EMULEX

Performance Series Communications Server Kerberos User's Guide

ER2054606-00, Rev A
February 1993

Information contained in this document is believed to be accurate and reliable. However, Emulex Corporation assumes no responsibility for its use nor for any infringements of patents or other rights of third parties which may result from its use. Emulex Corporation reserves the right to change product specifications at any time without notice.

The following trademarks of Emulex Corporation are used in this document:
Emulex, Performance Series,

The following are trademark acknowledgments:
Kerberos and Project Athena are a trademarks of the Massachusetts Institute of Technology

WARNING: This equipment generates, uses, and can radiate radio frequency energy. If its is not installed and used in accordance with the instruction manual, it may cause interference to radio communications. This equipment has been type tested and found to comply with the limits for a Class A computing device pursuant to Subpart J of Part 15 of the Federal Communication Commission Rules, which are designed to provide reasonable protection against such interference when operated in a commercial environment. Operation of this equipment in a residential area is likely to cause interference, in which case the user at his own expense will be required to take whatever measures may be required to correct the interference.

Shielded cables must be used between this equipment and attached peripheral devices to prevent radio frequency interference from this source.

The above statement applies to products marketed in the U.S.A.

WARNING: This digital apparatus does not exceed the Class A limits for radio noise emissions from digital apparatus as set out in the Radio Interference Regulations of the Canadian Department of Communications.

The above statement applies to products marketed in Canada.

Emulex Corporation
3545 Harbor Boulevard
Costa Mesa, California 92626
(714) 662-5600
FAX (714) 241-0792
TLX 183627

Printed in U. S. A.

Contents

About This Manual

Section 1 *Introduction*

Section 2 *Kerberos Configuration*

Section 3 *Logging In with Kerberos*

Section 4 *Kerberos Commands*

Appendix A ***Error and Status Messages***

Appendix B ***Glossary***

About This Manual

Audience and Scope

This manual describes the configuration and operation of the Kerberos security feature of the Emulex Performance Series communications servers. The reader must have a knowledge of Kerberos concepts and of the Emulex communications servers.

This manual is intended for those who are responsible for the operation of the Kerberos authentication system on their networks. Several procedures require that you modify certain system files on your host. These procedures should only be performed by a Network Administrator or others who are familiar with the concepts of network systems. For further information, see *Related Documentation.*

Document Organization

This manual contains the following sections:

- **Section 1, Introduction** - describes the Kerberos feature and lists the specifications.
- **Section 2, Configuring Kerberos** - describes the procedures for configuring Kerberos on your host and your server.
- **Section 3, Logging in with Kerberos** - describes the procedures for logging into a Kerberos protected service.
- **Section 4, Kerberos Commands** - provides the function and syntax of each Kerberos-related command.
- **Appendix A, Error and Status Messages**

After reading this guide, please take a few minutes to fill out and return the Reader's Comment Card. Your comments will help us to evaluate and improve our products and documentation.

Product Support

Emulex products are backed by a broad range of technical and educational support services. These services are available so that you can maximize your system performance and use Emulex products effectively.

For assistance, contact Emulex Corporate Headquarters as follows:

Emulex Corporation - Network Systems Division
3545 Harbor Boulevard
Costa Mesa, California 92626 USA

Telephone: (800) 854-7112 or (714) 662-5600
FAX (714) 966-1299
Internet: tech_support@emulex.com

Emulex Network System Division has multiple, worldwide locations. Contact coporate headquarters for the location of your local or regional support center.

Conventions Used

This document uses the following typographical conventions:

- Text that is displayed on the screen is presented in `computer type`.
- Text that you enter is presented in **`bold computer type`**.
- Variables and items of importance are displayed in *italics.*
- Notes are used to indicate useful or important information. These are presented as follows:

NOTE: information such as a time saving step, or situations to avoid.

Related Documentation

The following literature provides information on Kerberos concepts:

- J. G. Steiner, B. C. Neuman, and J. I. Schiller, "Kerberos: An Authentication Service for Open Network Systems," pp. 191-202 in *Usenix Conference Proceedings,* Dallas, Texas (February, 1988).
- S. P. Miller, B. C. Neuman, J. I. Schiller, and J. H. Saltzer, "Section E.2.1: Kerberos Authentication and Authorization System," *Project Athena Technical Plan,* M.I.T. Project Athena, Massachusetts Institute of Technology, Cambridge, Massachusetts (December 21, 1987).
- J. G. Steiner, "The Kerberos Network Authentication Service Overview," Request For Comments Draft: Network Working Group, March 28, 1989.
- B. Bryant, "Designing an Authentication System: a Dialogue in Four Scenes," M.I.T. Project Athena, Massachusetts Institute of Technology, Cambridge, Massachusetts (Draft, February 8, 1988).

The references listed above, as well as other Kerberos documentation, can be obtained over the DARPA Internet, via anonymous FTP, from the following host and directory:

Host: **aeneas.mit.edu** Directory: **/pub/kerberos/doc**

Information about the Performance Series servers and their command set is provided in the following Emulex documents:

- *Performance Series Printer and Terminal Server Macro User's Guide,* P/N ER2054603-00
- *Performance Series TCP/IP-LAT Protocol and Command Reference,* P/N ER2050006-00
- *Performance Series Ethernet Terminal Server Troubleshooting Guide,* P/N ER2056701-00

Section 1

Introduction

1.1 Overview of Kerberos

This section describes the Kerberos™ Authentication System and how it is implemented on Performance™ Series communications servers.

Kerberos is a user authentication system developed by the Massachusetts Institute of Technology (MIT) as part of its Project Athena™ environment. It is based on a trusted third-party authentication protocol.

Kerberos provides a means of verifying the identities of users or services on an unprotected network, without relying on the authentication mechanisms of the host's operating system. The Kerberos system does not require physical security on every host attached to the network because it does not trust host addresses. Kerberos assumes that packets on the network can be read, modified, or inserted at any time, and uses shared secret-key cryptography to prevent security breaches.

A service protected by Kerberos is called a *kerberized service.* Figure 1-1 illustrates the steps necessary to authenticate a user with a kerberized service. An example of a kerberized service could be the UNIX rlogind daemon. Rlogind is a UNIX program that provides remote login capability on the host.

In Figure 1-1, the Kerberos *client* is a Performance Series communications server. The *authentication server* and the *ticket-granting ticket* (TGT) server are programs running on a host. The host computer in the figure provides the desired service, such as RLOGIN. Arrows indicate the flow of *tickets* or other messages.

Kerberos is implemented on Emulex communications servers by a Product Authorization Key (PAK), on a server-by-server basis. The server-specific PAK enables the Kerberos feature for all ports on that server. The server may then be assigned a Kerberos Administrative host and up to four hosts which contain key distribution center software. Each port on a Kerberos-enabled server may be configured individually to enable or disable the Kerberos RLOGIN function. The commands for configuring the server and individual ports are described in Section 4.

