

Lucent Technologies
Bell Labs Innovations



Stinger® Compact Remote

Getting Started Guide

Part Number: 7820-0986-001
For software version 9.7.0
August 2004

Copyright © 2004 Lucent Technologies Inc. All rights reserved.

This material is protected by the copyright laws of the United States and other countries. It may not be reproduced, distributed, or altered in any fashion by any entity (either internal or external to Lucent Technologies), except in accordance with applicable agreements, contracts, or licensing, without the express written consent of Lucent Technologies. For permission to reproduce or distribute, please email your request to techcomm@lucent.com.

Notice

Every effort was made to ensure that the information in this document was complete and accurate at the time of printing, but information is subject to change. For latest information, refer to online product documentation at www.lucent.com/support.

European Community (EC) RTTE compliance

 Hereby, Lucent Technologies, declares that the equipment documented in this publication is in compliance with the essential requirements and other relevant provisions of the Radio and Telecommunications Technical Equipment (RTTE) Directive 1999/5/EC.

To view the official *Declaration of Conformity* certificate for this equipment, according to EN 45014, access the Lucent INS online documentation library at <http://www.lucentdocs.com/ins>.

Safety, compliance, and warranty Information

Before handling any Lucent Access Networks hardware product, read the *Edge Access and Broadband Access Safety and Compliance Guide* included in your product package. See that guide also to determine how products comply with the electromagnetic interference (EMI) and network compatibility requirements of your country. See the warranty card included in your product package for the limited warranty that Lucent Technologies provides for its products.

Security statement

In rare instances, unauthorized individuals make connections to the telecommunications network through the use of access features.

Trademarks

Lucent, the Lucent logo, and all Lucent brand and product names are trademarks or registered trademarks of Lucent Technologies Inc. Other brand and product names are trademarks of their respective holders.

Ordering Information

You can order the most up-to-date product information and computer-based training online at <http://www.lucentdocs.com/bookstore>.

Feedback

To comment on this information product, go to the Online Comment Form (<http://www.lucent-info.com/comments/enus/>) or email your comments to the Comments Hotline (comments@lucent.com).

Customer Service

Product and service information, and software upgrades, are available 24 hours a day. Technical assistance options accommodate varying levels of urgency.

Finding information and software

To obtain software upgrades, release notes, and addenda for this product, log in to Lucent OnLine Customer Support at <http://www.lucent.com/support>.

Lucent OnLine Customer Support also provides technical information, product information, and descriptions of available services. The center is open 24 hours a day, seven days a week. Log in and select a service.

Obtaining technical assistance

Lucent OnLine Customer Support at <http://www.lucent.com/support> provides access to technical support. You can obtain technical assistance through email or the Internet, or by telephone. If you need assistance, make sure that you have the following information available:

- Active service or maintenance contract number, entitlement ID, or site ID
- Product name, model, and serial number
- Software version
- Software and hardware options If supplied by your carrier, service profile identifiers (SPIDs) associated with your line
- Your local telephone company's switch type and operating mode, such as AT&T, 5ESS Custom or Northern Telecom National ISDN-1
- Whether you are routing or bridging with your Lucent product
- Type of computer you are using
- Description of the problem

Obtaining assistance through email or the Internet

If your services agreement allows, you can communicate directly with a technical engineer through Email Technical Support or a Live Chat. Select one of these sites when you log in to <http://www.lucent.com/support>.

Calling the technical assistance center (TAC)

If you cannot find an answer through the tools and information of Lucent OnLine Customer Support or if you have a very urgent need, contact TAC. Access Lucent OnLine Customer Support at <http://www.lucent.com/support> and click Contact Us for a list of telephone numbers inside and outside the United States.

Alternatively, call 1-866-LUCENT8 (1-866-582-3688) from any location in North America for a menu of Lucent services. Or call +1 510-747-2000 for an operator. You must have an active services agreement or contract.

Contents

Customer Service	iii
About This Guide	xv
What is in this guide	xv
What you should know.....	xv
Documentation conventions.....	xvi
Stinger documentation set	xvii
Chapter 1 Introduction to the Stinger Compact Remote	1-1
Stinger Compact Remote overview.....	1-1
Stand-alone operation	1-1
Operation with a control module.....	1-2
Operation with an IP2000 module.....	1-2
Hosted operation.....	1-3
Stinger Compact Remote Hardware.....	1-3
Stinger Compact Remote card cage chassis	1-5
Card-cage modular components.....	1-6
Host hardware	1-8
Chapter 2 Preparing to Install the CR Unit	2-1
Installation tools and equipment	2-1
Preventing static discharge damage.....	2-2
Use a wrist strap.....	2-2
Remove plastics from your work area	2-4
Store components properly	2-4
Unpacking the Stinger Compact Remote	2-4
Verifying the hardware	2-5
Checking modules and chassis	2-6
Checking modules in the control (COP) slot	2-7
The control module	2-7
Control module interfaces.....	2-7
The IP2000	2-8
IP2000 interfaces	2-9
The COP	2-10
COP interfaces	2-10
Checking the LIMs.....	2-11
48-port ADSL LIM.....	2-11
The T1-IMA LIM	2-12
Checking the LPMs	2-13

Checking the cooling unit.....	2-14
Checking the power supply.....	2-15
Chapter 3 CR Enclosure and Component Installation.....	3-1
Before you begin	3-1
Stinger CR Installation	3-1
Mounting hardware.....	3-2
Attaching the Stinger CR mounting bracket to a cabinet.....	3-4
Preparing the cabinet	3-4
Preparing the cable pass-through holes	3-4
Mounting the enclosure	3-4
Route and connect the cables.....	3-5
Route and connect the fibers	3-5
Grounding the enclosure	3-7
Installation and replacement of Stinger CR components.....	3-7
Slot numbering and module placement	3-8
Module installation and replacement for the COP slot.....	3-8
Removing a module from the COP slot.....	3-8
Installing a module in the COP slot.....	3-9
Installing and replacing LIMs.....	3-10
Installing a LIM	3-10
Replacing a LIM	3-11
Installing and replacing LPMs.....	3-12
Installing an LPM	3-12
Replacing an LPM	3-12
Replacing the chassis cooling module.....	3-13
Replacing the external cooling fan	3-15
Replacing the power supply.....	3-17
Physical connections to the Stinger CR unit	3-18
Connections to modules in the COP slot	3-18
PCMCIA slot.....	3-19
Gigabit Ethernet port.....	3-19
155Mbps optical port.....	3-20
10/100 Ethernet port	3-21
Diagnostic port	3-22
Alarm input port	3-23
Connections to the LPMs.....	3-24
Connecting the LPM.....	3-24
Turning on power to a Stinger CR unit.....	3-25
Status lights	3-26
IP2000 and control module status lights	3-26
COP status lights	3-28
LIM status lights.....	3-30
Cooling unit status lights	3-31
Power supply status lights.....	3-32
What's next	3-32
Chapter 4 Initial Stand-alone Configuration.....	4-1
Basic configuration overview	4-1
Administrative connections.....	4-2
Serial connection to a console	4-2

