UNICOS® Kerberos Enigma Installation Guide

S–5294–10010

The UNICOS operating system is derived from UNIX System V. The UNICOS operating system is also based in part on the Fourth Berkeley Software Distribution (BSD) under license from The Regents of the University of California.

Record of Revision

Version	*Description*
9.2	December 1996 Original printing to support the 9.2 release of the UNICOS operating system.
9.3	July 1997 This guide supports the 9.3 release of the UNICOS operating system.
10.0	November 1997 This guide supports the 10.0 release of the UNICOS operating system.
10.0.0.6	July 1999 This guide supports the 10.0.0.6 release of the UNICOS operating system.
10.0.0.7	February 2000 This guide supports the 10.0.0.7 release of the UNICOS operating system.
10010	October 2001 This guide supports the 10.0.1.0 release of the UNICOS operating system.

Contents

Preface

This publication is for analysts who install and maintain system software on Cray computer systems. It contains procedures for installing UNICOS Kerberos Enigma, using the Common Installation Tool (CIT).

Related Publications

The following documents contain additional information that may be helpful:

- *Kerberos Administrator's Guide*
- *Common Installation Tool (CIT) Reference Card*
- *General UNICOS System Administration*
- *UNICOS Resource Administration*
- *UNICOS Configuration Administrator's Guide*
- *UNICOS Networking Facilities Administrator's Guide*
- *NQE Administration*
- *Tape Subsystem Administration*

Ordering Printed Publications

To order printed copies of software publications, contact the Cray Software Distribution Center in any of the following ways:

E-mail:
`orderdsk@cray.com`

Web:
`http://www.cray.com/swpubs/`

Click on the `Download Request Form` link.

Telephone (inside U.S., Canada):
1–800–284–2729 (BUG CRAY), then 605–9100

Telephone (outside U.S., Canada):
Contact your account or service representative, or call +1–651–605–9100

Fax:
+1–651–605–9001

Mail:
Software Distribution Center
Cray Inc.
1340 Mendota Heights Road
Mendota Heights, MN 55120–1128
USA

Conventions

The following conventions are used throughout this document:

Convention	Meaning
`command`	This fixed-space font denotes literal items, such as file names, pathnames, man page names, command names, and programming language elements.
`manpage`(*x*)	Man page section identifiers appear in parentheses after man page names. The following list describes the identifiers:

1	User commands
1B	User commands ported from BSD
2	System calls
3	Library routines, macros, and opdefs
4	Devices (special files)
4P	Protocols
5	File formats
7	Miscellaneous topics
7D	DWB-related information
8	Administrator commands

Some internal routines (for example, the `_assign_asgcmd_info`() routine) do not have man pages associated with them.

variable	Italic typeface indicates an element that you will replace with a specific value. For instance, you may replace *filename* with the name `datafile` in your program. It also denotes a word or concept being defined.
`user input`	This bold, fixed-space font denotes literal items that the user enters in interactive sessions. Output is shown in nonbold, fixed-space font.
[ ]	Brackets enclose optional portions of a syntax representation for a command, library routine, system call, and so on.
...	Ellipses indicate that a preceding element can be repeated.

Reader Comments

Please contact us with any comments that will help us to improve the accuracy and usability of this manual. Be sure to include the title and number of the document with your comments. We value your comments and will respond to them promptly. Contact us in any of the following ways:

E-mail:
`swpubs@cray.com`

CRInform (for subscribers):
`http://crinform.cray.com`

Click on the `Report a Software Problem` link. Use `PUBLICATIONS` for the group name, `PUBS` for the command, and `NO-LICENSE` for the release name.

Telephone (inside U.S., Canada):
1–800–950–2729 (Cray Customer Support Center)

Telephone (outside U.S., Canada):
Contact your account or service representative, or call +1–715–726–4993 (Cray Customer Support Center)

Mail:
Software Publications
Cray Inc.
1340 Mendota Heights Road

Mendota Heights, MN 55120–1128
USA

Installing UNICOS Kerberos Enigma [1]

This chapter contains procedures for installing the UNICOS Kerberos Enigma software, using the Common Installation Tool (CIT).

Each release of the UNICOS operating system has a corresponding release of the Kerberos Enigma software. Before installing the Kerberos Enigma software, you should verify that the corresponding UNICOS release has been installed on the system and is properly configured.

> **Note:** Kerberos Enigma software must be reinstalled whenever the UNICOS operating system is updated or changed.

1.1 UNICOS Kerberos Enigma CD

The UNICOS Kerberos Enigma CD contains the Kerberos Enigma software that can be used for upgrade installations. Depending upon the type of system onto which you are loading the UNICOS Kerberos Enigma CD, the path to these packages can be:

`/cdrom/cdrom0` (SWS is a Sun SPARC 5 system.)

Three types of Kerberos Enigma software are distributed:

`krb_dom` *Domestic_Kerberos* is the Common Installation Tool (CIT) name for this package. It is a binary-only version of Kerberos for domestic sites.