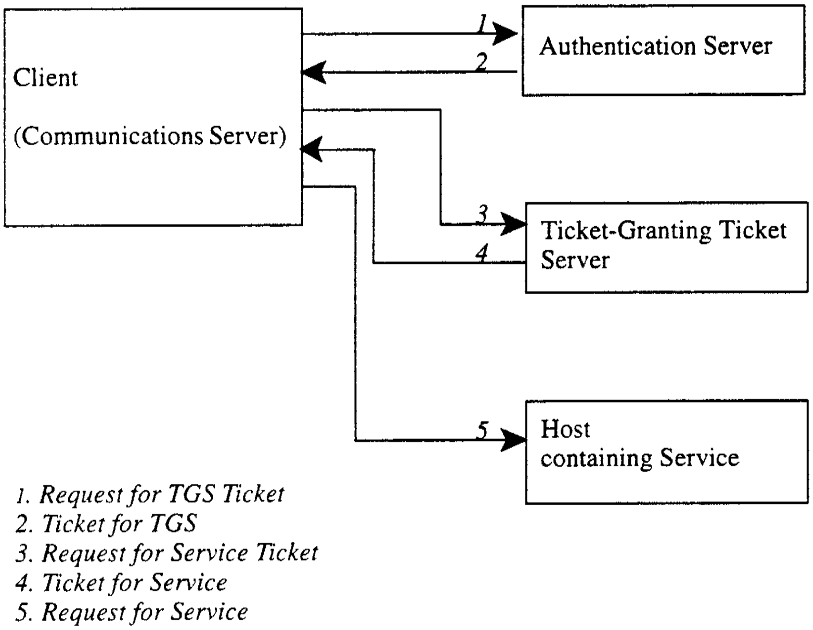


Figure 1-1. Kerberos Authentication

The *authentication server* validates the user's identity and issues the initial ticket to that user. This ticket then can request tickets for services from a *ticket-granting ticket* (TGT) *server.*

The TGT Server issues tickets for services (e.g., RLOGIN) needed on the communications server.

The client sends a request for the service containing the ticket it received from the TGT Server. The service verifies that the client's identify with the ticket, and if successful, provides the requested service.

The first exchange occurs when a user at the client (communications server) issues a KINIT command. The other exchanges occur when the user requests the service that uses Kerberos for authentication (for example, when the user issues an RLOGIN command).

1.2 Capabilities

Kerberos on a Performance Series communications server has the following capabilities:

- Kerberos can be enabled, disabled, and configured individually for each port on the server.
- The communications server can be configured to require individual Kerberos passwords (one for each user) for port login instead of a single, common password.
- Up to 4 Kerberos servers within a realm may be specified. When requesting a ticket, the communication server polls each Kerberos server in sequence until it locates an active ticket-granting server.
- Non-Kerberos RLOGIN procedures may be used to obtain unprotected services. If a communications server port is configured for Kerberos, the server will attempt kerberized RLOGIN by default.
- Kerberos on the communications server uses the encryption scheme of the National Bureau of Standards Data Encryption Standard (DES) only for Kerberos authentication.
- The communications server provides Kerberos Version 4 client support for RLOGIN.
- The communications server user may change their Kerberos password, acquire the initial ticket-granting ticket, list, and destroy any tickets that they have accumulated.

1.3 Requirements

To use Kerberos, the Kerberos host must meet the following requirements:

- The Kerberos-authenticated rlogin daemon on a Kerberos host (the klogin daemon) must be on TCP port 543.
- A host computer in the same Kerberos realm as the communications server must have the following software, or a functionally equivalent package:
  - Kerberos database
  - Kerberos authentication server
  - Kerberos TGT server
- The system clocks of all machines on the network that are running Kerberos-authenticated services must be loosely synchronized (within a few minutes).

  For proper time stamping of the Kerberos tickets and authenticators, the time server feature on the communications server must be enabled and operating properly. Parameters that must be set include timezone and daylight/standard savings time.

1.3.1 Software Compatibility

The Kerberos feature on Performance Series servers has been tested and is compatible with Kerberos host software packages from the following vendors:

- Massachusetts Institute of Technology (MIT)
- Cygnus
- TGV

Contact Emulex Technical Support for additional supported Kerberos packages.

1.4 Kerberos Implementation

The communications server implementation of Kerberos is based on the MIT public domain Kerberos source. The following Kerberos utilities are implemented as communications server commands:

- **RLOGIN** - with Kerberos enabled for a port, the server RLOGIN command is functionally equivalent to the MIT kerberized version. Alternatively, if Kerberos is disabled, the RLOGIN command functions in the normal fashion.
- **KPASSWD** - enables the user to modify his Kerberos password, stored in the Kerberos database on the Kerberos host computer.
- **KINIT** - obtains the initial ticket for the ticket-granting ticket (TGT) server in the local Kerberos realm.
- **KLIST** - lists tickets that the user has accumulated.
- **KDESTROY** - destroys tickets that the user has accumulated. When a user logs out of his port, the server destroys all outstanding tickets associated with the port.

1.5 Specifications

Table 1-1 lists the specifications for the communications server's Kerberos feature.

Table 1-1. Kerberos Specifications

Parameter	Range
Tickets held per communications server port	3 maximum (Up to 2 tickets in ticket cache, plus 1 initial ticket-granting ticket)
Kerberos realms	15 maximum
Kerberos hosts per realm	4 maximum
TCP port number for Kerberos klogin daemon (klogind)	Fixed at 543
TCP port number of Kerberos administration protocol (kadmind)	Fixed at 751
UDP port number of Kerberos KDC service	User-configured; factory default is 750

Section 2

Kerberos Configuration

2.1 Overview

This section discusses host software considerations and describes the steps required to configure Kerberos support on your Performance Series server. A complete list of Kerberos-related commands is provided in Section 4.

2.2 Host Software Installation

Emulex provides Kerberos software only for Emulex Performance Series communications servers (Kerberos clients); we do not provide Kerberos software for Kerberos host computers (Kerberos servers). To install the Kerberos software on the host and configure the host for Kerberos operation, you must refer to the documentation supplied with your Kerberos host software.

During the installation process, you should consider the following:

- The Kerberos *authentication* function may be provided from one host, or a maximum of four hosts on the network.
- The Kerberos *administration* function may only be provided from a single host on the network.
- The Emulex implementation of Kerberos is limited to the RLOGIN function.

