUTOSEND, use the following command:

```
SHOW PORT port-list ALT CHAR
```

TCP Outbound Address

A new command has been added that allows each serial port on the access server to have a unique IP address for outbound connections. The new command is:

```
DEFINE/SET PORT IP TCP OUTBOUND [ADDRESS] ip-address
```

If this parameter is set on a port, the IP address is used in any outgoing connections. If this parameter is not set, then the access server's IP address is used as normal.

Note, the access server responds to ARP requests for this IP address regardless of whether the connection is active or not.

TN3270 New Features

The following features are new to TN3270:

Insert Mode

A new parameter called SPACE_INSERT has been added. This parameter allows you to work on filled fields using the TN3270 Insert Mode. To use the new parameter, use the following command:

```
DEFINE PORT TELNET TN3270 SPACE_INSERT [ENABLED/DISABLED]
```

TN3270 TYPE_AHEAD Function

A new parameter called TYPE_AHEAD, prevents the buffering of keys in the user console buffer when the keyboard is locked via TN3270. To use the new parameter, use the following command:

```
DEFINE PORT TELNET TN3270 TYPE_AHEAD [ENABLED/DISABLED]
```

TN3270 Default Terminal Type

When using TN3270 you can now use a default terminal type when using the following command:

```
XYPLEX>> TN3270 ip-address
```

The menu that appears gives you the option of pressing the Return key to have the default terminal type (the type defined in the TN3270 device field) used. If no terminal type is defined in the TN3270 device field, the user receives a menu with no default option. The following is an example of the menu screen:

```
Select TN3270 Device Type
```

1. ANSI
2. VT100
3. VT220-7
4. VT220-8

```
<Return> for default (VT220-7) or enter number and <Return>
```

V6.0.1 Features

This section describes some of the new features as well as enhancements and problem fixes for V6.0.1. For more information about Access Server features, refer to Xyplex Network's World Wide Web page located at www.xyplex.com.

Features in V6.0.1 provide enhancements and problem fixes for V6.0. V6.0.1 also provides all the features of V6.0. For a list of problem fixes, refer to the [Fixed Problems](#) section.

Remote Authentication Dial In User Service (RADIUS)

Xyplex Networks uses *RFC draft-ietf-radius-05.txt* (July 1996) and *RFC draft-rigney-radius-02.txt* (February 1996) for the requirements of the RADIUS implementation.

The Remote Authentication Dial In User Service (RADIUS) is a distributed security system that secures networks against unauthorized access. Xyplex Networks access servers provide security for the following network services through RADIUS:

Service	Corresponding RADIUS Settings
Dedicated LAT Service	Service-Type = Login-User, Login-Service = LAT

Dedicated Telnet Service	Service-Type = Login-User, Login-Service = Telnet
Interactive	Service-Type = Shell-User*
Outbound Service (dialout)	Service-Type = Outbound-User
PPP	Service-Type = Framed-User, Framed-Protocol = PPP
SLIP	Service-Type = Framed-User, Framed-Protocol = SLIP

* Shell-User is the Livingston Dictionary Keyword. For Merit use Exec-User as the Service-Type. Also note that earlier versions of the RADIUS server used dictionary files with Service-Type of Shell-User or Exec-User set to the value of 6. The current RADIUS server uses the value of 7.

The RADIUS configuration settings allow RADIUS database characteristics to be passed back to the access server, determining the type of service provided.

NOTE: You can only configure one authentication method on any single port. If you try to enable RADIUS after another authentication method is defined (for example, Kerberos or SecurID), the attempt fails and produces an error message.

Understanding the RADIUS Authentication Process

The access server combined with the RADIUS server secures networks against unauthorized access. RADIUS authentication occurs through a series of communications between the access server and the RADIUS server. Once RADIUS has authenticated a user, the access server provides that user with access to the appropriate network services. The RADIUS server maintains a database that contains user authentication and network service access information.

The following example describes the steps in the RADIUS authentication process. In this example, the user attempts to gain access to an access server port.

1. The access server prompts the user for a username and password.
2. The access server takes the username and password, creates an access-request packet identifying the access server making the request, the username and password, and the port being used. The access server also suggests the Service-Type for the connection based on the configuration of the port. The default Service-Type is Shell-User. The access server then sends the packet to the designated RADIUS server for authentication.

NOTE: The user password is encrypted to prevent it from being intercepted and reused by an unwanted user.

3. The RADIUS server validates the request and then decrypts the password.
4. The username and password are authenticated by the RADIUS server.
5. Upon successful authentication, the RADIUS server sends an access-accept packet containing any specific configuration information associated with that user.

6. The access server then grants the user the services requested.

If at any point in the authentication process conditions are not met, the RADIUS server sends an authentication rejection to the access server and the user is denied access to the network. Figure 1 shows an example of the RADIUS authentication process.

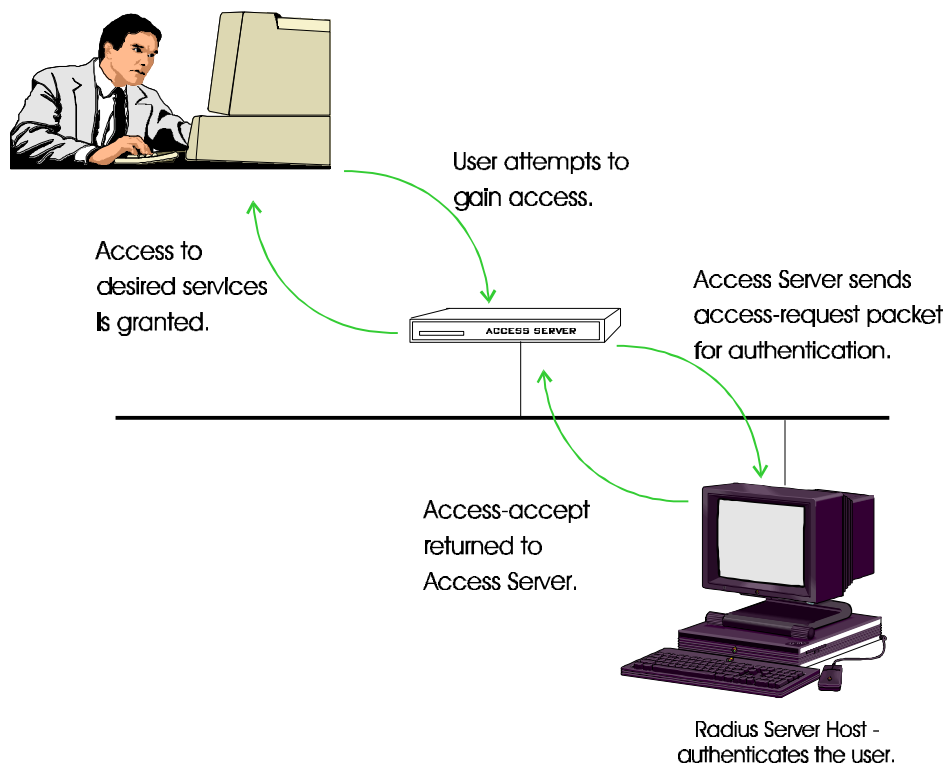


Figure 1 - RADIUS Authentication Process

Configuring the RADIUS Server on the Host

Before you can configure RADIUS on your access server you must configure a RADIUS server on your RADIUS server host.

In general, RADIUS server implementations are available on the Internet. These implementations generally use a daemon process that interacts with RADIUS clients (located on access servers and other remote access devices).

The daemon uses a list of clients and associated secrets that it shares with these clients. The per-client secret is used to encrypt and validate communications between the RADIUS server and the client. The file used to keep the client list and secrets is the “clients” file.

Another file used by the daemon to store the users that are authenticated is the “users” file. The “user” file contains the RADIUS attributes associated with a particular user. As a

minimum, this file must contain the user's username and password (depending on the RADIUS server used).

To configure the RADIUS server, refer to your RADIUS host documentation. Xyplex Networks recommends that you use the Merit RADIUS server implementation. Information for the Merit RADIUS server can be found at <http://www.merit.edu>. Refer to the GOPHER SERVER and the MERIT Network Information Center for new releases.

Configuring RADIUS on the Access Server

In order to configure RADIUS, ensure that the access server has a minimum of 3-megabytes of memory installed.

To configure RADIUS authentication on your access server, complete these steps:

1. Create a copy of your present parameter file.

For example, copy the present file to a file called `paramold`. This copy can be used in the event that you need to restore your old parameters.