`krb_for` *International_Kerberos* is the CIT name for this package, which is a binary-only version of Kerberos for international sites.

`krb_src` *Kerberos_Source* is the CIT name for this package, which is a source version of Kerberos for properly licensed domestic sites.

Sites should install the UNICOS Kerberos Enigma software after they have successfully completed installing and configuring the UNICOS operating system. Kerberos Enigma installation should be done as a separate step because it involves loading new software, rebuilding a UNICOS kernel, configuring various system daemons, and possibly restarting a system.

1.2 Select a UNICOS Kerberos Enigma Installation Procedure

Two different procedures exist for installing the UNICOS Kerberos Enigma software. One procedure is for installing the software on one system at a time, and the other procedure is for installing the software concurrently on four mainframes that make up a Cray SV1 SuperCluster building block.

If the UNICOS Kerberos Enigma software is to be installed on a single Cray mainframe, go to Section 1.3. If the UNICOS Kerberos Enigma software is to be installed on a Cray SV1 SuperCluster building block, go to Section 1.4.

1.3 Installation of the UNICOS Kerberos Enigma Package on a Single System

This section explains how to prepare for and install the UNICOS Kerberos Enigma software on a single system.

1.3.1 Prepare for the Upgrade on a Single System

Before you start the Kerberos Enigma installation process, you must have completed the following tasks:

- Completely loaded the corresponding UNICOS release.
- Completed the network system configuration so that it is up and running.
- Verified that the `/mnt/usr/src` partitions have already been made, labeled, and mounted.

Before starting the Kerberos Enigma installation and CIT, you must properly set up two `.rhosts` files.

For GigaRing based systems you must perform the following steps:

- Verify that the `~crayadm/.rhosts` file on the SWS allows root to send remote shell commands to the SWS from the mainframe.
- Verify that the `/.rhosts` file on the Cray mainframe allows `crayadm` to send remote shell commands to the mainframe from the SWS.

For Model E based systems you must perform the following steps:

- Verify that the `~cri/.rhosts` file on the OWS allows root to send remote shell commands to the OWS console from the mainframe.

- Verify that the `/.rhosts` file on the Cray mainframe allows `cri` to send remote shell commands to the mainframe from the OWS.

For Cray J90 systems you must perform the following steps:

- Verify that the `~crayadm/.rhosts` file on the OWS console allows `root` to send remote shell commands to the SWS from the mainframe.
- Verify that the `/.rhosts` file on the Cray mainframe allows `crayadm` to send remote shell commands to the mainframe from the OWS console.

Note: For more information on the communications path between the OWS/SWS console and the Cray mainframe, see the *Common Installation Tool (CIT) Reference Card*, which can be printed from the /*cdrom_mountpoint*/`CYRIinstall/2218.ps` PostScript file.

1.3.2 Start the Kerberos Enigma Software Installation for a Single System

Once you have prepared the workstation or console, perform the following steps to load the Kerberos Enigma software onto the Cray mainframe.

1. Insert the UNICOS Kerberos Enigma CD-ROM into the OWS/SWS console.
2. Log in to the OWS/SWS workstation as `crayadm`.
3. If your workstation does not automount the CD-ROM, you should be able to do so by:

```
OWS% su root
OWS# mount -t hsfs -r /dev/sr0 /CDROM
OWS# exit
```

4. Use CIT to install the Kerberos Enigma software by loading it from the OWS or SWS console to the Cray mainframe by executing the following command:

```
workstation% /cdrom_mountpoint/setup -c CrayNetworkNodeName -l root
```

The installation log files are located on the workstation as `/tmp/cit.`*workstation_username*`/*.log`.

For more information about using CIT, see the *Common Installation Tool (CIT) Reference Card*, which can be printed from the /*cdrom_mountpoint*/`CYRIinstall/2218.ps` PostScript file. You may also select the `Help` button from the GUI, or enter **`help all`** at the interactive interface prompt.

a. Select the Kerberos Enigma release.

b. Install the Kerberos Enigma release.

c. Verify that the Cray mainframe information is correct. If it is not, correct the information in CIT.

d. Quit CIT when you have finished loading the UNICOS release.

5. Undo the changes made in section 1.3.1.

   For GigaRing based systems you must perform the following steps:

   a. Remove the `root` entry from the `~crayadm/.rhosts` file on the SWS.

   b. Remove the `crayadm` entry from the `/.rhosts` file on the Cray system.

   For Model E based systems you must perform the following steps:

   a. Remove the `root` entry from the `~cri/.rhosts` file on the SWS.

   b. Remove the `cri` entry from the `/.rhosts` file on the Cray system.

   For Cray J90 systems you must perform the following steps:

   a. Remove the `root` entry from the `~crayadm/.rhosts` file on the OWS.

   b. Remove the `crayadm` entry from the `/.rhosts` file on the Cray system.