2.3 Server Configuration

The following procedure configures your Performance Series server for Kerberos operation. Before proceeding, you must obtain a new PAK which enabled Kerberos on your server:

1. Log in to the server using the console terminal or the RCF port from a host terminal. After logging in, obtain privileged status. For example, from a TCP host:

```
telnet 138.239.254.245
# access                 (default login password)
Local> su
Password> system         (default privilege password)
Local>
```

2. Use the following command to enter the Kerberos PAK:

```
change server key pak_string
```

   where *pak_string* is the 41-character PAK

3. Ensure the Performance Series server can get its time from a timeserver on the network as follows:

   a. Define the default timeserver using the command:

```
change node name ip addr timeserver default
```

   where *name* and *addr* are the node name and IP address of the node that is the network timeserver.

   b. Define the timezones (standard and daylight savings) and the date and time for switching between timezones. If your area remains at a single timezone, the alternate settings are not required. The command syntax is:

```
change server timezone sta #1 alt #2 cha
date_1 ret date_2 swit time_1 resync time_2
```

   where *#1* and *#2* are the standard (sta) and alternate (alt) timezones:
   (0-GMT, 5-EST, 6-CST, 7-MST, 8-PST)
   date_1 is the date (mmm dd) you change to timezone #2
   date_2 is the date you return to timezone #1
   time_1 is the time of day (24-hour) you switch between timezones

time_2 is the time of day (24-hour) you resync with the timeserver node

4. Enable Kerberos support on the Performance Series server by entering:

   ```
   define server kerberos enabled
   ```

5. Configure the size of the ticket pool and the Kerberos realm by entering:

   ```
   define server tickets value
   change server realm realm_name
   ```

   where *value* is the desired size of the ticket pool (number of tickets).

6. Define the Kerberos Administration host by entering:

   ```
   change node host_name kerbserver admin
   ```

   For example, to identify the node *King* as the administration host:

   ```
   change node King kerbserver admin
   ```

7. Define the port(s) for which you want Kerberos to be used by entering:

   ```
   change port list kerberos enabled
   ```

   For example, to enable Kerberos on ports 1, 3, and 5 though 16, enter:

   ```
   change port 1,3,5-16 kerberos enabled
   ```

8. Define the port(s) for which you want to obtain the initial ticket during port login by entering:

   ```
   change port list kerblogin enabled
   change port list password enabled
   ```

9. Reboot the server to ensure the changes are made in the configuration memory.

The server is now configured for basic Kerberos operation. Refer to Section 4 for details on other Kerberos-related commands.

2.4 Troubleshooting

If you experience problems, check the following:

1. Verify the server was assigned the correct IP address and subnet mask.
2. If the server is on a different network or subnet from the timeserver, KDC, or Kadmin host, you may need to use a gateway. Define a gateway with the command:

   ```
   change node node_name ip addr gateway default
   ```

   where *node_name* and *addr* are the name and IP address of the gateway node on your network.
3. Verify the timeserver you defined in step 3 of the previous subsection is an active node (`show server timezone`). If the node is correct, initiate the connection by entering:

   ```
   set server time tcp
   ```

Section 3

Logging In with Kerberos

3.1 Overview

This section describes the events that must occur for a user to access a Kerberos-protected service from the communications server. The actual sequence differs, depending on how the KERBLOGIN option is configured for the user's port. Most of the events are transparent to the user.

Each port on the communications server has two Kerberos-related options:

- KERBEROS - enables or disables Kerberos for the server port. If this option is enabled, the RLOGIN server command uses Kerberos for user-authentication and kerberos-related commands may be used.
- KERBLOGIN - determines how a user logs in to a server port. If this option is enabled, Kerberos obtains the initial ticket from the TGT server during port login. In this case, the user does not have to enter the KINIT command to obtain the initial ticket.

Because of the interactions between Kerberos and normal server security functions, this section includes a discussion of both features.

3.2 Server Security

Without using Kerberos, the Performance Series communications server provides a limited level of security with the standard server password and the `security enabled` function.

A user trying to log into the server must enter the server password before they are permitted access to any port on the communications server. If the port is connected to a dial-in modem, an unauthorized user may continually attempt a login until they give up or "guess" the password. If, however, `security` is *enabled*, the unauthorized user is only permitted a set number or retries. After this limit is reached, the port is "closed" to further login attempts until it is reset by the network administrator. If a dial-in modem is connected to the port, further connection attempts are greeted by a "busy" signal until the port is reset.

If the Kerberos option is used in *conjunction* with the server password, the server behaves as detailed in Table 3-1 below.

Table 3-1. Server Actions During Port Login

Server Port Option Settings		**Server Actions During Port Login**
KERBLOGIN	**PASSWORD**	
DISABLED	DISABLED	No password needed (server is not secure). KINIT is needed to access Kerberos-protected service.
DISABLED	ENABLED	Server prompts for port password and verifies it against server login password. KINIT is needed to access Kerberos-protected service.
ENABLED	DISABLED	No password needed (server is not secure). KINIT is needed to access Kerberos-protected service.
ENABLED	ENABLED	Server prompts for Kerberos password; gets TGT from TGT server.

3.3 Kerblogin Option

If the KERBLOGIN option is disabled, the server port login occurs as follows:

- If the port password is disabled, no password is required to log in to the server port.
- If the port password is enabled, you are prompted to enter a password. The server verifies the password against the server login password that was defined previously (SET SERVER LOGIN PASSWORD).
- To remotely login (RLOGIN) to a Kerberos-protected host you must use the following sequence:

```
kinit
rlogin host_name
```

If the KERBLOGIN option is enabled *and* the port password is enabled, the login procedure is as follows:

1. Press `<Return>` to log in to the server port. The server displays the following prompt:

   ```
   Kerberos password #
   ```

2. Enter your Kerberos password. If the port has a defined username, that username is used as the Kerberos username. If the port has no username, the server prompt is:

   ```
   Enter username, or HELP>.
   ```

3. After entering your username, the server attempts to get a ticket-granting ticket using the password and username.
4. If a ticket-granting ticket is issued, the server allows port access.
5. If access is denied, the password prompt in Step 1 is repeated. After three failed attempts, access is denied and the server displays an error message.

NOTE: When Kerberos is enabled on a port and the user logs out of the port, the server destroys all of the Kerberos tickets associated with the port.

Section 4

Kerberos Commands

4.1 Overview

This section describes the server commands that allow you to configure Kerberos support on your server and to monitor these parameters. Several existing commands were modified for Kerberos operation. In general, you will need privileged status to alter server parameters.

4.2 Server Configuration

The following server commands are used to configure Kerberos related parameters for the entire server.

4.2.1 DEFINE SERVER KERBEROS

This command enables or disables the Kerberos feature for the entire server. When the *enabled* is specified, Kerberos on each port is controlled by the parameters PORTS KERBEROS and PORTS KERBLOGIN options. When the *disabled* option is specified, Kerberos is disabled for all ports on the server, regardless of individual port configurations.