2. Insert the flash card supplied with your access server software kit or software update into the memory card slot.
3. Boot up the new image.
4. Enable RADIUS on the access server using the following command:

```
Xyplex>> DEFINE SERVER RADIUS ENABLED
```

5. Reboot the access server.
6. Confirm that RADIUS is enabled using the following command:

```
Xyplex> SHOW SERVER RADIUS
```

The system displays a screen similar to the following:

```

Xyplex>  SHOW SERVER RADIUS
AS/720 V6.0.1   Rom 4A0000 HW 00.02.00 Lat Protocol V5.2 Uptime: 0 04:31:26
                                     xx Mar 199x  20:28:29

RADIUS Primary Server:      140.179.248.145
Resolved Address:          140.179.248.145      Secret:  Configured

RADIUS Secondary Server:
Resolved Address:          0.0.0.0              Secret:  Default

RADIUS Port Number:        1645                Request Timeout (sec):  5
RADIUS Logging:            ENABLED              Chap Challenge Size:   16
RADIUS Server Retries:     3
RADIUS Ports Enabled:      2

Successful Logins:         4                    Configuration Failures: 0
Authentication Failures:  0                    Policy Failures:        0

Server access attempts
  Successful:              Primary      Secondary
  Failed:                  4           0
                          0           0

```

The Chap Challenge Size is the size of the challenge sent to the peer for Chap and to the RADIUS server for verification. Note, the peer should work with any size challenge. However, the current RADIUS servers only support challenge sizes of 16.

The following table describes the various RADIUS counters:

Field	Description
Successful Logins	Number of successful logins.
Authentication Failures	Number of rejections returned by the RADIUS Server.
Configuration Failures*	Number of failures returned by the RADIUS server due to incorrect values being entered for supported attributes.
Policy Failures*	<p>Number of failures returned by the RADIUS server due to a port being hard-configured for one type of RADIUS service-type, but the RADIUS server returned a different service-type.</p> <p>Policy failures also occur when the service-type selected by APD or Solicitation does not match the service-type returned by the RADIUS server.</p>

* These failures are local failures only and are not attributed to the RADIUS server. However, they may be a result of bad values from the RADIUS server that cannot be handled.

7. Check the primary/secondary RADIUS server host to ensure that the RADIUS server client database has been configured.
8. Define the client secret on the access server using the following command:

```
Xyplex>> DEFINE/SET SERVER RADIUS PRIMARY SECRET secret
```

NOTE: This secret must match the secret defined in the client file located on the RADIUS host.

9. Define the RADIUS primary server using the following command:

```
Xyplex>> DEFINE/SET SERVER RADIUS PRIMARY SERVER n.n.n.n
                                         domain name
                                         none
```

Where *n.n.n.n* is the IP address of the RADIUS server. When "none" is specified, the secret is reset to the default value.

NOTE: If you plan to use a secondary server, complete steps 8 and 9 again using the following commands:

```
Xyplex>> DEFINE/SET SERVER RADIUS SECONDARY SECRET secret
Xyplex>> DEFINE/SET SERVER RADIUS SECONDARY SERVER n.n.n.n
```

The secondary server is used when:

The primary server cannot be accessed.

The primary server rejects the authentication request (wrong password, no user record).

You can now enable RADIUS on the individual access server ports.

Defining RADIUS Authentication

RADIUS allows you to enable authentication on a per-port basis. The Service-Type used by a port can be selected in one of the following ways:

User Service-Selection — Uses either AutoProtocol Detect (APD) or RADIUS Solicitation modes to provide the Service-Type selection. These modes allow users to select a service explicitly by entering a choice at the solicitation prompt or implicitly by starting a protocol allowing APD to determine the protocol.

Access Server Service-Selection — Statically configure the port for a desired Service-Type (PPP, SLIP, Telnet, etc.). Once configured, this is the only service you can access.

RADIUS Service-Selection — Used when no service-type is configured using Access Service-Selection or User Service-Selection. The access server defaults to “Shell-User” but accepts whatever Service-Type is returned by the RADIUS server.

The following sections describe each Service-Selection method in detail.

User Service-Selection

The User Service-Selection uses either AutoProtocol Detect (APD) or RADIUS Solicitation modes to provide the Service-Type selection.

Using AutoProtocol Detect (APD)

For APD remote access login, the actual communication with the RADIUS server is held off until APD determines the protocol type being used. After the protocol is determined, the authentication is made with that protocol as the Service-Type. If a Service-Type other than the requested Service-Type is returned, the port is logged off (This is considered a policy failure.). If other attributes, such as Framed-Address are returned from a configuration record, they are applied to the current session only. Once the session is terminated, any parameters configured through RADIUS return to their original values.

Defining the RADIUS Solicitation Mode

The RADIUS Solicitation Mode allows you to configure individual ports to display a prompt before the username and password sequence. This prompt describes the Service-Type option and is used to determine what to send as the desired Service-Type to the RADIUS server. The access server sends the Service-Type to the RADIUS server. If the RADIUS server returns a Service-Type other than the Service-Type requested, the port is logged off.

To enable the RADIUS Solicitation Mode, enter the following command:

```
Xyplex>> DEFINE/SET PORT n RADIUS SOLICITS ENABLED
```

The port login sequence appears as follows:

```
Service-Type:
PPP=1, SLIP=2, Shell-User=3, Telnet=4, LAT=5
login (1-5):
Username>
Password>
```

To select a Service-Type, enter the corresponding number at the login: prompt. For example, to select the Service-Type Shell-User, enter the number 3 at the login: prompt.

Access Server Service-Selection

The Access Server Service-Selection mode operates when a Service-Type is defined on a port and no APD or RADIUS Solicitation is configured. Once defined, this Service-Type is the only service accessible.

Defining PPP and SLIP Authentication

To define PPP or SLIP on an access server port, use one of the following commands:

```
Xyplex> DEFINE PORT n PPP ENABLED  
Xyplex> DEFINE PORT n SLIP ENABLED
```

When an access server port has PPP or SLIP configured and RADIUS enabled, the access server sends the service type and frame protocol to the RADIUS server. The RADIUS server authenticates the information and returns the configuration information for the PPP or SLIP remote access login.

Your RADIUS authentication record must contain a service type of Framed-User and you must have Frame-Protocol PPP (or SLIP), or you are logged off the port. The following example shows an authenticated record returned from the RADIUS server.

```
Password = "password"  
User-Service-Type = Framed-User  
Framed-Protocol = PPP  
Framed-Address = 172.19.250.85
```

In this example, the Framed-Address returned by the RADIUS server is applied to the PPP link and is used as the remote IP address during PPP negotiations. No other address may be used by this PPP peer.

NOTE: If RADIUS is enabled on a port (not by PAP/CHAP), the port expects the username and password to be entered interactively.

Defining PPP PAP Authentication

To define PPP PAP authentication to an access server port, enter the following command:

```
Xyplex>> DEFINE/SET PORT n PPP PAP RADIUS|KERBEROS|ENABLED|DISABLED
```

The access server uses the RADIUS database to authenticate the username and password in a PPP PAP authentication request. The RADIUS server authenticates the user and returns the IP and/or IPX configuration information if it is contained in the user record.

NOTE: When using PPP PAP authentication, you may also have normal RADIUS authentication enabled. The result of this is that authentication occurs twice. Once for normal RADIUS and again for PPP PAP. When this occurs, the username and password may be the same or different but in either case, the Service-Type and protocol must be appropriate.

Defining PPP CHAP Authentication

To define PPP CHAP authentication to an access server port, enter the following command:

```
Xyplex>> DEFINE/SET PORT n PPP CHAP RADIUS|DISABLED
```

PPP CHAP provides dial-in users and attaching peers with an authentication method. This method is more powerful than PAP because no passwords are exchanged in the open.

You can also configure access server ports to require CHAP authentication for attaching PPP peers or to authenticate the access server to a peer. This is accomplished by defining a CHAP remote password that only the authenticator and peer know. This password is only used when the peer challenges the access server. CHAP may then periodically challenge the identity of the peer. To define the CHAP remote password, enter the following command:

```
Xyplex>> DEFINE/SET SERVER PPP CHAP REMOTE PASSWORD "password"
```

NOTE: The CHAP password defined on the peer should match the password field in the user record on the RADIUS server.

To define the period of time (in minutes) that a peer is re-challenged after the connection is established, enter the following command:

```
Xyplex>> DEFINE PORT n PPP CHAP CHALLENGE TIMER n
```

NOTES: A timer value of "0" disables this feature. You must log out of the port before this command is activated. This is the default value.

When using PPP CHAP authentication, you may also have normal RADIUS authentication enabled. The result of this is that authentication occurs twice. Once for normal RADIUS and again for PPP CHAP. When this occurs, the username and password may be the same or different but in either case, the Service-Type and protocol must be appropriate.

RADIUS Server-Selection

The RADIUS Service-Selection is the default service selection method used when no Service-Type is configured. When an authentication request is made to the RADIUS server, the Service-Type requested by the access server is the default; Shell-User (interactive login user). The RADIUS server selects the type of service that user is allowed to use based on the information in the user file for that username and password.

NOTE: If another Service-Type, other than Shell-User, is returned by the RADIUS server, it is accepted by the access server replacing the Shell-User default Service-Type.

To enable RADIUS authentication on an interactive port, enter the following command at the access server prompt:

```
Xyplex>> DEFINE/SET PORT n RADIUS ENABLED
```

Once RADIUS is enabled on the port, you are prompted for your username and password. To access the port, enter this information.

The configured RADIUS server authenticates your username and password, and sends the configuration record of the authenticated user back to the access server.

NOTE: As a minimum, the entry in the "User File" must contain the username and password for the RADIUS Service-Selection mode to work.

