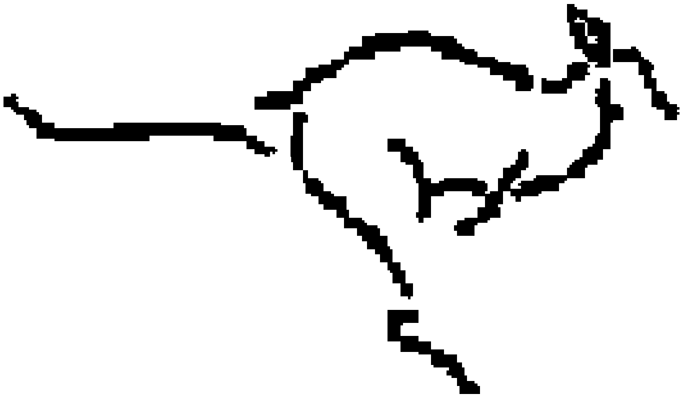
SKIP Reference Implementation

Installation and User's Guide

Release 2.0



Export Control Notice – The SKIP Reference Implementation is an export controlled product. It can only be distributed within the United States of America and Canada.

SKIP Reference Implementation Installation and User's Guide

Version: Release 2.0
Date: November 1995

© 1995 Sun Microsystems, Inc.

2550 Garcia Avenue, Mountain View, California 94043-1100 U.S.A.

All rights reserved. This product and related documentation are protected by copyright and are distributed under the license agreement displayed during installation. Please read the license agreement before using this product. Use of this product indicates acceptance of the license agreement.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

THIS PUBLICATION IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT.

THIS PUBLICATION COULD INCLUDE TECHNICAL INACCURACIES OR TYPOGRAPHICAL ERRORS. CHANGES ARE PERIODICALLY ADDED TO THE INFORMATION HEREIN; THESE CHANGES WILL BE INCORPORATED IN NEW EDITIONS OF THE PUBLICATION. SUN MICROSYSTEMS, INC. MAY MAKE IMPROVEMENTS AND/OR CHANGES IN THE PRODUCT AND/OR PROGRAM DESCRIBED IN THIS MANUAL AT ANY TIME.

TRADEMARKS:

Sun, Sun Microsystems, the Sun Microsystems logo SunScreen, and Solaris are all trademarks or registered trademarks of Sun Microsystems, Inc. All other product names mentioned herein are the trademarks of their respective owners.

All SPARC trademarks, including the SCD Compliant Logo, are trademarks or registered trademarks of SPARC International, Inc. SPARCstation, SPARCserver, SPARCengine, SPARCworks, and SPARCompiler are licensed exclusively to Sun Microsystems, Inc. Products bearing the SPARC trademarks are based upon an architecture developed by Sun Microsystems, Inc.

BUG REPORTING:

Bugs in the software or errors in the documentation should be reported to:
freeskip@incog.com

Table of Contents

List of Figures

Introduction

This document describes the *SKIP Reference Implementation v. 2.0* software package.

What is SKIP?

SKIP is an IP layer encryption package. Any two (or more) systems running SKIP will have the ability to encrypt all traffic between them.

How it Works

Assume we have two machines: alice.skip.com and bob.skip.com. Both sites have two keys: a public key, and a private key. Both have their public key signed by a trusted third party (the Certification Authority). Each system gets the other system's authenticated public key. By using the Diffie-Hellman Key Agreement algorithm, these two systems establish a *shared secret* unique to them. This shared secret could be used to encrypt data between the machines. But, since we plan on keeping the secret key for a medium to long term period of time, we want to use it more sparingly. So, we use this long-term key as a key to encrypt randomly generated traffic keys. These randomly generated keys will, in turn, be used to encrypt data. These traffic keys are sent as part of an IP Security Protocol (IPSP) packet.

Requirements

- The following platforms are supported:
  Sun SPARCstation 1, 1+, 2, Classic, LX, 5, 10 or 20 running Solaris 1.1.1 (SunOS 4.1.3 U1)
  Any Sun SPARC workstation running Solaris 2.4
  Any x86 personal computer running Solaris 2.4
- A minimum of 16 MB RAM is required, 32 MB RAM is recommended.
- A minimum of 6 MB free disk space is required for installation, 3MB of which will be permanently used.

Algorithms Supported

There are 3 sets of algorithms used with the SKIP Reference Implementation:

- **The long term secret key algorithm**. The Diffie-Hellman Key Agreement algorithm is used. SKIP uses a 1024-bit modulus and a 256-bit exponent by default.
- **The secret key encryption algorithm**. Keys are encrypted using conventional symmetric key cryptography:
  - 56 bit DES
  - 3 key Triple-DES, or
  - 64 bit Simplecrypt.

  The low order bits of the Diffie-Hellman secret functions as the key.
- **The traffic encryption algorithm**. Traffic is also encrypted using conventional symmetric key cryptography. A random traffic key is used as a key to encrypt data. The algorithms supported for traffic encryption are:
  - 56 bit DES,
  - 3 key Triple-DES, or
  - 64 bit Simplecrypt.

Installation - Solaris 1.x Systems

This section provides instructions for installing the SKIP Reference Implementation on Solaris 1.x (SunOS 4.1.3 u1) systems. If you are using Solaris 2.0, skip this section, and proceed to the next section.

Get the Software

If you do not already have the SKIP Reference Implementation software use the procedure below to obtain it.

1. Use your WWW browser and connect to ***http://skip.incog.com***.
2. Select whether you want to download the source and build `skip.tar.Z`, or whether you want to download the binaries. This section assumes that you have either built `skip.tar.Z`, or downloaded the binaries from the web site. For more information about downloading and building the source, refer to the information on the web site.
3. Follow the menus to the SKIP distribution page. This page will determine if you are eligible to receive the software.

Export Control Notice – The SKIP Reference Implementation is an export controlled product. It can only be downloaded to sites within the U.S.A. and Canada.

4. If you are eligible to receive the software, select **Solaris 1.x for SPARC**. Save it as a file named ***skip.tar.Z*** in a temporary directory where there is at least 20 MB free.

Get a Certificate

You must have a certificate in order to use the software. Use the procedure below to obtain a certificate.

1. Use your browser to follow the link from ***http://skip.incog.com*** to the *SKIP Experimental Certificate Issuer*. There is a link from both the SKIP distribution page and the SKIP software package retrieval page to the Certificate Issuer.
2. Fill in the form on that page and you will be issued a certificate.

Note – You will need to know the IP address of the machine on which you wish to install & run the software.

3. Save it in the same directory that you saved ***skip.tar.Z***. For this example, we will assume you save it in a file named ***issue-dsa***.