10/100 Ethernet connection to a workstation console.....	4-3
Gigabit Ethernet connection to a workstation console	4-3
Logging into the IP2000 or control module	4-4
Restricting administrative access	4-5
Changing defaults for serial-port logins.....	4-5
Changing the default admin password	4-5
Setting a Telnet password	4-6
Providing a basic system IP configuration	4-7
IP address syntax	4-7
Netmasks.....	4-7
Subnets.....	4-8
Assigning the Ethernet IP addresses	4-9
The 10/100BaseT Ethernet interface	4-10
The IP2000 Gigabit Ethernet interface	4-10
Chapter 5 Hosted System Configuration	5-1
Stinger CR configuration overview for hosted operation	5-1
Setting the chassis ID (optional)	5-1
Introduction to the host management interface	5-3
Configuring a hosted Compact Remote system	5-4
Configuring the host system to operate in master mode.....	5-4
Identifying the remote shelves	5-5
Enabling RLIM and host trunk interfaces.....	5-6
Provisioning a virtual circuit from a remote LIM	5-7
Traffic management in hosted Compact Remote systems.....	5-8
slot-level LIM CAC default behavior	5-8
Hosted system bandwidth and CAC calculations.....	5-9
Upstream traffic shaping in a hosted system	5-11
Internal queue priorities on an OLIM	5-11
LIM-trunk VP switching capacity via an OLIM	5-11
Working with the remote-shelf-config profile	5-11
Overview of profile contents	5-11
Minimal configuration for a remote shelf.....	5-12
Specifying a remote shelf name and location	5-13
Configuring shelf validation	5-13
Chapter 6 Hosted System Management.....	6-1
Upgrading hosted system software.....	6-1
Required steps before initializing NVRAM in the host	6-1
Typical hosted system upgrade procedure	6-2
Hosted system upgrades that include bootloader code	6-3
Reset options for hosted systems	6-3
Monitoring remote LIMs and connections.....	6-3
Displaying RLIM status	6-3
Displaying shelf-specific ATM connection and signaling information.....	6-4
Monitoring the status of remote shelves.....	6-4
Using the remote-shelf-stat profile	6-5
Using the remoteself command	6-7
Raising and clearing alarm events in a hosted system.....	6-7
Configuring alarms for remote shelves	6-8
Remote shelf alarm events	6-8

Sample alarm for remote shelf 3 state change	6-9
Sample alarm for input-relay closure status on any remote shelf	6-9
Sample alarm for internal fan failure on shelf 2	6-10
Enabling traps for remote-shelf events	6-10
Trap optimization	6-10
Modified traps to include shelf numbers	6-11
Enabling remote shelf watchdog warning traps	6-11

Appendix A Stinger CR Intended Use.....A-1

User line interfaces	A-1
COP interfaces	A-1
IP2000 interfaces	A-2
Control module interfaces	A-2

Appendix B The Host Stinger OLIM B-1

Introducing the Stinger OLIM	B-1
Installing an OLIM	B-1
Interpreting OLIM status lights	B-2
OLIM specifications	B-3
Configuring a Stinger OLIM	B-4

Appendix C Cables and Connectors C-1

Diagnostic port and cable pinouts	C-1
Alarm input port pinouts	C-2
Stinger CR cabling for the 48-port LPM with splitters	C-2
LPM connectors	C-3
LPM connections and protection blocks	C-3
LPM cables	C-3
LPM to protection block associations	C-4
Protection block Port numbering vs. TAOS port indexing	C-5
Protector orientation details	C-6
Connection block LPM cable associations	C-6
Cable stub connections to protection blocks	C-15
Cable and protection associations	C-15
Protection block power connections	C-17
Chassis door alarm connections	C-18
Door alarm for hosted operation	C-18
Door alarm connection for stand-alone operation	C-18
Enclosure cable exit points	C-19
Optical connectors	C-20

**Appendix D Safety-Related Electrical, Physical, and Environmental Information .
D-1**

Electrical and electronic information	D-1
Protection block elements	D-2
Laser safety	D-2
Laser classifications	D-2
Laser warning instructions	D-3
Laser warning labels	D-3
Handling optical fibers	D-4

Routing and connecting	D-4
Splicing	D-4
Cleaning optical connectors and couplings	D-4
Safety certifications	D-5
Physical specifications	D-5
Site specifications	D-6
Operating environment	D-6
Weight and lifting requirements	D-6
Index	Index-1

Figures

Figure 1-1	Example of Compact Remote stand-alone operation.....	1-2
Figure 1-2	Example of Compact Remote hosted operation.....	1-3
Figure 1-3	The Stinger Compact Remote	1-4
Figure 1-4	Stinger CR card-cage	1-5
Figure 1-5	OLIMs installed in a Stinger FS+ host.....	1-8
Figure 1-6	Stinger CR units connected to a host Stinger unit	1-9
Figure 2-1	Wrist grounding strap	2-3
Figure 2-2	Wrist strap plugged into a grounding jack	2-3
Figure 2-3	Stinger CR enclosure details.....	2-5
Figure 2-4	Front view of a Stinger Compact Remote chassis	2-6
Figure 2-5	Stinger Compact Remote control module interfaces.....	2-8
Figure 2-6	The IP2000 module	2-9
Figure 2-7	Control and optics pack.....	2-10
Figure 2-8	The 48-port low-power LIM	2-12
Figure 2-9	The T1-IMA LIM (24-port version).....	2-13
Figure 2-10	The 48-port LPM with splitters	2-14
Figure 2-11	The Stinger CR cooling unit	2-15
Figure 2-12	The Stinger CR power supply.....	2-15
Figure 3-1	Stinger CR enclosure side mounting bracket assemblies	3-2
Figure 3-2	Stinger CR enclosure pedestal mounting bracket assemblies.....	3-3
Figure 3-3	Stinger CR enclosure pole mounting bracket assemblies.....	3-3
Figure 3-4	Enclosure fiber tray details.....	3-6
Figure 3-5	Enclosure grounding connector	3-7
Figure 3-6	Slot labeling on the Stinger CR chassis	3-8
Figure 3-7	Removing a module from the COP slot	3-9
Figure 3-8	Installing a module in the COP slot.....	3-10
Figure 3-9	Removing LPMs	3-13
Figure 3-10	Removing the cooling module	3-14
Figure 3-11	Replacing the enclosure cooling fan.....	3-16
Figure 3-12	Removing the power supply	3-17
Figure 3-13	Connectors for modules in the COP slot	3-18
Figure 3-14	Gigabit Ethernet connection to IP2000 module.....	3-20
Figure 3-15	155Mbps optical connection to the COP.....	3-21
Figure 3-16	Ethernet connection.....	3-21
Figure 3-17	Serial management connection for a stand-alone Stinger CR	3-22
Figure 3-18	Connecting the door alarm to the ALARM input port.....	3-24
Figure 3-19	Connecting an LPM.....	3-25
Figure 3-20	IP2000 status lights	3-27
Figure 3-21	COP status lights	3-29
Figure 3-22	ADSL 48-port low-power LIM	3-30
Figure 3-23	The Stinger CR cooling unit	3-31