To confirm that RADIUS is enabled, enter the following command at the access server prompt:

```
Xyplex>> SHOW PORT n CHARACTERISTICS
```

The system displays a screen similar to the following:

```
Xyplex>> show port n characteristics

Port n:  rhw

Character Size:           8           Input Speed:           9600
Flow Control:            XON         Output Speed:          9600
Parity:                  None        Modem Control:         Enabled

Access:                  Local       Local Switch:          None
Backwards Switch:        None        Name:                  PORT_2
Break:                   Local       Session Limit:         4
Forwards Switch:         None        Type:                  Ansi
CCL Modem Speaker:       Inaudible    CCL Name:              None
APD Timeout:             Unlimited    APD Default: Interactive
APD:                     INTERACTIVE PPP SLIP
Dialout Action:          Logout

Preferred Service:  None

Authorized Groups:  0
(Current) Groups:  0

Enabled Characteristics:
Autoprompt, Broadcast, CHAP-Radius, Internet Connections, Line Editor,
Loss Notification, Menu, Message Codes, Outbound Security, Output Flow
Control, PAP-Radius, Radius, ULI, Verification

Xyplex>>
```

Displaying RADIUS Server Parameters

To display your defined RADIUS server parameters, enter the following command:

```
Xyplex> show radius
```

The system displays a screen similar to the following:

Xyplex> SHOW SERVER RADIUS		
AS/720 V6.0.1 Rom 4A0000 HW 00.02.00 Lat Protocol V5.2 Uptime: 0 04:31:26 xx Dec 199x 20:28:29		
RADIUS Primary Server:	140.179.248.145	
Resolved Address:	140.179.248.145	Secret: Configured
RADIUS Secondary Server:		
Resolved Address:	0.0.0.0	Secret: Default
RADIUS Port Number:	1645	Request Timeout (sec): 5
RADIUS Logging:	ENABLED	Chap Challenge Size: 16
RADIUS Server Retries:	3	
RADIUS Ports Enabled:	2	
Successful Logins:	4	Configuration Failures: 0
Authentication Failures:	0	Policy Failures: 0
Server access attempts	Primary	Secondary
Successful:	4	0
Failed:	0	0

The Chap Challenge Size is the size of the challenge sent to the peer for Chap and to the RADIUS server for verification. Note, the peer should work with any size challenge. However, the current RADIUS servers only support challenge sizes of 16.

The following table describes the various login fields:

Field	Description
RADIUS Primary Server	The RADIUS primary server used for authentication attempts. Valid values are text strings up to 51 ASCII characters, specifying a DNS host name or a valid IP address. The default value is no configured primary server or the null string "".
Primary Resolved Address	The resolved IP address for the primary server. When the RADIUS primary server is specified as a DNS name, the name must be resolved to an IP address. The default value is the address 0.0.0.0.
RADIUS Secondary Server	The DNS name of the RADIUS secondary server used when the RADIUS primary server is not used or available. The default value is no configured secondary server or the null string "".
Secondary Resolved Address	The resolved address of the RADIUS server used for user verification when the primary server does not respond. The default value is the address 0.0.0.0.

Field	Description
RADIUS Port Number	The UDP port that RADIUS user verification requests are transmitted and received from. The default UDP port is 1645.
Request Timeout	The time between RADIUS client retransmissions to the RADIUS server when trying to authenticate a user. The default value is 5 seconds.
RADIUS Logging	Controls whether the access server logs messages to the access server accounting log file. The default setting is disabled.
RADIUS Server Retries	The number of times a particular server is tried. These tries are in succession for RADIUS accounting. The default value is 3.
RADIUS Ports Enabled	A list of ports that have RADIUS enabled for either interactive or PPP use.
Successful Logins	Number of successful logins.
Authentication Failures	Number of rejections returned by the RADIUS server.
Configuration Failures*	Number of failures returned by the RADIUS server due to incorrect values being entered for supported attributes.
Policy Failures*	<p>Number of failures returned by the RADIUS server due to a port being hard-configured for one type of RADIUS service-type, but the RADIUS server returned a different service-type.</p> <p>Policy failures also occur when the service-type selected by APD or Solicitation does not match the service-type returned by the RADIUS server.</p>
Successful Server Access Attempts	The number of times the RADIUS server and the access server successfully exchanged messages.
Failed Server Access Attempts	The number of times the secondary RADIUS server and the access server failed to exchange messages.

* These failures are local failures only and are not attributed to the RADIUS server.

Monitoring RADIUS During Login

To monitor the port login process during login, enter the following commands and reboot the access server.

```
Xyplex>> DEFINE RADIUS LOGGING ENABLED
Xyplex>> DEFINE SERVER ACCOUNTING ENTRIES <1-1000>
Xyplex>> DEFINE SERVER VERBOSE ACCOUNTING ENABLED
Xyplex>> DEFINE SERVER VERBOSE PRIORITY 7
```

Flash Card Enhancements for V6.0.1

V6.0.1 includes the following flash card enhancements:

- **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 Xyplex Networks 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

NOTE: Earlier versions of the remote access server software 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 V6.0.1 or V6.0.2. 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 Xyplex Networks 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 Xyplex Networks home page on the World Wide Web (<http://www.xyplex.com>) or contact your Xyplex Networks sales representative or distributor.

- **4 and 8 Megabyte Formatting Options** V6.0.2 and V6.0.1 support new options for formatting 4 and 8 Megabyte flash cards. For more information on these options, refer to the section on [Flash Card Formatting Options](#).

Configurable Username and Password Prompts

You can now configure your username and password prompts. To do this, use the following command syntax:

```
SET/DEF PO # USERNAME PROMPT "string"
SET/DEF PO # PASSWORD PROMPT "string"
```

The default username/password prompt length is 26 characters.

If the server booted from the default parameters, the default values are, "Enter username>" and "Enter user password>."

If the server booted from an existing parameter file, the username prompt is, "Enter username>."

For the password prompt, the default value is "Enter user password>." However, if SecurID is enabled on the port, the default password prompt is "Enter PASSCODE:."

These new prompts are displayed in the SHOW PO ALT CHAR screen.

```

XYPLEX>> show port alt char
Port 0:  a                               05 Jan 1900  09:54:04
Resolve Service:      Any_Lat           DTR wait:      Disabled
Idle Timeout:         0                 Typeahead Size: 128
SLIP Address:         N/A              SLIP Mask:      N/A
Remote SLIP Addr:     N/A              Default Session Mode: Interactive
TCP Window Size:      256              Prompt:        X021812
DCD Timeout:         N/A              Dialback Timeout: N/A
Stop Bits:           N/A              Script Login:    Disabled
TCP Keepalive Timer:  N/A              Username Filtering: None
Nested Menu:         Disabled          Nested Menu Top Level: 0
Command Size:        132              Clear Security Entries: Disabled
Rlogin Transparent Mode: N/A          Login Duration: 0
Xon Send Timer:      N/A              RADIUS Accounting: Disabled
Username Prompt:     Enter username>
Password Prompt:     Enter user password>

```

The LINE EDITOR character display has been moved. To view the LINE EDITOR characters, use the following command:

```
SHOW PO LINE [EDITOR] CHAR.
```

```

XYPLEX>> show port line edit char
Port 0:  a                               05 Jan 1900  09:53:36
Line Editor Characters
Backspace Character:  ^D      Forwards Character: ^F
Delete Beg Character: ^U      Delete Line Character: ^X
End of Line Character: ^E     Begin Line Character: ^H
Previous Line Character: ^B    Next Line Character: ^N
Quoting Character:    ^V      Insert Toggle Character: ^A
Cancel Character:     ^Z      Redisplay Character: ^R

```

Outbound Port Security

The Outbound Port Security feature allows you to enable the RADIUS, Kerberos, Securid, or simple port password security features on remote or dynamic ports.

Outbound Port Security allows you to:

- Restrict access to telephone lines that connect to remote locations. It prevents the unauthorized use of dial-out lines and provides a monitoring trial (provided you have accounting enabled).
- Prevent unauthorized access to an async port of a device from LAN users.

Without this feature, these security mechanisms do not apply to remote or dynamic ports. You can enable only one security mechanism on a port. To enable the Outbound Port Security feature, use the following command:

```
DEFINE/SET PORT [port-list] OUTBOUNDSECURITY ENABLED
```

The default setting for this command is ENABLED. This is a privileged command.

Login Duration Timer

The Login Duration Timer feature allows you to limit the time a user can remain logged in to a port, regardless of the activity on the port. To define the login duration, use the following command:

```
DEFINE/SET PORT [port-list] LOGIN DURATION [timer]
```

The *timer* variable is the number of minutes in the range of 0 through 480. This is a privileged command that applies only to ports being used in local access mode.

The default setting is 0, which indicates that no login duration timer is assigned.

Kerberos Error Messages

The Kerberos Error Message feature allows you to specify the text in the Kerberos 739 error message. This error message appears when Kerberos authentication fails due to a communications failure. To specify the text in the Kerberos 739 error message, use the following command:

```
DEFINE/SET SERVER KERBEROS ERROR MESSAGE "character-string"
```

The "*character-string*" variable can contain up to 132 ASCII characters. The character string must be enclosed in quotes. This is a privileged command.