Unpack the Software

The software must be unpacked before it can be installed. Use the procedure below to do this.

1. Become root on your local system.
2. Change directory to `/usr` and verify that there is approximately 7 Mbytes of free space in `/usr`.
3. Type the following command, exactly as it is written below, substituting the name of the directory where you put skip.tar.Z for *directoryname*.

```
example# zcat directoryname/skip.tar.Z|tar -xvf -
```

You will see the files being extracted.

Install the Software

Before you can use the software, it must be installed. Use the procedure below to install the software.

1. Open a terminal window and become root.
2. Change directory to `/usr/skip`:
3. Use the `install.skip` command to install SKIP:

```
example# ./install.skip
```

4. The program will ask you a number of questions. For most of these you can safely use the default answer. Figure 1 shows the questions and responses for the installation.

```
example# cd /usr/skip
example# ./install.skip
install.skip: starting

install.skip: installing /etc/skip
                               saved old /etc/skip/rc file as rc.bak
install.skip: installing /var/skip
install.skip: updating /etc/rc.local
install.skip: verifying that your kernel configuration is suitable

Do you wish to continue with this script (y/n) [y]: y

Please enter the name of your current config file (ex: SKIP)

Current System Config File: [GENERIC]

your current kernel is suitable, no rebuild is needed

install.skip: installation successfully completed.  Please reboot your system.
install.skip: exiting
example#
```

Figure 1 Software Package Installation, Solaris 1.X

If the install program needed to reboot your system, then log in once more as root, switch to the directory where you stored the certificate for the system and continue as shown below:

5. Add */usr/skip/bin* to your path by typing:

   ```
   example# set path = ( /usr/skip/bin $path )
   ```

6. Install the certificate by typing:

   ```
   example# install_skip_keys issue-dsa
   ```

   This script will unpack the certificate file, verify the md5 checksums, and install the certificates, as shown in Figure 2.

```
example# install_skip_keys issue-dsa
uudecode...
Comparing MD5 Checksums...
Checksums are good.
Moving files into place....

Installation succesfully completed.
Please install your keys and reboot your system.
example#
```

Figure 2 Certificate Installation, Solaris 1.X

▼ Finishing Up

After the installation is completed, the temporary files should be deleted, and the system must be rebooted.

1. Add ***/usr/skip/bin*** to the path in your ***.login*** file.
2. Add the man pages by typing exactly:

```
example# setenv MANPATH /usr/share/man:/usr/skip/man
```

3. Still as root, reboot your system by typing:

```
example# reboot
```

4. After the system has rebooted, log back in and delete the ***skip.tar.Z*** file.
5. The machine is now ready to run SKIP.

Installation - Solaris 2.x Systems

This section provides instructions for installing the SKIP Reference Implementation on Solaris 2.0 systems. If you are using Solaris 1.x (SunOS 4.1.3 u1), use the previous section to install the SKIP Reference Implementation.

Get the Software

If you do not already have the SKIP Reference Implementation software use the procedure below to obtain it.

1. Use your WWW browser and connect to ***http://skip.incog.com***.
2. Select whether you want to download the x86 or SPARC binaries.
3. Follow the menus to the SKIP distribution page. This page will determine if you are eligible to receive the software.

Export Control Notice – The SKIP Reference Implementation is an export controlled product. It can only be downloaded to sites within the U.S.A. and Canada.

4. If you are eligible to receive the software, select Solaris 2.x for SPARC/x86. Save it as a file named ***skip.tar.Z*** in a temporary directory where there is at least 20 MB free.

Get a Certificate

You must have a certificate in order to use the software. Use the procedure below to obtain a certificate.

1. Use your browser to follow the link from ***http://skip.incog.com*** to the *SKIP Experimental Certificate Issuer*. There is a link from both the SKIP distribution page and the SKIP software package retrieval page to the Certificate Issuer.
2. Fill in the form on that page and you will be issued a certificate.

Note – You will need to know the IP address of the machine on which you wish to install & run the software.

3. Save it in the same directory that you saved ***skip.tar.Z***. For this example, we will assume you save it in a file named ***issue-dsa***.

▼ Unpack the Software

The software must be unpacked before it can be installed. Use the procedure below to do this.

1. Become root on your local system.
2. If you are not already in the directory where you saved `skip.tar.Z`, switch to it now. Make sure you have enough space in the directory (7 Mb.)
3. Type the following command, exactly as it is written below.

```
example# zcat skip.tar.Z|tar -xvf -
```

It will create a new directory `SUNWicgES`. You will see the files being extracted.

▼ Install the Software

Before you can use the software, it must be installed. Use the procedure below to install the software.

Note – You must be able to become root on your system in order to install this software.

1. Open a terminal window and become root.
2. If you are using NFS, make sure root can read the directory into which you unpacked the software.
3. Use the standard Sun *pkgadd* command to add the software. In the same directory which holds `SUNWicgES`, type:

```
# pkgadd -d `pwd`
```

Note – be careful to use the back-quote character in the command above

4. You should be prompted with a small menu of packages to install, similar to Figure 3. Choose `SUNWicgES`.

```
example# pkgadd -d `pwd`

The following packages are available:
  1  SUNWicgES     Solaris SKIP 2.0 Software
                   (sparc) 2.0

Select package(s) you wish to process (or 'all' to process
all packages). (default: all) [?,??,q]: 1
```

Figure 3 Package Installation Menu, Solaris 2.0

5. The program will ask you a number of questions, all of which must be answered **y** as shown in Figure 4. When you get back to the same small menu of packages, type **q** to quit.

```
.
             (header and standard license stuff)
.
.
This package contains scripts which will be executed with super-user
permission during the process of installing this package.

Do you want to continue with the installation of <SUNWicgES> [y,n,?] y

Installing Solaris SKIP 2.0 Software as <SUNWicgES>

## Installing part 1 of 1.

.
.
             (files are listed as they are installed)
.
.
## Done ##

Installation of <SUNWicgES> was successful.

The following packages are available:
  1  SUNWicgES     Solaris SKIP 2.0 Software
                   (sparc) 2.0

Select package(s) you wish to process (or 'all' to process
all packages). (default: all) [?,??,q]: q
```

Figure 4 Software Package Installation

6. Add */opt/SUNWicg/bin* to your path by typing:

```
# PATH=/opt/SUNWicg/bin:$PATH
# export PATH
```

7. Install the certificate by typing:

```
# install_skip_keys issue-dsa
```

This script will unpack the certificate file, verify the md5 checksums, and install the certificates, as shown in Figure 5.

```
example# install_skip_keys issue-dsa
uudecode...
Comparing MD5 Checksums...
Checksums are good.
Moving files into place....

Installation succesfully completed.
Please install your keys and reboot your system.
example#
```

Figure 5 Certificate Installation

▼ Finishing Up

After the installation is completed, the temporary files should be deleted, and the system must be rebooted.

