Replacing an E4SA CRU

This procedure describes how to replace an Ethernet 4 ServerNet adapter (E4SA) CRU in a NonStop S-series server online. You might need to replace an E4SA CRU if it has failed or partially failed. You do not need to shut down the system before replacing an E4SA CRU.

The following is a high-level summary of the tasks required to complete the E4SA CRU replacement procedure. Each task in this outline is linked to step-by-step instructions about how to perform the task. Angle-brackets (for example, <line-name>) are used in command syntax to indicate values that you must provide. After you complete a task, click the check box.

Preparation:

1 Read the notes and cautions.

2 Gather the proper tools.

3 Identify any communications lines and ServerNet wide area network (SWAN) concentrators using the E4SA CRU to be replaced.

4 Quiesce any customer applications using the E4SA CRU to be replaced.

5 Stop the communications lines and SWAN concentrators using the E4SA CRU to be replaced.

Note: This step is optional. Most communications lines are suspended when an E4SA CRU is removed and are automatically resumed when the E4SA CRU is replaced. You should be aware that numerous Event Management Service (EMS) messages are generated if communications lines are not stopped before the E4SA CRU is removed; these messages do not require any recovery action.

6 Determine the physical location of the E4SA CRU to be replaced.

7 Abort the E4SA CRU to be replaced.

8 Label the communications cables connected to the E4SA CRU to be replaced.

Replace the E4SA CRU:

1 Remove the E4SA CRU to be replaced.

2 Inspect the new E4SA CRU and backplane.

3 Install the new E4SA CRU.

Note: Wait a minimum of 30 seconds after removing the old E4SA CRU before installing the new E4SA CRU.

4 Check the installation of the new E4SA CRU.

Resume Operations:

1 Start the new E4SA CRU.

2 Restart the communications lines and SWAN concentrators.

Note: You need to perform this step if you stopped communications lines or if an IPXPROTO process was using the E4SA CRU that was replaced. IPXPROTO processes **must** be manually restarted after an E4SA CRU is replaced.

3 Verify that the communications lines and SWAN concentrators are restarted.

4 Resume customer applications.

Related Topics

The following topics contain information related to this procedure:

- Viewing the Operator Log ($0) Using the OSM or TSM Event Viewer
- Viewing the Service Log ($ZLOG) Using the OSM or TSM Event Viewer
- Managing the Windows NT Event Viewer Application Log
- Managing the Windows Event Viewer Application Log

Change History for Replacing an E4SA CRU

August 21, 2000

- Updated the following topics for Parallel Library TCP/IP:
  - Starting the Comm Lines and SWANs That Use an E4SA
  - Stopping the Comm Lines and SWANs That Use an E4SA
  - Verifying Comm Lines and SWANs That Use an E4SA Are Started
- Added a navigation bar to some topics.
- Created the following separate pages:
  - Change History
  - Notes
  - Version Information

Version Information for Replacing an E4SA

The information in this procedure is valid for the G03, G05, and G06 RVUs.

Notes for Replacing an E4SA CRU

Caution: If a previously installed E4SA CRU and backplane connector have damaged pins, remove the E4SA CRU and install a filler panel in the vacant slot. Attach red tags to the filler panel to identify the slot. Do not move the damaged E4SA CRU to a different, undamaged slot. Both the E4SA CRU and backplane (or enclosure) must be replaced. For backplane replacement, see the backplane replacement section of the NonStop S-Series Service Provider Supplement.

Note: Whenever you handle an E4SA CRU, you should follow standard operating practices to avoid damage to the equipment.

Standard Operating Practices

Caution. Replace only one CRU or FRU at a time. Attempting to replace more than one hardware component at a time might cause serious system outages, processor halts, and connectivity problems.

Whenever you replace a CRU or a FRU, use the following standard operating practices to minimize any potential damage to the equipment:

- Complete HP training courses on system support for NonStop S-series servers.
- Inspect the replacement CRU or FRU for any physical damage before installing it. Check the connectors on the CRU, FRU, or backplane for bent or broken pins and for any other obvious damage. If there is damage to the CRU or FRU, you need to order another one.
- Remove all jewelry and metal accessories, such as rings, watches, and necklaces, before working with the equipment. These items can damage electrical equipment or result in personal injury.
- Restrain any dangling items that can get caught in electromechanical equipment, such as long hair and sleeves, before working with the equipment.
- Follow the ESD Guidelines for working in an electrostatic discharge (ESD)-protected environment and for handling CRUs and FRUs.
- Avoid permanent damage to components from overheating by observing the time limits for an enclosure door to be open with only one fan running.

  The following table indicates the amount of time that components in a fully loaded NonStop S-series system enclosure, with the appearance-side door open and only one fan operating, can operate before overheating.

Safe Operating Times With Enclosure Door Open

	Ambient Room Temperature			
Altitude	**25°C (77°F)**	**30°C (86°F)**	**35°C (95°F)**	**38°C (100°F)**
Sea level	>45 minutes	36 minutes	21 minutes	13 minutes
1,524 meters (5,000 feet)	38 minutes	22 minutes	13 minutes	8 minutes
3,048 meters (10,000 feet)	25 minutes	14 minutes	10 minutes	5 minutes

For example, if your computer room has an ambient room temperature of 25°C (77°F) and is at an altitude of 1,524 meters (5,000 feet), you have approximately 38 minutes to replace or reinstall the second fan before components inside a system enclosure overheat.

Related Topic

ESD Guidelines

ESD Guidelines

 Figure: Working in an ESD-Protected Environment

Observe the following electrostatic discharge (ESD) guidelines whenever servicing electronic components:

- Obtain an ESD protection kit and follow the directions that come with the kit. You can purchase an ESD kit from HP (T99247-A00) or from a local electronics store. Ensure that your ESD wriststrap has a built-in series resistor and that the kit includes an antistatic table mat.
- Before you unpack a replacement CRU or FRU, place the CRU or FRU package on the antistatic table mat and attach the grounding clip on your wriststrap to the mat.
- When you unpack the CRU or FRU, do not cut into the ESD protective bag surrounding the CRU or FRU. The protective bag protects the CRU or FRU and can be reused for storing the CRU or FRU that has been replaced.
- Before you move the CRU or FRU from the antistatic table mat, attach the grounding clip from your ESD wriststrap to any unpainted metal surface on the CRU or FRU frame.
- Before you bring a CRU or FRU in contact with a system enclosure, attach the grounding clip on your ESD wriststrap to any unpainted metal surface on the enclosure frame.
- When you remove a CRU or FRU from a system enclosure, first pull the CRU or FRU partway out of the slot and then attach the grounding clip on your ESD wriststrap to any unpainted metal surface on the CRU or FRU frame.
- Store CRUs or FRUs that require ESD protection in ESD protective bags.
- The figure Working in an ESD-Protected Environment illustrates how to use an ESD kit when servicing CRUs or FRUs.

Note: An ESD protection kit can be purchased from HP using the following order number and part number:

Order Number: ESD-kit

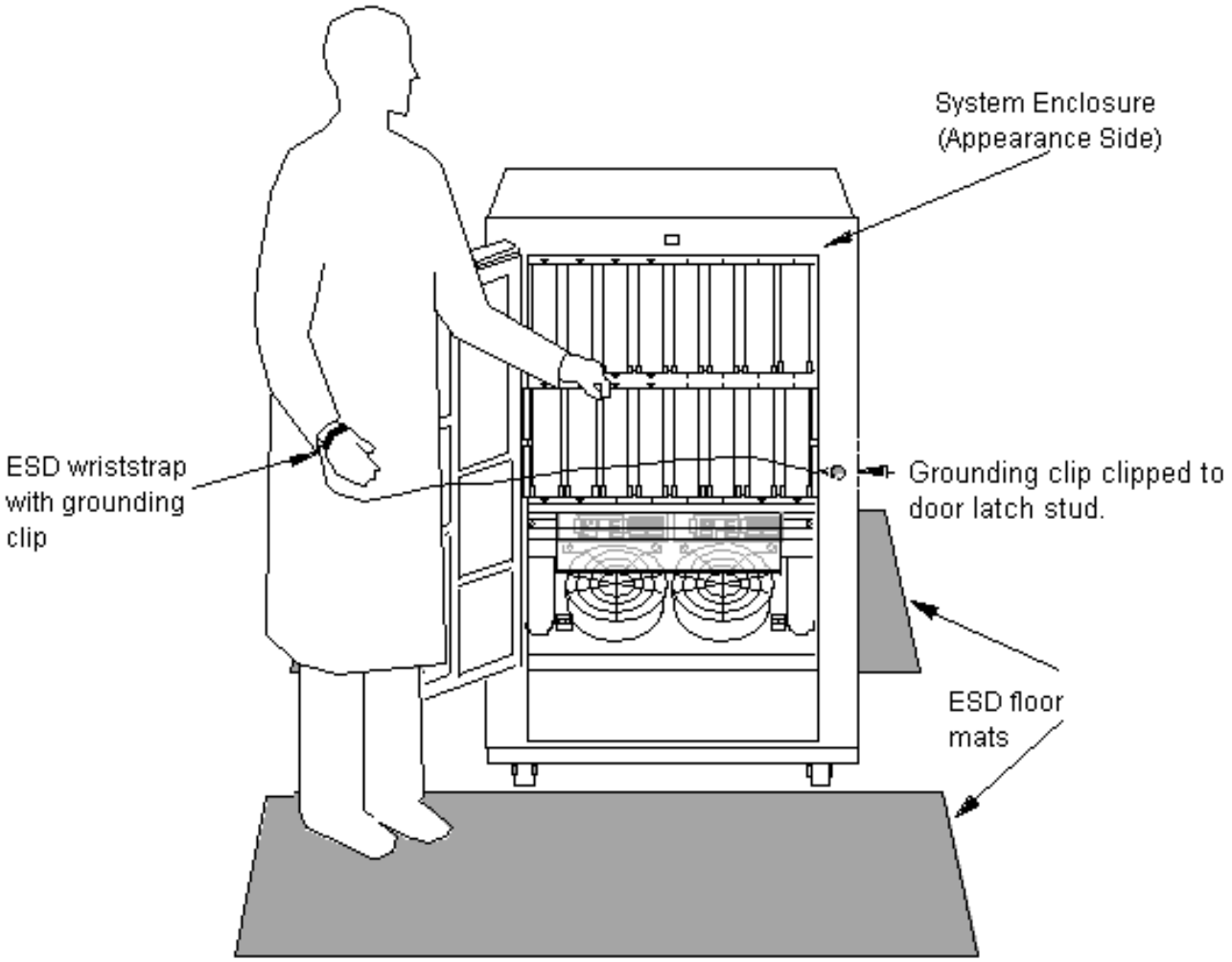
Part Number: T99247-A00

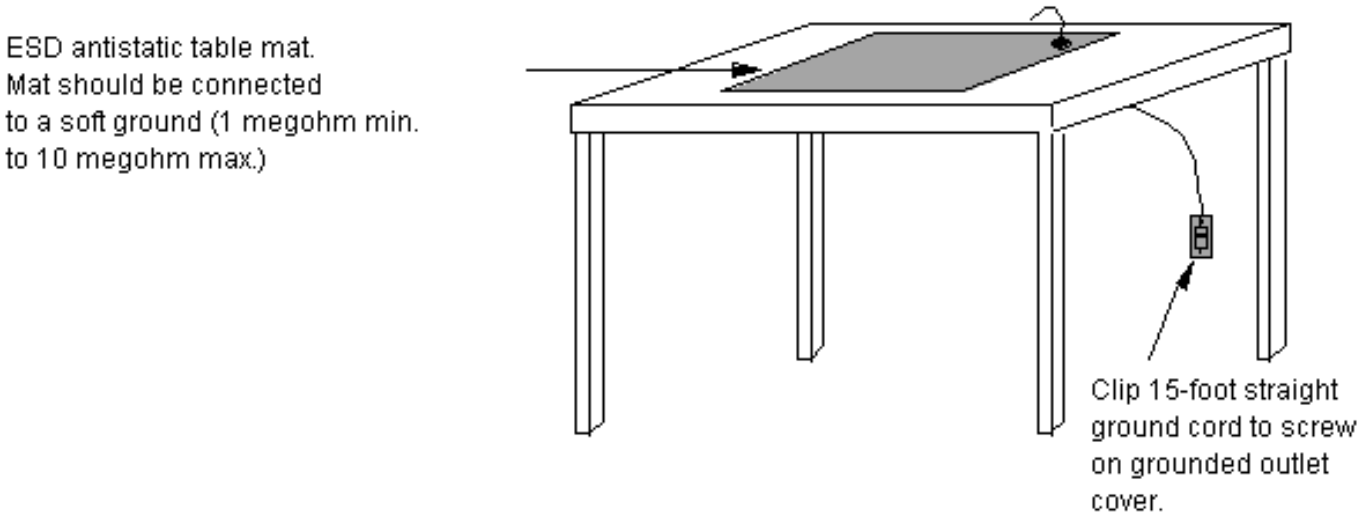
Related Topic

Standard Operating Practices

Figure: Working in an ESD-Protected Environment

This figure illustrates how to use an ESD kit when servicing customer-replaceable units (CRUs) and field-replaceable units (FRUs).