The default character string is "Please contact your system administrator."

Privileged Commands in Scripts

The new script keyword, #PRIVILEGE, allows the access server to execute privileged commands in a script file on a port that does not have Privileged mode set. This new keyword is useful when you want to execute privileged commands in a script, but you do not want to include the privileged password in the script. When a script includes this keyword, the access server executes any subsequent privileged commands. When the script execution completes, the port reverts to the privilege level that was enabled prior to the script execution. This keyword cannot be abbreviated.

PPP Port Mapped to Several Internet Addresses

A mask has been added that allows one PPP port to be mapped to a small subnet of Internet addresses. This subnet is specified by logically ANDing the mask and the remote IP address.

To configure a PPP mask, use the following command:

```
SET/DEFINE PORT PPP INTERNET|IP MASK internet-address
```

where the internet-address is in the format 255.255.255.255.

The SHOW/LIST/MONITOR PPP INTERNET CHARACTERISTICS is modified to include a new label "IP Mask:" followed by the IP mask value.

For example, if a customer wants to have four devices off of the PPP link, then the PPP IP MASK is 255.255.255.252, which is 0xFF FF FF FC, and the Range would include 4 addresses. This works when the PPP IP MASK is more restrictive than the access server's subnet mask, and the PPP IP addresses are within the same subnet as the access server.

The default PPP IP MASK is 255.255.255.255.

PPP Local Address Range

A local PPP address range may be defined that prevents remote clients from overwriting the local address if it has been left undefined (0.0.0.0). To define a local PPP address range, use the following command syntax:

```
DEFINE/SET PORT n PPP IP LOCAL ADDRESS RANGE n.n.n.n - x.x.x.x
```

The default value is 0.0.0.0 - 255.255.255.255.

TN3270 Enhancements

TN3270 Default Port

The TN3270 Default Port feature allows you to define a default port number for TN3270 sessions. If you do not define a default, the access server uses the Telnet default port, port 23. To define a TN3270 default port, use the following command:

```
DEFINE/SET PORT [port-list] TELNET TN3270 DEFAULT PORT port-number
```

The valid values for the *port-number* variable are 1 through 32767. This is a privileged command.

The default value is 23.

Keymap Command DevCncl Used to Cancel Queued Print Requests

A TN3270 keymap command called “DevCncl” (device cancel) has been added that allows TN3270 users to cancel a queued print request.

When the printer is busy, the user can cancel the request and unlock the keyboard. Hitting the device cancel key when a printer is not busy or when no jobs are queued, functions as a no operation. That is, the device cancel key has no effect.

To define a device cancel key, enter the following syntax:

```
DEFINE SERVER TN3270 DEVICE (name) KEYMAP DEVCNCL "escape sequence" "description"
```

There is no default value for this item.

ExitReset Screenmap Command

A TN3270 screenmap command called “ExitReset” sends up to a 9 hexadecimal command string to the terminal when a TN3270 session is terminated.

The EXITRESET screenmap is executed only upon termination of the TN3270 session and after the four RESET strings have been transmitted to the terminal.

To define an ExitReset command, enter the following syntax:

```
DEFINE SERVER TN3270 DEVICE (name) screenmap exitreset "up to 9 hex values"
```

There is no default value for this item.

Time Server Enhancement

A new configurable command that specifies where the access server obtains the time.

When an access server has a configured time server, the access server shortly after it boots does a directed UDP query for TIME service to the Time server. If there is no response, and the time server is ENABLED (Not Required), there is an attempt to get the time from other servers according to the following priority:

Time Server (via UDP port 37)

Kerberos Server(s)(via UDP port 37)

SecurID Server(s)(via UDP port 37)

XMOP/MOP load server

UDP Broadcast (via UDP port 37)

Clock starts at zero

Time, Kerberos, or SecurID servers are configurable together but implemented as mutually exclusive with regard to querying for the time. If both the Time and Kerberos Servers are defined, then only the Time Server is used. If both the Time and SecurID servers are defined, then only the Time Server is used. If no Time server is defined but a Kerberos and SecurID servers are defined, then the Kerberos servers are used. If no Time and no Kerberos server are defined but a SecurID server is defined, then the SecurID server is used.

Daily there is an attempt to resynchronize with the TIME SERVER at 2:00 a.m, just as there currently is an attempt to resynchronize with Kerberos or SecurID Time Servers.

Servers which run Kerberos or SecurID should have the Time Server address set to 0. Kerberos works with a configured Time Server matching the Primary Kerberos Server. However, if the customer has a secondary Kerberos Server, the secondary Kerberos server never is queried for the time if the Time Server is non-zero.

Once the time is obtained by one of the methods listed above, the time server is saved in the value labeled "Time Received From:" in the SERVER ALTERNATE STATUS display.

The command syntax is as follows:

```
SET/DEFINE SERVER TIME SERVER ENABLED | REQUIRED n.n.n.n
SET/DEFINE SERVER TIME SERVER DISABLED
```

If the timer server is required, only this time server is used to obtain the time. On failure, a repeat every minute to request the time from the required server occurs. If the time server is ENABLED, then this server is tried first before the other servers. Repeated attempts are made to query that server for one minute before checking time by other methods. A time server of zero and/or DISABLED means the time server is not used.

When the command is SET and the Time Server is ENABLED or REQUIRED, an immediate query time call to that time server occurs. Repeated attempts are made to query that server for one minute or until a response is received.

NOTE: The SET SERVER TIME SERVER DISABLED does not disable the time server until the next resynchronization time, or 2:00 a.m. This may result in an extra broadcast going out at resynchronization time, or 2:00 a.m.

Only the DEFINE SERVER TIME ZONE command is implemented. The SET SERVER TIME ZONE command is ignored.

Longer Username Support

The access server software supports the following username lengths:

RADIUS authentication, the username can be up to 121 characters.

Kerberos, the username can be a maximum of 119 characters (bytes), consisting of three sections of a maximum of 39 bytes each in the form "username.instance@realm."

SecurID authentication, the username can be up to 32 characters.

All displays which show the username continue to print only the first 16 characters.

NOTE: When PAP is enabled, PAP usernames are restricted to 16 characters. Also when a port name is defined for a port, the defined 16 character username is used, rather than asking for a new name.

V6.0 Features

Features in V6.0 provide enhancements and problem fixes for V5.3.1 and V5.3. V6.0 also provides all the features in V5.3.1 and V5.3. For a list of problem fixes, refer to the [Problems Fixed Section](#).

MIB Support for New Variables

Xyplex Networks MIB kit 6-3 (and later MIB kits) contains Simple Network Management Protocol (SNMP) MIB support for new PPP, IPXCP, and Auto Protocol Detect (APD) variables.

Stampede™ Remote Office™ Support

Beginning with Access Server V6.03, Xyplex Networks will no longer support Stampede Remote Office and will no longer include a demonstration version of it.

Future Support for 1-Megabyte Units

With the shipment of V6.0, the 1-Megabyte images are full and Xyplex Networks can no longer add new features to the software load images that run on 1-Megabyte access servers. As a result, V6.0 is the last release to contain changes and enhancements to the 1-Megabyte load images.

In addition, Xyplex only plans to continue distribution of these access server load images on a request basis. However, 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 Xyplex Sales representative or distributor.

Future Support for 2-Megabyte Units

With the shipment of V6.0.1, the 2-Megabyte images are full. Xyplex can no longer add 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.

Xyplex Networks 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 Xyplex Networks Sales representative or distributor.

Software Kit Changes

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

CD-ROM kits:

Software kits in ISO-9660 compatible CD-ROM format are now available.

Print filters and related files no longer distributed:

The following files have been removed from access server software kits:

`xyp_filter.c`

`xyp_interface.sys5`

`xyp_printcap.bsd`

`xyp_ptyd.c`

`xyp.mk.`

These files have been replaced by the `csportd` daemon.

The following access server load images are no longer distributed by Xyplex Networks:

`mx1400.sys`

`npc11t.sys`

`tsj81t.sys`

`tsj8t2.sys`

`tslj161.sys.`

Beginning with this Kit (Kit 13), Xyplex Networks no longer distributes the following access server load images:

`mx1500.sys`

`tsmj81t.sys`

DEC Alpha Workstation Supported for Load/Parameter/Dump Serving

In Access Server Kit CS12, Xyplex Networks 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 Xyplex Networks Sales Representative or Distributor.

1710 TCP/IP-LAT Gateway Software to be No Longer Supported

Beginning with Kit 15, Xyplex Networks will no longer support the 1710 TCP/IP-LAT Gateway software.

Restrictions and Notes

The following restrictions and notes should be read and followed before upgrading to V6.0.2.

Saving the Parameter File

CAUTION

V6.0.1 parameter files are not backwards compatible with parameter files for previous versions of Multiprotocol Access Server software.

Xyplex Networks recommends that you save a renamed copy of your parameter file on the network or on separate media before you upgrade to V6.0.2.