The command syntax is:

```
DEFINE SERVER KERBEROS [ENABLED|DISABLED]
```

This command required privileged status. Refer to SET PORTS KERBEROS and SET PORTS KERBLOGIN for further details.

4.2.2 DEFINE SERVER TICKETS LIMIT

This command configures the number of records assigned to the memory pool. Individual ports receive memory from this pool to store their tickets. The amount of memory allocated to the ticket memory pool affects (reduces or increases) the amount of memory allocated to the nodes and services on the server.

The command syntax is:

```
DEFINE SERVER TICKETS [LIMIT] value
```

Where *value* is the desired number of records to be maintained in the memory pool. The maximum value should not exceed 3 times the number of ports on the communications server. The factory default value is 0.

This command is available to privileged users only.

4.2.3 SET NODE KERBSERVER

This command identifies the Kerberos hosts that contain the KDC.

A host can be a KDC for only one realm at a time. The communications server supports up to 15 Kerberos realms, with a maximum of four Kerberos hosts in each realm.

The DEFINE and CHANGE forms of the command, establish one Kerberos Administration host and one KDC host in the communications server's EAROM. Any attempts to save multiple KDC nodes to EAROM cause the server to display an error message. Kerberos services defined with this command must be within the realm specified with the `CHANGE SERVER KERBEROS REALM` command (subsection 4.2.4).

To access additional KDC nodes in other realms, you must use the SET command to temporarily store the additional realms and associated nodes in the node table. *This information will be lost when the server loses power.* The Macro feature may be used to load additional realms and associated KDC nodes each time the server is powered up.

If you do not specify an IP address for a host, the server attempts to get the IP address from a nameserver.

This command is available to privileged users only. The syntax is:

```
SET NODE [NAME node_name] KERBSERVER    [ADMIN          ]
DEFINE   [IP ip_address]                [REALM realm_name]
CHANGE
```

Where *realm_name* is a string of up to 39 characters that defines the realm name. If no name is specified, the server realm (SET SERVER KERBEROS REALM) or the server domain name is used.

If the ADMIN keyword is specified, the host is identified as a Kerberos Administration host as well as a KDC host.

4.2.4 SET SERVER KERBEROS REALM and SET SERVER KERBEROS KERBPORT

These commands set the Kerberos realm name and UDP port of the TGT servers.

The REALM keyword specifies the Kerberos realm. The server looks in two places for a valid realm name. It first looks in the realm name field. If there is no valid name there, it uses the server domain name as the Kerberos realm name.

The KERBPORT keyword specifies the UDP port that the KDC uses to exchange information with the communications server.

This command is available to privileged users only. The syntax is:

```
SET    SERVER[KERBEROS][REALM realm_name]
DEFINE       [        ][KERBPORT udp_port_number]
CHANGE
```

Where: *realm_name* is a string of up to 39 characters that define the realm name. To clear the realm name field, enter none.

udp_port_number may be between 0 and 65535. The factory setting is 750.

4.2.5 CLEAR NODE KERBSERVER

This command removes the specified node from the list of hosts designated as KDC servers. Privileged status is required. The syntax is:

```
CLEAR NODE NAME node_name KERBSERVER
```

4.2.6 Login Security Commands

The following standard commands set security options for the communications server to prevent unauthorized login:

change server login password

This command defines the login password for the entire server. If the password option is enabled for a port, the user must enter this password before they can be logged in. The command syntax is:

```
SET SERVER LOGIN PASSWORD password
DEFINE
CHANGE
```

In order for the password to be effective, the port must be set to password enabled.

change port password

This command enables or disables password protection for the specified port. The command syntax is:

```
SET PORT n PASSWORD [ENABLED|DISABLED]
DEFINE
CHANGE
```

where *n* is the specific port number or a list of ports to be enabled/disabled.

change server password limit

This command sets a limit on the number of login attempts using an incorrect password before the port is locked from further login attempts. If the number is exceeded, the port is locked out until a privileged user logs out the port from the console. The command syntax is:

```
SET SERVER PASSWORD LIMIT value
DEFINE
CHANGE
```

Where *value* is the number of login attempts before the port is locked. This function is only used if a password is defined for the server *and* the password is enabled for the port.

4.3 Port Configuration

The following commands allow you to configure Kerberos options for individual ports.

4.3.1 SET PORTS KERBLOGIN

This command enables or disables automatic requests for an initial-ticket during login on the specified ports. If disabled, the user must enter the KINIT command before using RLOGIN to log on to a Kerberos-protected host.

If RLOGIN is enabled for the port, the process of obtaining the initial ticket occurs transparently.

This command is available to privileged users only. The syntax is:

```
SET PORTS [port_list] KERBLOGIN [ENABLED|DISABLED]
DEFINE
CHANGE
```

4.3.2 SET PORTS KERBEROS

This command enables or disables Kerberos support for one or more ports on the server. Before enabling support, the server must have Kerberos enabled.

This command requires privileged status. The syntax is:

```
SET PORTS [port_list] KERBEROS [ENABLED|DISABLED]
DEFINE
CHANGE
```

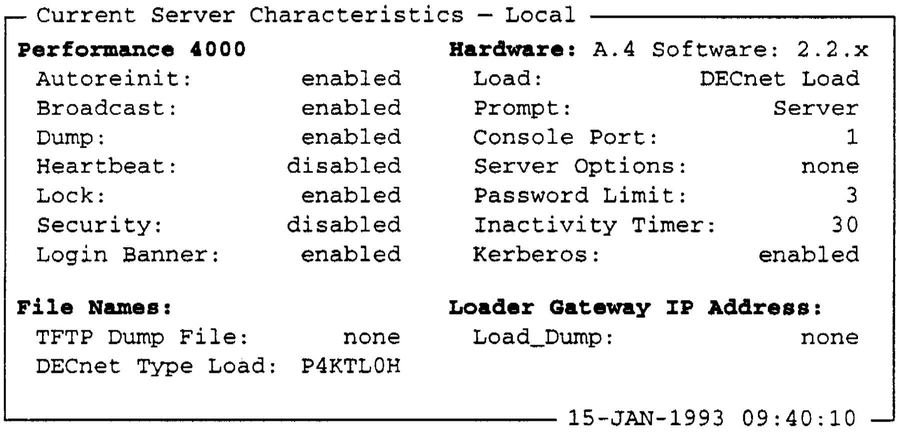
4.4 *Monitor Configuration*

The following commands maybe used to examine the status of Kerberos parameters for the server and for individual ports.

4.4.1 *SHOW SERVER CHARACTERISTICS LOCAL*

As shown in Figure 4-8, this command displays various local characteristics about the communications server.

The Kerberos-related field is `Kerberos`. This field shows the current status of the option (enabled or disabled).