Gathering the Proper Tools to Assist With CRU and FRU Replacement

You will need some or all of the following tools to replace a CRU or a FRU:

Tool	Used to...
Electrostatic discharge (ESD) wriststrap with grounding clip	Protect the CRU or FRU from damage caused by electrostatic discharge.
Antistatic mat (recommended)	Provide a static-free environment for removal and installation of a CRU or FRU.
Flashlight	Check the connectors for bent or broken pins.
Phillips screwdriver	Loosen the captive thumbscrews on a disk drive CRU.

Note: An ESD protection kit can be purchased from HP using the following order number and part number:

Order Number: ESD-kit

Part Number: T99247-A00

Identifying the Communications Lines and SWAN Concentrators That Use an E4SA CRU

The ServerNet LAN Access Method (SLSA) subsystem provides access to the Ethernet 4 ServerNet adapter (E4SA) CRU. The following NonStop subsystems and utilities may be configured to access an E4SA CRU through the SLSA subsystem:

- The TCP/IP subsystem, which can interface to the SLSA subsystem to provide connectivity to TCP/IP networks. The following NonStop subsystems and utilities can interface to the TCP/IP subsystem to use an E4SA CRU:
    - The WAN subsystem, which interfaces to the TCP/IP subsystem to provide access to ServerNet wide area network (SWAN) concentrators, and the WAN subsystem input/output processes (IOPs) that use the SWAN concentrators.
    - The Expand subsystem, which interfaces to the TCP/IP subsystem to provide Expand-over-IP connections.
    - Telserv and the File Transfer Protocol (FTP), which use the socket library to establish remote connections and communicate through the TCP/IP subsystem.
    - Other NonStop subsystems, such as Remote Server Call (RSC), that can be configured to establish connections through the TCP/IP subsystem.
- The Port Access Method (PAM) subsystem, which can interface to the SLSA subsystem to provide an independent interface to Ethernet networks, and the user applications written using the PAM subsystem port interface.
- The IPX/SPX subsystem, which can interface to the SLSA subsystem to provide access to Novell NetWare networks. The following NonStop utilities and subsystems can interface to the IPX/SPX subsystem to use an E4SA CRU:
    - Telserv and FTP, which use the socket library to establish remote connections and communicate through the IPX/SPX subsystem.
    - NonStop subsystems, such as Remote Server Call (RSC), that can be configured to establish connections through the IPX/SPX subsystem.
- The SNAX/XF and SNAX/APN subsystems, which can interface to the SLSA subsystem to provide SNAX/Ethernet connectivity.

The figure illustrates how some of these subsystems and utilities use the SLSA subsystem to access an E4SA CRU.

The following procedure should help you identify the NonStop subsystems and utilities that are configured to use an E4SA CRU. Specific instructions are provided for

identifying Expand-over-IP lines, SWAN concentrators, and WAN subsystem IOPs.

Tip: You will need to make a note of the information you obtain during this procedure. You can record this information on the planning worksheet provided or you can use the SCF LOG command to capture both the command and the display that is produced to a file. To start logging, type LOG <logfilename> at the SCF prompt. To stop logging, type LOG at the SCF prompt.

1 Determine the names of the logical interfaces (LIFs) and the physical interfaces (PIFs) associated with the E4SA CRU to be replaced.

   Use the SCF INFO LIF command:

   ```
   INFO LIF $ZZLAN.*
   ```

   Scan the output of the command for the name of the E4SA CRU to be replaced. Make a note of the LIF names and PIF names.

   The example shows the output of this command.

2 Determine the TCP/IP processes, subnets, and Internet Protocol (IP) addresses associated with the LIFs on the E4SA CRU to be replaced.

   Use the SCF INFO SUBNET command:

   ```
   INFO SUBNET $*.*
   ```

   Scan the output of the command for each LIF you identified in Step 1 and then find the associated TCP/IP processes, subnets, and IP addresses. Make a note of this information.

   The example shows the output of this command.

3 Identify the PAM lines configured on the system.

   Use the SCF NAMES command:

   ```
   NAMES $ZZPAM
   ```

   The example shows the output of this command.

4 Determine the PAM lines associated with the LIFs on the E4SA CRU to be replaced.

Use the SCF INFO LINE command for each PAM line you identified in Step 3:

```
INFO LINE $<line-name>
```

Scan the output for a LIF on the E4SA CRU to be replaced. Make a note of the PAM lines associated with the LIFs on the E4SA CRU.

The example shows the output of this command.

5 Identify the IPXPROTO processes configured on the system.

Use the SCF NAMES SUBSYS command:

```
NAMES SUBSYS $ZMGR
```

The example shows the output of this command.

6 Determine the IPXPROTO processes associated with the LIFs on the E4SA CRU to be replaced.

Use the SCF INFO PROCESS command for each IPXPROTO process you identified in Step 5:

```
INFO PROCESS $<process-name>
```

Scan the output of the command for each LIF you identified in Step 1 and then find the associated IPXPROTO processes. Make a note of the IPXPROTO process names associated with the LIFs on the E4SA CRU.

The example shows the output of this command.

7 Identify the names of Expand-over-IP lines configured on the system.

Use the following SCF LISTDEV command to display the single-line Expand-over-IP lines:

```
LISTDEV TYPE 63,0
```

Use the following SCF LISTDEV command to display the Expand-over-IP lines that are part of a multiline path:

```
LISTDEV TYPE 63,2
```

The example shows the output of these commands.

8 Determine if any of the Expand-over-IP lines configured on the system use ports on the E4SA CRU to be replaced.

Use the SCF INFO LINE command with the DETAIL option for each Expand-over-IP line you identified in Step 7:

```
INFO LINE $<line-name>, DETAIL
```

Scan the output of the command for the TCP/IP process and IP address used by the Expand-over-IP line and compare this information to the TCP/IP processes and IP addresses that you found in Step 2. Make a note of the Expand-over-IP lines that use these TCP/IP processes and IP addresses.

The example shows the output of this command.

9 Identify the names of the SWAN concentrators configured on the system.

Use the SCF NAMES ADAPTER command:

```
NAMES ADAPTER $ZZWAN.#*
```

The example shows the output of this command.

10 Determine if any of the SWAN concentrators configured on the system are connected to the E4SA CRU to be replaced.

Use the SCF INFO ADAPTER command for each SWAN concentrator you identified in Step 9:

```
INFO ADAPTER $ZZWAN.#<adapter-name>
```

Scan the output of the command for the TCP/IP processes and IP addresses used by the SWAN concentrator and compare this information to the TCP/IP processes and IP addresses that you found in Step 2. Make a note of the names of the SWAN concentrators that are connected to the E4SA CRU.

The example shows the output of this command.

11 If you determined that a SWAN concentrator is connected to the E4SA CRU to be replaced, determine the names of the WAN subsystem IOPs configured to use that SWAN concentrator.

Use the SCF INFO DEVICE command:

```
INFO DEVICE $ZZWAN.#*
```

Scan the output of the command for the SWAN concentrators you identified in Step 10. Make a note of the WAN subsystem IOPs that use the SWAN concentrators connected to the E4SA CRU.

The example shows the output of this command.

12 Identify the SNAX/Ethernet lines configured on the system.

```
LISTDEV TYPE 58,6
```

The example shows the output of this command.

13 Determine if any of the SNAX/Ethernet lines configured on the system use the LIFs on the E4SA CRU to be replaced.

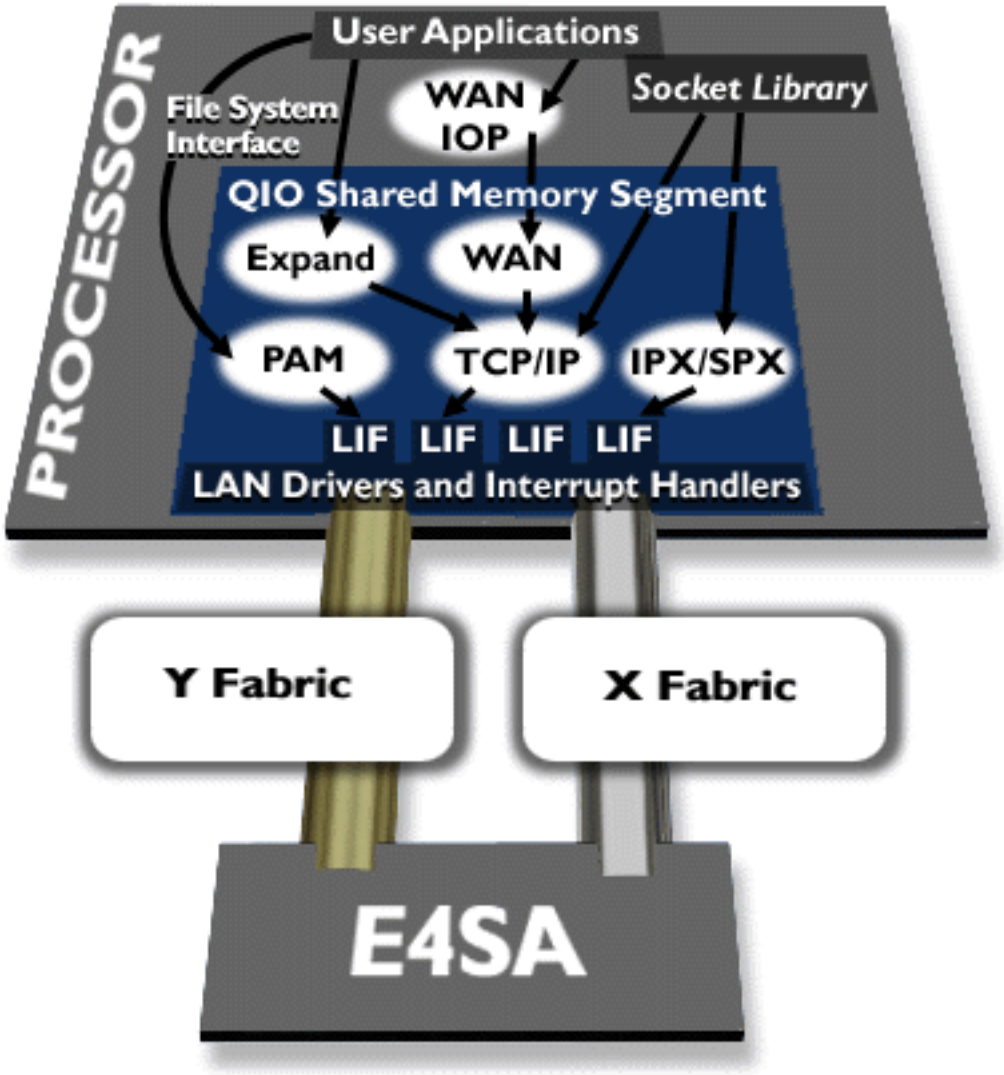
Use the SCF INFO LINE command with the SUB PU and ASSOCIATESUBDEV options for each SNAX line you identified in Step 12:

```
INFO LINE $<line-name>, SUB PU,
ASSOCIATESUBDEV
```

Scan the output of the command for the names of the LIFs you identified in Step 1. Make a note of the SNAX lines that use the LIFs.

The example shows the output of this command.