Upgrading to V6.0.2 overwrites the existing parameter file on the parameter servers. The saved copy of your parameter file is needed to reload an earlier version of Multiprotocol Communication Server software when necessary.

Using the CARDCOPY Command

The access server does not support the use of the CARDCOPY command between a traditional flash card and a series 2 flash card, or between cards of different sizes (for example, 2 and 4-Megabytes). Attempting to use the CARDCOPY command under these conditions produces the following errors:

```
Xyplex - 778 - I/O error 101, media type conflict
```

```
Xyplex - 778 - I/O error 102, media size conflict
```

To copy the contents of a traditional flash card to a series 2 flash card, first use the FORMAT CARD command to format the Series 2 card, then use the COPY command. For example:

```
COPY "/MC/SYSTEM/AREA2/xpcs00s.sys" "/MC/SYSTEM/AREA2/xpcs00s.sys" AREA 2
```

Insert the destination card and press any key to continue.

To download images and the loader file, `mcffsl.sys`, to a Series 2 flash card, use the GET CARD LOAD FILE command. For example:

```
GET CARD LOAD FILE "/xyplex/xpcs00s.sys" 172.19.12.101
```

The GET CARD LOAD FILE command does not copy parameter files. Before you use either the COPY or GET CARD LOAD FILE commands with a series 2 flash card, format the card first with the FORMAT CARD command. For more information about these commands, refer to the [Software Installation Guide for Xyplex Loader Kits \(420-0392\)](#).

Auto Protocol Detect and Script Logins

AutoProtocol Detect (APD) only executes Login Scripts for Interactive ports. The access server does not execute Script Logins when APD sets the port to either AppleTalk Remote Access Protocol (ARAP), Compressed Serial Link Interface Protocol (CSLIP), Serial Link Interface Protocol (SLIP), or Point-to-Point (PPP). To avoid this situation, do not use script logins on APD ports.

Flash Cards with Redundant Parameter Areas

The following types of Xyplex Networks products can use flash cards formatted with a redundant parameter directory:

- Network 9000 10BASE-T Concentrators and Bridge/Router modules running V3.1 or greater.
- Network 9000 Access Server 720 modules running V4.4 or greater
- MAXserver 1608A, 1620, and 1640 Access Servers running V4.4.1 or greater

These products can also use flash cards that are not formatted with a redundant parameter directory.

Note on Using Flash Cards

Network 9000 Access Server 720 modules can obtain a software load image and parameter file from a flash card. These modules can also provide load images for clients on the network, and act as parameter servers for clients. However, beginning with V6.0.1, this functionality requires 4 Megabytes of memory.

Flash Card Formatting Options**CAUTION**

Before reformatting a flash card, back up any software images that are on the card to another load server. This allows you to copy them back onto the flash card after reformatting.

After reformatting the card, use the DEFINE command to copy the units parameters to the card (that is, issue the command `DEFINE PORT 1 TYPE ANSI.`). Do not power off the unit before it has finished copying its parameters onto the reformatted flash card.

Multi-Megabyte images support four options for formatting flash memory cards. These options allow you to format a card with more areas of lesser size or fewer areas of greater size.

For example, to accommodate a large software load image, you need to format a card for two larger areas rather than four smaller areas. To do this, use the `FORMAT CARD` command with the `NONREDUNDANT` keyword. For example:

```

Xyplex>  FORMAT CARD  [OPTION 1] [NONREDUNDANT]
                        [OPTION 2]
                        [OPTION 3]
                        [OPTION 4]

```

By using the FORMAT CARD command with the NONREDUNDANT keyword, the flash card releases an additional 256 Kbytes of memory on a 1 or 2 Megabyte flash card. This eliminates the redundant parameter area.

NOTE: Xyplex Networks recommends that you do not use this option under most conditions because parameters could be lost during a power outage.

The following table shows the size of each area on a flash card when you use Options 1, 2, 3, and 4 to format the card. Issuing the FORMAT CARD command without specifying any options, the command defaults to Option 1.

Card Type	Option 1 Area Sizes (Kbytes)	Option 2 Area Sizes (Kbytes)	Option 3 Area Sizes (Kbytes)	Option 4 Area Sizes (Kbytes)
1 MB Card with redundant parameter storage	Area 1: 64 Area 2: 197 Area 3: 262	Area 1: 64 Area 2: 459	Area 1: 64 Area 2: 459	Area 1: 261 Area 2: 786 (no parameters)
1 MB Card without redundant parameter storage	Area 1: 64 Area 2: 197 Area 3: 524	Area 1: 64 Area 2: 721	Area 1: 64 Area 2: 721	Area 1: 261 Area 2: 786 (no parameters)
2 MB Card with redundant parameter storage	Area 1: 64 Area 2: 197 Area 3: 786 Area 4: 524	Area 1: 64 Area 2: 983 Area 3: 524	Area 1: 64 Area 2: 1507	Area 1: 261 Area 2: 1834 (no parameters)
2 MB Card without redundant parameter storage	Area 1: 64 Area 2: 197 Area 3: 786 Area 4: 786	Area 1: 64 Area 2: 983 Area 3: 786	Area 1: 64 Area 2: 1769	Area 1: 261 Area 2: 1834 (no parameters)

Card Type	Option 1 Area Sizes (Kbytes)	Option 2 Area Sizes (Kbytes)	Option 3 Area Sizes (Kbytes)	Option 4 Area Sizes (Kbytes)
4 MB Card with redundant parameter storage	Area 1: 64 Area 2: 1507 Area 3: 1572	Area 1: 64 Area 2: 458 Area 3: 1048 Area 4: 1572	Area 1: 64 Area 2: 3079	Area 1: 524 Area 2: 3669 (no parameters)
8 MB Card with redundant parameter storage	Area 1: 64 Area 2: 1507 Area 3: 1572 Area 4: 2096 Area 5: 2096	Area 1: 64 Area 2: 983 Area 3: 1048 Area 4: 2621 Area 5: 2621	Area 1: 64 Area 2: 1507 Area 3: 2621 Area 4: 3145	Area 1: 524 Area 2: 7862 (no parameters)

Flash Card Vendors

For the most up-to-date list of flash card vendors, refer to the Xyplex Networks home page on the World Wide Web located at <http://www.xyplex.com>.

Reply Message String Limited to 97 Characters

With logging enabled, a reply message string received that is greater than 97 characters (96 + NULL) causes the client server to crash. To correct this problem, restrict reply message strings (defined in the user record) to 97 characters or disable logging on the client server.

Notes on SNMP

The following sections provide general SNMP information.

NOTE: At the current time there is no RADIUS MIB and as a result SNMP does not support RADIUS.

MIB Support for New Variables

Xyplex Networks MIB kit 6-3 (and later MIB kits) contain SNMP MIB support for new PPP, IPXCP, and APD variables.

Performance Impact of SNMP Get Next Processing

Intense use of SNMP Get Next processing may degrade access server performance.

IP Routing Tables

You can add more than one entry with the same destination to the IP routing table. However, SNMP returns only one of the entries.

SNMP GET and SET Processing and Access Server Databases

SNMP GET processing reads the operational database. SNMP SET processing modifies both the operational and permanent databases. If the unit is managed by SNMP, you may want to keep all ports Non-privileged or Secure. This reduces the possibility of the permanent and operational databases becoming unsynchronized. In the case of tables with a variable number of entries, such as local services or domain names, this is particularly significant.

The port security table and the menu table are accessed by an index number that may or may not point to the same data item in the two databases.

Creating and Deleting Entries in SNMP Tables

Use the following guidelines to create and delete SNMP table entries:

- To create an SNMP entry:

Send an SNMP *set request* with a unique (non existent) objectId, and the table status value set to valid.

The objectId contains the keys needed to create the table entry. No other values are required to create the entry. Any additional values needed are given defaults by the agent.

Any table item that is part of the Key is set read-only to prevent conflicting entries. Most Keys in standard MIBs are read/write.

- To delete an SNMP entry:

Send an SNMP *set request* with the objectId of the table entry you want to delete, and the table status entry set to invalid.

The tables affected by these guidelines are:

- latOfferedServiceTable
- lpdQueueTable
- namedTable (domain names)
- portSecurityTable
- parameterServerTable
- clientTable
- rotaryTable
- tn3270DeviceTable
- tn3270LanguageTable
- networkLoginServerTable

SecurID Notes

Xyplex Network's SecurID client software is based on V1.1 of the ACE/Server software supplied by Security Dynamics Technologies, Inc. The SecurID client software operates with ACE/Server host running ACE/Server software V1.1, or later.

AppleTalk Remote Access (ARAP) Notes

The following notes apply to the ARAP implementation:

- When there is no TFTP script server available on the network, Command Control Language (CCL) scripts and dial back scripts are unavailable.
- ARAP supports only one login password that is shared by all ARAP users. When Kerberos or SecurID authentication is performed, a username may be used that has an associated password and/or passcode.
- When Kerberos or SecurID authentication is not used, the server does not restrict access by user name. A user can login through Remote Access using any user name as long as the user specifies the correct server password. Specific user names are only used for locating a telephone number for dial back.
- To prevent AppleTalk "name collisions," do not have more than one Remote Access Server with a given name on an AppleTalk network.