Figure 3-24	The Stinger CR power supply.....	3-32
Figure 4-1	Serial management connection to a Stinger CR unit.....	4-2
Figure 4-2	10/100 Ethernet connection	4-3
Figure 4-3	Gigabit Ethernet connection	4-4
Figure 4-4	Default netmask for class C IP address	4-8
Figure 5-1	Chassis validation ID DIP switches	5-2
Figure 5-2	Setting the Validation ID DIP switch.....	5-3
Figure 5-3	Slot-level CAC bandwidth calculations performed with default settings	5-10
Figure 5-4	Port-level CAC sequence (performed only at provisioning time) ...	5-10
Figure 5-5	Factory-default validation ID setting on Compact Remote	5-14
Figure B-1	the Stinger OLIM.....	B-2
Figure C-1	LPM 64-pin connector	C-3
Figure C-2	Protection block cables	C-4
Figure C-3	LPMs and related protection blocks	C-4
Figure C-4	Protection block port assignments.....	C-5
Figure C-5	Protection plug orientation example.....	C-6
Figure C-6	Stub cables for connection to the protection blocks.....	C-15
Figure C-7	Protection block power connectors	C-17
Figure C-8	Door alarm connectors on the Stinger CR chassis	C-18
Figure C-9	Door alarm cable for stand-alone operation	C-19
Figure C-10	Enclosure cable exit points.....	C-19
Figure C-11	Optical connectors.....	C-20
Figure D-1	Warning labels for identification of Class 1 laser devices.....	D-4

Tables

Table 1-1	Functional listing of card-cage components.....	1-6
Table 3-1	Connectors for modules in the COP slot.....	3-19
Table 3-2	Number of pairs for providing power.....	3-26
Table 3-3	Status lights on the IP2000 module	3-27
Table 3-4	Status lights on the COP module	3-29
Table 3-5	ADSL 48-port Annex A LIM status lights	3-31
Table 3-6	Cooling unit status light	3-32
Table 4-1	IP address classes and number of network bits	4-7
Table 4-2	Decimal subnet masks and prefix lengths	4-9
Table 5-1	Validation ID DIP switch setting values	5-2
Table 5-2	Default allocation of unique nailed-group numbers to remote shelves.....	5-7
Table 5-3	New locations for traffic management settings	5-8
Table 6-1	Compact Remote alarm events	6-8
Table B-1	OLIM status lights	B-3
Table B-2	OLIM specifications	B-3
Table C-1	Control port and cable pinouts.....	C-1
Table C-2	Alarm input pinouts.....	C-2
Table C-3	Tip/Ring connections to protection blocks 1, 3, and 5	C-6
Table C-4	Tip/Ring connections to protection blocks 2, 4, and 6	C-10
Table C-5	OSP cable binders, pairs, and protection block connections	C-15
Table C-6	Wiring connection from the power stub.....	C-17
Table D-1	Stinger electronic and electrical specifications	D-1
Table D-2	Laser classifications	D-2
Table D-3	Stinger CR physical specifications	D-5
Table D-4	Stinger CR site specifications.....	D-6
Table D-5	Stinger CR weight details	D-6

About This Guide

What is in this guide

This guide explains how to perform the following installation and basic configuration tasks on a Stinger Compact Remote unit:

- Physical installation of a Stinger Compact Remote unit
- Connection of an administrative terminal to a Stinger Compact Remote unit
- Basic configuration for a Stinger Compact Remote unit as a stand alone unit to provide administrative network access.
- Physical configuration of a Stinger Compact Remote as a remotely hosted unit
- Configuration of a Stinger host to utilize a hosted Stinger Compact Remote

This guide also provides Stinger Compact Remote technical specifications and an operational overview of the Stinger Compact Remote. When you finish performing the instructions in this guide, your Stinger Compact Remote will be installed and you will be able to configure individual lines on the unit from a remote administrative terminal or a Stinger host.



Note This manual describes the features for Stinger Compact Remote units running software version 9.7 or later. Some features might not be available with earlier versions or specialty loads of the software.



Warning Before installing or operating your Stinger unit, be sure to read the safety instructions in the *Edge Access and Broadband Access Safety and Compliance Guide*. For information specific to your unit, see Appendix D, "Safety-Related Electrical, Physical, and Environmental Information," in this manual.

What you should know

This guide is for the person who installs and configures and maintains Stinger Compact Remote units. To perform these tasks, you need the following:

- Knowledge and understanding of local hardware installation practices, including physical and electrical safety standards.
- The ability to solve problems related to the facilities that connect to the Stinger Compact Remote. This includes optical facilities, supply voltages, and local cable pairs that provide DSL and POTS service.
- The ability to connect and use a serial terminal and knowledge of the TAOS software, if verification or configuration of the TAOS parameters will be performed.

Some understanding of the following technologies may also be helpful:

- IP networking
- ATM networking
- DSL technologies and protocols



Warning Before installing your Stinger Compact Remote unit, be sure to read the safety instructions in the *Edge Access and Broadband Access Safety and Compliance Guide*. For information specific to your unit, see Appendix D, “Safety-Related Electrical, Physical, and Environmental Information,” in this guide.

The procedures in this guide require you to understand and follow the safety practices at your site, as well as those identified in this guide. Before installing any hardware, check the installation location for adequate temperature, humidity, and electrical requirements. Work closely with the network manager and other systems integration personnel to ensure a functional installation.

Documentation conventions

Following are all the special characters and typographical conventions used in this manual:

Convention	Meaning
Monospace text	Represents text that appears on your computer’s screen, or that could appear on your computer’s screen.
Boldface monospace text	Represents characters that you enter exactly as shown (unless the characters are also in <i>italics</i> —see <i>Italics</i> , below). If you could enter the characters but are not specifically instructed to, they do not appear in boldface.
<i>Italics</i>	Represent variable information. Do not enter the words themselves in the command. Enter the information they represent. In ordinary text, italics are used for titles of publications, for some terms that would otherwise be in quotation marks, and to show emphasis.
[]	Square brackets indicate an optional argument you might add to a command. To include such an argument, type only the information inside the brackets. Do not type the brackets unless they appear in boldface.
	Separates command choices that are mutually exclusive.
>	Points to the next level in the path to a parameter or menu item. The item that follows the angle bracket is one of the options that appear when you select the item that precedes the angle bracket.
Key1+Key2	Represents a combination keystroke. To enter a combination keystroke, press the first key and hold it down while you press one or more other keys. Release all the keys at the same time. (For example, Ctrl+H means hold down the Ctrl key and press the H key.)