Figure: How NonStop Subsystems and Utilities Access an E4SA CRU



E4SA CRU Planning Worksheet

Print this worksheet and use it to record information about an Ethernet 4 ServerNet adapter (E4SA) CRU.

Logical Interfaces (LIFs) and Physical Interfaces (LIFs):

LIF: _____ PIF: _____

LIF: _____ PIF: _____

LIF: _____ PIF: _____

LIF: _____ PIF: _____

TCP/IP Processes, Subnets, and Internet Protocol (IP) Addresses:

LIF: _____ TCP/IP Process: _____ Subnet: _____ IP Address: _____

LIF: _____ TCP/IP Process: _____ Subnet: _____ IP Address: _____

LIF: _____ TCP/IP Process: _____ Subnet: _____ IP Address: _____

LIF: _____ TCP/IP Process: _____ Subnet: _____ IP Address: _____

Port Access Method (PAM) Lines:

LIF: _____ PAM Line: _____

LIF: _____ PAM Line: _____

LIF: _____ PAM Line: _____

LIF: _____ PAM Line: _____

IPXPROTO Processes:

LIF: _____ IPXPROTO Process: _____

LIF: _____ IPXPROTO Process: _____

LIF: _____ IPXPROTO Process: _____

LIF: _____ IPXPROTO Process: _____

Expand-Over-IP Lines:

TCP/IP Process: _____ IP Address: _____ Expand Line: _____

TCP/IP Process: _____ IP Address: _____ Expand Line: _____

TCP/IP Process: _____ IP Address: _____ Expand Line: _____

TCP/IP Process: _____ IP Address: _____ Expand Line: _____

ServerNet Wide Area Network (SWAN) Concentrators:

TCP/IP Process: _____ IP Address: _____ SWAN Concentrator: _____

TCP/IP Process: _____ IP Address: _____ SWAN Concentrator: _____

TCP/IP Process: _____ IP Address: _____ SWAN Concentrator: _____

TCP/IP Process: _____ IP Address: _____ SWAN Concentrator: _____

WAN Subsystem Input/Output Processes (IOPs):

SWAN Concentrator: _____ WAN IOP: _____

SWAN Concentrator: _____ WAN IOP: _____

SWAN Concentrator: _____ WAN IOP: _____

SWAN Concentrator: _____ WAN IOP: _____

SNAX/Ethernet Lines:

LIF: _____ SNAX/Ethernet Line: _____

LIF: _____ SNAX/Ethernet Line: _____

LIF: _____ SNAX/Ethernet Line: _____

LIF: _____ SNAX/Ethernet Line: _____

Example: Determining the LIFs and PIFs for an E4SA CRU

This is an example of the SCF INFO LIF command:

```
->INFO LIF $ZZLAN.*

SLSA Info LIF

Name           PIF           MAC Address          Type
$ZZLAN.L018    E0153.0.A     08:00:8E:00:5C:85    Ethernet
$ZZLAN.L019    E0153.0.B     08:00:8E:00:5C:86    Ethernet
$ZZLAN.L01A    E0153.1.A     08:00:8E:00:5C:87    Ethernet
$ZZLAN.L01B    E0153.1.B     08:00:8E:00:5C:88    Ethernet
```

Logical interface (LIF) names are shown in the **Name** column and physical interface (PIF) names are shown in the **PIF** column. The name of the adapter is the first part of the PIF name (for example, E0153).

The PIF name indicates the physical port on the adapter. For example, the PIF named E0153.0.A. identifies port ENET 0A, and the PIF named E0153.0.B identifies port ENET 0B on the E4SA named E0153. In this example, the LIFs associated with the Ethernet 4 ServerNet adapter (E4SA) named E0153 are named L018, L019, L01A, and L01B.

Example: Determining the TCP/IP Process and IP Address for a LIF

This is an example of using the SCF INFO SUBNET command:

```
->INFO SUBNET $*.*

TCPIP Info SUBNET \DRAGON.$ZB018.*

Name     Devicename     *IPADDRESS       TYPE      *SUBNETMASK
SuName  QIO  *R

#LOOP0   \NOSYS.$NOIOP  127.0.0.1        LOOP-BACK  %HFF000000
OFF   N
#SN1     \DRAGON.L018   172.16.40.64     ETHERNET   %HFFFFFF00
ON    N
#SN2     \DRAGON.L01C   172.16.35.15     SNAP       %HFFFFFF00
 ON    N
```

The following information should help you interpret the display:

- The TCP/IP process name is displayed in the first line of output.
- The subnet name is displayed in the **Name** column.
- The logical interface (LIF) name is shown in the **Devicename** column.
- The Internet Protocol (IP) address is shown in the ***IPADDRESS** column.

Note: You can easily scan for Ethernet subnets by looking at the **TYPE** column. Ethernet subnets are displayed as type ETHERNET.

In this example, which is partial output, the LIF named L018 is associated with the subnet named #SN1 on the TCP/IP process named $ZB018 and has the IP address 172.16.40.64.

Example: Identifying the PAM Lines on a System

This is an example of the SCF NAMES command:

```
-> NAMES $ZZPAM

PAM Names \SAMCAT.$ZZPAM

PROCESS
$TOK1  $ZZPAM

LINE
$TOK1

PORT
$TOK1.#L1P0002  $TOK1.#L1P0004

MSAP
$TOK1.#SNATR
```

Port Access Method (PAM) line names are shown under the `LINE` heading. In this example, which is partial output, one PAM line is configured named $TOK1.

Example: Determining the PAM Lines Associated with the LIFs on an E4SA CRU

This is an example of the SCF INFO LINE command:

```
-> SCF INFO LINE $TOK1

PAM Info LINE

Name     MAXREQUESTSIZE  LIF NAME   LIF TYPE  LIF MAC ADDRESS
$TOK1    3200            L018       ENET      08:00:8E:00:D1:96
```

The LIF name is shown in the `LIF NAME` column. The type of CRU is shown in the `LIF TYPE` column. Ethernet 4 ServerNet adapter (E4SA) CRUs are have the LIF type ENET. In this example, the E4SA CRU LIF named L018 is associated with the PAM line named $TOK1.

Example: Identifying the IPXPROTO Processes on a System

This is an example of the SCF NAMES SUBSYS command:

```
->NAMES SUBSYS $ZMGR

IPXSPX Names SUBSYS \HIMA.$ZMGR

SUBSYS
$ZMGR

PROCESS
$ZNV0

SERVER
$ZNV0.#SAP

PROCESS
$ZNV1

SERVER
$ZNV1.#SAP
```

IPXPROTO process names are shown under the **PROCESS** heading. In this example, two IPXPROTO processes are configured named $ZNV0 and $ZNV1.

Example: Determining the IPXPROTO Processes Associated with the LIFs on an E4SA CRU

This is an example of an SCF INFO PROCESS command:

```
->SCF INFO PROCESS $ZNV0

IPXSPX Info PROCESS

Process Name  Primary CPU  Backup CPU  *I/O Port Name  I/O Port Type
$ZNV0         2            3           L018 IPXETH     802.3
```

The LIF name is shown in the `I/O Port Name` column. In this example, which is partial output, the LIF named L018 is associated with the IPXPROTO process named $ZNV0.

Example: Identifying the Expand-Over-IP Lines on a System

This is an example of the SCF LISTDEV command display for single Expand-over-IP lines:

```
->LISTDEV TYPE 63,0

LDev Name    PPID  BPID  Type  Rsize  Pri   Program
109  $IPYEA  3,9   2,7   (63,0)   3  199   \COWBOY.$DATA00.T9057ADJ.LHOBJ
159  $IPCORE 0,16  1,15  (63,0)   3  199   \COWBOY.$DATA00.T9057ADJ.LHOBJ
```

In this example, two Expand-over-IP lines (named $IPYEA and $IPCORE) are configured on the system.

This is an example of the SCF LISTDEV command display for Expand-over-IP lines that are part of a multiline path:

```
->LISTDEV TYPE 63,2

LDev Name    PPID  BPID  Type  Rsize  Pri   Program
56   $IPC03  2,16  3,16  (63,2)   3  199   \COWBOY.$DATA00.T9057ADJ.LHOBJ
84   $IPC02  2,16  3,16  (63,2)   3  199   \COWBOY.$DATA00.T9057ADJ.LHOBJ
```

In this example, two Expand-over-IP lines (named $IPC03 and $IPC02) are configured as part of a multiline path.

Example: Determining the Expand-Over-IP Lines That Use an E4SA CRU

This is an example of the SCF INFO LINE command with the DETAIL option:

```
-> INFO LINE $IPYEA,DETAIL

EXPAND   Detailed Info  LINE   $IPYEA

*Associatedev...    $ZTC23  *Maxconnects.          0  Delay.... 0:00:00.10
Framesize......        132  *Speed.......      74666 *Retryprobe         3
*Timerinactivity 0:00:00.00 *Timerprobe.. 0:00:30.00  Txwindow..         7
*AfterMaxRetries    PASSIVE  StartUp......        OFF Rsize.....         3
*Timerreconnect. 0:00:30.00  L2Protocol...     Net^IP
*DestIpAddr 172.17.203.37  *DestIpPort  2003
*SrcIpAddr  172.17.208.20  *SrcIpAddr   2003
```

The TCP/IP process used by the Expand-over-IP line is shown in the `Associatedev` field and the local IP address is shown in the `SrcIpAddr` field. In this example, the Expand-over-IP line named $IPYEA uses the TCP/IP process named $ZTC23 and the IP address 172.17.203.37.

Example: Identifying the SWAN Concentrators on a System

This is an example of the NAMES ADAPTER command:

```
->NAMES ADAPTER $ZZWAN.#*

WanMgr Names ADAPTER $ZZWAN.#*

ADAPTER
$ZZWAN.#S01
$ZZWAN.#S02
```

Example: Determining the TCP/IP Processes and IP Addresses for a SWAN Concentrator

This is an example of the SCF INFO ADAPTER command:

```
-> INFO ADAPTER $ZZWAN.#S01

WAN MANAGER Detailed Info Adapter \TAHITI.$ZZWAN.#S01

*TrackId.......... ZWXFF            *TCPIP Name.....  $ZB019
*ALTTCPIP Name.... $ZB01D           Concentrator Type. SYNC
KERNELCODE........ $SYSTEM.CSS00.C7953P00
*SNMPCODE......... $SYSTEM.CSS00.C7849P00
*HOSTIP Address... 172.16.35.16
*ALTHOSTIP Address 172.16.45.16
SUBNETMASK........ %HFFFFFF00
ALTSUBNETMASK..... %HFFFFFF00
```

A ServerNet wide area network (SWAN) concentrator uses two TCP/IP processes and two Internet Protocol (IP) addresses. The preferred TCP/IP process used by the SWAN concentrator is shown in the **TCPIP Name** field and its associated IP address is shown in the **HOSTIP Address** field. The alternate TCP/IP process used by the SWAN concentrator is shown in the **ALTTCPIP Name** field, and its associated IP address is shown in the **ALTHOSTIP Address** field.

In this example, the SWAN concentrator named **S01** uses the preferred TCP/IP process **$ZB019**, the preferred IP address **172.16.35.16**, the alternate TCP/IP process **$ZB01D**, and the alternate IP address **172.16.45.16.** Note that the preferred and alternate IP addresses are on different subnets.

Example: Determining the WAN Subsystem IOPs that Use a SWAN Concentrator

This is an example of the SCF INFO DEVICE command:

```
->INFO DEVICE $ZZWAN.#*

WAN MANAGER Detailed Info Device \TAHITI.$ZZWAN.#A10

*Adapter Name..... S01          *Clip.......... 1
*Line............. 0            *Path.......... A
Profile........... MLHSWAN      *Recsize....... 12
Preferred Cpu..... 2             Alternate Cpu... 3
*Type............. (63,06)
*MULTINAME........ $PMAU1
*IOPOBJECT........ \TAHITI.$SYSTEM.SYS00.LHOBJ
```

The ServerNet wide area network (SWAN) concentrator used by the WAN subsystem input/output process (IOP) is shown in the `Adapter Name` field. In this example, which is partial output, the IOP named $A10 uses the SWAN concentrator named S01.