CCL Notes (Using Modem-Based Compression)

The following notes apply to the CCL Notes:

ARAP connections cannot use modem-based compression. Compression must be done by the communication server. Typically, CCL scripts contain commands that prevent the modem from negotiating V.42 LAM-M error correction or V.42bis compression. To use modem-based V.42 LAM-M error correction or V.42bis compression for connections that are made using particular protocols (excluding AppleTalk Remote Access Protocol (ARAP)), use CCL scripts which permit this feature to be negotiated. For more information about using CCL scripts, refer to the [Configuring Access Serving Features guide](#).

Modem-based MNP error correction is not supported on ports using CCL scripts.

CCLs are not supported on a port with RADIUS Authentication enabled.

APD Notes

To use APD, the access server port must be configured with PORT ACCESS set to LOCAL or DYNAMIC (applies only to dial-in connections).

To enable APD and have the APD prompt display on a specific port, use the following command:

```
DEFINE PORT APD PROMPT ENABLED|DISABLED
```

The default prompt is “”.

Fixed Problems

This section describes the problems that have been resolved with V6.0.3, V6.0.2, V6.0.1 and V6.0.

Problems Fixed in V6.0.4

Problem Writing to Series II Flashcards with 1608B Terminal Servers

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

Solution: V6.0.4 has corrected the problem. 1608B Terminal Servers can now write to a Series II Flashcard.

Problem Calculating Leap Year

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

Solution: V6.0.4 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: V6.0.4 has corrected the problem.

Problems Fixed in V6.0.3

Error Displays

Problem: Errors displayed (or those that do not need to be displayed) when setting/defining a combination of port accesses, and protocols such as PPP, SLIP, CSLIP, APD, and ARAP.

Solution: V6.0.3 will now display the correct error messages.

PPP Port Logout

Problem: Port set-up as Dynamic with PPP to have a CCL on that port dial out and the modem would logout the port in 120 seconds.

Solution: V6.0.3 will now support the above configuration.

Line Printer Daemon and AIX Machine

Problem: AIX queues were being reported as down. Running a trace would show that AIX had sent a SYN, the job completed and then sent another SYN within the same second of each other. The Access Server was assigning the same sequence numbers in response to the SYNs. This caused the AIX and Access Server to send ACKs back and forth trying to correct this.

Solution: A code change has been made with V6.0.3 which increments the sequence number once every 5 microseconds.

IP Address Resolution by DNS Server

Problem: When a user defined or set a RADIUS server (if defined as a domain name) and the DNS server was not reachable, the IP address did not get filled in and RADIUS authentication would not be completed. The system would not try a new query to the DNS Server even after a reboot.

Solution: At initialization time, the system sends a RADIUS Accounting query out to the network (even if RADIUS Accounting is disabled). The system queries the DNS server on every RADIUS request for IP resolution. If the DNS server is down at initialization time, then another query is done for each authentication if the RADIUS IP resolved address is 0.0.0.0.

SNMP BasicPortIndex

Problem: If an SNMP “walk” was attempted, the output would go into an infinite loop.

Solution: V6.0.3 includes a fix to resolve this problem.

Accounting Log - Invalid Parameter Server Reply Message

Problem: The following message was displaying over and over in the Accounting Log:

`“Xyplex - Ignoring Invalid Parameter Server Reply - 0.0.0.0.”`

This problem occurred because a BOOTP reply was being sent to the broadcast address on the network.

Solution: V6.0.3 has been modified to not respond to a BOOTP reply if sent to the broadcast address.

RADIUS Attributes - Service-Type and Framed-Protocol

Problem: Xyplex Networks required the following RADIUS attributes to be present in the Access-Accept packet from the RADIUS Host (on some implementations):

- Service-Type
- Framed-Protocol

This resulted in the server not authenticating the user and the port was logged out.

Solution: Per the RADIUS specifications, these attributes are not required. V6.0.3 has been changed to reflect this.

RADIUS Authentication - Framed Compression

Problem: Livingston V1.16 and all versions of Merit send back a Framed-Compression = None if Framed-Compression = Van-Jacobson-TCP-IP has not been included in the user’s entry in the Users file. When this problem occurred, Xyplex would flag it as an unsupported RADIUS attribute and deny authentication.

Solution: V6.0.3 includes a code change that does not flag Framed-Compression as unsupported and allows authentication to continue.

Securid - Entering New PIN Mode

Problem: A user logged in to Securid and entered their passcode (6 to 8 digits). The user was then prompted to enter a new PIN. When they entered a 7- or 8-digit number, it was stored in “inbuf” but got truncated to 6 digits. When the user confirmed the new PIN by entering the new 7 or 8 digit number, the login would fail.

Solution: In V6.0.3, truncation no longer occurs. The field length was changed to 16 digits. The 16-digit length was used because on a normal login, the user can potentially enter up to 16 digits (e.g., 8 for the PIN and 8 for the Passcode).

Show Server Securid Display

Problem: When Securid and APD (in interactive mode) were enabled on a port, the SHOW SERVER SECURID screen would display 3 additional Logins without Securid for every successful login. This occurred because the code was counting each carriage return for going into interactive mode with APD as a login.

Solution: The code has been changed to not count the carriage returns as logins.

Packet Rejection Message

Problem: Once in awhile, a PPP LCP Packet was received that had a 0 length for the options header. This caused the Access Server to go into an infinite loop.

Solution: During normal PPP LCP negotiations, a packet is rejected if the options header has a length of 0, and a new packet is sought. If this packet is accepted, the PPP negotiations proceed. The following message will now display in the Accounting Log (if Verbose priority is set to 5 or above) when a packet is rejected:

LCP - Received Bad Structured Frame

If Kerberos or Securid is in use then the username and port number will also display. If no security or PAP is in use, then only the port number displays with the message.

Problems Fixed in V6.0.2

Access Server Hangs When Running IP Filtering

Problem: The access server could hang when running IP filtering on a busy network.

Solution: This problem has been corrected and IP filtering can be run on any network without problems.

Ports Hang in WAIT INPUT State

Problem: A port configured with a DEDICATED SERVICE, AUTOCONNECT, and AUTOHANGUP enabled, go into a WAIT INPUT state if the service is not available.

Solution: The failed connection to the unavailable service is tried for a number equal to the Access Server Password Limit. If all retries fail, the port is logged out.

IPX IEEE 802.2 Packet Causes Crash

Problem: If an Ethernet frame type of IEEE802.2 is defined on the access server, the server crashes when the first IPX packet is received.

Solution: IPX packets in an IEEE 802.2 form are now correctly processed.

RADIUS Attribute Idle-Timeout

Problem: When the RADIUS attribute “Idle-Timeout” is given a value of zero, which means the idle timeout on the port is disabled, the bogus syslog message “invalid entry of zero” is logged.

Solution: A default Idle-Timeout value is now accepted and correctly processed by RADIUS.

ARAP Crash

Problem: Occasionally, an ARAP Link Acknowledgment (LA) received with an acknowledgment number less than the expected value causes the access server to crash.

Solution: This type of LA is now correctly treated as a duplicate.

SecurID Failure

Problem: A port with SecurID, DYNAMIC ACCESS, and APD does not prompt the user for the SecurID username or passcode.

Solution: The user is now correctly authenticated via SecurID.

Active User and Active Ports

Problem: The Active User and Port counters incremented twice when a user logged into a port using RADIUS.

Solution: These counters are now only incremented once.

APD/ARAP

Problem: When the DEFINE PORT ALL APD DISABLE command is issued, the error “Option Conflict” is given for the protocol ARAP.

Solution: The ARAP protocol byte is now correctly zeroed when ARAP is enabled on the access server.

APD Timeout

Problem: On a port with DYNAMIC ACCESS and APD TIMEOUT, the APD timer would not expire for two minutes in all cases.

Solution: The APD TIMEOUT value is now correctly set when modem signals are asserted on the port.

Windows95 with GET CARD Command

Problem: A GET CARD LOAD FILE issued to a Windows95 PC most often fails with a TFTP timeout error.

Solution: The access server now correctly sends an acknowledgment for the final data packet and the TFTP file transfer completes successfully.

PPP Negotiations Fail When a Port Has PPP and RADIUS Enabled

Problem: On a port with PPP, RADIUS, and an IDLE TIMEOUT enabled, the IDLE TIMEOUT begins counting down as soon as the port logged out. This causes the next PPP user to fail when trying to dial in.

Solution: The IDLE TIMEOUT is now correctly started when the port detects a modem signal.

“Local Accesses” Counter Does Not Increment When Using PPP/SLIP

Problem: The “Local Accesses” counter typically gets incremented by 1 every time an interactive user logs into a port. However, if the port is in PPP/SLIP mode, the counter Does Not get incremented.

Solution: The incrementing of the “Local Accesses” counter, for ports in PPP/SLIP mode, is not supported. As before, Local Accesses on a Show Port Counters screen only get incremented for interactive logins.

Problems Fixed in V6.0.1

The following problems have been fixed with the V6.0.1 release.