Convention	Meaning
Press Enter	Means press the Enter or Return key or its equivalent on your computer.
	Introduces important additional information.
Note	
	Warns that a failure to follow the recommended procedure could result in loss of data or damage to equipment.
Caution	
	Warns that a failure to take appropriate safety precautions could result in physical injury.
Warning	
	Warns of danger of electric shock.
Warning	

Stinger documentation set

The Stinger documentation set consists of the following manuals, which can be found at <http://www.lucent.com/support> and <http://www.lucentdocs.com/ins>:

■ **Read me first:**

- *Edge Access and Broadband Access Safety and Compliance Guide*. Contains important safety instructions and country-specific information that you must read before installing a Stinger unit.
- *TAOS Command-Line Interface Guide*. Introduces the TAOS command-line environment and shows you how to use the command-line interface effectively. This guide describes keyboard shortcuts and introduces commands, security levels, profile structure, and parameter types.

■ **Installation and basic configuration:**

- *Getting Started Guide* for your unit. Shows how to install your Stinger chassis and hardware. This guide shows you how to use the command-line interface to configure and verify IP access and basic access security on the unit.

The Getting Started Guides for Stinger models with redundant control modules describe configuration of this feature.

- The *Stinger MRT Getting Started Guide* describes the features and basic configuration of the trunk modules that are specific to a Stinger MRT.
- Module guides for each type of module designed for the Stinger FS, Stinger FS+, Stinger LS, Stinger RT, Stinger CR, or Stinger MS+ an individual guide describes the module's features and provides instructions for configuring the module and verifying its status.

■ **Configuration:**

- *Stinger ATM Configuration Guide*. Describes how to use the command-line interface to configure Asynchronous Transfer Mode (ATM) operations on a Stinger unit. The guide explains how to configure permanent virtual circuits

About This Guide

Stinger documentation set

(PVCs), and shows how to use standard ATM features such as quality of service (QoS), connection admission control (CAC), and subtending.

- *Stinger IP2000 Configuration Guide*. For Stinger systems with the IP2000 control module, this guide describes how to integrate the system into the IP infrastructure. Topics include IP-routed switch-through ATM PVCs and RFC 1483 PVCs that terminate on the IP2000, IEEE 802.1Q VLAN, and forwarding multicast video transmissions on DSL interfaces.
- *Stinger Private Network-to-Network Interface (PNNI) Supplement*. Provides quick-start instructions for configuring PNNI and soft PVCs (SPVCs), and describes the related profiles and commands in the Stinger command-line interface.
- *Stinger SNMP Management of the ATM Stack Supplement*. Describes Simple Network Management Protocol (SNMP) management of ATM ports, interfaces, and connections on a Stinger unit to provide guidelines for configuring and managing ATM circuits through any SNMP management utility.
- **RADIUS:** *TAOS RADIUS Guide and Reference*. Describes how to set up a TAOS unit to use the Remote Authentication Dial-In User Service (RADIUS) server and contains a complete reference to RADIUS attributes.
- **Administration and troubleshooting:** *Stinger Administration Guide*. Describes how to administer the Stinger unit and manage its operations. Each chapter focuses on a particular aspect of Stinger administration and operations. The chapters describe tools for system management, network management, and Simple Network Management Protocol (SNMP) management.
- **Reference:**
 - *Stinger Reference*. An alphabetic reference to Stinger profiles, parameters, and commands.
 - *TAOS Glossary*. Defines terms used in documentation for Stinger units.

Introduction to the Stinger Compact Remote

1

Stinger Compact Remote overview	1-1
Stinger Compact Remote Hardware.....	1-3
Host hardware	1-8

Stinger Compact Remote overview

The Stinger Compact Remote (CR) is a temperature-hardened unit that can be installed outdoors, close to subscriber locations. Power is provided over dedicated copper telecommunications facilities from the central office. It can be configured with different hardware components to function as a small stand-alone digital subscriber line access multiplexer (DSLAM), or as a hosted optical network unit (ONU).

Stand-alone operation

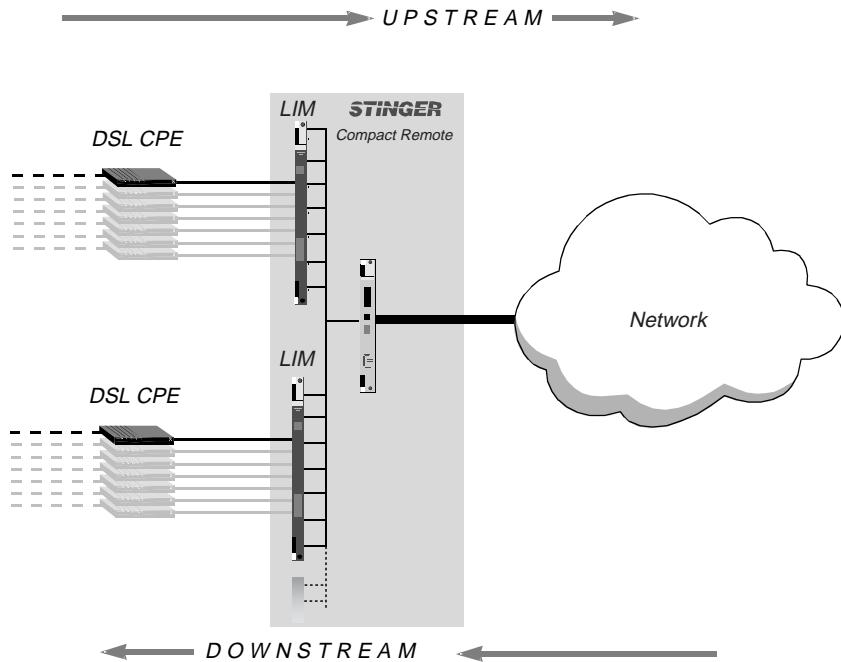
The Compact Remote unit is configured for stand-alone operation with the same procedures used to configure a Stinger FS or Stinger LS unit in a central office. Configuration and management of the unit is handled through the local TAOS management interface. This interface and all local configuration and management capabilities are provided by installing the correct control module, or an IP2000 module in the unit.