1. Add `/opt/SUNWicg/bin` to the PATH in your `.profile` file.
2. Add the man pages by typing exactly:

   ```
   example# export MANPATH=/usr/share/man:/opt/SUNWicg/man
   ```

3. Still as root, reboot your system by typing:

   ```
   example# reboot -- -r
   ```

4. After the system has rebooted, log back in and delete the `skip.tar.Z` file and the `SUNWicgES` directory.
5. The machine is now ready to run SKIP.

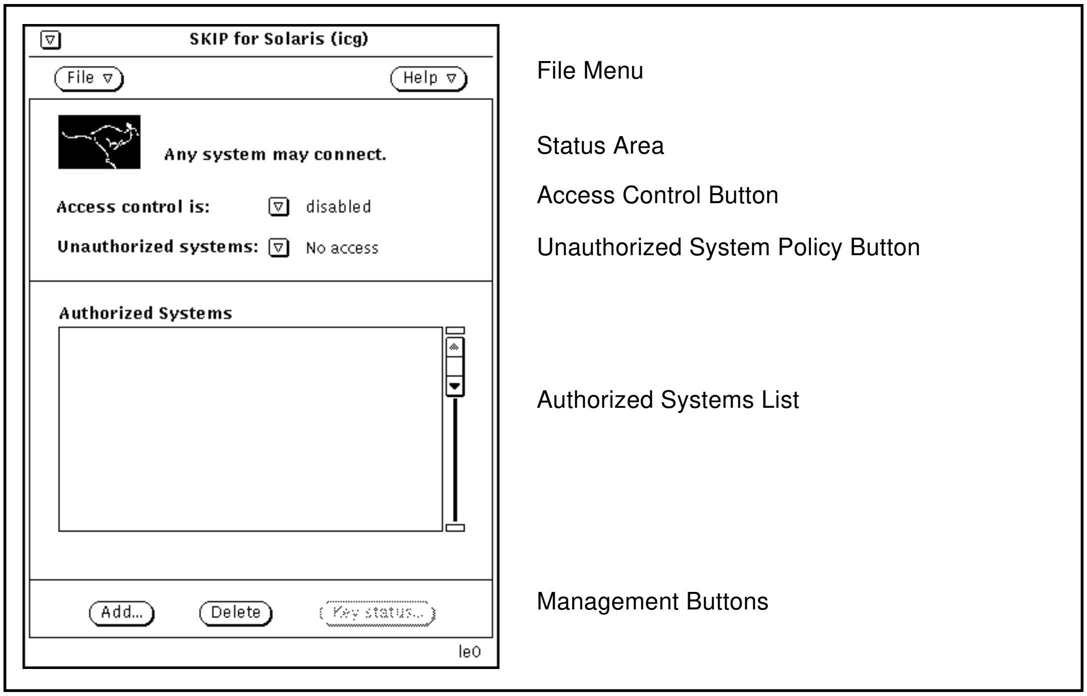
Using skiptool

The main tool you will use to administer SKIP on your machine is skiptool. This is a graphical user interface which will allow you to enable SKIP, set the type of encryption used, and set up how to deal with hosts that do not use SKIP. This section describes how to use skiptool. Similar functionality is available using the command line tool `skiphost(1/1m)`.

Starting skiptool

Note – You must be able to become root on your system in order to run skiptool.

1. Open a window and become root.
2. As root, type **`skiptool &`**. The main window of skiptool will appear (Figure 6).



Any system may connect.

Access control is: disabled

Unauthorized systems: No access

Figure 6 skiptool Main Window

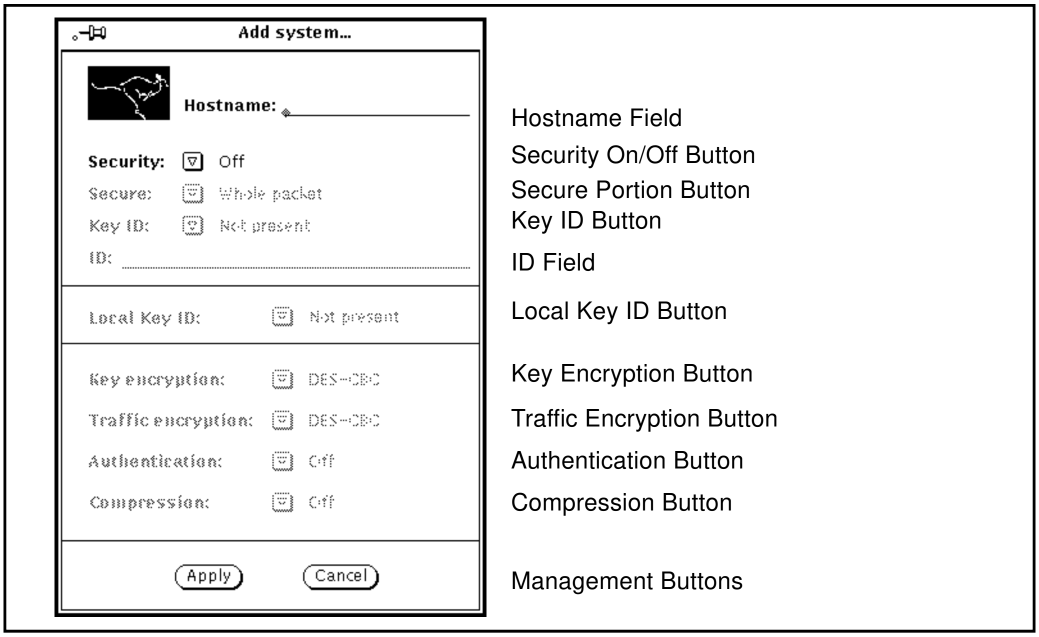
▼ skiptool Main Menu

The main screen of the skiptool GUI has six major components. They are described below, and shown in Figure 6.