Ping Not Working for a Host on a Different Subnet

Problem: This problem is caused by the access server not looking at the subnet bits in a received IP packet. When a host from a different subnet sent an IP packet to the access server, if the host bits of the source address were all one's, the Xyplex Networks access server incorrectly discards the packet thinking it is a broadcast packet. For example:

```
AS----->GW----->Host
194.64.183.251                194.195.192.199
MASK 255.255.255.248
```

The Host is the broadcast address for the AS.

Solution: The IP code now looks at both the subnet and host portions of an IP address when determining what is a broadcast address.

Modems Echoing Error “Xyplex – 702” Causing the Access Server to Hang

Problem: The access server hangs, resulting from a modem echoing the “-702- error” message from the port back to the modem. This occurs when a user at a “remote” modem escapes to local command mode by entering the Escape to Local Command Mode sequence (+++ is the normal default), and then hangs up their local modem via “ath.” The modem connected to the Xyplex Networks access server then sends the “+++” to the port. This is an invalid token and the command parser can not parse the token, generating a “702 error”

followed by a list of valid commands. In the list of valid commands there are occurrences of the string "AT." This causes the modem to echo back "OK" or "ERROR" to the port and the modem and port become locked in an infinite loop.

Disabling local echo on the modem prevents this problem. However, when you execute a CCL script, the CCL init string enables local echo on the modem so the script can execute.

Solution: If modem control is enabled and the modem has DCD deasserted when the 702 error is generated, the port is logged out.

Syslogd Messages Not Sent When the IPX Frame Type is Set to 802.3

Problem: Syslogd messages are not sent when the access server IPX frame type is set to 802.3.

Solution: The syslogd messages are now sent when the access server IPX frame type is set to 802.3.

Idle Time Causing Kerberos Error 62 (Bad Password) and Error 37 (Clock Skew Too Great)

Problem: This problem occurs after the user has entered a username, and then sits idle at the "Enter User Password>" prompt for more than 5 minutes. This causes the access server software to use incorrect time information when communicating with the Kerberos authentication server. The Kerberos authentication server then fails to authenticate the user because the access server's time is not synchronized with the authentication server's time.

Solution: The access server now uses the current time when sending authentication information to the Kerberos authentication server.

Non-Privileged Users Able to Enable or Disable PPP PAP Authentication

Problem: A non-privileged user could connect interactively and disable PPP PAP authentication, and then establish a PPP connection without PAP authentication.

Solution: The following command has been made a privileged command:

```
DEFINE/SET PORT PPP PAP ENABLED/DISABLED
```

Documentation Clarifications

The following section provides clarifications and additions to the following documents:

Commands Reference Guide

This guide incorrectly indicates that you can create a maximum of eight TN3270 devices. The correct number is 20.

MAXserver 1620/1640 — Installation of SIMM Memory (451-0044A)

On Page 4 of this guide, Step 6 describes holding SIMM memory chips “facing the rear.” This should read, “facing the front.”

In Figure 4 on Page 6, the top of the SIMM angled 30 degrees toward the front should be angled 30 degrees toward the rear.

Software Installation Guide for Xyplex Loader Kits (420-0392)

On a MAXserver 1620/1640, loading and parameter service are enabled by default. To disable loading, either remove the flash card or disable both loading and parameter service, using the following commands:

```
DEFINE SERVER MANAGER LOAD DISABLED  
DEFINE SERVER MANAGER PARAMETER SERVICE DISABLED
```

If you only issue the DEFINE MANAGER LOAD DISABLED command, loading appears to be disabled in the SHOW/LIST MANAGER CHARACTERISTICS display but this function is still enabled.

Using the Multiprotocol Access Server

This manual should indicate that when using Multisessions, queued connections requests are aborted if the user selects another window and enters data in at the keyboard.

Obtaining Load Images for Multi-Megabyte Servers

NOTE: If you are loading a MAXserver 1600 Access Server from a flash card that contains a V2.6 (or later version) of the flash card loader file, you do not need to perform the procedures described in this section.

The procedures contained in this section do not apply to the Network 9000 Access Server 720 and MAXserver 1608A, 1620, and 1640 Access Servers.

Many keyed software features are supported only on Xyplex Networks units that contain a minimum of two megabytes of memory. Therefore, the unit must run a Multi-Megabyte load image (`xpcs00c.sys` and `xpcs00s.sys` are covered in this section) in order to use these features.

When you initialize an access server, it automatically obtains a load image from a network load host, a Xyplex Networks loader, a diskette, or a flash card, depending on the access server model and its configuration. For some access servers, the default load image is an image that can run on a unit with only one megabyte of memory. The 1-Megabyte or default load image does not contain the additional features that are contained in the enhanced or Multi-Megabyte load images.

The [Software Kit Information CD](#), supplied with your software kit, lists the default load image name for each access server type.

The following table, lists the access servers that have optional Multi-Megabyte load images available to them instead of the default 1-Megabyte load image. The load image `xpcsrv20.sys`

is the default image for the Network 9000 Access Server 720 and MAXserver 1608A, 1620 and 1640 Access Servers. This image includes all the enhancements in the load image for Multi-Megabyte access servers.

Product	Multi-Megabyte Load Image Name
Chassis-Based Access Servers:	
MX2120	xpcs00c.sys
MX2220	
Standalone Access Servers:	
MX800	xpcs00s.sys
MX1120	
MX1520	
MX1600 (See Note above)	
MX1608	
MX1820	

To obtain the enhanced load image for these access servers, specify the new image name for the access server and initialize the server with that image.

To determine the amount of memory on the access server, use the SHOW SERVER ALTERNATE STATUS command. The memory amount appears in the Installed Memory field.

If your implementation uses “tokens,” you change only the image name on the Xyplex Network’s loader or the Network Control Protocol (NCP) database of the MOP loader. Tokens specify that a Xyplex Network’s loader determine the appropriate load file based on the access server’s hardware type, or that a MOP loader determine the appropriate load file based on the contents of the NCP database.

If your implementation requests a specific load image name, you must also change the load image name through the ROM configuration menu.

The following Sections describes how to obtain the new load image and how to change the load image name.

MX2120 and MX2220 Chassis-Based Access Servers

MX2120 and MX2220 chassis-based access servers obtain the load image from a UNIX host, VAX/VMS host, or Xyplex Networks loader. To obtain the new load image, xpcs00c.sys:

Load the new software on the host.

Change the load image name in the host’s client table or the Xyplex Networks loader’s client table. For more information about changing load image names, refer to *Software Installation* on CD.

Standalone Access Servers

Standalone access servers use different procedures to obtain the new load image, xpcs00s.sys.

MAXserver 800

The MAXserver 800 with 3 Megabytes of installed memory can support the enhanced load image for Multi-Megabyte access servers. However, you must enter a password or “key” to enable the image. The following example shows how to enter the key to enable the enhanced load image. To obtain a key, contact your Xyplex Networks sales representative or distributor.

The MAXserver 800 Access Server obtains a load image from a UNIX host, VAX/VMS host, or Xyplex Networks loader on the network. The factory default, 1-Megabyte image for this unit is `mx800.sys`. To obtain the new load image, `xpcs00s.sys`:

1. Load the new software on the host.
2. Change the load image name in the host's client table or the Xyplex Networks loader's client table. For more information about changing load image names, refer to *Software Installation* on CD.

After you install the additional memory, and you have obtained a key to load `xpcs00s.sys`, perform the following:

1. While the MAXserver 800 is running with the `mx800.sys` load image, enter the `DEFINE SERVER SOFTWARE` command with the enhanced load image name at the command interface:

```
Xyplex>> define server software xpcs00s.sys
```

2. Initialize the access server.

After initialization is complete, the interface prompts you for a username, and then prompts you to either specify `mx800.sys` from the configuration menu, or enable the enhanced load image. It also displays the command you used to enable the enhanced load image, `DEFINE SERVER PROTOCOL MX800 ENABLED`.

```
Enter Username> chris
```

Warning! MX800 has no protocols enabled.

Return to configuration menu and pick `mx800.sys` as load image or enter `DEFINE SERVER MX800 ENABLED` and supply correct password

```
Xyplex>
```

3. Set the privilege level of the port to Privileged. To do this, enter the `SET PRIVILEGE` command at the access server prompt:

```
Xyplex> set privilege
```

You are prompted for a password.

4. Enter a Privileged password at the access server prompt. The default password is `SYSTEM` but the password on your access server may be different. When you enter the password, it is not displayed on your screen.

```
Enter password> xxxxxx
```

Welcome to the Xyplex Communications Server
For information on software upgrades contact your local representative,
or call Xyplex directly at

In USA: (800) 435-7997

In Europe: +44 81 759-1633

In Asia: +65 225-0068

Xyplex>

5. Enter the DEFINE SERVER PROTOCOL MX800 ENABLED command to enable the enhanced load image.

```
Xyplex>> define server protocol MX800 enabled
```

The interface prompts you for the MX800 password.