Individual subscriber lines are physically terminated on the line interface modules (LIMs) of Stinger Compact Remote unit. A Stinger CR unit that is equipped for stand alone operation with an IP2000 module, routes subscriber traffic over the gigabit Ethernet interface of the IP2000 module installed in the COP slot. A Stinger CR unit that is equipped for stand alone operation with a control module in the COP slot, routes subscriber traffic over the T1 interfaces of a TI-IMA module in one of the LIM slots.

Introduction to the Stinger Compact Remote

Stinger Compact Remote overview

Figure 1-1. Example of Compact Remote stand-alone operation



Operation with a control module

A Stinger Compact Remote unit can be equipped for stand-alone operation with a Revision 2 or Revision 2.1 control module (STGR-CM-A or STGR-CM-A2). The control module is equipped with a 10/100 Ethernet port for connection to a management network, but it is not equipped with a port that provides bandwidth for end-user traffic.

A temperature hardened T1 module (STGRRT-LIM-T1-8 or STGRRT-LIM-T1-24) can be installed in a LIM slot to provide interfaces with bandwidth for end-user traffic. Physical connections for the T1 span lines are provided by the 48-port LPM with splitters, installed in the adjacent LPM slot. For wiring details, see Appendix C, "Cables and Connectors."

The information for basic configuration of a unit with a control module is included in this document. These configuration tasks establish an administrative network connection so that complete configuration of the unit and its individual lines can be accomplished from a remote administrative terminal.

Complete information about the T1-IMA LIMs and configuration of T1-IMA interfaces is contained in the *Stinger T1/E1 with Inverse Multiplexing for ATM (IMA) Module Guide*. Complete information about connecting 4-wire circuits through a standard LPMs without protection is contained in the *Stinger Line Protection Module (LPM) Guide*.

Operation with an IP2000 module

The Stinger Compact Remote unit can be also equipped with an IP2000 module for stand-alone operation. The IP 2000 module (STGRRT-CM-IP2000-F) provides the control capabilities of a standard Stinger control module, and also provides a fiber gigabit Ethernet port for end-user traffic.

Units manufactured and equipped for stand-alone operation with an IP2000 module have a modified enclosure door. This door is manufactured with a 0.5 inch (1.3cm) bulge in the door at the location of the fiber connector on the IP2000. This bulge allows space for the curvilinear guide fiber cable to physically route the fiber light guides downward (see Figure 1-3 on page 1-4 and Figure 3-14 on page 3-20).

Information in this document for basic configuration can be applied to the IP2000 module. However, for complete information about configuration of the IP capabilities of this module, see the *Stinger IP2000 Configuration Guide*.

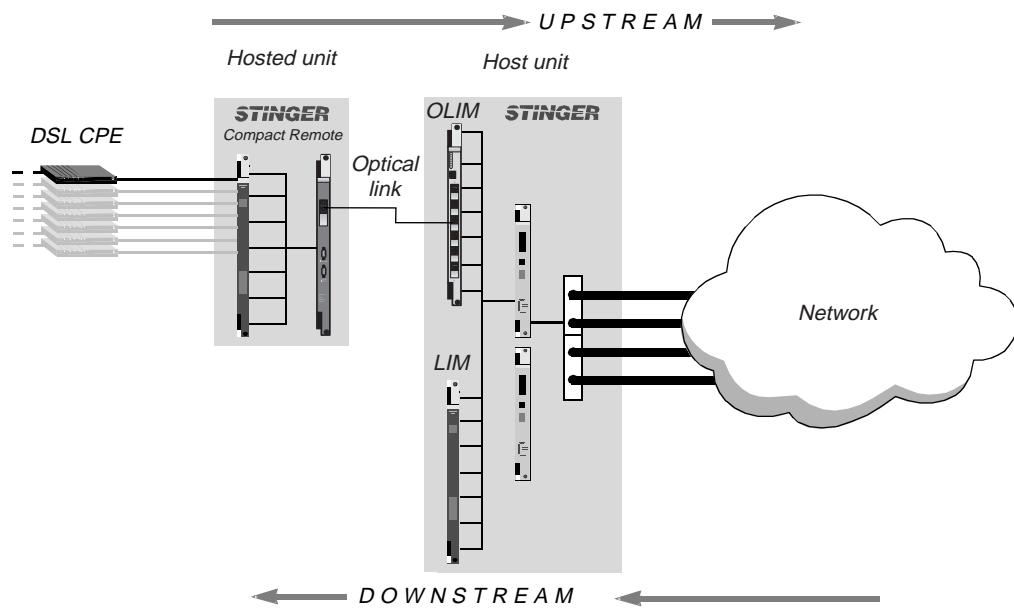
Hosted operation

The Stinger Compact Remote can function as a hosted optical network unit (ONU), to extend the reach of a host Stinger unit in a central office. For hosted operation, the Compact Remote unit is equipped with a control and optics pack (COP). This circuit pack contains hardware to control the operation of components in the local chassis, and a 155Mbps optical port for an optical connection to a host Stinger unit.

Management and configuration for the Stinger Compact Remote is handled through the TAOS management interface on the host Stinger unit.

Subscriber DSL lines are physically terminated on the Stinger Compact Remote chassis. However, these lines appear as ATM connection endpoints within the TAOS management interface for the host Stinger unit. Their configuration is also handled through the host management interface. The optical link between the host Stinger unit and a hosted Stinger CR unit is transparent to the ATM connections.

Figure 1-2. Example of Compact Remote hosted operation



Stinger Compact Remote Hardware

The Stinger Compact Remote unit, shown in Figure 1-3, consists of a card-cage chassis in an integrated outdoor enclosure. The unit is designed for installation in outdoor locations to bring DSL service close to customer locations. The enclosure is pre-wired with protection blocks for the copper telecommunications facilities, and