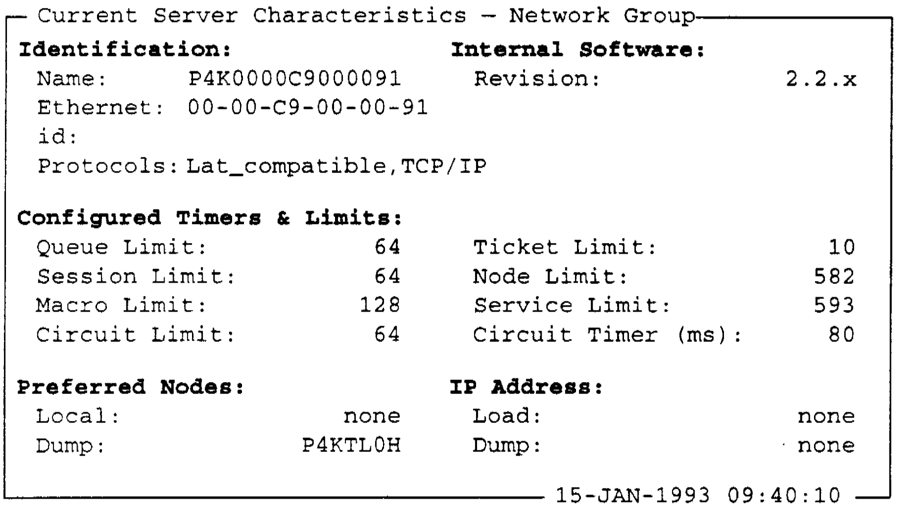


```
 Current Server Characteristics - Local
Performance 4000              Hardware: A.4 Software: 2.2.x
 Autoreinit:        enabled    Load:          DECnet Load
 Broadcast:         enabled    Prompt:             Server
 Dump:              enabled    Console Port:            1
 Heartbeat:        disabled    Server Options:       none
 Lock:              enabled    Password Limit:          3
 Security:         disabled    Inactivity Timer:       30
 Login Banner:      enabled    Kerberos:          enabled

File Names:                   Loader Gateway IP Address:
 TFTP Dump File:       none    Load_Dump:            none
 DECnet Type Load:  P4KTL0H

                                        15-JAN-1993 09:40:10
```

Figure 4-1. SHOW SERVER CHARACTERISTICS LOCAL Display

4.4.2 SHOW SERVER CHARACTERISTICS NETWORK

As shown in Figure 4-2, this command displays various network characteristics about the server. The field `Ticket Limit` shows the actual number of tickets allocated to the ticket memory pool.



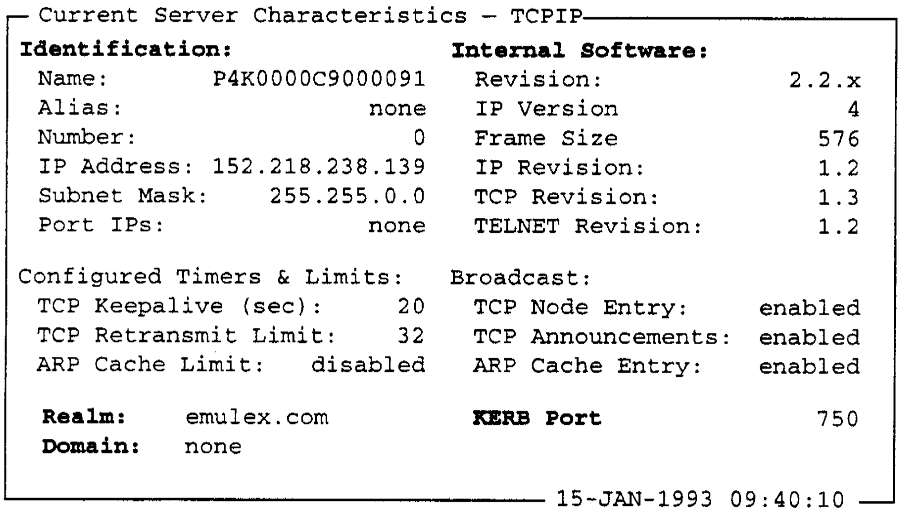
```
- Current Server Characteristics - Network Group
Identification:                            Internal Software:
  Name:       P4K0000C9000091               Revision:                 2.2.x
  Ethernet:   00-00-C9-00-00-91
  id:
  Protocols: Lat_compatible,TCP/IP

Configured Timers & Limits:
  Queue Limit:               64             Ticket Limit:               10
  Session Limit:             64             Node Limit:                582
  Macro Limit:              128             Service Limit:             593
  Circuit Limit:             64             Circuit Timer (ms):         80

Preferred Nodes:                           IP Address:
  Local:                   none             Load:                     none
  Dump:                 P4KTL0H             Dump:                     none

                                                  15-JAN-1993 09:40:10
```

Figure 4-2. SHOW SERVER CHARACTERISTICS NETWORK Display

4.4.3 SHOW SERVER CHARACTERISTICS TCPIP

As shown in Figure 4-8, this command displays various characteristics of the server related to a TCP/IP network. The kerberos-related fields are:

- `Realm` - displays the Kerberos realm name of the server.
- `KERB Port` - displays the UDP port number that the server uses to communicate with Kerberos KDC services.



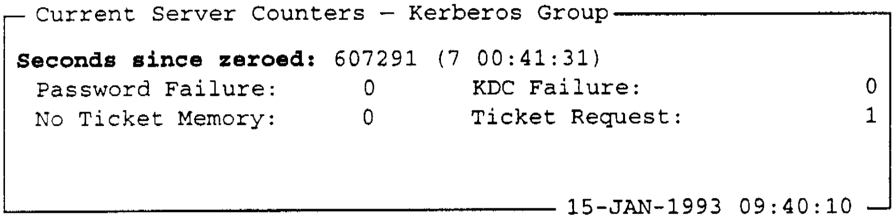
```
- Current Server Characteristics - TCPIP
Identification:                          Internal Software:
 Name:         P4K0000C9000091            Revision:                2.2.x
 Alias:                   none            IP Version                   4
 Number:                     0            Frame Size                 576
 IP Address: 152.218.238.139              IP Revision:               1.2
 Subnet Mask:     255.255.0.0             TCP Revision:              1.3
 Port IPs:                none            TELNET Revision:           1.2

Configured Timers & Limits:              Broadcast:
 TCP Keepalive (sec):       20            TCP Node Entry:        enabled
 TCP Retransmit Limit:      32            TCP Announcements:     enabled
 ARP Cache Limit:     disabled            ARP Cache Entry:       enabled

 Realm:     emulex.com                    KERB Port                  750
 Domain:    none

                                             15-JAN-1993 09:40:10
```