Example: Identifying the SNAX/Ethernet Lines on a System

This is an example of the SCF LISTDEV command:

```
-> LISTDEV TYPE 58,6

LDev Name  PPID  BPID  Type  Rsize Pri   Program
109  $ETP1 3,9   2,7   (58,6)   3  199   \COWBOY.$DATA00.T9057ADJ.SNATSOBJ
159  $ETP2 0,16  1,15  (58,6)   3  199   \COWBOY.$DATA00.T9057ADJ.SNATSOBJ
```

In this example, two SNAX-over-Ethernet lines, one named $ETP1 and one named $ETP2, are configured on the system.

Example: Determining the LIF Used by a SNAX/Ethernet Line

This is an example of the SCF INFO LINE command with the SUB PU and ASSOCIATESUBDEV options:

```
->INFO LINE $ETS2, SUB PU, ASSOCIATESUBDEV

SNAX Detailed Info PU \SNACKS.$ETS2.#ZNT21

AssociateSubDev.. \SNACKS.$LAN24.#PO41
```

The **Associatesubdev** attribute shows the name of the logical interface (LIF) associated with the SNAX/Ethernet line. In this example, the SNAX/Ethernet line named $ETS2 is associated with the LIF named LAN24.

Quiescing Customer Applications

1. Notify end users that applications will be temporarily unavailable.
2. Perform any actions necessary to quiesce customer applications.

   Note: The actions required to perform this step depend on the customer's application.

Stopping the Communications Lines and SWAN Concentrators That Use an E4SA CRU

To stop a ServerNet wide area network (SWAN) concentrator and its associated WAN subsystem IOPs and communications lines:

Note: A SWAN concentrator has dual Ethernet ports, which can be configured to connect to ports on two different E4SA CRUs; only one Ethernet connection is needed for full function. If the SWAN concentrator's second Ethernet port is connected to another E4SA CRU (other than the E4SA CRU that you are replacing), you do not need to perform the following steps. However, the SWAN concentrator will not be fault-tolerant while the E4SA CRU is being replaced.

1 Abort the communications lines.

Use the SCF ABORT LINE command to stop a single line:

```
ABORT LINE $<line-name>
```

Use the SCF ABORT PATH command to stop all the lines in an Expand multiline path:

```
ABORT PATH $<path-name>
```

2 Verify that the lines are in the STOPPED state.

Use the SCF STATUS LINE command for a single line:

```
STATUS LINE $<line-name>
```

Use the SCF STATUS PATH command for an Expand multiline path:

```
STATUS PATH $<path-name>
```

The example shows the output of these commands.

3 Stop the WAN subsystem IOPs.

Use the SCF STOP DEVICE command:

```
STOP DEVICE $ZZWAN.#<device-name>
```

4 Verify that the WAN subsystem IOPs are in the STOPPED state.

Use the SCF STATUS DEVICE command:

```
STATUS DEVICE $ZZWAN.#<device-name>
```

The example shows the output of this command.

5 Stop the the SWAN concentrator.

Use the SCF STOP ADAPTER command with the SUB ALL option:

```
STOP ADAPTER $ZZWAN.#<adapter-name>, SUB ALL
```

The SUB ALL option stops the ADAPTER object and its subordinate objects.

6 Verify that the SWAN concentrator is in the STOPPED state.

Use the SCF STATUS ADAPTER command:

```
STATUS ADAPTER $ZZWAN.#<adapter-name>
```

The example shows the output of the SCF STATUS ADAPTER command.

To stop an Expand-over-IP line:

1 Abort the Expand-over-IP line.

Use the SCF ABORT LINE command to stop a single line:

```
ABORT LINE $<line-name>
```

Use the SCF ABORT PATH command to stop all the lines in an Expand multiline path:

```
ABORT PATH $<path-name>
```

2 Verify that the Expand-over-IP line is in the STOPPED state.

Use the SCF STATUS LINE command for a single line:

```
STATUS LINE $<line-name>
```

Use the SCF STATUS PATH command for an Expand multiline path:

```
STATUS PATH $<path-name>
```

The example shows the output of these commands.

3 Stop the WAN subsystem IOP.

Use the SCF STOP DEVICE command:

```
STOP DEVICE $ZZWAN.#<device-name>
```

4 Verify that the WAN subsystem IOP is in the STOPPED state.

Use the SCF STATUS DEVICE command:

```
STATUS DEVICE $ZZWAN.#<device-name>
```

The example shows the output of this command.

To stop an IPXPROTO process:

1 Stop the IPXPROTO process.

Use the SCF STOP PROCESS command:

```
STOP PROCESS $<process-name>
```

2 Verify that the IPXPROTO process is in the STOPPED state.

Use the SCF STATUS PROCESS command:

```
STATUS PROCESS $<process-name>
```

The example shows the output of this command.

To stop a Port Access Method (PAM) line:

1 Stop the PAM line.

Use the SCF STOP command with the SUB ALL option.

```
STOP LINE $<line-name>, SUB ALL
```

The SUB ALL option aborts the LINE object and all subordinate objects.

2 Verify that the PAM line is in the STOPPED state.

Use the SCF STATUS LINE command:

```
STATUS LINE $<line-name>
```

The example shows the output of this command.

To stop a TCP/IP subnet:

Caution: Make sure that the TACL session from which you are issuing SCF commands is not running on the subnet that you are about to stop.

1 Stop the TCP/IP subnet.

Use the following SCF STOP SUBNET command for conventional TCP/IP:

```
STOP SUBNET
$<tcpip-process-name>.#<subnet-name>
```

Or use the following SCF STOP SUBNET command for Parallel Library TCP/IP:

STOP SUBNET $<tcpip-process-name>.*.<subnet-name>

2 Verify that the TCP/IP subnet is in the STOPPED state.

Use the following SCF STATUS SUBNET command for conventional TCP/IP:

```
STATUS SUBNET
$<tcpip-process-name>.#<subnet-name>
```

Or, use the following SCF STATUS SUBNET command for Parallel Library TCP/IP:

```
STATUS SUBNET $<tcpip-process-name>.*.<subnet-name>
```

The example shows the output of this command.

Example: Verifying That a Line Is Stopped

This is an example of the SCF STATUS LINE command:

```
-> STATUS LINE $LINE1

EXPAND   Status LINE

Name         State       PPID     BPID     CIU-Path  ConMgr-LDEV
$LINE1     STOPPED     2, 10    3, 7          A          91
```

Note that the line is in the STOPPED state.

This is an example of the SCF STATUS PATH command:

```
-> STATUS PATH $PATH

EXPAND  Status PATH

Name             State        PPID     BPID      Lines #
$PATH           STOPPED      2, 15    3, 15       2
```

Note that the path is in the STOPPED state.

Example: Verifying That a WAN Subsystem IOP Is Stopped

This is an example of the SCF STATUS DEVICE command:

```
-> STATUS DEVICE $ZZWAN.#LINE1

WAN Manager STATUS DEVICE for DEVICE \COWBOY.$ZZWAN.#LINE1
   State :........ STOPPED

   LDEV number.... 110
   PPIN.......... 2  ,13         BPIN......... 3  ,14
```

Note that the WAN subsystem input/output process (IOP) is in the STOPPED state.

Example: Verifying That a SWAN Concentrator Is Stopped

This is an example of the SCF STATUS ADAPTER command:

```
-> STATUS ADAPTER $ZZWAN.#S01

WAN Manager STATUS ADAPTER for ADAPTER \COWBOY.$ZZWAN.#S01
  State....... STOPPED

  Number of clips. 3

  Clip 1 status : CONFIGURED
  Clip 2 status : CONFIGURED
  Clip 3 status : CONFIGURED
```

Note that the ServerNet wide area network (SWAN) concentrator is in the STOPPED state.

Example: Verifying That an IPXPROTO Process Is Stopped

ThIs is an example of the SCF STATUS PROCESS command:

```
->STATUS PROCESS $ZNV2

IPXSPX Status PROCESS

Process Name     State      Diagnostic State    Trace
$ZNV2            STOPPED    NORMAL               OFF
```

Note that the IPXPROTO process is in the STOPPED state.

Example: Verifying That a PAM Line Is Stopped

This is an example of an SCF STATUS LINE command:

```
-> STATUS LINE $TOK1

PAM Status LINE

                          Primary          Backup
Name            State     CPU    PIN       CPU     PIN       Trace
$TOK1           STOPPED   1      278       -1      -1        OFF
```

Note that the Port Access Method (PAM) line is in the STOPPED state.

Example: Verifying That a TCP/IP Subnet Is Stopped

This is an example of the SCF STATUS SUBNET command:

```
-> STATUS SUBNET $ZTC01.#SN2

TCPIP Status SUBNET \COWBOY.$ZTC01.#SN2

Name                 Status

#SN2                 STOPPED
```

Note that the subnet is in the STOPPED state.

Determining the Physical Location of an E4SA CRU

Use the SCF INFO ADAPTER command:

```
INFO ADAPTER $ZZLAN.<adapter-name>
```

Scan the output of the command for the group, module, and slot location.

The example shows the output of this command.

Note: If Ethernet 4 ServerNet adapters (E4SA) CRUs are named using the manufacturing naming convention, you can easily identify the physical location of the E4SA CRU by its name as follows:

```
E<cabid><slot>
```

where **<cabid>** is the two-digit number that identifies the enclosure and **<slot>** is the actual physical slot number in the enclosure. For example, the E4SA CRU named E0153 is located in enclosure 01, slot 53.

Example: Determining the Location of an E4SA CRU

This is an example of the SCF INFO ADAPTER command:

```
-> INFO ADAPTER $ZZLAN.E0153

SLSA Info ADAPTER

Name              Group       Module     Slot    Type
$ZZLAN.E0153        1           1        53      E4SA
```

Note that, for this example, the Ethernet 4 ServerNet adapter (E4SA) CRU named E0153 is located in group 1, module 01, slot 53.

Aborting an E4SA CRU

1 Stop access to the logical interfaces (LIFs) associated with the Ethernet 4 ServerNet adapter (E4SA) CRU to be replaced.

Use the SCF ABORT LIF command for each LIF:

```
ABORT LIF $ZZLAN.<lif-name>
ABORT LIF $ZZLAN.<lif-name>
ABORT LIF $ZZLAN.<lif-name>
ABORT LIF $ZZLAN.<lif-name>
```

2 Verify that the LIFs associated with the E4SA CRU to be replaced are in the STOPPED state.

Use the SCF STATUS LIF command:

```
STATUS LIF $ZZLAN.*
```

The example shows the output of this command.

3 Abort the E4SA CRU ADAPTER object and its subordinate objects.

You can use either SCF, the OSM Service Connection, or the TSM Service Application to perform this step.

Note: TSM Service Application T8154AAE (G06.01) or later is required.

Using SCF:

Use the SCF ABORT ADAPTER command with the SUB ALL option:

```
ABORT ADAPTER $ZZLAN.<adapter-name>, SUB ALL
```

The SUB ALL option stops the ADAPTER object and its subordinate objects.

Using OSM or TSM:

1. In the Tree view, select the E4SA CRU.
2. From the **Display** menu, choose **Actions**.
3. Select **Abort**.
4. Click **Perform action**.

4 Verify that the SACs are in the STOPPED state.

Use the SCF STATUS SAC command:

```
STATUS SAC $ZZLAN.<adapter>.*
```

The example shows the output of this command.

5 Verify that the PIFs are in the STOPPED state.

Use the SCF STATUS PIF command:

```
STATUS PIF $ZZLAN.<adapter>.*
```

The example shows the output of this command.

6 Verify that the E4SA CRU ADAPTER object is in the STOPPED state.

Use the SCF STATUS ADAPTER command:

```
STATUS ADAPTER $ZZLAN.<adapter-name>
```

The example shows the output of this command.

Example: Verifying That the LIFs for an E4SA CRU Are Stopped

This is an example of the SCF STATUS LIF command:

```
->STATUS LIF $ZZLAN.*

SLSA Status LIF

Name           State     Access State
$ZZLAN.L018    STOPPED      DOWN
$ZZLAN.L019    STOPPED      DOWN
$ZZLAN.L01A    STOPPED      DOWN
$ZZLAN.L01B    STOPPED      DOWN
```

Note that the logical interfaces (LIFs) are in the STOPPED state.