1.4 Installation of the UNICOS Kerberos Enigma Package on a Cray SV1 SuperCluster Building Block

This section explains how to prepare for and install the UNICOS Kerberos Enigma software on a Cray SV1 SuperCluster building block.

1.4.1 Prepare for the Upgrade on a Cray SV1 SuperCluster Building Block

Before you start the Kerberos Enigma installation process, you must have completed the following tasks on each mainframe in the SuperCluster building block.

- Completely loaded the corresponding UNICOS release.
- Completed the network system configuration so that it is up and running.
- Verified that the `/mnt/usr/src` partitions have already been made, labeled, and mounted.

Before starting the Kerberos Enigma installation and CIT, you must properly set up the `.rhosts` files on each mainframe in the SuperCluster building block and on the SWS.

- Verify that the `~crayadm/.rhosts` file on the SWS allows root to send remote shell commands to the SWS from each mainframe in the SuperCluster building block.
- Verify that the `/.rhosts` file on each Cray mainframe in the SuperCluster building block allows `crayadm` to send remote shell commands to the mainframe from the SWS.

For more information on the communication path between the SWS and the Cray mainframe, see the *Common Installation Tool (CIT) Reference Card*, which can be printed from the /*cdrom_mountpoint*/`CYRIinstall/2218.ps` PostScript file.

1.4.2 Start the Kerberos Enigma Software Installation for a Cray SV1 SuperCluster Building Block

Once you have prepared the mainframes in the SuperCluster building block and the SWS, perform the following steps to install the UNICOS Kerberos Enigma software on a Cray SV1 SuperCluster building block.

Note: Throughout this procedure, you must replace every occurrence of `sn`*SuperClusterSerialNumber* with your Cray SV1 SuperCluster system name.

1. Find the `SuperClusterMap` file, which should be located on the SWS in `/opt/CYRIos/sn`*SuperClusterSerialNumber*, and enter the following command to create an environment variable to define the location of the `SuperClusterMap` file for future use:

```
sws% export SUPERCLUSTERMAP=/opt/CYRIos/snSuperClusterSerialNumber/SuperClusterMap
```

2. Edit the `SuperClusterMap` file. Update the file's parameters to match your site's SuperCluster building block. Execute the following command on the SWS:

```
sws% vi $SUPERCLUSTERMAP
```

This file contains information that is needed to automatically load the Kerberos Enigma software on the SuperCluster building block. Any entry with a `[#]` value means that there are four entries of this type that need to be provided in the map file, for example:

```
CRAYHOST[1]=value
CRAYHOST[2]=value
CRAYHOST[3]=value
```

```
CRAYHOST[4]=value
```

All array entries with the same number identify information for the same machine in the SuperCluster building block (that is, all array entries with the number 1 refer to the first system's related information).

The critical parts of the `SuperClusterMap` file that are needed for the installation are as follows:

`SYS_CDROM` Path to the CD-ROM image on the SWS after being mounted (be sure to include `UNICOS_exe` at the end of the path).

`CRAYHOST[#]` Cray network node name.

3. On the SWS, load the CD-ROM that contains the UNICOS Kerberos Enigma release.

4. On the SWS, change directories to the CD-ROM mount point and run the setup script. This script will start a CIT invocation for each mainframe in the SuperCluster building block.

```
sws% cd /cdrom_mount/Kerberos_package_directory
sws% ./SuperCluster.load -l root
```

The preceding script will allow four installations of the Kerberos Enigma software to take place simultaneously instead of sequentially.

The installation log files are located on the workstation as `/tmp/cit.`*workstation_username*`/*.log`.

For more information about using CIT, see the *Common Installation Tool (CIT) Reference Card*, which can be printed from the /*cdrom_mountpoint*/`CYRIinstall/2218.ps` PostScript file. You may also select the `Help` button from the GUI, or enter **`help all`** at the interactive interface prompt.

5. Select the Kerberos Enigma package in CIT and install it in each CIT invocation, one for each mainframe in the SuperCluster building block.

   a. Verify that the Cray mainframe information is correct. If it is not, correct the information in CIT.

   b. Quit CIT when the Kerberos Enigma package has finished loading on each mainframe in the SuperCluster building block.

6. To undo the `/.rhosts` file changes made in section 1.4.1, perform the following steps:

   a. Remove the `root` entry for each mainframe from the `~crayadm/.rhosts` file on the SWS.

   b. Remove the `crayadm` entry from the `/.rhosts` file on each Cray mainframe.

Configuring UNICOS Kerberos Enigma [2]

This chapter contains procedures for configuring UNICOS Kerberos Enigma software using the Installation and Configuration Menu System (ICMS). See *UNICOS System Configuration Using ICMS*, for instructions on importing the UNICOS configuration into ICMS.