- **File Menu**. The file menu has three submenus:
    - *Key Management* - Defines the parameters for key usage, including when to delete an unused key (in seconds), and how much to transmit per key (in Kbytes).
    - *SKIP Statistics*- Brings up one of four *Statistics* windows: *Interface Stats, Header Stats, Algorithm Stats*, or *Key Stats.*
    - *Save*
- **Status Area**. This area shows the status of the SKIP kernel. This will be either *Any system may connect* (if Access Control is disabled), or *[number] systems may connect,* (if Access control is enabled).
- **Access Control Button**. This button toggles whether SKIP is enabled or disabled. When enabled, only those systems listed in the Authorized Systems List can connect. When disabled, any system can connect.
- **Unauthorized System Policy Button**. This button is used to set the policy regarding Unauthorized System. The policy can be:
    - *No access* - don't allow unauthorized systems to connect.
    - *Ask For Confirmation* - Every time a host connects, a pop up window asks whether or not it should be authorized.
    - *Add Automatically* - Add any host to the Authorized System List which sends packets to this system.
- **Authorized System List.** This is a list of authorized systems which may connect and whether or not they are doing so securely. Secure systems are denoted by the lock or the Sun Microsystems logo next to the system name, depending on the type of security they are using.
- **Management Buttons**. These three button allow you to add and delete authorized systems and find out the key status on an authorized system that is using security.
    - *Add* - brings up the *Add system* popup menu.
    - *Delete* - Deletes the selected system from the Authorized System list.
    - *Key Status* - When an encrypted system is highlighted in the Authorized Systems list, clicking on this button brings up a popup menu showing the status of the keys in use between the two systems.

▼ Add System Popup Menu

Hosts are added to the Authorized System list using the **Add** button, located at the bottom left of the skiptool main window. When you click on the **Add** button, the *Add system* popup window appears (Figure 7).



Add system...

Hostname:

Security: Off

Secure: Whole packet

Key ID: Not present

ID:

Local Key ID: Not present

Key encryption: DES-CBC

Traffic encryption: DES-CBC

Authentication: Off

Compression: Off

Figure 7 Add System Popup Window

The *Add system* popup window has 11 major components, as shown in Figure 7. They are described below.

- **Hostname Field**. This is where you type in the name or the IP address of the host system you want to have access to your system.
- **Security Button.** This is a three-position button. If the remote host system also has SKIP, and you want the traffic between your systems to be encrypted, turn this button *on*. To add hosts without encryption, select *off*. The third option, *On (SunScreen Compatibility)*, is used to communicate with the Sun Microsystem's SunScreen(tm) product. SunScreen uses an older version of SKIP.
- **Secure Portion Button.** Not currently implemented.
- **Key ID Button.** The Key ID button is only available when the **Security** button is on. The Key ID button selects whether or not the keyid of the remote system should be sent in the SKIP packet and, if so, which namespace the ID lives in. If *Not present* is selected, no receiver keyid is sent in the packet. The following namespaces are supported in this release:
    - *Not present*
    - *IPv4 Address*
    - *POSIX/XOPEN User ID*
    - *IPv6 Address*
    - *MD5 (DNS name)*
    - *MD5 (ASN.1 DH)*
    - *MD5 (Social Sec. #)*
    - *802.x Address*
    - *MD5 (DH Pub.Value)*
    - *MD5 (Email Address)*
    - *MD5 (Bank Account #)*
    - *MD5 (NIS Name)*

Not Present (default) will use the IP address of the remote system to identify its certificate. If you specify a Key type here, you must fill in the key ID in the **ID Field** (manual keying). For a more complete discussion about keys and namespaces, refer to the *advanced.TOPICS* document in `/usr/skip/doc` (Solaris 1.x) or `/opt/SUNWicg/doc` (Solaris 2.x).

- **ID Field.** This field is only available when the **Security** button is *on*. If a remote system has a Node ID (or certificate) other than that identified by its IP address then this field should contain the appropriate ID (as specified by the Key ID button) expressed in hexadecimal (such as 0x0a000000).
- **Local Key ID Button.** This button is only available when the **Security** button is *on*. TThe Local Key ID button specifies whether your want your keyid included in the SKIP packet and, if so, what namespace that keyid lives in. If Not present is selected, no sender keyid is sent in the packet. The possible key ID types are the same as for the **Key ID** button, listed above. For a more complete discussion about keys and namespaces, refer to the *advanced.TOPICS* document in `/usr/skip/doc` (Solaris 1.x) or `/opt/SUNWicg/doc` (Solaris 2.x).
- **Key Encryption Button.** This button is only available when the **Security** button is *on*. It is used to select the encryption algorithm used to encrypt the session key. Selecting this button will list the available key encryption algorithms. Typically, these may include:
  - *des_cbc*
  - *des-ede-k3*
  - *simplecrypt*
- **Traffic Encryption Button.** This button is only available when the **Security** button is *on*. It is used to select the encryption algorithm used to encrypt the traffic between your system and the remote system. Possible traffic encryption algorithms may include:
  - *des_cbc*
  - *des-ede-k3*
  - *simplecrypt*
- **Authentication Button.** Not currently implemented.
- **Compression Button.** Not currently implemented.
- **Management Buttons.** The management buttons are used to add the information in the popup window to the system, or to cancel the window.

▼ Adding and Modifying Hosts

Any remote host that you want to send traffic to must be configured using the *Add system* popup window. This section describes how to add and modify a host that is not using encryption, is using encryption, or is using SunScreen(tm) compatible encryption.

▼ Encryption OFF

Remote systems that you will not be sending encrypted SKIP traffic should be added using the next section, unless you want any system that sends packets to your system to be added automatically.

Note – Be sure to include any NFS servers and name servers on the Authorized System list, otherwise your system will hang. Use the command `mount` to find out which file servers your system is using. If you are using NIS, the command `ypwhich` will display the name server.

1. Click on the **add** button. The *Add System* popup window appears.
2. Enter the hostname or IP address in the **Hostname** field.
3. Make sure the **Security** button is in the *Off* position, and click on **Apply**.
4. Repeat steps 2 and 3 for all authorized hosts. When you have finished adding hosts, click on the **Cancel** button to dismiss the popup window.
5. To modify a host, double-click on the host's entry in the **Authorized Systems** list. The *Add system* popup menu will appear.

▼ Encryption On

Any remote host that you want to send encrypted SKIP traffic to must be configured using the Add system popup window. Remote systems that you will not be sending encrypted SKIP traffic should be added using the previous section.

Note – Be sure to include any NFS servers and name servers on the Authorized System list, otherwise your system will hang. Use the command `mount` to find out which file servers your system is using. If you are using NIS, the command `ypwhich` will display the name server.

1. Click on the **add** button. The *Add System* popup window appears.
2. Enter the hostname or IP address in the **Hostname** field.
3. Click the **Security** button *ON*. The **Key ID**, **Local Key ID**, **Key encryption**, and **Traffic encryption** buttons become active.
4. Use the **Key ID** button to select whether you would like the remote system's keyid included in SKIP packets and, if so, what namespace that keyid lives in. By selecting *Not Present*, you can disable the sending of the receiver keyid.
5. If you selected something other than *Not Present*, the **ID Field** becomes active. Enter the ID in hexadecimal (For more information on namespaces, refer to the *advanced.TOPICS* document in `/usr/skip/doc` (Solaris 1.x) or `/opt/SUNWicg/doc` (Solaris 2.x)).
6. Next, use the **Local Key ID** button to whether you want your local system to send it's keyid in the SKIP packet and, if so, what namespace the key lives in. If you select *Not Present*, no sender Keyid will be sent in the packet. You can only use a key ID that has already been defined. It is not necessary to use the same type of Key ID as the remote system.
7. Now select the key and traffic encryption algorithms you wish to use for communication with the remote system.