Example: Verifying That a SAC Is Stopped

This is an example of the SCF STATUS SAC command:

```
-> STATUS SAC $ZZLAN.E0153.1

SLSA Status SAC

Name             Owner     State    Trace Status
$ZZLAN.E0153.1     1       STOPPED  OFF
```

Note the SAC is in the STOPPED state.

Example: Verifying That a PIF Is Stopped

This is an example of the SCF STATUS PIF command:

```
-> STATUS PIF $ZZLAN.E0153.1.A

SLSA Status PIF

Name                State       Trace Status
$ZZLAN.E0153.1.A    STOPPED     OFF
```

Note that the PIF is in the STOPPED state.

Example: Verifying That the ADAPTER Object for an E4SA CRU Is Stopped

This is an example of the SCF STATUS ADAPTER command:

```
-> STATUS ADAPTER $ZZLAN.E1053

SLSA Status ADAPTER

Name             State
$ZZLAN.E0153     STOPPED
```

Note that the ADAPTER object is in the STOPPED state.

Labeling Communications Cables for an E4SA CRU

1. Find the group, module, and slot in which the Ethernet 4 ServerNet adapter (E4SA) CRU is installed.

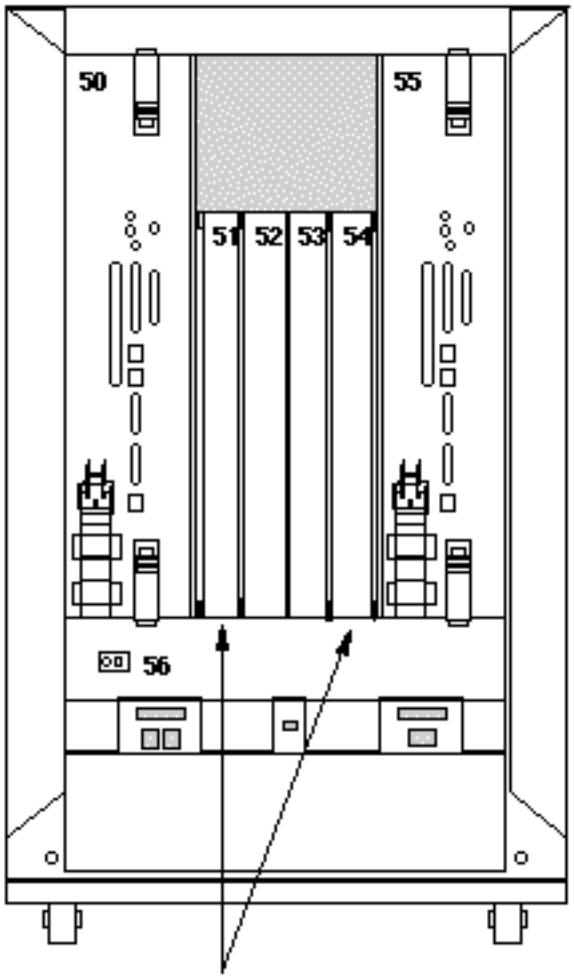
   The figure shows the E4SA CRU slot locations.

2. Tag each communications cable connected to the E4SA CRU with a physical label, preferably at both ends. The label should include the following information:

   - The physical interface (PIF) name assigned to the line. For example, E0154.0.A.
   - A description of the equipment and connector to which the cable is to be connected.
   - The slot location of the E4SA CRU to which the cable is connected.

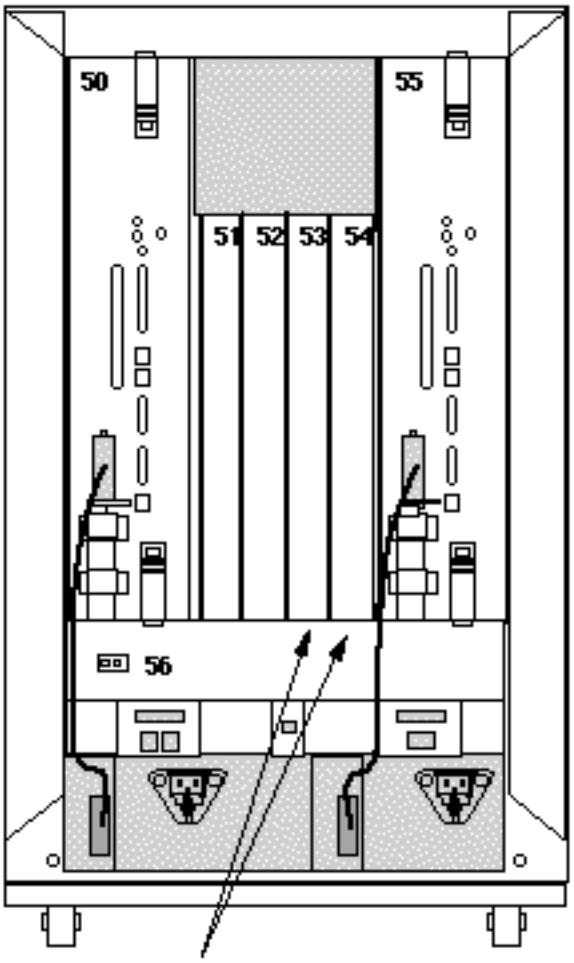
Figure: E4SA, TRSA, and ATM3SA CRU Slot Locations

Himalaya S-Series I/O Enclosures
(Service Side)



I/O enclosures can use slots 51 through 54 for E4SA, ATM3SA, and TRSA CRUs.

Himalaya S-Series Processor Enclosure
(Service Side)



Processor enclosures can only use slots 53 and 54 for E4SA, ATM3SA, and TRSA CRUs.

Removing an E4SA CRU

Note: Whenever you handle an Ethernet 4 ServerNet adapter (E4SA) CRU, you should follow standard operating practices to avoid damage to the equipment.

1. Disconnect the communications cables from the E4SA CRU.
2. Put on your electrostatic discharge (ESD) wriststrap and connect the grounding clip securely to an exposed, unpainted, metal surface on the service side of the system enclosure, such as the processor multifunction (PMF) CRU or I/O multifunction (IOMF) CRU ventilation holes.

   The figure shows how to connect the grounding clip to the ventilation holes on the PMF CRU or IOMF CRU.
3. Unlatch the ejector on the E4SA CRU by pressing the blue-green tab on the ejector and pulling the ejector outward to unseat the E4SA CRU from the backplane.
4. Grasp the E4SA CRU by its ejector with one hand and slowly pull the E4SA CRU out of the slot while supporting the bottom edge of the E4SA CRU with the other hand.

   Note: The E4SA CRU weighs 6.75 pounds (3 kilograms).

   The figure shows how to pull the E4SA CRU out of the slot.
5. Place the E4SA CRU in the ESD protective bag and return it to its original packing container.

Figure: Grounding Clip Connected to PMF CRU or IOMF CRU Ventilation Holes

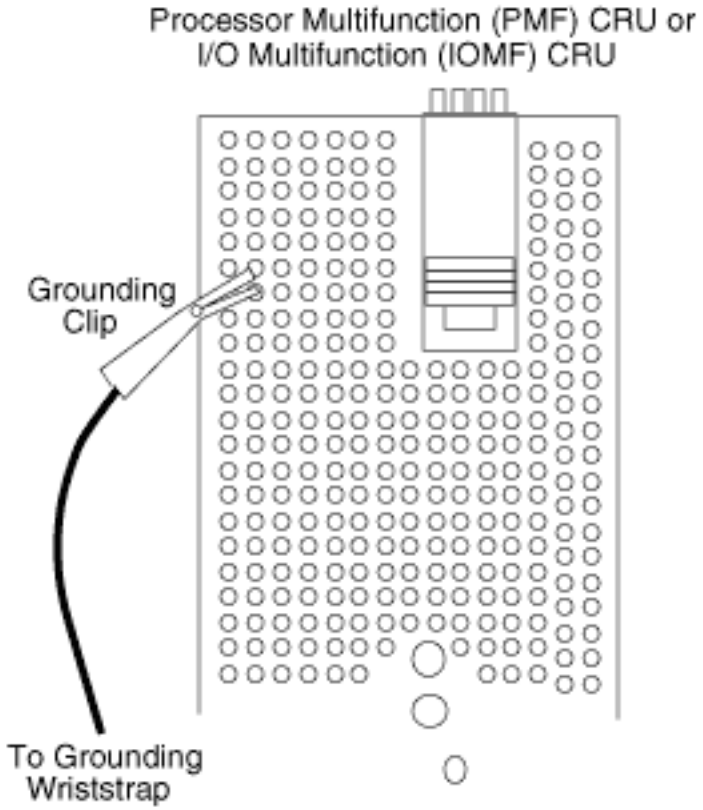
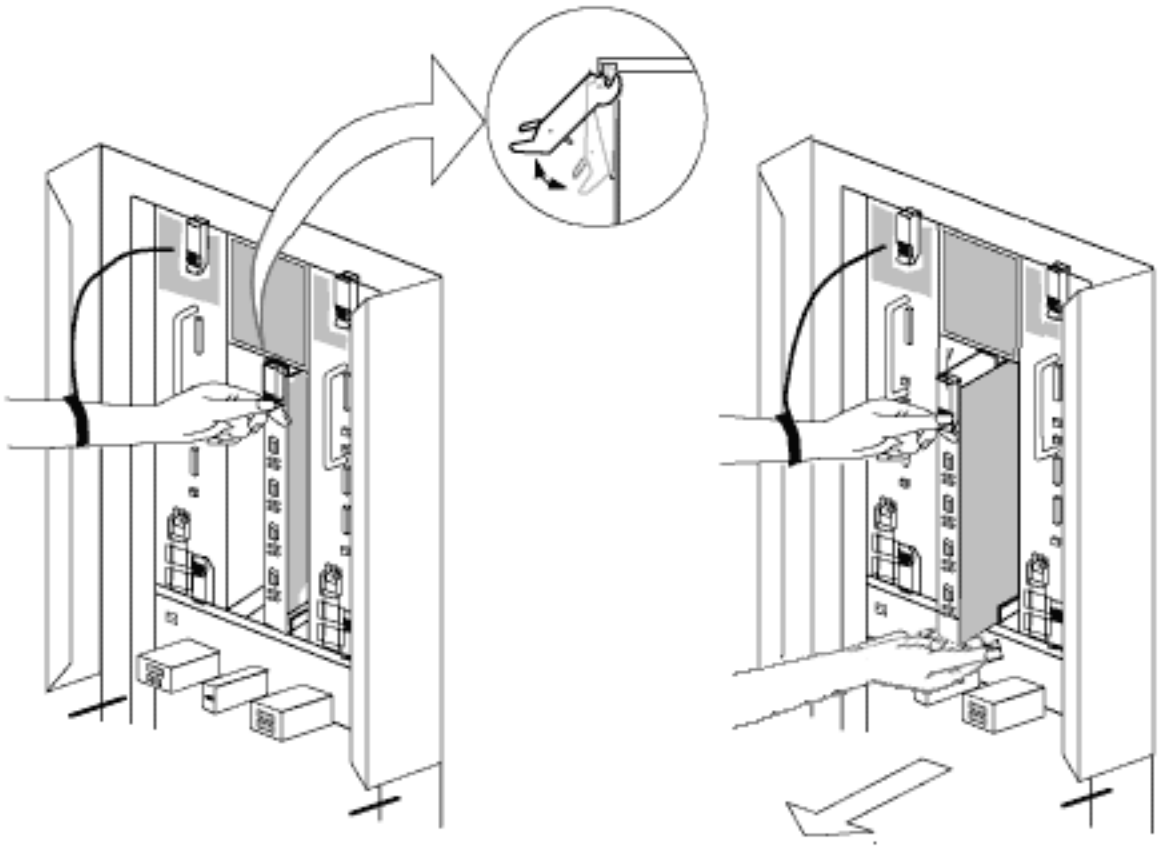


Figure: Removing an E4SA CRU



Inspecting an E4SA CRU

Note: Whenever you handle an Ethernet 4 ServerNet adapter (E4SA) CRU, you should follow standard operating practices to avoid damage to the equipment.

Visually inspect the new E4SA CRU and the backplane connector for damage. Use a flashlight, if necessary, to check for bent or broken pins. You can damage pins by bumping or jamming the E4SA CRU's shell against a surface, which can partially close the hole in the connector-pin socket. If the E4SA CRU has a damaged connector-pin socket, do not install it.