2.1 Using ICMS to Configure `config.h` for Kerberos

Before starting `nmake`, be sure you have imported the latest UNICOS configuration into ICMS. See *UNICOS System Configuration Using ICMS* for instructions.

If your site chooses to run AUTH-KERB NFS:

1. Install UNICOS Kerberos Enigma per the instructions in Chapter 1 of this manual.
2. Ensure your site has an ONC+ license to run the `NFSKRB` package (NSF with Kerberos encryption).
3. Configure the `Network File System Kerberos (NFSKRB)` to `on` from the ICMS `Major Software Configuration` menu.
4. Build and configure Kerberos per the instructions in this chapter. (Pay special attention to AUTH-KERB and `NFSKRB` information.)

2.1.1 Updating `config.mh`

From the `Configure System` menu in ICMS, select the `Major Software Configuration` menu. Configure the `Kerberos network data encryption` to `on`. If you are not running the `Network File System Kerberos (NFSKRB)` configure it to `off`. Note both of these values in the following screen snapshot.

```
Major Software Configuration

     Cray machine system name                     unicos
     Cray machine node name                       unicos
     System version name
     BMM functional unit support                  off
     HIPPI device support                         on
     File quotas                                  on
     Ipi3 tape driver support
     TCP/IP network system (TCP)                  on
     X11 window management system                 on
     Remote Procedure Call (RPC)                  on

 S-> Kerberos network data encryption             on

     Network File System (NFS)                    on
     Network File System Version 3 (NFS3)         on

     (if not configuring AUTH-KERB)
     Network File System Kerberos (NFSKRB)        off

     Network Information Service (NIS)            off
     Cray-based network monitor                   on
     Network testing tools                        on
     Online tape support                          on
     Cray/REELlibrarian                           off
     DCE Distributed File Service (DFS)           on
     Online diagnostics directory                 /ce
     Cross-targeted (XLIBS) libraries             off
     Cross-targeted library characteristics
     Mixed-mode CPU (MIXED) libraries             off
     Mixed-mode library characteristics

     Asychronous Software

     MPP support
     Cray/REELlibrarian                            off
     Data migration (DMF)                          off
     Import the major configuration ...
     Activate the major configuration ...

          The values below are updated by the
          mainframe hardware configuration menu

     Cray machine serial number                    0
```

2.1.2 Activating Kerberos with ICMS

The following procedure saves the changes you made previously into a new `config.mh` file.

From the `Configure System` menu, select the `Major Software Configuration` menu.

In the `Major Software Configuration` menu, press the TAB key to move to `Activate the major configuration` (shown in bold type below) and press RETURN.

```
Major Software Configuration

     .
     .
     .
     Data migration (DMF)

     Import the major configuration ...
 A-> Activate the major configuration ...

          The values below are updated by the
          mainframe hardware configuration menu

     Cray machine serial number                    0
```

2.2 Building Kerberos when UNICOS Is Already Built

Follow the steps in this section to add Kerberos to a running or assembled UNICOS system.

It is recommended that you install and build the NFSKRB software **after** the UNICOS operating system is configured and built. When you have completed all the instructions in this chapter and UNICOS Kerberos Enigma software is added, you will need to rebuild the kernel.

2.2.1 Step 1. Remove Executables

Before you build the Kerberos libraries, commands, and daemons, you must remove the old executable files from the related directories. You will remove executables from:

`crypt`

`ed`

`makekey`

`vi`

`kerberos/appl`

`kerberos/cmd`

`ftp`

`ftpd`

`telnet`

`telnetd`

`tftp`

`tftpd`

`mountd`

`kerbd` (Remove the `kerbd` executable only if `NFSKRB` is configured to `on` in the `Major Software Configuration` menu.)

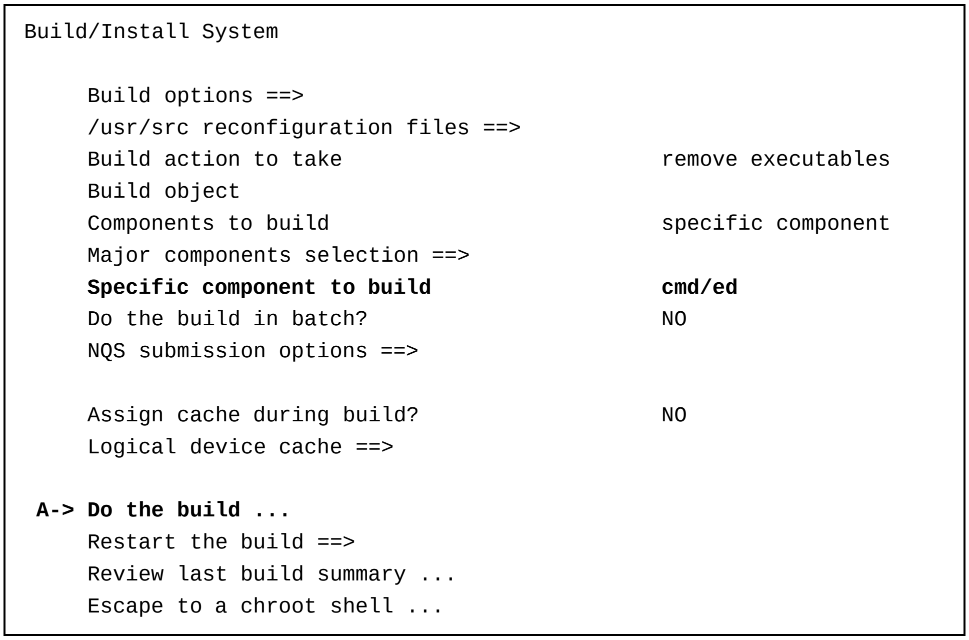
To remove executables from these directories, enter ICMS and select the `Build/Install System` menu. Set `Specific component to build` values (shown in bold type in the sample screen snapshot on page 13) as follows:

Product	`Specific_component_to_build` setting
`crypt`	`cmd/crypt`
`ed`	`cmd/ed`
`makekey`	`cmd/makekey`
`vi`	`cmd/vi`

appl	net/kerberos/appl
cmd	net/kerberos/cmd
ftp	net/tcp/usr/ucb/ftp
ftpd	net/tcp/usr/etc/ftpd
telnet	net/tcp/usr/ucb/telnet
telnetd	net/tcp/usr/etc/telnetd
tftp	net/tcp/usr/ucb/tftp
tftpd	net/tcp/usr/etc/tftpd
mountd	net/nfs/cmd/mountd
kerbd	net/onc/cmd/kerberos (only if Network File System Kerberos (NFSKRB) is configured on in the Major Software Configuration)

Activate new executable values by pressing RETURN after entering each one. Check output for warnings and error messages.

Example screen snapshot:



```
Build/Install System

     Build options ==>
     /usr/src reconfiguration files ==>
     Build action to take                          remove executables
     Build object
     Components to build                           specific component
     Major components selection ==>
     Specific component to build                   cmd/ed
     Do the build in batch?                        NO
     NQS submission options ==>

     Assign cache during build?                    NO
     Logical device cache ==>

 A-> Do the build ...
     Restart the build ==>
     Review last build summary ...
     Escape to a chroot shell ...
```

2.2.2 Step 2. Build Libraries, Commands, and Daemons

The next step is to build the necessary libraries, commands, and daemons for Kerberos. Install and build them in the following order:

`libcrypt`

`libc`

`crypt`

`ed`

`makekey`

`vi`

`krb`

`appl`

`cmd`

`libtelnet` (only if this is a Kerberos installation at a domestic site)

`telnet`

`telnetd`

`ftp`

`ftpd`

`tftp`

`tftpd`

`mountd`

`kerbd` (only if `Network File System Kerberos (NFSKRB)` is configured to `on` in the `Major Software Configuration` menu)

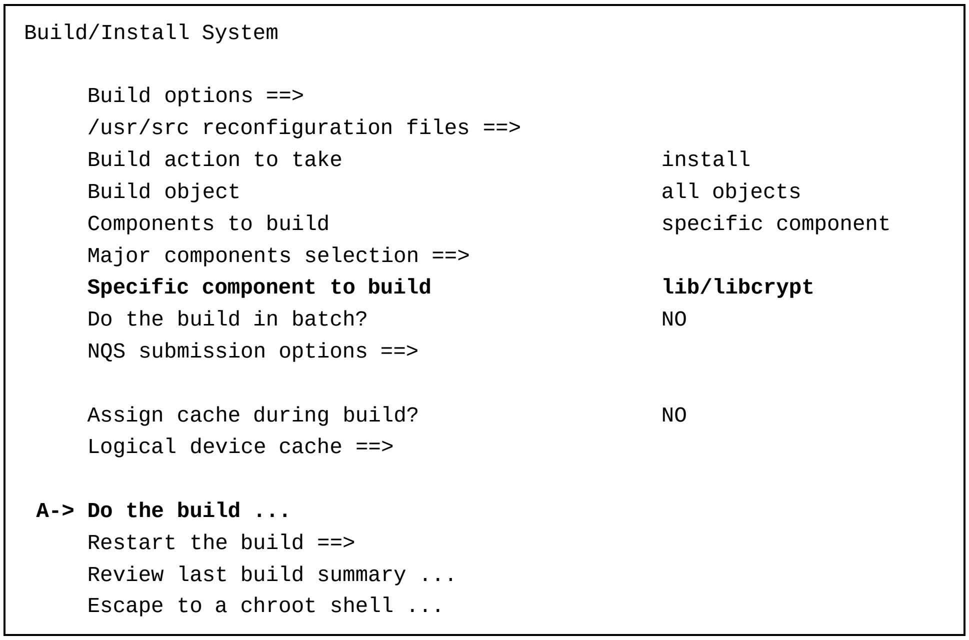
To install and build the preceding libraries, commands, and daemons, stay in ICMS and select the `Build/Install System` menu. Set the `Specific component to build` values (shown in bold type in the screen snapshot on page 15) as follows:

Product	`Specific_component_to_build` setting
`libcrypt`	`lib/libcrypt`
`libc`	`lib/libc`
`crypt`	`cmd/crypt`

`ed`	`cmd/ed`
`makekey`	`cmd/makekey`
`vi`	`cmd/vi`
`krb`	`net/kerberos/lib/krb`
`appl`	`net/kerberos/appl`
`cmd`	`net/kerberos/cmd`
`libtelnet`	`net/tcp/usr/libtelnet` (only if this is a UNICOS Kerberos Enigma installation at a domestic site)
`ftp`	`net/tcp/usr/ucb/ftp`
`ftpd`	`net/tcp/usr/etc/ftpd`
`telnet`	`net/tcp/usr/ucb/telnet`
`telnetd`	`net/tcp/usr/etc/telnetd`
`tftp`	`net/tcp/usr/ucb/tftp`
`tftpd`	`net/tcp/usr/etc/tftpd`
`mountd`	`net/nfs/cmd/mountd`
`kerbd`	`net/onc/cmd/kerberos` (only if `NFSKRB` is turned `on` in the `Major Software Configuration` menu)

Activate new executables values by pressing `RETURN` after entering each value. Check the output for warnings and error messages.

Example screen snapshot:



```
Build/Install System

     Build options ==>
     /usr/src reconfiguration files ==>
     Build action to take                          install
     Build object                                  all objects
     Components to build                           specific component
     Major components selection ==>
     Specific component to build                   lib/libcrypt
     Do the build in batch?                        NO
     NQS submission options ==>

     Assign cache during build?                    NO
     Logical device cache ==>

 A-> Do the build ...
     Restart the build ==>
     Review last build summary ...
     Escape to a chroot shell ...
```

2.2.3 Step 3. Set Multilevel Security Parameters

Because the multilevel security (MLS) feature is available by default in the UNICOS operating system, sites that run with the Privilege Assignment Lists (PAL)-based privilege mechanism are required to run the `privcmd`(8) command when changes are made in which new system configuration files are created or new kernels are built.

The `privcmd` command must be executed on the running `root` and `usr` file systems. When running `privcmd` on backup or non-running `root` and `usr` file systems, you will need to run `privcmd` in a `chroot`(8) environment. The following example shows how this is typically done:

```
unicos# /bin/chroot /mountpoint /usr/gen/bin/ksh
unicos# /etc/privcmd
unicos# exit
```

2.3 Configuring Kerberos

The following sections describe how to modify specific system files in order for your site to use Kerberos.

2.3.1 Configuring /etc/krb.conf

Usually the Kerberos configuration file is named /etc/krb.conf in UNICOS applications. This file contains information about the local Kerberos configuration.

Create this file using vi or another editor. A sample /etc/krb.conf file follows. The /etc/krb.conf file should have permissions set to 644 and be owned by root.

```
CRAY.COM
CRAY.COM   krb_server_1
CRAY.COM   krb_server_2
CRAY.COM   krb_server_1            admin server
```

Line 1 specifies the name of the local realm. In the example file, this is simply CRAY.COM. (You are free to name your realm whatever you choose; however, the realm name in the /etc/krb.conf file must match the realm name used to create the Kerberos database on the Kerberos server.) Lines 2 and 3 list the host names for two Kerberos servers, krb_server_1 and krb_server_2. These are the servers that the Kerberos software will ask for tickets. The software searches the /etc/krb.conf file from the top and tries each listed server until it obtains a response.

The last line indicates the location at which the Kerberos administrative server process is running. It is recommended that only one administrative server process be configured, because no mechanism is in place to propagate changes to the Kerberos principal database from a slave to the primary server.

2.3.2 Configuring /etc/services

The network services configuration file, /etc/services, should be modified to support running Kerberos utilities and/or kerberized clients and servers on the Cray system. Specifically, the following lines should be added:

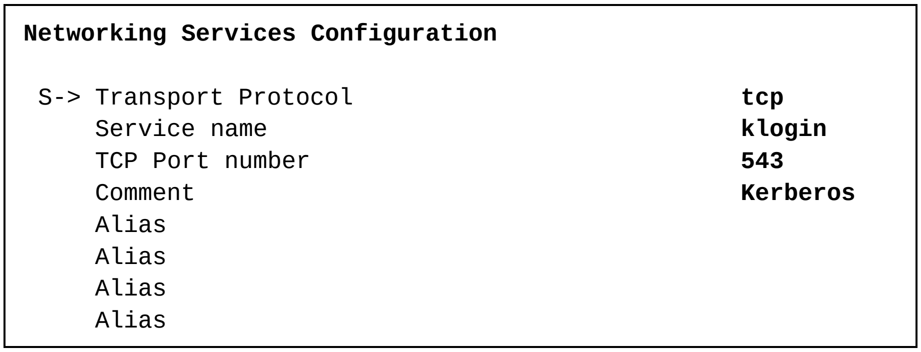
```
klogin            543/tcp         # Kerberos authenticated rlogin
kshell            544/tcp         # Kerberos authenticated rshell
kerberos          750/udp         # Kerberos server
kerberos_master   751/tcp         # Kerberos administrator
eklogin           2105/tcp        # Kerberos encrypted login
```