Figure 4-3. SHOW SERVER CHARACTERISTICS TCPIP Display

4.4.4 SHOW SERVER COUNTERS KERBEROS

This command displays various Kerberos-related counters. These counters include:

- Password Failure - records the number of times the KINIT server command or port login using the Kerberos RLOGIN fails because the user entered the wrong Kerberos password or username.
- KDC Failure - records the number of times the communications server fails to get a response from a KDC.
- No Ticket Memory - records the number of times a command fails because it cannot obtain memory for a Kerberos ticket from the ticket memory pool.
- Ticket Request records the number of times the server successfully obtained a Kerberos ticket requested from a KDC.



```
Current Server Counters – Kerberos Group
Seconds since zeroed: 607291 (7 00:41:31)
 Password Failure:       0       KDC Failure:                 0
 No Ticket Memory:       0       Ticket Request:              1

                                        15-JAN-1993 09:40:10
```

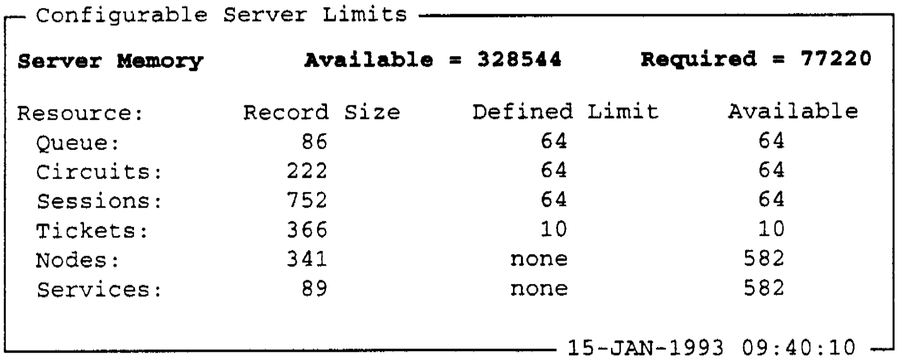
Figure 4-4. SHOW SERVER COUNTERS Display

4.4.5 SHOW SERVER LIMITS

This command displays a screen (Figure 4-5) which shows the memory resources used. The Kerberos ticket memory pool displays the following fields:

- `Tickets Record Size` - the size of a ticket record, in bytes.
- `Tickets Defined Limit` - the maximum number of tickets to allocate.
- `Tickets Available` - the actual number of tickets available. This field may be used to determine memory allocation after entering the command:

```
SHOW SERVER LIMITS TICKETS value
```

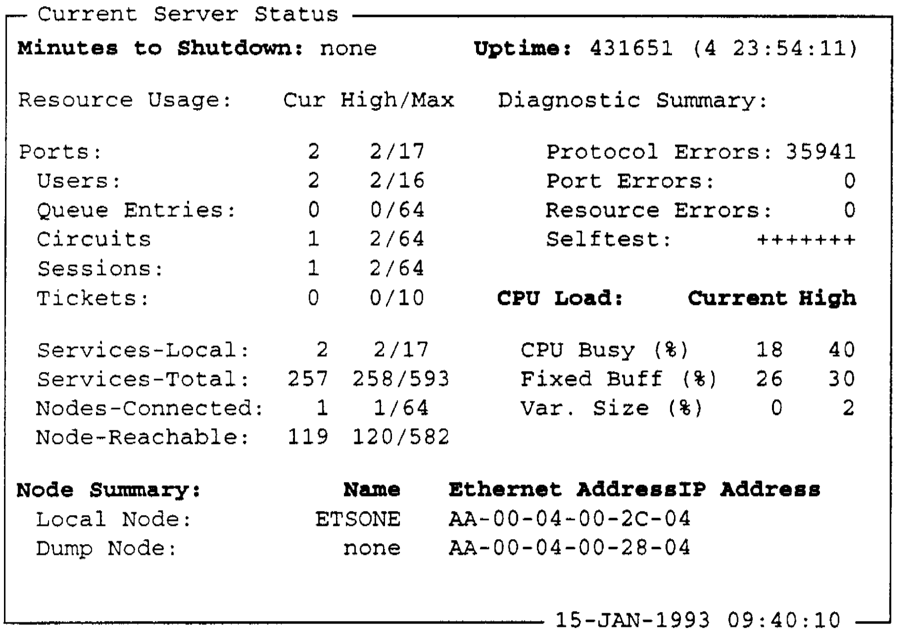


```
— Configurable Server Limits ————————————————————————————————
Server Memory        Available = 328544      Required = 77220

Resource:          Record Size      Defined Limit     Available
  Queue:                86                64              64
  Circuits:            222                64              64
  Sessions:            752                64              64
  Tickets:             366                10              10
  Nodes:               341              none             582
  Services:             89              none             582

———————————————————————————————————— 15-JAN-1993 09:40:10 —
```

Figure 4-5. SHOW SERVER LIMITS Display

4.4.6 SHOW SERVER STATUS

This command displays (Figure 4-6) the current server status, including the number of Kerberos tickets being used, the high number used, and maximum number of tickets.



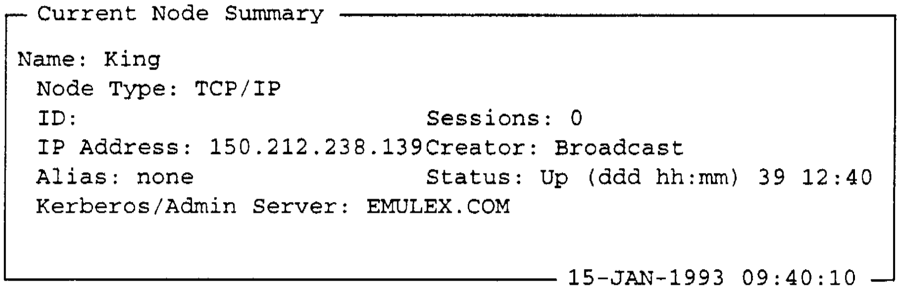
```
- Current Server Status ---------------------------------------------------
Minutes to Shutdown: none       Uptime: 431651 (4 23:54:11)

Resource Usage:    Cur High/Max   Diagnostic Summary:

Ports:               2   2/17       Protocol Errors: 35941
 Users:              2   2/16       Port Errors:         0
 Queue Entries:      0   0/64       Resource Errors:     0
 Circuits            1   2/64       Selftest:      +++++++
 Sessions:           1   2/64
 Tickets:            0   0/10     CPU Load:     Current High

 Services-Local:     2   2/17       CPU Busy (%)     18   40
 Services-Total:   257 258/593      Fixed Buff (%)   26   30
 Nodes-Connected:    1   1/64       Var. Size (%)     0    2
 Node-Reachable:   119 120/582

Node Summary:          Name    Ethernet AddressIP Address
 Local Node:         ETSONE    AA-00-04-00-2C-04
 Dump Node:            none    AA-00-04-00-28-04

------------------------------------------------- 15-JAN-1993 09:40:10 ---
```

Figure 4-6. SHOW SERVER STATUS Display

4.4.7 SHOW NODE SUMMARY SHOW NODE STATUS

These commands display information about each node in the server's Node Table. Figure 4-7 is an example of the display screen from the command SHOW NODE SUMMARY.