8. Click **Apply** to add the host to the Authorized systems list.
9. Repeat steps 2 though 8 for all encrypted hosts. When you have finished adding hosts, click on the **Cancel** button to dismiss the popup window.
10. To modify a host, double-click on the host’s entry in the **Authorized Systems** list. The *Add system* popup menu will appear.

▼ SunScreen(tm) Compatibility

Sun Microsystems has created a security product called SunScreen(tm) that uses an earlier version of the SKIP protocol. The SKIP Reference Implementation package can also communicate with SunScreen, provided it has the proper key installed. Call SunService for help in getting the key installed properly.

1. Click on the **add** button. The *Add System* popup window appears.
2. Enter the hostname or IP address in the **Hostname** field.
3. Select *ON (Sunscreen Compatibility)* from the **Security** button. The **ID** field, and the **Key** and **Traffic encryption** buttons become active.
4. Enter the Key ID in the **ID** field. The key ID should be an 8-digit hexadecimal number preceded by `0x`**.**
5. Select the appropriate key and traffic algorithms from the **Key** and **Traffic encryption** buttons.
6. Repeat steps 2 through 5 for all authorized hosts. When you have finished adding hosts, click on the **Cancel** button to dismiss the popup window.
7. To modify a host, double-click on the host’s entry in the **Authorized Systems** list. The *Add system* popup menu will appear.

▼ Certificate Fetches

In order for two hosts running SKIP to communicate, they must exchange certificates. The system provides two automated methods to exchange certificates. You can also insert keys acquired manually.

1. Directory Server - hosts may provide directory service. If a host provides this service, it may be specified.
2. Certificate Discovery Protocol - hosts running SKIP request each other’s certificates through a clear channel.
3. You can also manually exchange certificates and add them as described in the previous section, or by using the **skip_add_cert** command. By default, the key manager will try to “ping.”

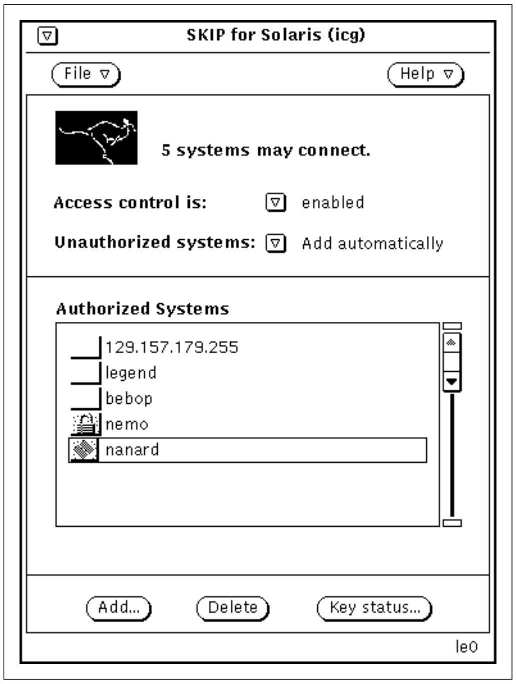
For more information on configuring certificate fetching protocols and certificate management, please see the manual pages for skip_keymgrd, skip_keymgrd.conf and skip_add_cert. By default, the key manager will ask the host its trying to communicate with for it's certificate.

▼ Enabling SKIP

Once you have entered the authorized systems using the *Add system* popup window, you need to determine what should happen when unauthorized systems attempt access, and finally, enable the access control for the system.

Figure 8 shows the skiptool main window after hosts have been added and access control enabled. The **Authorized Systems** area lists all the hosts allowed access. The graphic preceding the host name or IP address depicts what type of security is being used with that host.

- A blank box preceding the host name indicates no encryption (Security = *off*).
- A box with a lock in it indicates that the system is using encryption (Security = *on*)
- A box with the Sun Microsystems logo in it indicates that the system is using Sunscreen Compatibility mode (Security = *on (Sunscreen Compatibility)*).



SKIP for Solaris (icg)

5 systems may connect.

Access control is: enabled

Unauthorized systems: Add automatically

Authorized Systems

129.157.179.255
legend
bebop
nemo
nanard

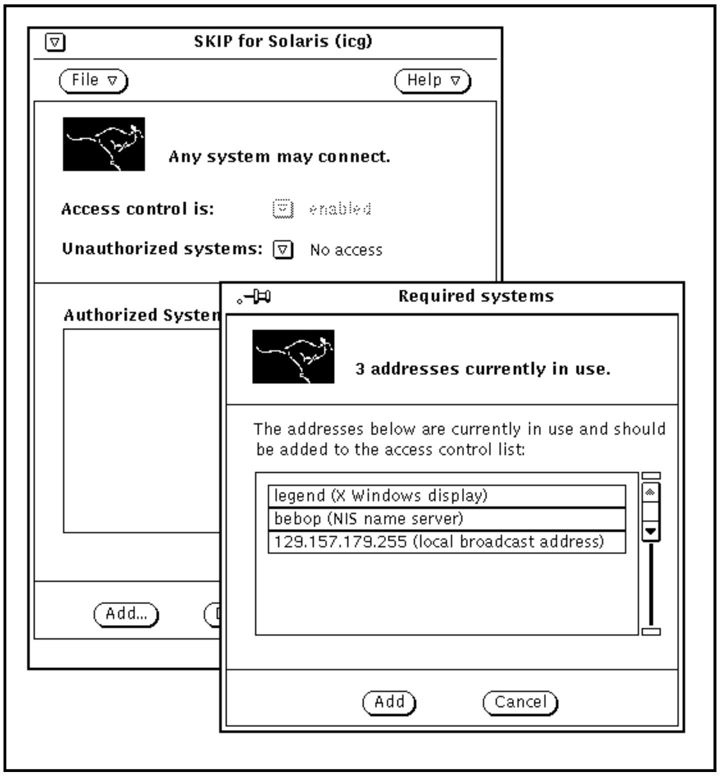
le0

Figure 8 Skiptool Configured with Access Control Enabled.

1. Use the **Unauthorized Systems** button on the main window to select what action the SKIP Reference Implementation should take when an unauthorized system attempts access. Refer back to the “skiptool Main Menu” section on page 12 for information on the possible selections.