Introduction to the Stinger Compact Remote

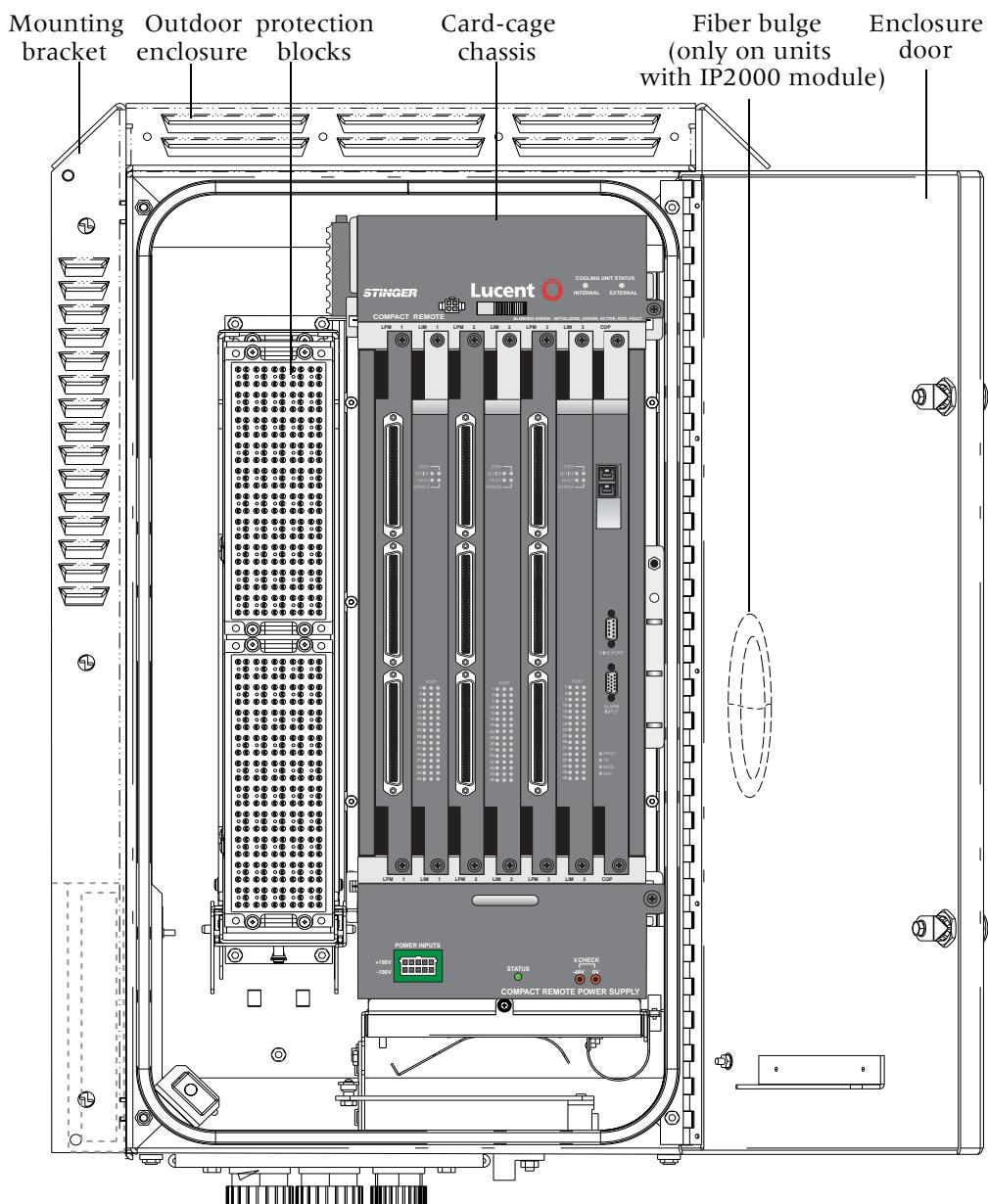
Stinger Compact Remote Hardware

provides an operating environment that can range between -40°F (-40°C) and 114.8°F (+46°C). (For more environmental information, see “Operating environment” on page D-6.) The card-cage chassis accommodates modular circuit packs, a cooling unit, and a power supply.



Caution Stinger Compact Remote enclosures are produced in three colors, light gray, brown, and green. Because of the heat dissipation characteristics, the maximum operating temperature for brown enclosures is 104°F (+40°C). Also, green enclosures equipped with an IP2000 module must not contain more than two sets of LIM/LPM modules in environments where ambient temperatures exceed 104°F (+40°C).