Caution: If you plug an E4SA CRU that has a damaged socket into a slot, that E4SA CRU's backplane pins and the connectors on other adapter boards that are plugged into that slot can be damaged. Moving a damaged board from slot to slot can damage other slots and other adapter boards.

Installing an E4SA CRU

Note: Whenever you handle an Ethernet 4 ServerNet adapter (E4SA) CRU, you should follow standard operating practices to avoid damage to the equipment.

1. Put on the electrostatic discharge (ESD) wriststrap and attach the grounding clip to the antistatic mat.
2. Place the package containing the E4SA CRU on the antistatic mat.
3. **Caution:** When opening the packing container, be careful not to cut into the ESD protective bag.

   Open the packing container and remove the E4SA CRU.
4. Disconnect the grounding clip of your ESD wriststrap from the antistatic mat and connect it to an exposed, unpainted metal surface on the E4SA CRU.
5. Grasp the E4SA CRU by its ejector in one hand, support the bottom edge of the E4SA CRU with the other hand, and carry the E4SA CRU to the service side of the system enclosure and set it down.

   Note: The E4SA CRU weights 6.75 pounds (3 kilograms).
6. Disconnect the grounding clip of your ESD wriststrap from the E4SA CRU and connect it to an exposed, unpainted, metal surface on the service side of the system enclosure, such as the processor multifunction (PMF) CRU or I/O multifunction (IOMF) CRU ventilation holes.

   The figure shows how to connect the grounding clip to the ventilation holes on the PMF CRU or IOMF CRU .
7. With the ejector on the E4SA CRU in the full-open position, grasp the E4SA CRU by its ejector with one hand and support the bottom edge of the E4SA CRU with the other hand. Hold the E4SA CRU so that its ejector is at the top and insert the E4SA CRU into the upper part of the carrier.

8 **Caution:** Apply equal pressure to both the top and bottom of the E4SA CRU when pushing it into the slot to avoid damaging the connector pins. If pins are damaged, both the E4SA CRU and the backplane (or enclosure) must be replaced.

Push the E4SA CRU to the rear of the slot, but don't force the E4SA CRU into the slot.

The figure shows how to install an E4SA CRU.

9 Press the blue-green tab on the E4SA CRU ejector and latch the ejector to seat the E4SA CRU against the backplane.

10 Disconnect the grounding clip of your ESD wriststrap from the enclosure.

11 Connect the RJ-45 connectors to the Ethernet ports on the E4SA CRU. Connect the other ends of the cables to your Ethernet hub. Use the labels on the cables to make sure you connect each cable to the proper port and Ethernet hub.

The figure shows how to connect the communications cables to the E4SA CRU and Ethernet hub.

Figure: Installing an E4SA CRU

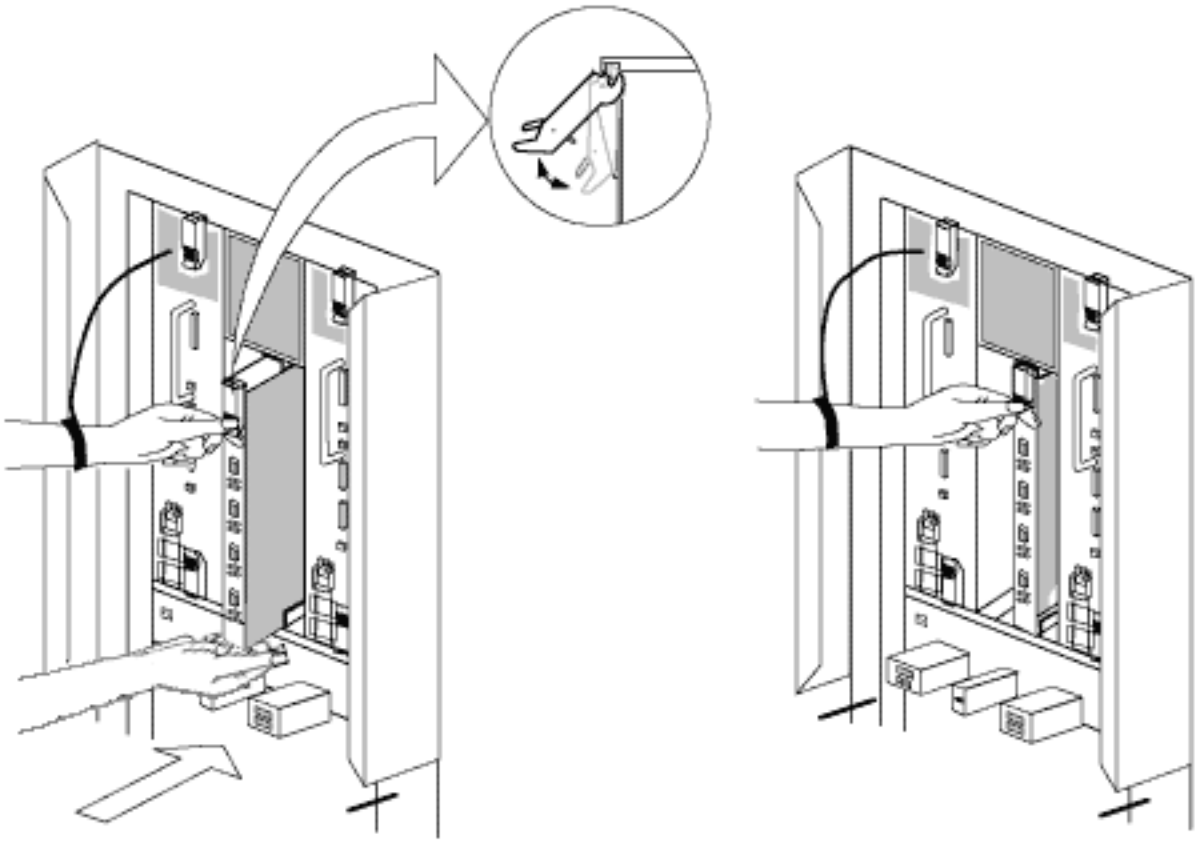
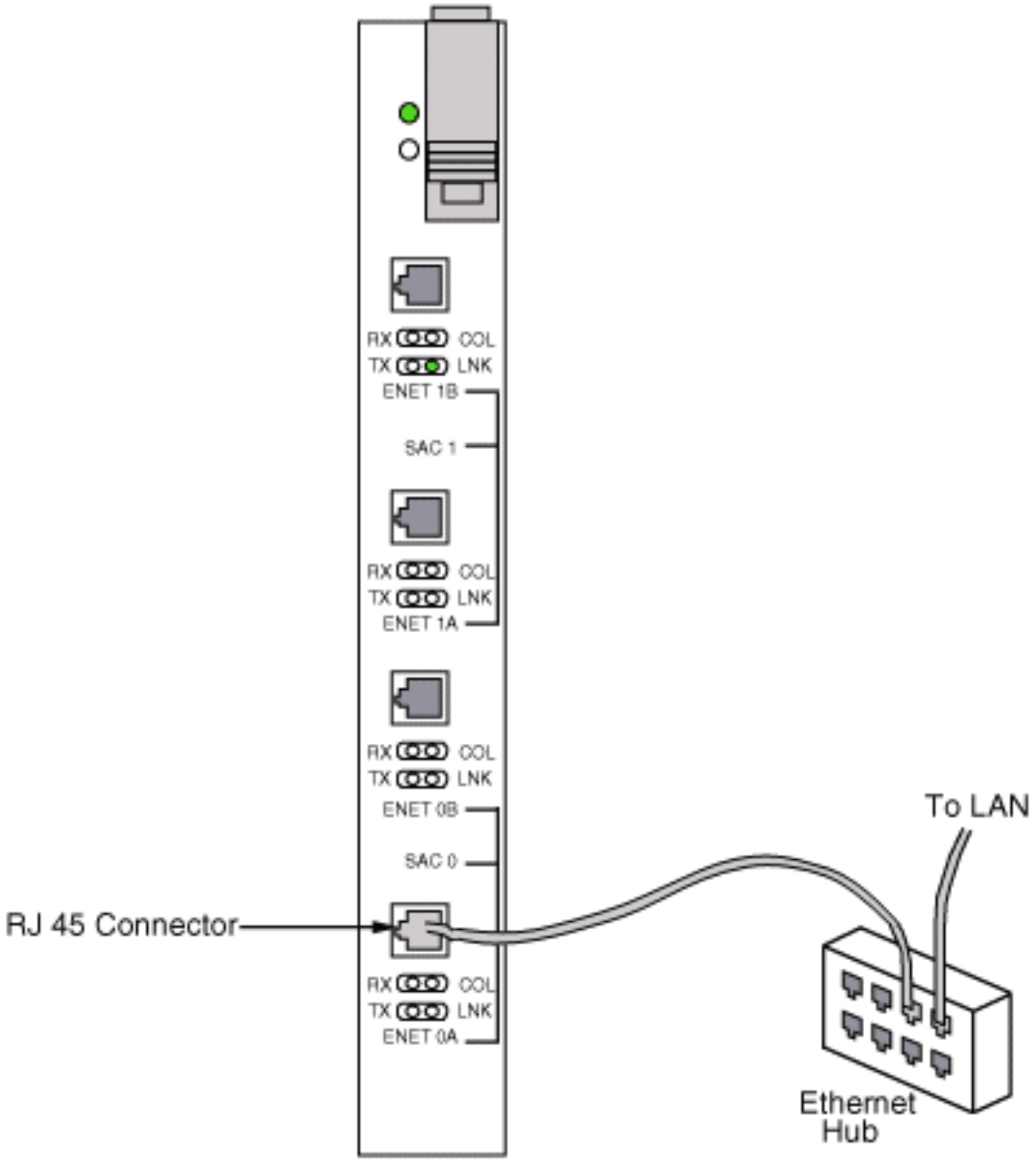


Figure: E4SA CRU Hardware Connection



Checking the Installation of an E4SA CRU

1 Make sure that the power-on LED (green light) is on.

Note: The fault LED (amber light) flashes when the Ethernet 4 ServerNet adapter (E4SA) CRU is installed and continues to flash while the condition of the E4SA CRU is tested. The test that is executed is the power-on self-test (POST). The fault LED goes off when the POST successfully finishes.

The figure shows the location of the power-on LED and fault LED.