2. Enable the SKIP Reference Implementation by selecting *enabled* from the **Access Control Button** on the main window. If the system has detected addresses that should be in the access control list that are not, it will bring up a window as shown in Figure 9. Select *Add* to add the listed systems, or *Cancel* to dismiss the popup without changing the access control list.

Note – If you choose *Cancel*, your system may hang.



Any system may connect.

Access control is: enabled

Unauthorized systems: No access

3 addresses currently in use.

The addresses below are currently in use and should be added to the access control list:

legend (X Windows display)
bebop (NIS name server)
129.157.179.255 (local broadcast address)

Figure 9 Required Systems Warning Popup

Once enabled, it is no longer necessary to keep the window open. The best thing to do is to iconify the main window. The skiptool icon shows whether SKIP is enabled or not (See Figure 10).

If you quit the window, SKIP will stay in whatever mode it was last in (enabled or disabled). The **Unauthorized Systems** policy will automatically change to *No Access*, since there is no longer any way to notify you if an unauthorized system is attempting to gain access.

Figure 10 SKIP Reference Implementation Icon, Enabled and Disabled

Managing skiptool

This chapter describes some of the management functions for skiptool, including viewing statistics, testing, debugging, and key management.

Checking SKIP Statistics

You can view the Interface, Header, Algorithm and Key statistics in real-time by selecting **SKIP Statistics** from the **File** menu on the main skiptool. Below are sample windows of each, with the fields explained. Fields are updated approximately every 3 seconds. An *updated* next to the field indicates that the field had changed the last time the window was updated. Figure 11 shows the menu path to bring up a Statistics window.

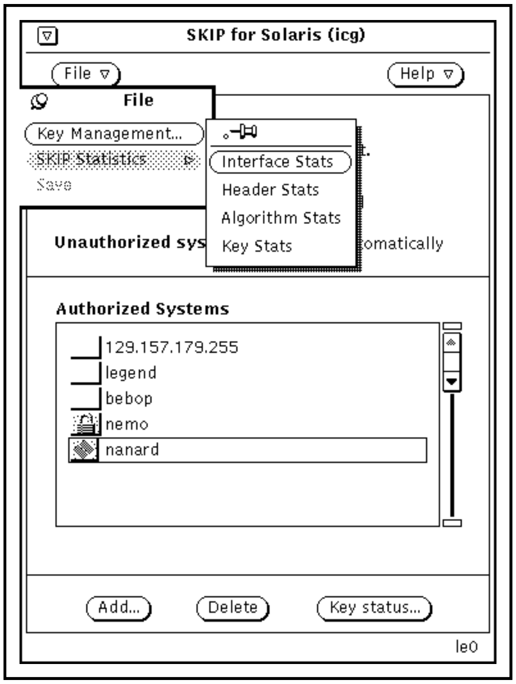
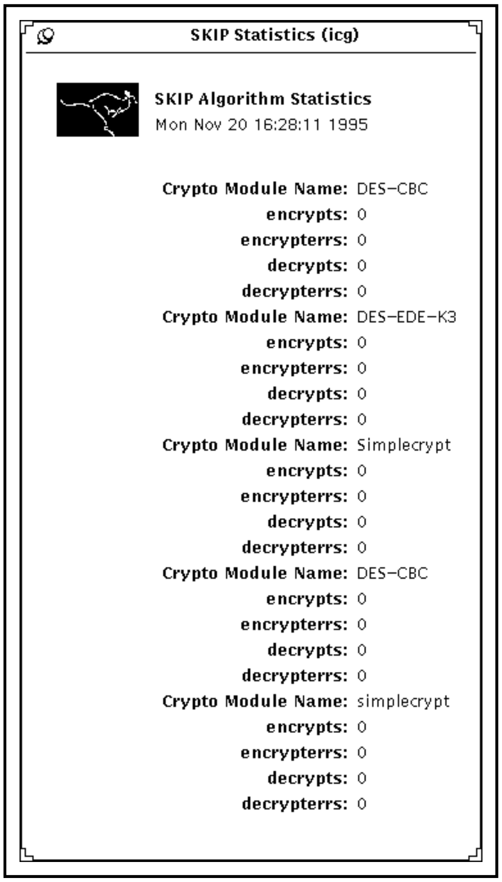


Figure 11 Bringing up a Statistics Window

▼ SKIP Algorithm Statistics

Selecting **File - SKIP Statistics-Algorithm Stats** displays the SKIP Algorithm Statistics window (Figure 12). Description follow the figure.



SKIP Statistics (icg)

SKIP Algorithm Statistics
Mon Nov 20 16:28:11 1995

```
Crypto Module Name: DES-CBC
          encrypts: 0
       encrypterrs: 0
          decrypts: 0
       decrypterrs: 0
Crypto Module Name: DES-EDE-K3
          encrypts: 0
       encrypterrs: 0
          decrypts: 0
       decrypterrs: 0
Crypto Module Name: Simplecrypt
          encrypts: 0
       encrypterrs: 0
          decrypts: 0
       decrypterrs: 0
Crypto Module Name: DES-CBC
          encrypts: 0
       encrypterrs: 0
          decrypts: 0
       decrypterrs: 0
Crypto Module Name: simplecrypt
          encrypts: 0
       encrypterrs: 0
          decrypts: 0
       decrypterrs: 0
```

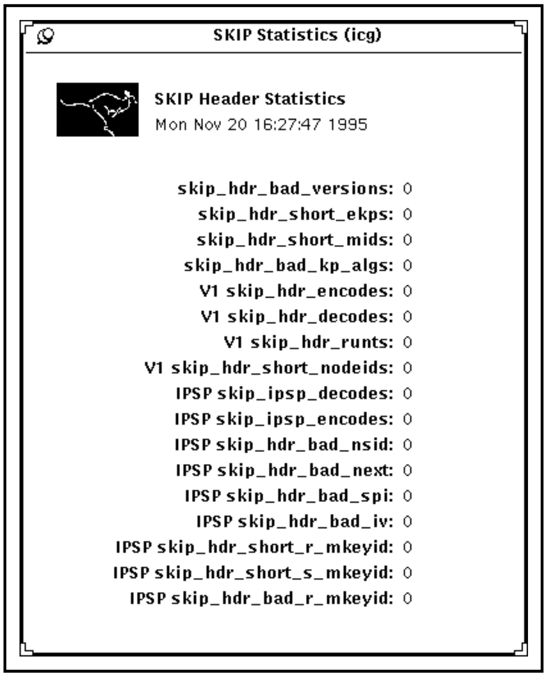
Figure 12 SKIP Algorithm Statistics Window

One set of statistics is displayed for each different traffic and key encryption module. Statistics are broken down into the following areas:

- **Crypto Module Name:** The name of the cryptographic module for which the statistics are being displayed.
- **encrypts:** The number of successful encryptions.
- **encrypterrs:** The number of failed encryptions.
- **decrypts:** The number of successful decryptions.
- **decrypterrs:** The number of failed decryptions.