If the keyword /Admin appears, the node was defined as a Kerberos Administration server.



```
Current Node Summary

Name: King
  Node Type: TCP/IP
  ID:                          Sessions: 0
  IP Address: 150.212.238.139Creator: Broadcast
  Alias: none                  Status: Up (ddd hh:mm) 39 12:40
  Kerberos/Admin Server: EMULEX.COM

                                          15-JAN-1993 09:40:10
```

Figure 4-7. Example of SHOW NODE Display

4.4.8 KLIST

This command displays the user's active tickets in the following format:

```
Principal: your_user_name@REAL_TIME
```

For example:

```
      Issued           Expires            Principal
May 6 10:15:23   May 6 18:15:23   krbtgt.REALNAME@REALNAME
```

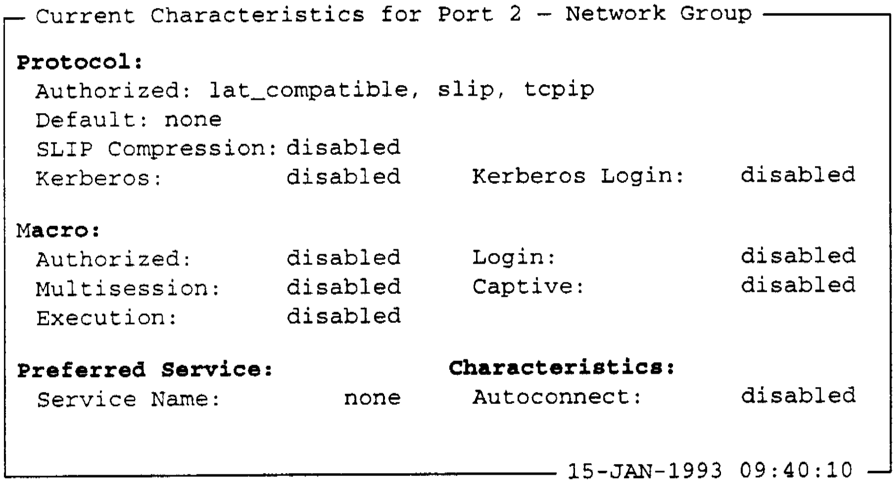
4.4.9 SHOW PORT CHARACTERISTICS NETWORK

This command displays various network characteristics about the specified port. If you do not specify a port number, the current port is displayed. For example, Figure 4-8 shows the screen displayed after you issue the command:

```
show port 2 characteristics network.
```

The two Kerberos related fields are:

- `Kerberos` - indicates whether the KERBEROS port option is enabled or disabled.
- `Kerberos Login` - indicates whether the KERBLOGIN port option is enabled or disabled.



```
Current Characteristics for Port 2 - Network Group

Protocol:
 Authorized: lat_compatible, slip, tcpip
 Default: none
 SLIP Compression: disabled
 Kerberos:         disabled     Kerberos Login:    disabled

Macro:
 Authorized:       disabled     Login:             disabled
 Multisession:     disabled     Captive:           disabled
 Execution:        disabled

Preferred Service:             Characteristics:
 Service Name:         none     Autoconnect:       disabled

                                   15-JAN-1993 09:40:10
```

Figure 4-8. SHOW PORT CHARACTERISTICS NETWORK Display

4.5 User Commands

The following commands are used to set your individual password and to log in to a Kerberos-protected host.

4.5.1 RLOGIN

The kerberos version of this command uses two additional options for Kerberos operation. This command is available to all users. The syntax is:

```
RLOGIN [NODE]node_name  [-l user_name]
                        [-k realm_name]
                        [-o]
```

If you use the `-k` option, you instruct the login daemon to obtain tickets for the remote host in the realm designated by *realm_name* instead of the server's local realm. The realm name is a string of up to 40 characters.

If you use the `-o` option, you force RLOGIN to perform a non-Kerberos authentication. Use this option when your port is enabled for Kerberos but you want to RLOGIN to a remote host that does not support Kerberos.

4.5.2 KDESTROY

This command destroys the user's active tickets. The command is available to all users. The syntax is:

```
KDESTROY
```

NOTE: The server will also destroy all of a user's active tickets when the user logs out of the port.

4.5.3 KINIT

This command is used to log into the Kerberos authentication system and to reissue the initial ticket after it has expired, or you have destroyed it (KDESTROY). The KINIT command is issued transparently when your use the Kerberos version of RLOGIN with KERBLOGIN enabled for your port.

If you enter KINIT without options, the server prompts you for your Kerberos password. It then attempts to authenticate your login using the local Kerberos authentication server. The command is available to all users. The syntax is:

```
KINIT[-n name][-i instance][-r realm][-l lifetime]
              [-u username[.instance][@realm]]
```

Use the -n option to specify the Kerberos principle name. Do no use a period (.) or the @ character. If you omit the -n option, the server uses the port login username as the Kerberos principle name.

Use the -i option to specify a Kerberos instance rather than the null instance. Do not use a period (.) or the @ character in the string. This option is useful for assigning different privileges at different times. You can have a different identifier assigned to each set of privileges. For example, John Smith operating as a system administrator might have different privileges from John Smith operating as a normal user.

The -r option specifies a realm instead of using the server's local realm. Do not use the @ character in the realm name (periods are acceptable).
The -r option lets you authenticate yourself with a remote Kerberos authentication server.

The -l option specifies the lifetime of a ticket, in minutes. The value of *lifetime* must be between 5 minutes and 1275 minutes.

The -u option allows you to specify a fully-qualified Kerberos principle identifier without the -n, -i, and -r options. You can enter any valid full names. Names that use the characters period (.) and @ are acceptable.

4.5.4 KPASSWD

This command changes your Kerberos password. The server prompts you for your current Kerberos password, then verifies it with the KDC. If the old password is correct, you are prompted twice for a new password. The server displays a message indicating the success or failure of the operation.

The command is available to all users.The syntax is:

```
KPASSWD[-n name][-i instance][-r realm]
        [-u username[.instance][@realm]]
```

The -n allows you to specify the Kerberos principle name. Do not use a period (.) or the @ character. If you omit the -n option, the server uses the port login username as the Kerberos principle name.

The -i option specifies the Kerberos instance rather than the null instance. The *instance* string cannot use a period (.) or the @ character.