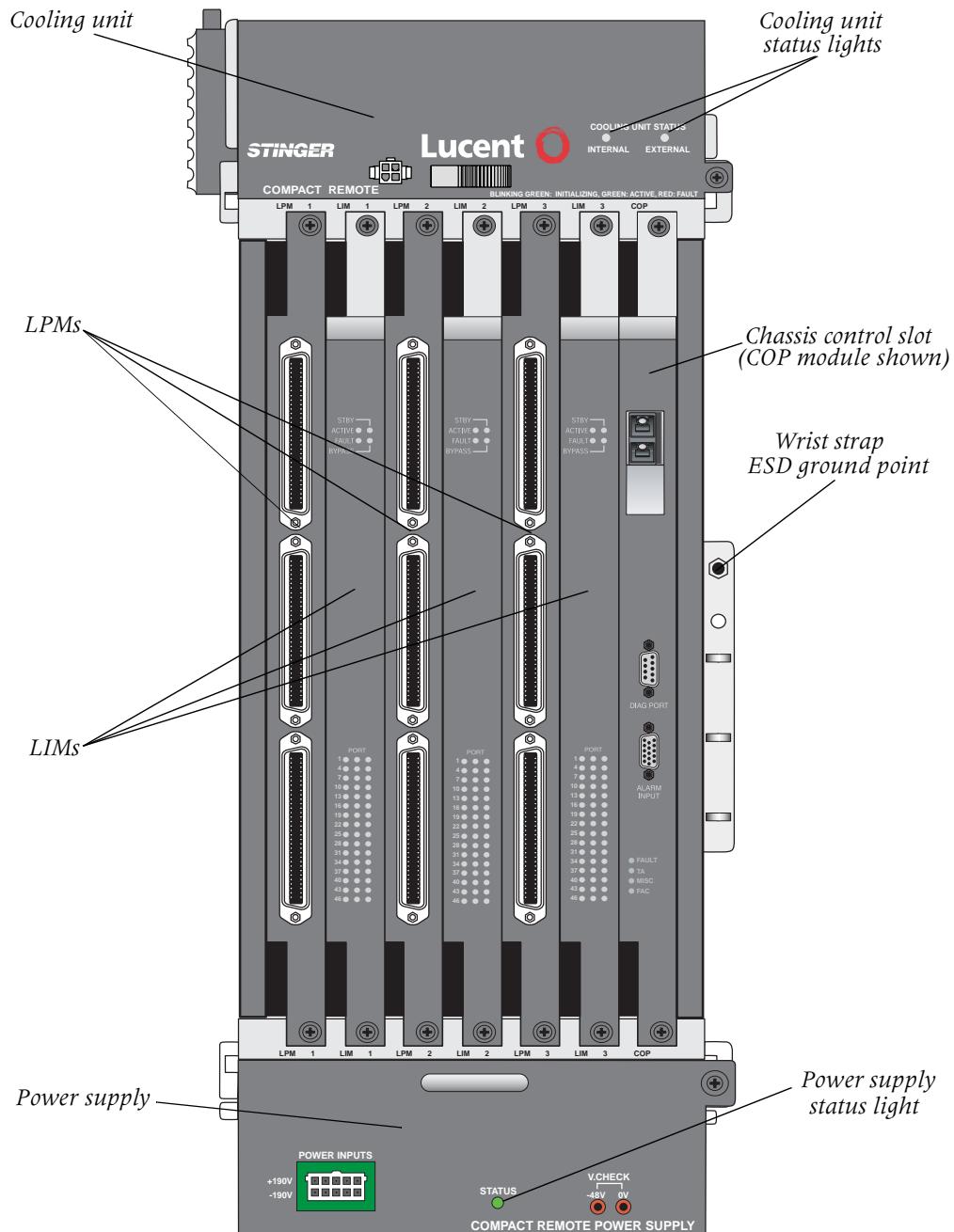
Figure 1-3. The Stinger Compact Remote



Stinger Compact Remote card cage chassis

The front of the Stinger Compact Remote card-cage has seven vertical slots for designated plug-in components and two larger bays for the cooling unit and power supply. Vertical slots accept up to three sets of line circuit packs and one module for chassis control. Each line circuit pack consists of a line interface module (LIM), and a line protection module (LPM). A cooling unit is installed in a bay at the top of the chassis, and a power supply is installed in a bay at the bottom of the chassis. These components are illustrated in Figure 1-4.

Figure 1-4. Stinger CR card-cage



Card-cage modular components

The modular components in the Stinger Compact Remote card-cage support one or more of the three primary functional requirements of the unit:

- Operational control and support of the local chassis
- Upstream connections that provide bandwidth for aggregate user traffic
- Local connection to individual users

Specific components that are installed in the Stinger Compact Remote card-cage to support these functional requirements depend upon the operational mode for which the unit is being configured. Different components are installed to support stand-alone or hosted operation. The Table 1-1 identifies the components that can be installed in the Stinger CR card-cage, the functions that they provide, and the type of operation that they support.

Table 1-1. Functional listing of card-cage components

Component	Function(s) provided	Operational mode
Control module	Operational control of the unit, including local management interface for configuration and management	Stand-alone
IP2000 module	Operational control of the unit, including local management interface for configuration and management Upstream connection from a gigabit Ethernet interface	Stand-alone
COP	Operational control of the unit (no local management interface) Upstream connection from a 155Mbps optical interface	Hosted
T1-IMA LIM	Upstream connections from T1 interfaces	Stand-alone
LIM/RLIM	DSL connections to individual end-users Note A LIM in a hosted unit is identified as an RLIM in the TAOS interface of the host.	Hosted or stand-alone
LPM with splitters	Physical connections for analog facilities from the central office, and facilities providing analog service with DSL to end-users. Physical connections for T1 interfaces from an adjacent T1-IMA LIM.	Hosted or stand-alone
Cooling unit	Operational support (cooling: self-contained internal fan and power to an external fan)	Hosted or stand-alone
Power supply	Operational support (power conversion)	Hosted or stand-alone

Each of the replaceable modular components support different capabilities.

- The control module—The control module provides a TAOS management interface for configuration and management of the unit. It controls the operation of the Stinger Compact Remote, and manages traffic through the unit. It also maintains information about the configuration of the components and lines associated with the unit. The control module does not provide an interface with sufficient bandwidth to provide an upstream connection for end-user traffic.
- The IP2000 module—The IP2000 module provides a TAOS management interface for configuration and management of the unit. It controls the operation of the Stinger Compact Remote, manages traffic through the unit, and maintains information about the configuration of the unit. It also provides a gigabit Ethernet interface that supports an upstream connection for end-user traffic.
- The COP—The COP is a specialized module that controls the Stinger Compact Remote. It contains controller hardware found in control modules on larger Stinger units but does not provide a local management interface for system configuration. An internal daughter card supports a 155Mbps optical interface that links the Stinger Compact Remote unit to a specialized optical line interface module (OLIM) installed in a host Stinger unit. End-user traffic and a control link for management of the Compact Remote unit are both carried over this connection.
- LIMs and RLIMs—Line interface modules (LIMs) provide the internal interfaces that are configured to provide service for individual DSL subscriber lines. LIMs installed in a Stinger CR unit that is configured for hosted operation are referred to as remote line interface modules (RLIMs), because they are accessed remotely through the management interface of the host unit to configure and maintain the DSL subscriber lines that they support.



Caution Because of the heat dissipation characteristics, green enclosures equipped with an IP2000 module must not contain more than two sets of LIM/LPM modules in locations where ambient temperatures exceed 104°F (+40°C).

- The T1-IMA LIM—The T1-IMA LIM occupies a LIM slot and provides T1 interfaces that support upstream links for end-user traffic when a control module is used to support stand-alone operation of the Stinger CR unit. Physical connections of the T1 interfaces are provided by an associated LPM.
- Line protection modules (LPMs)—The LPMs provide protection for the unit from transient conditions on the subscriber lines and facilities to the central office. LPMs with splitters, designed for the Stinger CR, combine analog voice service from the central office and DSL service from the Stinger on the same pair of wires to the subscriber. This LPM is also used to connect the T1-IMA LIM to the physical T1 line facilities.
- Cooling unit—The cooling unit contains a fan and electronics to control and monitor its operation. This fan maintains airflow to distribute heat produced by the Stinger CR. The cooling unit also monitors, controls, and provides power to an external ventilation fan, mounted in the side of the enclosure.
- Power supply—The power supply converts +190Vdc and -190Vdc provided from the central office into -48Vdc needed to operate the Stinger CR.