▼ SKIP Header Statistics

Selecting **File - SKIP Statistics-Header Stats** displays the SKIP Header Statistics window (Figure 13). Descriptions of the items follow the figure.



```
SKIP Header Statistics
Mon Nov 20 16:27:47 1995

        skip_hdr_bad_versions: 0
           skip_hdr_short_ekps: 0
           skip_hdr_short_mids: 0
         skip_hdr_bad_kp_algs: 0
          V1 skip_hdr_encodes: 0
          V1 skip_hdr_decodes: 0
             V1 skip_hdr_runts: 0
     V1 skip_hdr_short_nodeids: 0
       IPSP skip_ipsp_decodes: 0
       IPSP skip_ipsp_encodes: 0
        IPSP skip_hdr_bad_nsid: 0
        IPSP skip_hdr_bad_next: 0
         IPSP skip_hdr_bad_spi: 0
          IPSP skip_hdr_bad_iv: 0
  IPSP skip_hdr_short_r_mkeyid: 0
  IPSP skip_hdr_short_s_mkeyid: 0
    IPSP skip_hdr_bad_r_mkeyid: 0
```

Figure 13 SKIP Header Statistics Window

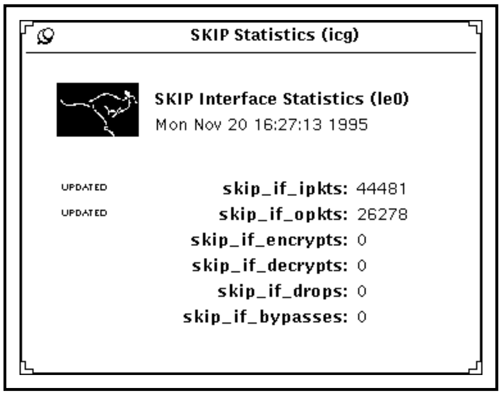
In the items below, V1 refers to SKIP's SunScreen compatibility mode (based on an earlier version of the SKIP protocol).

- **skip_hdr_bad_versions**: The number of headers with invalid protocol versions.
- **skip_hdr_short_ekps**: The number of headers with short eKp fields.
- **skip_hdr_short_mids**: The number of headers with short MID fields.
- **skip_hdr_bad_kp_algs**: The number of headers with unknown cryptographic algorithms.
- **V1 skip_hdr_encodes**: The number of SKIP V1 headers encoded.
- **V1 skip_hdr_decodes**: The number of SKIP V1 headers decoded.
- **V1 skip_hdr_runts**: The number of headers with short SKIP V1 packets.
- **V1 skip_hdr_short_nodeids**: The number of headers with short SKIP V1 node ids.
- **IPSP skip_ipsp_encodes**: The number of SKIP V2 headers encoded.
- **IPSP skip_ipsp_decodes**: The number of SKIP V2 headers decoded.
- **IPSP skip_hdr_bad_nsid**: The number of headers with a bad V2 name space id.
- **IPSP skip_hdr_bad_next**: The number of headers with a bad V2 next protocol field.
- **IPSP skip_hdr_bad_spi**: The number of headers with a bad V2 SPI field.

- **IPSP skip_hdr_bad_iv**: The number of headers with a bad V2 initialization vector.
- **IPSP skip_hdr_short_r_mkeyid**: The number of headers with a short V2 receiver key id.
- **IPSP skip_hdr_short_s_mkeyid**: The number of headers with a short V2 sender key id.
- **IPSP skip_hdr_bad_r_mkeyid**: The number of headers with a bad V2 receiver key id.

▼ SKIP Interface Statistics

Selecting **File - SKIP Statistics-Interface Stats** displays the SKIP Interface Statistics window (Figure 14). Descriptions of the items follow the figure.



SKIP Interface Statistics (le0)
Mon Nov 20 16:27:13 1995

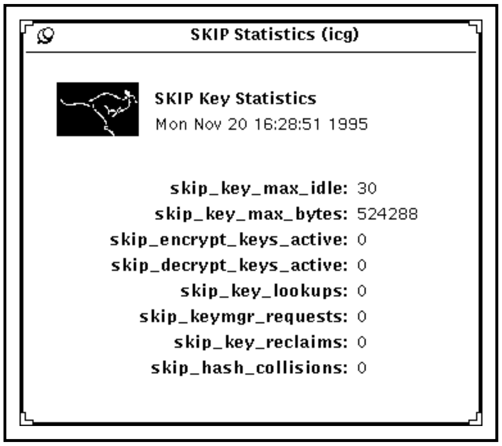
skip_if_ipkts: 44481
skip_if_opkts: 26278
skip_if_encrypts: 0
skip_if_decrypts: 0
skip_if_drops: 0
skip_if_bypasses: 0

Figure 14 SKIP Interface Statistics Window

- **skip_if_ipkts**: The number of packets received by interface.
- **skip_if_opkts**: The number of packets sent by interface.
- **skip_if_encrypts**: The number of packets encrypted.
- **skip_if_decrypts**: The number of packets decrypted.
- **skip_if_dropped**: The number of packets dropped.
- **skip_if_bypasses**: The number of certificate packets.

▼ SKIP Key Statistics

Selecting **File - SKIP Statistics-Key Stats** displays the SKIP Key Statistics window (Figure 15). Descriptions of the items follow the figure.



SKIP Key Statistics
Mon Nov 20 16:28:51 1995

skip_key_max_idle: 30
skip_key_max_bytes: 524288
skip_encrypt_keys_active: 0
skip_decrypt_keys_active: 0
skip_key_lookups: 0
skip_keymgr_requests: 0
skip_key_reclaims: 0
skip_hash_collisions: 0

Figure 15 SKIP Key Statistics

- **skip_key_max_idle**: The time, in seconds until an unused key is reclaimed.
- **skip_key_max_bytes**: The maximum number of bytes to encrypt before discarding a key.
- **skip_encrypt_keys_active**: The number of encryption keys in the cache.
- **skip_decrypt_keys_active**: The number of decryption keys in the cache.
- **skip_key_lookups**: The total number of key cache lookups.
- **skip_keymgr_requests**: The total number key cache misses (key not found).
- **skip_key_reclaims**: The total number of key entries reclaimed.
- **skip_hash_collisions**: The total number of table collisions.

▼ Testing SKIP

The following list of procedures are designed so that you can make sure SKIP is running correctly on your system.