To use ICMS to configure the /etc/services file, follow these steps:

1. Select the following menu: `Configure System->Network Configuration->General Network Configuration->Networking Services Configuration`
2. At the `Networking Services Configuration` menu, press `n` to create a new record.
3. Press `RETURN` to select the new record.
4. Make new records for `klogin`, `kshell`, `kerberos`, `kerberos_master`, and `eklogin` as shown below:

   ```
   klogin            543/tcp      # Kerberos authenticated rlogin
   kshell            544/tcp      # Kerberos authenticated rshell
   kerberos          750/udp      # Kerberos server
   kerberos_master   751/tcp      # Kerberos administrator
   eklogin           2105/tcp     # Kerberos encrypted login
   ```

   Example screen snapshot:



```
Networking Services Configuration

 S-> Transport Protocol                                    tcp
     Service name                                          klogin
     TCP Port number                                       543
     Comment                                               Kerberos
     Alias
     Alias
     Alias
     Alias
```

5. After you have added all the records, press `e` to escape and respond `y` to the question,

   ```
   Do you want to update form file? (y/n):
   ```

2.3.3 Configuring `/etc/inetd.conf`

Use the menu system to add `kshd`, `klogin`, and `eklogin` to the `/etc/inetd.conf` file. Perform the following steps:

1. Select `Network Configuration->TCP/IP Configuration->Generic Internet Daemon Configuration` menu.

2. At the bottom of the `Generic Internet Daemon Configuration` menu, press `n` to create a new record.

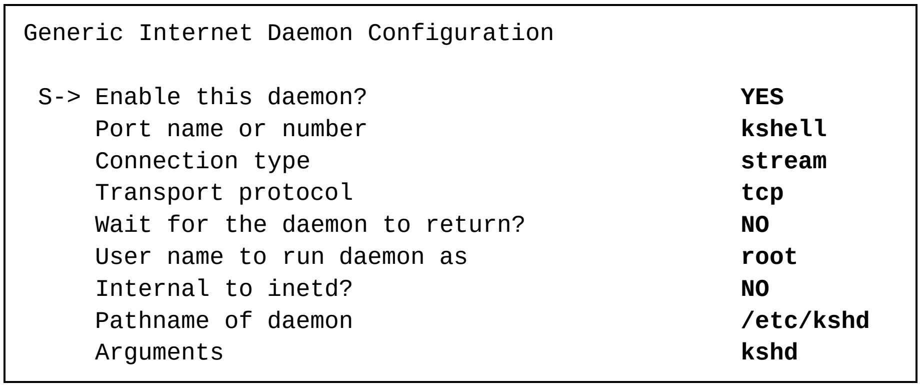
3. Press `RETURN` to select the new record.

4. Create the following new records:

   Note: If this is an international site (not United States or Canada) do not add `eklogin` to the `inetd.conf` file.

Port name or number	Pathname of daemon	Arguments
kshell	/etc/kshd	kshd
klogin	/etc/klogind	klogind
eklogin	/etc/klogind	eklogind

   Example screen snapshot:



```
Generic Internet Daemon Configuration

 S-> Enable this daemon?                                  YES
     Port name or number                                  kshell
     Connection type                                      stream
     Transport protocol                                   tcp
     Wait for the daemon to return?                       NO
     User name to run daemon as                           root
     Internal to inetd?                                   NO
     Pathname of daemon                                   /etc/kshd
     Arguments                                            kshd
```

5. After you have added the daemons, press `e` to escape and respond `y` to the question,

   ```
   Do you want to update form file? (y/n):
   ```

6. Activate the TCP/IP configuration. The menu system determines which components need updating. Respond `y` to the question:

   ```
   Do you want to proceed with the configuration update? (y/n)
   ```

2.3.4 Configuring /etc/srvtab

The `/etc/srvtab` file is generated on your site's Kerberos server by the Kerberos administrator on the Kerberos master server machine. The master server generates this binary file. This file must be securely transferred to the

Cray system and installed in `/etc/srvtab` with permissions set to `600` and ownership by `root`.