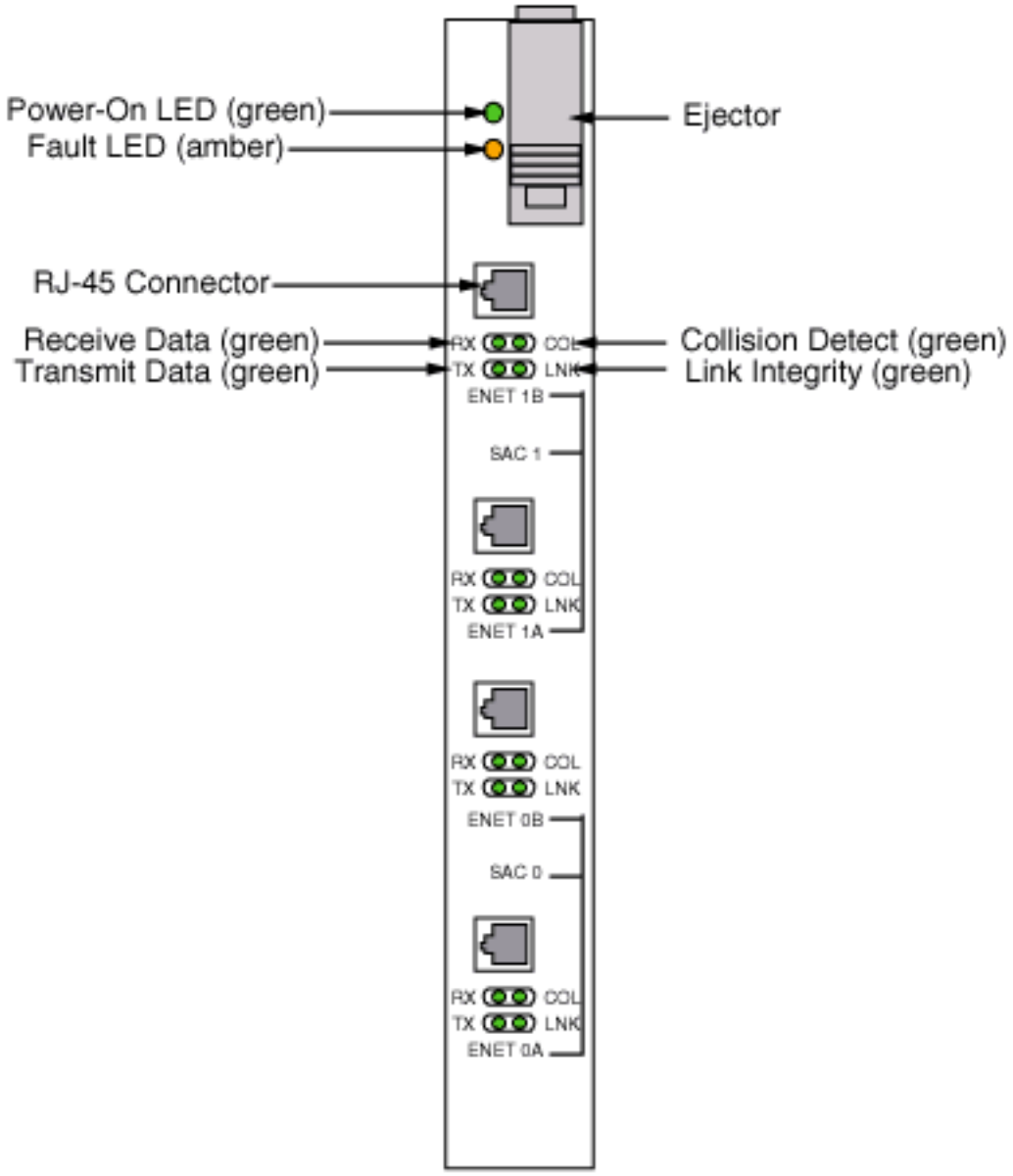
2 If the power-on LED does not come on, one or more of the POST tests might not have passed or the POST was never started. Do one or both of the following:

- Reseat the E4SA CRU.
- Check the E4SA CRU and backplane connector for damaged pins.

If the power-on LED does not come on after you reseat the E4SA CRU, you must replace the E4SA CRU. Click here to return to the beginnning of this procedure.

If the E4SA CRU or backplane connector have damaged pins, both the E4SA CRU and backplane (or enclosure) must be replaced. For backplane replacement instructions, see the NonStop S-Series Service Provider Supplement. For E4SA CRU replacement instructions, click here to return to the beginning of this procedure.

Figure: E4SA CRU External Indicators



Starting an E4SA CRU

1 Start the Ethernet 4 ServerNet adapter (E4SA) CRU ADAPTER object and its subordinate SAC and PIF objects.

You can use either SCF, the OSM Service Connection, or the TSM Service Application to perform this step.

Note: TSM Service Application product Version 5.0 with SPR T7945AAF or later is required.

Using SCF:

Use the SCF START ADAPTER command with the SUB ALL option:

```
START ADAPTER $ZZLAN.<adapter-name>, SUB ALL
```

The SUB ALL option starts the ADAPTER object and its subordinate objects.

Using OSM or TSM:

1. In the Tree pane, select the E4SA CRU.
2. Select **Display> Actions**.
3. Click **Start**.
4. Click **Perform action**.

2 Verify that the E4SA CRU ADAPTER object is in the STARTED state.

Use the SCF STATUS ADAPTER command:

```
STATUS ADAPTER $ZZLAN.<adapter-name>
```

The example shows the output of the SCF STATUS ADAPTER command.

3 Verify that the ServerNet addressable controllers (SACs) are in the STARTED state.

Use the SCF STATUS SAC command:

```
STATUS SAC $ZZLAN.<adapter-name>.*
```

The example shows the output of the SCF STATUS SAC command.

4 Verify that the physical interfaces (PIFs) are in the STARTED state.

   Use the SCF STATUS PIF command:

   ```
   STATUS PIF $ZZLAN.<adapter-name>.*
   ```

   The example shows the output of the SCF STATUS PIF command.

5 Start the logical interfaces (LIFs).

   Use the SCF START LIF command for each LIF:

   ```
   START LIF $ZZLAN.<lif-name>
   START LIF $ZZLAN.<lif-name>
   START LIF $ZZLAN.<lif-name>
   START LIF $ZZLAN.<lif-name>
   ```

6 Verify that the LIFs are in the STARTED state.

   Use the SCF STATUS LIF command:

   ```
   STATUS LIF $ZZLAN.*
   ```

   The example shows the output of the SCF STATUS LIF command.

If the SCF STATUS ADAPTER command shows that the E4SA CRU SAC object is still in the STARTING state after a few minutes or if OSM or TSM indicates that the resource needs attention, do the following:

1 Check for messages in the event log by using the OSM or TSM Event Viewer. See Finding SLSA Subsystem Event Messages in the Event Log for more information.

2 Check the firmware version of the new E4SA CRU. See Updating the Firmware on a SLSA Adapter for more information.

Example: Verifying That the ADAPTER Object for an E4SA CRU Is Started

This is an example of the SCF STATUS ADAPTER command:

```
->STATUS ADAPTER $ZZLAN.E0153

SLSA Status ADAPTER

Name             State
$ZZLAN.E0153     STARTED
```

Note that the ADAPTER object is in the STARTED state.

Example: Verifying That the SACs for an E4SA CRU Are Started

This is an example of using the SCF STATUS SAC command:

```
->STATUS SAC $ZZLAN.E0153.*

SLSA Status SAC

Name               Owner  State
$ZZLAN.E0153.0      0     STARTED
$ZZLAN.E0153.1      0     STARTED
```

Note that the ServerNet addressable controllers (SACs) are in the STARTED state.

Example: Verifying That the PIFs for an E4SA CRU Are Started

This is an example of the SCF STATUS PIF command:

```
->STATUS PIF $ZZLAN.E0153.*

SLSA Status PIF

Name                    State
$ZZLAN.E0153.0.A        STARTED
$ZZLAN.E0153.0.B        STARTED
$ZZLAN.E0153.1.A        STARTED
$ZZLAN.E0153.1.B        STARTED
```

Note that the physical interfaces (PIFs) are in the STARTED state.

Example: Verifying That the LIFs for an E4SA CRU Are Started

This is an example of the SCF STATUS LIF command:

```
->STATUS LIF $ZZLAN.*

SLSA Status LIF

Name           State     Access State
$ZZLAN.L018    STARTED       UP
$ZZLAN.L019    STARTED       UP
$ZZLAN.L01A    STARTED       UP
$ZZLAN.L01B    STARTED       UP
```

Note that the logical interfaces (LIFs) are in the STARTED state.

Starting the Communications Lines and SWAN Concentrators That Use an E4SA CRU

To start a TCP/IP subnet:

Use the following SCF START SUBNET command for conventional TCP/IP:

```
START SUBNET
$<tcpip-process-name>.#<subnet-name>
```

Or use the following SCF START SUBNET command for Parallel Library TCP/IP:

```
START SUBNET
$<tcpip-process-name>.*.<subnet-name>
```

To start an IPXPROTO process:

Use the SCF START PROCESS command:

```
START PROCESS $<process-name>
```

To start a Port Access Method (PAM) line:

Use the SCF START LINE command with the SUB ALL option:

```
START LINE $<line-name>, SUB ALL
```

The SUB ALL option starts the LINE object and its subordinate objects.

To start an Expand-over-IP line:

1. Start the WAN subsystem input/output process (IOP).

   Use the SCF START DEVICE command:

   ```
   START DEVICE $ZZWAN.#<device-name>
   ```

2. Start the line.

   Use the SCF START LINE command to start a single line:

   ```
   START LINE $<line-name>
   ```

   Use the SCF START PATH command to start all the lines in an Expand multiline path:

   ```
   START PATH $<path-name>
   ```

To start a ServerNet wide area network (WAN) concentrator and its associated

WAN subsystem IOPs and communications lines:

1 Start the SWAN concentrator.

Use the SCF START ADAPTER command with the SUB ALL option:

```
START ADAPTER $ZZWAN.#<adapter-name>, SUB ALL
```

The SUB ALL option starts the ADAPTER object and its subordinate objects.

2 Start the WAN subsystem IOPs.

Use the SCF START DEVICE command:

```
START DEVICE $ZZWAN.#<device-name>
```

3 Start the lines.

Use the SCF START LINE command to start a single line:

```
START LINE $<line-name>
```

Use the SCF START PATH command to start all the lines in an Expand multiline path:

```
START PATH $<path-name>
```

Verifying That the Communications Lines and SWAN Concentrators That Use an E4SA CRU Are Started

To verify that a TCP/IP subnet is started:

Use the following SCF STATUS SUBNET command for conventional TCP/IP:

```
STATUS SUBNET
$<tcpip-process-name>.#<subnet-name>
```

Use the following SCF STATUS SUBNET command for Parallel Library TCP/IP:

```
STATUS SUBNET
$<tcpip-process-name>.*.<subnet-name>
```

The example shows the output of this command.

To verify that an IPXPROTO process is started:

Use the SCF STATUS PROCESS command:

```
STATUS PROCESS $<process-name>
```

The example shows the output of this command.

To verify that a Port Access Method (PAM) line is started:

Use the SCF STATUS LINE command:

```
STATUS LINE $<line-name>
```

The example shows the output of this command.

To verify that an Expand-over-IP line is started:

1. Verify that the WAN subsystem IOP is in the STARTED state.

   Use the SCF STATUS DEVICE command:

   ```
   STATUS DEVICE $ZZWAN.#<device-name>
   ```

   The example shows the output of this command.

2 Verify that the line is in the STARTED state.

Use the SCF STATUS LINE command for a single line:

```
STATUS LINE $<line-name>
```

Use the SCF STATUS PATH command for an Expand multiline path:

```
STATUS PATH $<path-name>
```

The example shows the output of these commands.

To verify that a ServerNet wide area network (WAN) concentrator and its associated WAN subsystem IOPs and communications lines are started:

1 Verify that the SWAN concentrator is in the STARTED state.

Use the SCF STATUS ADAPTER with the SUB ALL option:

```
STATUS ADAPTER $ZZWAN.#<adapter-name>, SUB ALL
```

The SUB ALL option displays status information for the ADAPTER object and its subordinate objects.

The example shows the output of this command.

2 Verify that the WAN subsystem IOPs are in the STARTED state.

Use the SCF STATUS DEVICE command:

```
STATUS DEVICE $ZZWAN.#<device-name>
```

The example shows the output of this command.

3 Verify that the lines are in the STARTED state.

Use the SCF STATUS LINE command for a single line:

```
STATUS LINE $<line-name>
```

Use the SCF STATUS PATH command for an Expand multiline path:

```
STATUS PATH $<path-name>
```

The example shows the output of these commands.

If an object is not in the STARTED state, check the event log using the OSM or TSM Event Viewer.

Refer to the Operator Messages Manual for cause, effect, and recovery information for event messages.

Example: Verifying That a TCP/IP Subnet Is Started

This is an example of the SCF STATUS SUBNET command:

```
-> STATUS SUBNET $ZTC01.#SN2

TCPIP Status SUBNET \COWBOY.$ZTC01.#SN2

Name                 Status

#SN2                 STARTED
```

Note that the subnet is in the STARTED state.

Example: Verifying That an IPXPROTO Process Is Started

This is an example of an SCF STATUS PROCESS command:

```
-> STATUS PROCESS $ZNV2

IPXSPX Status PROCESS

Process Name     State      Diagnostic State    Trace
$ZNV2            STARTED    NORMAL               OFF
```

Note that the IPXPROTO process is in the STARTED state.

Example: Verifying That a PAM Line Is Started

This is an example of the SCF STATUS LINE command:

```
-> STATUS LINE $TOK1

                    Primary         Backup
Name      State     CPU    PIN      CPU    PIN    Trace
$TOK1     STARTED   1      278      -1     -1     OFF
```

Note that the Port Access Method (PAM) line is in the STARTED state.