6. Enter your password at the MX800 Password> prompt. The password does not appear on the screen. If you do not have a password, contact your Xyplex Networks sales representative.

```
MX800 Password> xxxxx
```

```
Press <RETURN> to modify configuration; any other key to abort
```

7. Press the Return key to load the enhanced image, then initialize the access server.

```
Xyplex -705- Change leaves approximately 2211136 bytes free
```

```
Xyplex>>
```

```
Xyplex>> initialize delay 0
```

MX1120 and MX1520

The MX1120 and MX1520 standalone access servers obtain a load image from a UNIX host, VAX/VMS host, or Xyplex Networks loader. To obtain the new load image name, `xpcs00s.sys`, on these access servers, load the new software on the host. For more information about changing load image names, refer to the appropriate *Software Installation Guide*.

The [Hardware Installation and Maintenance Manual for MAXserver 1000 Series](#) access servers explains in detail how to start up and use the Terminal Server configuration menu. However, the following procedure summarizes the process:

1. Start up the Terminal Server configuration menu.
2. Press the Reset switch once to enter Reset mode.
3. All lights on the front panel should illuminate.
4. Press the Reset switch again, and hold the switch in.

5. With the switch held in, observe the port lights. The following should occur:
6. Port lights 16 and 15 should illuminate.
7. Port lights flash in sequence from 1 to 16 and then back to 1 again.
8. Port lights 14 through 16 then illuminate.
9. Release the Reset switch.

The MAXserver runs a self-test diagnostics that takes approximately 20 seconds. When the self test is completed, the RUN light flashes rapidly.

At a terminal connected to a serial port, press the Return key several times to set the *autobaud* for the serial port. When the MAXserver selects a port speed, the following messages appear:

```
Access Server, type xx Rev x
Ethernet address 08-00-87-00-46-DD, port 1
Configuration in process. Please wait.
```

10. Enter the password ACCESS (note there is no prompt), and press the Return key. The main Configuration Menu appears.
11. Select option 2 from the Configuration Menu.

2. Modify load and dump settings.

The menu prompts you as follows:

```
Initialize load and dump settings [N] ?
```

12. Press the Return key to select the default, N (no). The menu returns:

Load parameters from (Local or Remote) [L]:

NOTE: The MAXserver 1120 and 1520 Access Servers cannot load a software load image locally.

13. Enter the option appropriate for your site, depending on where the access server obtains parameters. The menu returns:

```
Enable ALL protocols for loading and dumping [Y]:
```

14. Valid choices are Y (yes) or N (no):

Y	Use any protocol: MOP, XYPLEX, BOOTP, RARP
N	Use only specified protocols

15. Enter the appropriate choice. If you enter Y, the menu skips the protocol selection prompt and proceeds to prompt you to enter a load file name:

LOAD file name (16 characters max) [MX1500]:

16. Enter the new file name, xpcs00s. The menu returns:

Select a temporary TFTP load server [N]?

17. If you do not want a temporary TFTP load server, enter N (no) and go to step 13.

If you enter Y (yes), the menu prompts you for Internet information about the location of the load/parameter server and the name of the load image file.

18. Enter xpcs00s as the name of the load image file. The menu returns:

Type any key to continue

19. Type any key. The main Configuration Menu appears. Select option 6 from the Configuration Menu.

6. Exit saving configuration changes.

The menu returns:

Save changes and exit [Y]?

20. Press the Return key to select the default option, Y (yes). The following message appears:

Changes made.

The unit begins the software loading process.

MX1820

The MAXserver 1820 Access Servers obtains a load image from the network or locally from a floppy disk. The procedure used to load the software from the network is similar to the procedure used for MX1120 and MX1520 Access Servers. Specifically, you need to change the load image name on the load host.

To load from a floppy disk, you must also change the name of the load image in the ROM configuration menu, but the procedure is slightly different. The following describes this procedure:

1. Start up the ROM configuration menu.
2. Press the Reset switch once to enter Reset mode.
3. All lights on the front panel should illuminate.

4. Press the Reset switch again, and hold the switch in.
5. With the switch held in, observe the port lights. The following should occur:
6. Port lights 16 and 15 should illuminate.
7. Port lights flash in sequence from 1 to 16 and then back to 1 again.
8. Port lights 14 through 16 then illuminate.
9. Release the Reset switch.
10. The MAXserver runs a self-test diagnostics that takes approximately 20 seconds. When the self test is completed, the RUN light flashes rapidly.
11. At a terminal connected to a serial port, press the Return key several times to set the *autobaud* for the serial port. When the MAXserver selects a port speed, the following messages appear:

```
Access Server, type xx Rev x
Ethernet address 08-00-87-00-46-DD, port 1
Configuration in process. Please wait.
```

12. Enter the password ACCESS (note there is no prompt), and press the Return key. The main Configuration Menu appears.
13. Select option 2 from the Configuration Menu.

```
2. Modify load and dump settings.
```

The menu prompts you as follows:

```
Initialize load and dump settings [N] ?
```

14. Press the Return key to select the default, N (no). The menu returns:

```
Load software from (Local or Remote) [L]:
```

15. Enter R (remote). The menu returns:

```
Load parameters from (Local or Remote) [L]:
```

16. Enter the option appropriate for your site, depending on where the access server obtains parameters.

17. If you enter R (remote), the menu prompts you to answer questions about protocols and the TFTP load server. Respond to these prompts as described in the [Hardware Installation and Maintenance Manual for 1000 Series Access Servers](#), or the network loading procedure for MX1120 and MX1520 Standalone access servers. The menu returns:

```
Enable ALL protocols for loading and dumping [Y]:
```

18. Valid choices are Y (yes) or N (no):

```
Y      Use any protocol: MOP, XYPLEX, BOOTP, RARP
N      Use only specified protocols
```

19. Press the Return key to select the default Y (yes). The menu returns:

```
LOAD file name (16 characters max) [MX1500]:
```

20. Enter the new file name, xpcs00s.

NOTE: To obtain the load image from the network, continue with the procedure described here.

21. To obtain the load image locally from the floppy disk, return to the main Configuration Menu. Then select option 2 from the main Configuration Menu: 2. Modify load and dump settings. Enter L (local), and continue with the procedure described here. This time omit steps 11 and 12.

22. After entering xpcs00s as the file name, the menu prompts you to:

```
Select a temporary TFTP load server [N]?
```

23. Enter N (no). The menu returns:

```
Type any key to continue
```

24. Type any key. The main Configuration Menu appears.

25. Select option 6 from the Configuration Menu. The menu returns:

```
Save changes and exit [Y]?
```

26. Press the Return key to select the default option, Y (yes). The following message appears:

```
Changes made.
```

The unit begins the software loading process.

MX1600 and MX1608

The MAXserver 1600 and 1608 Access Servers obtain a load image from the network, or locally, from a memory card. To obtain the new load image from the network, load the software onto a network host, and follow the steps described for the MX1120 and MX1520 Access Servers. The procedure is the same for the MX1600 and 1608, except that in Step 1, the menu prompts:

Load parameters from (Local or Remote) [L]:

1. Select R (remote). The menu then continues with the prompt for parameter loading.
2. If your access server is running a software version of V4.4 or earlier, you need to update the image on a flash memory card as follows:
3. Load both images onto a network host; either a UNIX host, a VAX/VMS host, or a Xyplex Networks loader.
4. Load the default, 1-Megabyte load image on the card (`mx1500.sys`) and initialize the access server.
5. Load `xpcs00s.sys` on the card.
6. Initialize the access server with the new load image.
7. The following describes this procedure in detail.
8. After you have loaded both images on the network host, insert the memory card into the card drive of the access server and format the card. For example:

```
Xyplex>> format card
XXX format    WARNING: all data will be lost.
Press <RETURN> to start format, any other character to abort.
```

9. Press the Return key to format the card. The following message appears:

```
Format in progress, please wait.  xx% complete
```

10. After the formatting is complete, enter one of the following versions of the GET CARD LOAD FILE command, depending on where the load image files are located:

- **For a VAX/VMS host, or Xyplex Networks loader:**

```
Xyplex>> get card load file "mx1500.sys" address ethernet-address
```

- **For a UNIX host:**

```
Xyplex>> get card load file "/pathname/mx1500.sys" internet address
internet-address
```

The flash card loader file, **mcffs1.sys**, is automatically copied to the card when you issue a GET CARD LOAD FILE command. This file must be located in the same directory on the host as the `mx1500.sys` file.

11. After you load the flash card with `mx1500.sys`, initialize the access server as follows:

```
Xyplex>> initialize delay 0
```

NOTE: To use the 1-Megabyte load image on the flash card, you can stop at this point.

12. To obtain the enhanced load image, re-format the flash card and enter the GET CARD LOAD FILE command again with the new image name:

- **For a VAX/VMS host, or Xyplex Networks loader:**

```
Xyplex>> get card load file "xpcs00s.sys" address  
ethernet-address
```

- **For a UNIX host:**

```
Xyplex>> get card load file /pathname/ "xpcs00s.sys" internet address  
internet-address
```

13. After you load the flash card with `xpcs00s.sys`, initialize the access server to load the new image as follows:

```
Xyplex>> initialize delay 0
```