2.3.5 Signaling `inetd`

If your site has installed Kerberos on a running root, you must send a `kill` signal to the `inetd` daemon so that it will reread the configuration file (`inetd.conf`) to start using Kerberos.

```
ps -e | grep inetd
  1719 ?     0:27 inetd
# kill -1 1719
```

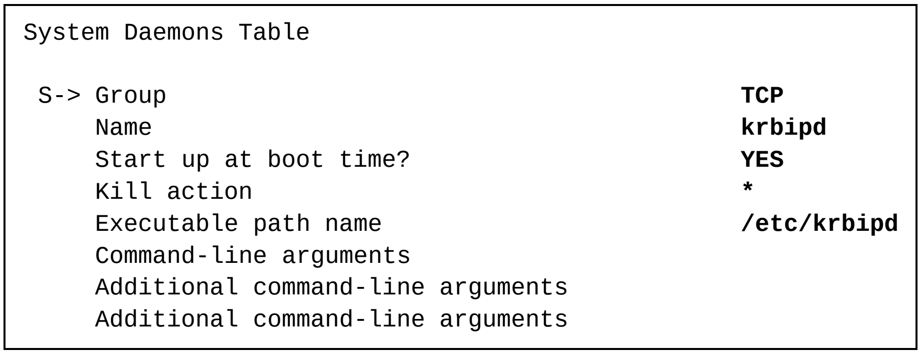
2.3.6 Configuring `krbipd` into `/etc/config/daemons`

If your site decides to run `krbipd`, the Kerberos RPC daemon for multi-homed machines (more than one network interface), configure the `krbipd` daemon to be started at boot time. Specifically, the following line should be added to `/etc/config/daemons`:

```
TCP   Krbipd  YES  *  /etc/krbipd
```

Use the menu system to add `krbipd` to the `/etc/config/daemons` file.

1. Select `Configure System->System daemons configuration->System daemons table` menu.
2. At the bottom of the `System daemons table` menu, press `n` to create a new record.
3. Press RETURN to select the new record.
4. Enter the new `krbipd` daemon as shown in the following example.



```
System Daemons Table

 S-> Group                                                **TCP**
     Name                                                 **krbipd**
     Start up at boot time?                               **YES**
     Kill action                                          *****
     Executable path name                                 **/etc/krbipd**
     Command-line arguments
     Additional command-line arguments
     Additional command-line arguments
```

5. When done, press `e` to end editing of the table.

6. When asked to update the system daemons table, enter `y` .

7. Select `Activate the daemons configuration`.

8. Press RETURN to activate the new system daemons configuration.

2.3.7 Restarting `/etc/krbipd`

To start `krbipd` on a running root, without rebooting the system, enter the following command:

```
# /etc/krbipd
```

2.3.8 Configuring kerbd into `/etc/config/daemons`

If your site has decided to run kerberized NFS (NFSKRB) as specified in the `Major Software Configuration` menu, you must add `kerbd` to the daemons to be started at boot time. Specifically, the following line should be added:

```
NFS  kerbd  YES  *  /etc/kerbd
```

Use the menu system to add `kerbd` to the `/etc/config/daemons` file.

1. Select `Configure System->System daemons configuration->System daemons table` menu.

2. At the bottom of the `System daemons table` menu, press `n` to create a new record.

3. Press RETURN to select the new record.

4. Enter the new kerbd daemon as follows.

```
System Daemons Table

 S-> Group                                           NFS
     Name                                            kerbd
     Start up at boot time?                          YES
     Kill action                                     *
     Executable path name                            /etc/kerbd
     Command-line arguments
     Additional command-line arguments
     Additional command-line arguments
```

5. When done, press e to end editing of the new record.
6. When asked to update the system daemons table, enter y .
7. Select Activate the daemons configuration.
8. Press RETURN to activate the new system daemons configuration.

2.4 Restarting /etc/kerbd

> **Note:** If you are not running a UNICOS kernel with UNICOS Kerberos Enigma included, proceed to Section 2.5 to complete the necessary tasks to finish your UNICOS Kerberos Enigma configuration.

You may be able to start /etc/kerbd on a running root without rebooting by entering the following command:

```
unicos# sdaemon -s kerbd
```

If this does not work, you will need to reboot the system **after** performing the tasks described in Section 2.5.

2.5 Tasks to Be Completed before Going into Multiuser Mode with Kerberos

The following tasks must be completed before running your system in multiuser mode with Kerberos. These tasks are described in section 4.2.1, ”Building a UNICOS Kernel from an Executable Release,”and subsequent sections in the book *UNICOS System Configuration Using ICMS*.

- Build a new kernel with UNICOS Kerberos Enigma included
- Prepare to test your UNICOS system with Kerberos
- Transfer UNICOS files to the workstation/console
- Shut down the current system
- Boot the UNICOS system with Kerberos
- Turn off MLS security logging
- Run the `instartup` script
- Run `/etc/privcmd`
- Complete the multilevel security configuration
- Turn on MLS security logging
- Enter multiuser mode
- Restart NQE checkpointed jobs or processes
- Access accounting data from the previous system

Index