The -r option specifies the Kerberos realm instead of the communications server's local realm. The *realm* string cannot use the @ character (periods are acceptable). This option lets you authenticate yourself with a remote Kerberos authentication server.

Use the -u option to specify a fully-qualified Kerberos principle identifier without using -n, -i, and -r options. You can enter any valid full name. Names that use the characters period (.) and @ are acceptable.

Appendix A

Error and Status Messages

A.1 Overview

This appendix lists the Kerberos-related communications server status and error messages.

A.2 Kerberos-Specific Messages

The following messages report the status of Kerberos related operations and identify any problems. Each message may also be identified by the associated message number in parentheses.

`Kerberos operation successful (400)`*:* the Kerberos login completed successfully.

`Software inconsistency (401):` a potentially fatal error was encountered by the server software. Consult your network manager for assistance.

`No KDCs in node table for specified realm (402):` Your server's node table does not contain any nodes designated as KERBSERVER. Contact your network manager to add a Kerberos host running KDCs to your servers node table. Also verify that Kerberos server nodes have an IP address associated with the node.

`Kerberos protocol error (403) :` a protocol error occurred while processing a Kerberos response or when preparing the request. Repeat the operation.

`Port not authorized for Kerberos protocol (404):` You either tried the Kerberos login from a port that is not set for Kerberos operation or you tried to use Kerberos from the RCF port. Verify that your terminal port has Kerberos enabled and try again.

`No Initial Ticket (405)`: You did not get the initial ticket. Enter `KINIT` before using the kerberos `RLOGIN`.

`KDC Not Contacted (406)`: The server did not receive a response from a KDC host. Verify that the server's node table contains a host with an active KDC.

`Bad Kerberos name format (407)`: The user name, instance, or realm you specified using the -u, -i, -r, or -n options was invalid. Verify that you did not use the illegal characters (. or @).

`Insufficient resources (408)`: The communications server has exhausted its memory, UDP ports, or tickets in the ticket pool. If the ticket pool is exhausted, the network manager may increase the pool size.

`Remote Kerberos error (409)`: The KDC or a Kerberized service has reported an error. Consult your network manager.

`No defined Kerberos Administration Server (410)`: You used the KPASSWD command without defining a node as the Kerberos Administration Server.

`No defined instance/host name (411)` : The communications server must have a host name specified in the Node Table for the rlogin instance.

The following messages, although not Kerberos specific, are used by the Kerberos feature. Numbers in parentheses are the message number.

`Insufficient resources - realm table full (719)`: You tried to add a host node to the realm table with 4 nodes previously assigned as KDC hosts.

`Maximum of 39 characters allowed in realm name (735)`: You entered a realm name that is too long. abbreviate the name to 39 or less characters.

`Password verification failed (742)`: You entered an incorrect username or password during port login with Kerberos login enabled or with the KINIT command.

A.3 Console Messages

The following messages contain error codes that are reported on the console terminal port.

```
981 - nonfatal software warning, code = 8500 at "..."
Unknown Kerberos event, type xx, port yy, chan nn
```

Kerberos received information it cannot process: type is *xx*, port number is *yy*, and *nn* is the channel number where the error occurred.

```
981 - nonfatal software warning, code = 8502 at "..."
```

Kerberos cannot parse the specified name, instance, or realm in KINIT or KPASSWD commands because an illegal state occurred.

```
981 - nonfatal software warning, code = 8504 at "..."
981 - nonfatal software warning, code = 8505 at "..."
```

Clock Skew - `There has been too large a difference in time between the comunications server's time and the Kerberos ticket. Check the timeserver or timezone settings for the server.`

```
980 - Fatal software error, code = 8501 at "..."
980 - Fatal software error, code = 8503 at "..."
982 - Software Exception Information, code = 8501 at ".."
982 - Software Exception Information, code = 8503 at ".."
```

These errors indicate Kerberos tried to notify another task in the server and the notification system failed.

Appendix B

Glossary

authenticator Information which, when compared to information in a Kerberos ticket, proves or disproves that a client (user) presenting the ticket is the same one to which the ticket was issued. When a client sends a ticket to a Kerberos server or service (other than to the authentication server), the client always sends an authenticator along with the ticket.

authentication server A Kerberos server that validates the identity of a user and issues the initial ticket (the ticket-granting ticket) to the user. The user then can use this ticket to request service tickets from a TGT server. The authentication server runs on a host computer.

Cerberus An alternate spelling of Kerberos. See **Kerberos**

communications server. A device on the network that distributes communications between hosts that contain applications and files, and display terminals or printers.

instance A distinct occurrence of a client or service. For example, an instance can specify a host computer that provides the service. The rlogin service on the host computer named *accounting* is distinct from the rlogin service on the host computer named *engineering*. For a client, the instance can identify different privileges in different situations. For example, John Smith operating as a project leader might have different privileges from John Smith operating as a normal user.

KDC Key Distribution Center. A Kerberos server that performs the functions of both the authentication server and the ticket-granting ticket (TGT) server.

Kerberos™ An authentication and authorization system for open network computing environments that was developed as part of Project Athena™ at the Massachusetts Institute of Technology. The name Kerberos refers to the authentication service itself, its protocol, or its (program) code.

kerberized, kerberized service A service protected by Kerberos.

PAK Product Authorization Key. The PAK is a unique, server-specific code that is used by the server software to determine which optional features (e.g., Kerberos) are authorized for use.

Performance Series server An Emulex communications server. Models that support the Kerberos feature must run software release 2.2.1 or greater and have the appropriate PAK.

private key A type of key that only the client (user) or host server knows. This key is used to encrypt information that only one or the other can read or modify. This key is a permanent key.

realm The name of an administrative entity (domain) that maintains authentication data and within which the user is to be authenticated. A realm in Kerberos is similar in concept to an Internet domain.

RLOGIN Remote login. A protocol implemented in some versions of the UNIX operating system that provides remote terminal access. RLOGIN allows a terminal user to interact with a remote computer system at another site as if the user's terminal were connected directly to the remote computer.

rlogind Remote login daemon. A program ("daemon") that runs on a UNIX-based host computer and provides the RLOGIN feature on that computer. See **RLOGIN**.

server When used generically, refers to an Emulex Performance Series communications server.

session key A type of key that both client and host server "know". It is used to encrypt information that both the client and host server can read and modify. It is only good for one "session" between the client and host server.

ticket A Kerberos record that helps a client authenticate itself to a Kerberos server. A ticket is used to securely pass the identity of the person to whom the ticket was issued between the Kerberos authentication server and host-based end servers, as well as between users and host-based end servers.

ticket-granting ticket (TGT) server A Kerberos server that provides tickets for services (such as RLOGIN) to a user on a Performance Series server. The TGT server runs on a host computer.

Index