1. Ping the remote system. The remote system must have SKIP enabled, and be using the same key and traffic encryption algorithms as your system.

   If you have the remote site's certificate, you will immediately start sending Encrypted IP. Otherwise, your keymanager will need to do a remote certificate fetch. By default, this is done by asking the remote site for it's certificate over a clear channel. If you have configured other hosts to act as key servers, they will be asked. See the man pages for *skip_keymgrd* and *skip_keymgrd.conf* for details. If there are no problems at the remote site, you will receive replies to your pings.

2. You can run snoop on your local system or a sniffer and see that packets are encrypted.

If the above tests do not work, it could be several things:

- SKIP is not correctly installed.
- SKIP is not enabled.
- You do not have certificates.

- Any of the above for the remote system.
- The remote system got certificates from a different Certificate issuing system. In Release 2.0 both systems must get their certificates from the same Certificate issuing system.
- The boxid of the remote system is incorrect.
- The keyserver listed in `skip_keymgrd.conf` is not an authorized system in skiptool.
- You are behind a firewall which is blocking traffic to or from UDP ports 6455 & 6456.

Debugging Tips

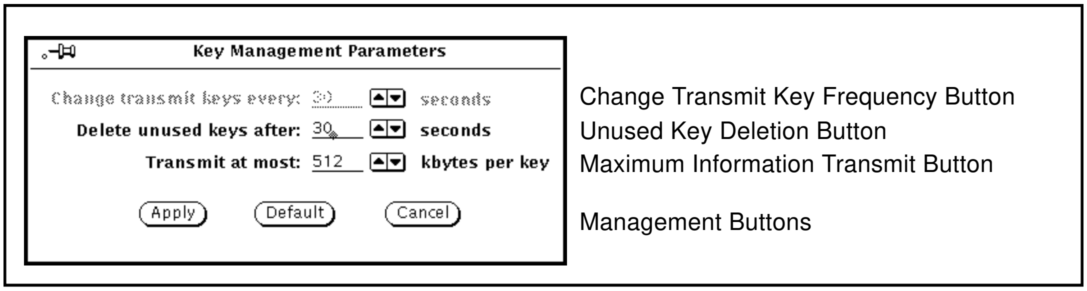
This section describes things to look at if SKIP is not working.

1. Check the file */var/log/skip_keymgrd.log* to see if the keymanager has set the boxid to what you think it should be. If it is not the correct boxid, get certificates for the correct boxid.
2. Check and see if the key server is up. Use the command **`certreq`** to try and retrieve a certificate.
3. Make sure you have the certificate of the remote system. The command **`skip_dump_certs`** will dump the certificate database to *stdout*.
4. Use the **`skipstat`** command to display status information.
5. Restart the key manager by sending a HUP signal to it. Perhaps the key manager could not reach the key directory earlier and marked the key as dead.

If none of these tips work, you may have to delete everything and start over.

Key Management Policies

The *Key Management Parameters* window (Figure 16) is displayed by selecting **Key Management** from the **File** pulldown menu. Key management parameters are global, that is, one set of key management parameters governs the activity of all keys on a particular system. The *Key Management Parameters* window has four major components, as shown in Figure 16. They are described after the figure.


Key Management Parameters

Change transmit keys every: 30 seconds

Delete unused keys after: 30 seconds

Transmit at most: 512 kbytes per key

Change Transmit Key Frequency Button

Unused Key Deletion Button

Maximum Information Transmit Button

Management Buttons

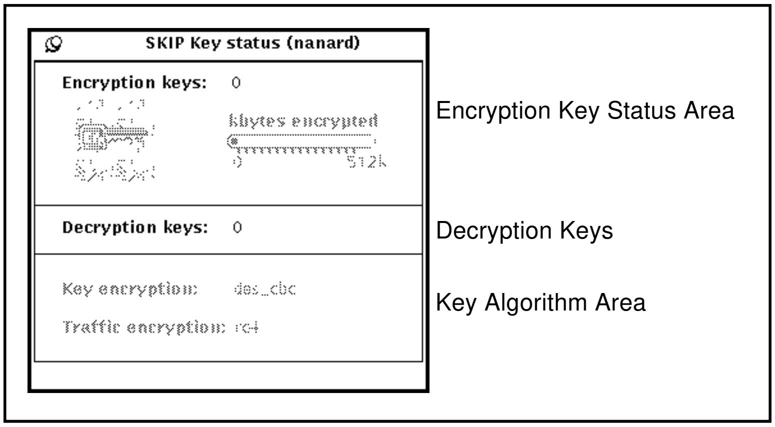
Figure 16 Key Management Parameters Window

- **Change Transmit Key Frequency Button.** This button sets how often the transmit key should be changed. It is not currently implemented.

- **Unused Key Deletion Button.** This button sets the number of seconds an unused key is kept before it is deleted. The number may be changed by either typing in a new number, or clicking on the up and down arrows until the desired number is reached. The minimum value is 5 seconds, the maximum value is 10,000 seconds, and the default value is 30 seconds.
- **Maximum Information Transmit Button.** This button sets the maximum amount of information that can be transmitted using a particular key. When the set amount is reached, the key is changed. The number may be changed by either typing in a new number, or clicking on the up and down arrows until the desired number is reached. The minimum value is 1 Kbyte per key, the maximum value is 10,000 Kbytes per key, and the default value is 512 Kbytes per key.
- **Management Buttons.** These three buttons allow you to apply the new values, return to the default values, or dismiss the window without changes.
    - *Apply* - Makes the changes made in the window active.
    - *Default* - Returns the values in the window to the default values (30 seconds and 512 Kbytes).
    - *Cancel* - Dismisses the window without changing anything.

▼ Key Status Window

The *SKIP Key Status* window is displayed by selecting a remote host from the **Authorized Systems** list that uses encryption, and then pressing the **Key Status** button at the bottom of the main skiptool window. It is shown in Figure 17, and described below.


SKIP Key status (nanard)

Encryption keys: 0

Decryption keys: 0

Key encryption: des_cbc

Traffic encryption: rc4

Figure 17 SKIP Key Status Window

If there is no active traffic passing between the two systems, this window will be grayed out. Also, there is nothing in this window that can be modified directly.

- **Encryption Key Status Area.** This area gives the status of the encryption keys.
    - *Encryption Keys* - This is the number of keys used between the two systems.
    - *Kbytes Encrypted* - This slider bar shows how much has been encrypted using the current key.
    - *Rotating Key* - Shows that information is being encrypted.

- **Decryption Keys.** This is the total number of keys received by your system from this host.
- **Key Algorithm Area**. This area shows the traffic and key encryption algorithms in use for this host.