Example: Verifying That a WAN Subsystem IOP Is Started

This is an example of the SCF STATUS DEVICE command:

```
-> STATUS DEVICE $ZZWAN.#LINE1

WAN Manager STATUS DEVICE for DEVICE \COWBOY.$ZZWAN.#LINE1
   State :........ STARTED

   LDEV number.... 110
   PPIN.......... 2  ,13         BPIN......... 3  ,14
```

Note that the WAN subsystem input/ouput process (IOP) is in the STARTED state.

Example: Verifying That a Line Is Started

This is an example of the SCF STATUS LINE command:

```
-> STATUS LINE $LINE1

EXPAND   Status LINE1

Name         State       PPID     BPID     CIU-Path  ConMgr-LDEV
$SATHO0    STARTED     2, 10    3, 7          A          91
```

Note that the line is in the STARTED state.

This is an example of the SCF STATUS PATH command:

```
-> STATUS PATH $PATH

EXPAND  Status PATH

Name             State        PPID     BPID      Lines #
$PSHOT           STARTED      2, 15    3, 15       2
```

Note that the path is in the STARTED state.

Example: Verifying That a SWAN Concentrator Is Started

This is an example of the SCF STATUS ADAPTER command with the SUB ALL option. Detailed information for only one communications line interface processor (CLIP) is included in the display.

```
->STATUS ADAPTER $ZZWAN.#S01, SUB ALL

WAN Manager STATUS ADAPTER for ADAPTER \COWBOY.$ZZWAN.#S01
  State....... STARTED

  Number of clips. 3

  Clip 1 status : CONFIGURED
  Clip 2 status : CONFIGURED
  Clip 3 status : CONFIGURED

WAN Manager STATUS SERVER for CLIP \COWBOY.$ZZWAN.#S01.1
  State :...... STARTED
  Path A.......: CONFIGURED
  Path B.......: CONFIGURED

  Number of lines. 2

  Line............ 0    : FREE
  Line............ 1    : FREE

WAN Manager STATUS PATH for PATH \COWBOY.$ZZWAN.#S01.1.A
  State :...... STARTED

  MEDIA TYPE..... ETHERNET
  MEDIA ADDRESS.. %H08008E004814

WAN Manager STATUS PATH for PATH \COWBOY.$ZZWAN.#S01.1.B
  State :...... STARTED

  MEDIA TYPE..... ETHERNET
  MEDIA ADDRESS.. %H08008E004815

WAN Manager STATUS TASK for TASK \COWBOY.$ZZWAN.#S01.1.DIAG
  State :...... STARTED

WAN Manager STATUS TASK for TASK \COWBOY.$ZZWAN.#S01.1.DLC0
  State :...... STARTED

CLIP Path Name.... A              TCPIP Port used.... 5000
CLIP Protocol Id.. 1              Interface Type..... 0
```

```
Clip Program...... $SYSTEM.CSS01.C1096P00
Program timestamp. 17 Jan 1997, 11:35:04.890

WAN Manager STATUS TASK for TASK \COWBOY.$ZZWAN.#S01.1.DLC1
State :........ STARTED
CLIP Path Name.... A              TCPIP Port used.... 5001
CLIP Protocol Id.. 1              Interface Type..... 0
Clip Program...... $SYSTEM.CSS01.C1096P00
Program timestamp. 26 Mar 1997, 13:36:04.981
```

Note that the ADAPTER, SERVER, PATH, and TASK objects are in the STARTED state.

Resuming Customer Applications

1. Perform any actions necessary to resume customer applications.

   Note: The actions required to perform this step depend on the customer's application.

2. Notify end users that applications are now available.

Viewing the Operator Log ($0) Using the OSM or TSM Event Viewer

You can use either the OSM or the TSM Event Viewer to view $0.

Using OSM

1. From a system console, launch the OSM Event Viewer or by doing one of the following:
   - From the Start button:
     a. Select: **Start>Programs>HP OSM>OSM Event Viewer**. The OSM Event Viewer Home Page appears.
     b. Select a system.
   - **From the OSM Service Connection:**
     a. **Log on to the server using the OSM Service Connection**
     b. **Select Tools>Event Viewer.**

   The Log On dialog box appears.
2. Enter a NonStop Kernel operating system user ID and password and click **Log on**.
3. In the Event Source(s) field, enter **$0**.

   Note: You can also select the timeframe and other filter criteria.
4. Click **Show Events**.
5. Browse through the event messages that are stored in $0 for information on when these events were generated.

   For detailed information about an event, click the link for that event. The Event Detail dialog box appears.

   For more information on event messages, refer to the Operator Messages Manual.

See the OSM Migration Guide or the OSM User's Guide for more information on launching and logging on to the OSM Event Viewer. See OSM Event Viewer online help for information on using the OSM Event Viewer.

Using TSM

1. From a system console, launch the TSM Event Viewer Application by doing one of the following:
   - From the Start button, select:
     - For TSM client software Versions 2000A and later: **Start>Programs> Compaq TSM>TSM Event Viewer**
     - For TSM client software Versions 10.0 and earlier: **Start>Programs>TSM Client> TSM Event Viewer**
   - Log on to the server using the TSM Service Application and select **Display>Events**.
   - Open the TSM Low-Level Link and select **Display>Events**.

   The TSM EMS Event Viewer dialog box appears.
2. Select **File>Log on**. The Log on to NSK System dialog box appears.
3. Select a server, type in a NonStop Kernel operating system user ID, and click **OK**.
4. From the **Setup** menu, choose **Source** criteria.
5. On the Setup Search Criteria **Sources** tab, under **Available Sources**, choose **$0**, and, if necessary, click **Add** to add it to the list of Selected Sources. If there are other sources listed in the Selected Sources list, you might want to remove them. Select the source you wish to remove, and click **Remove**. When you are done, click **OK**.

   Note: You can also select the timeframe and subsystem events you wish to view.
6. Browse through the event messages that are stored in $0 for information on when these events were generated.

   For detailed information about an event, select the event and from the **Display** menu, choose **Detail**. The Event Detail dialog box appears.

   For more information on event messages, see the Operator Messages Manual.

See the TSM Online User Guide for more information on launching and logging on to the TSM Event Viewer. See TSM Event Viewer online help for information on using the

TSM Event Viewer.

Viewing the Service Log ($ZLOG) Using the OSM or TSM Event Viewer

You can use either the OSM or the TSM Event Viewer to view $ZLOG.

Using OSM

1. From a system console, launch the OSM Event Viewer or by doing one of the following:
   - **From the OSM Service Connection:**
     a. **Log on to the server using the OSM Service Connection**
     b. **Select Tools>Event Viewer.**
   - From the Start button:
     a. Select: **Start>Programs>HP OSM>OSM Event Viewer**. The OSM Event Viewer Home Page appears.
     b. Select a system.

   The Log On dialog box appears.
2. Enter a NonStop Kernel operating system user ID and password and click **Log on**.
3. In the Event Source(s) field, enter **$ZLOG**.

   Note: You can also select the timeframe and other filter criteria.
4. Click **Show Events**.
5. Browse through the event messages that are stored in the $ZLOG for information on when these events were generated.

   For detailed information about an event, click the link for that event. The Event Detail dialog box appears.

   For more information on event messages, refer to the Operator Messages Manual.

See the OSM Migration Guide or the OSM User's Guide for more information on launching and logging on to the OSM Event Viewer. See OSM Event Viewer online help for information on using the OSM Event Viewer.

Using TSM

1. From a system console, launch the TSM Event Viewer Application by doing one of the following:
   - From the Start button, select:
     - For TSM client software Versions 2000A and later: **Start>Programs> Compaq TSM>TSM Event Viewer**
     - For TSM client software Versions 10.0 and earlier: **Start>Programs>TSM Client> TSM Event Viewer**
   - Log on to the server using the TSM Service Application and select **Display>Events**.
   - Open the TSM Low-Level Link and select **Display>Events**.

   The TSM EMS Event Viewer dialog box appears.
2. Select **File>Log on**. The Log on to NSK System dialog box appears.
3. Select a server, type in a NonStop Kernel operating system user ID, and click **OK**.
4. From the **Setup** menu, choose **Source** criteria.
5. On the Setup Search Criteria **Sources** tab, under **Available Sources**, choose **$ZLOG**, and if necessary, click **Add** to add it to the list of Selected Sources. If there are other sources listed in the Selected Sources list, you might want to remove them. Select the source you wish to remove, and click **Remove**. When you are done, click **OK**.

   Note: You can also select the timeframe and subsystem events you wish to view.
6. Browse through the event messages that are stored in the $ZLOG for information on when these events were generated.

   For detailed information about an event, select the event and from the **Display** menu, choose **Detail**. The Event Detail dialog box appears.

   For more information on event messages, see the Operator Messages Manual.

See the TSM Online User Guide for more information on launching and logging on to the TSM Event Viewer. See TSM Event Viewer online help for information on using the

TSM Event Viewer.

Managing the Windows NT Event Viewer Application Log

The event viewer has 3 logs: an Application log, a Security log, and a System log. Each log can contain a limited number of entries; for example, 512 KB. The Application log can hit the maximum size when you are running the TSM service application or performing a system discovery using the TSM Low-Level Link.

Note: OSM is not supported on workstations running the Windows NT operating system.

To prevent a log from becoming full, clear or reconfigure the log. You can change the size of the log and select options such as "Overwrite events as needed" and "Overwrite events older than xx days." Normally, the default is "Overwrite events older than 7 days."

To clear the NT Application Event Log:

1. Log on as an administrator or a member of the administrator's group.
2. On the task bar, select **Start> Programs> Administrative Tools (Common)> Event Viewer**. The Event Viewer window appears.
3. From the log menu, select **Application**.
4. From the log menu, select **Clear All Events**. All NT Application events are cleared from the log file.
5. Close the Event Viewer window.

To configure the NT Application Event Log:

1. On the tool bar, select **Status.** The Event Viewer window appears.
2. From the log menu, select **Application**.
3. From the log menu, select **Log Settings**. The Event Log Settings dialog box appears.
4. You can increase the size of the log file, and select one of the overwrite options.
5. Close the Event Viewer window.

For more information, refer to the NT Event Viewer online help.

Managing the Windows Event Viewer Application Log

The event viewer has 3 logs: an Application log, a Security log, and a System log. Each log can contain a limited number of entries; for example, 512 KB. The Application log can hit the maximum size when you are running the TSM Service Application (but not the OSM Service Connection) or performing a system discovery using the OSM or TSM Low-Level Link. To prevent a log from becoming full, clear or reconfigure the log. You can change the size of the log and select options such as "Overwrite events as needed" and "Overwrite events older than xx days." Normally, the default is "Overwrite events older than 7 days."

To clear the Application Log:

1. Log on as an administrator or a member of the administrator's group.
2. On the task bar, select **Start**>**Settings**>**Control Panel**, and then double-click **Administrative Tools** and **Event Viewer**. The Event Viewer window appears.
3. In the control tree pane, click the log you want to clear.
4. Select **Action>Clear all Events**. A message appears "Do you want to save xx Log before clearing it?" Click **Yes** to save the log entries. Click **No** to permanently discard the entries.
5. Close the Event Viewer window.

To configure the Application Log:

1. Log on as an administrator or a member of the administrator's group.
2. On the task bar, select **Start**>**Settings**>**Control Panel**, and then double-click **Administrative Tools** and **Event Viewer**. The Event Viewer window appears.
3. In the control tree pane, click the log you want to change.
4. Select **Action>Properties** and click the **General** tab.
5. To change the log's size, change the setting in the **Maximum log size** box.

6 Select an option under **When the maximum log size is reached:**
   - Overwrite events as needed.
   - Overwrite event older than xx days (default= 7 days).
   - Do not overwrite events (clear log manually).

7 Click **Clear Log** to put the new settings into effect. A message appears "Do you want to save xx Log before clearing it?" Click **Yes** to save the log entries. Click **No** to permanently discard the entries.

8 Click **OK** to close the xx Log Properties window..

9 Close the Event Viewer window.

Notes:

- After you clear a log, only new events will appear in the log.
- If you select **Do not overwrite events (clear log manually)** in the Properties dialog box of an active log, you must periodically clear the System Log when the log reaches a certain size or when a message notifies you that the log is full.
- You must delete archived logs. These logs cannot be cleared.

For more information, refer to Event Viewer online help. Click **Action** and then **Help**.