Host hardware

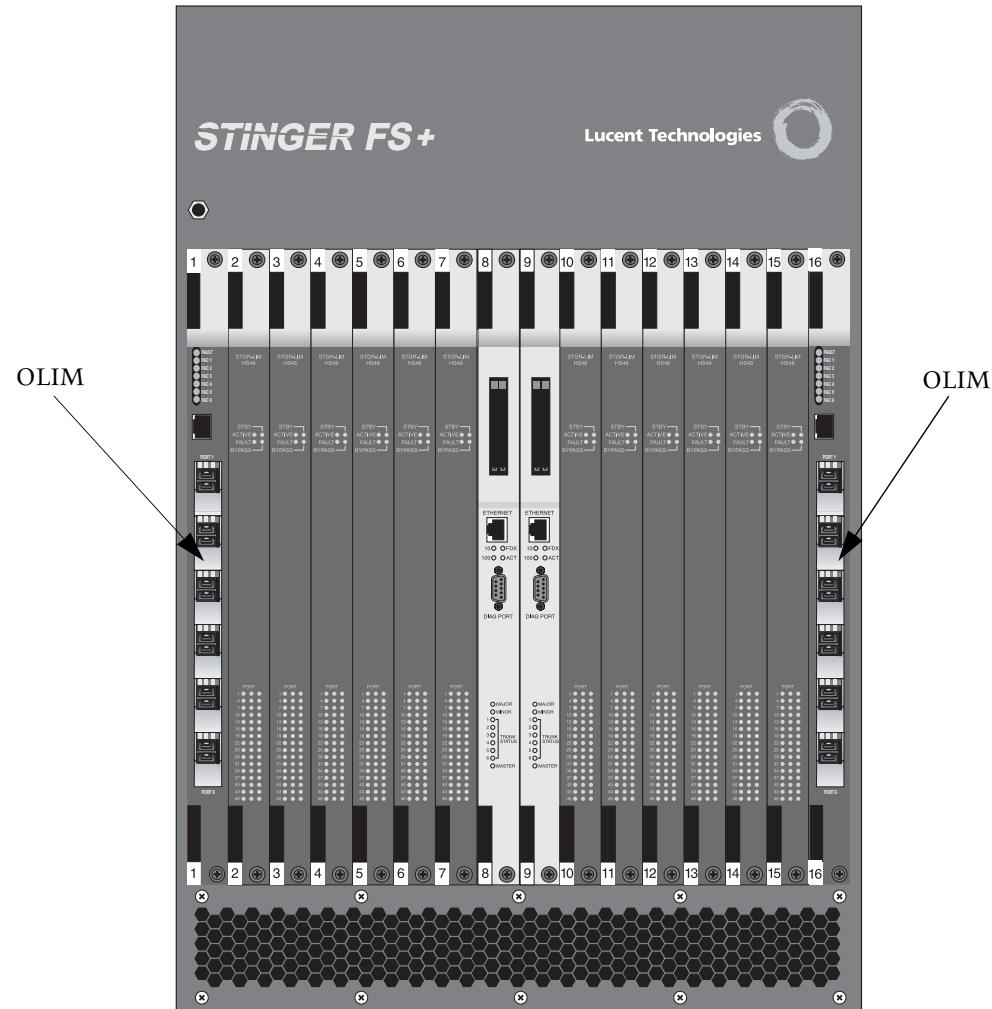
A hosted Stinger Compact Remote unit depends on an 155Mbps optical link to a host Stinger unit. This link depends on the COP installed in the Stinger CR chassis and an OLIM installed in the host Stinger unit. Each OLIM in a host unit contains six 155Mbps optical interfaces and can support connections for up to six hosted Stinger Compact Remote units.

A Stinger host must contain at least one installed OLIM to support optical connections to Stinger CR units. These connections carry subscriber data traffic from the CR unit and a control channel that integrates the control and configuration of lines on RLIMs in the CR unit into the management interface of the host Stinger unit. A single OLIM supports connections for up to 6 Stinger CR units, and a Stinger host can support up to a total of 24 remote Stinger CR units.

An OLIM can be installed in any LIM slot on a Stinger host unit. The installation procedure is identical to the standard LIM installation procedure documented in the Getting Started Guides for the Stinger FS, FS+, LS, and RT units.

Figure 1-5 shows a Stinger FS+ with OLIMs installed in LIM slots 1 and 16.

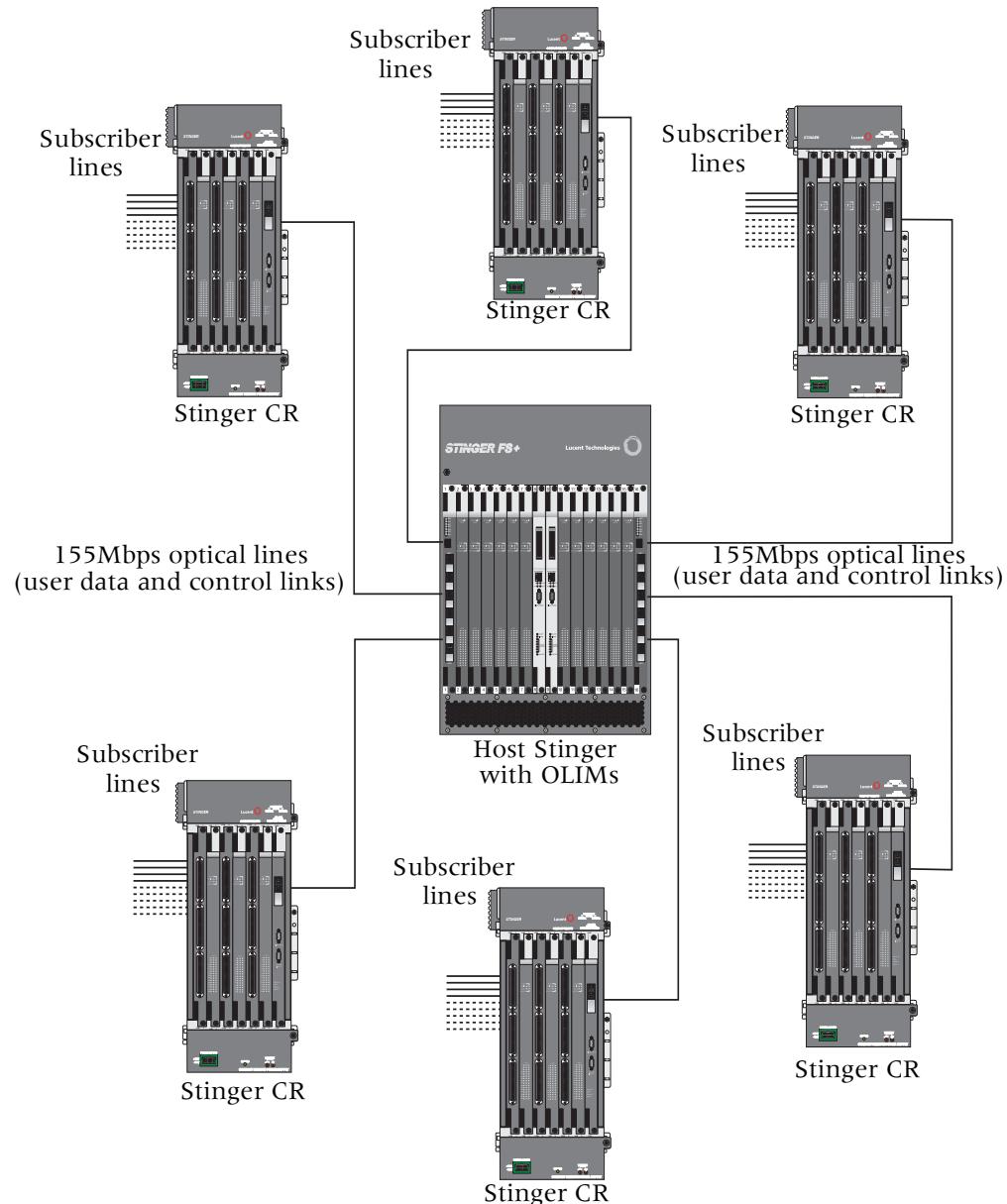
Figure 1-5. OLIMs installed in a Stinger FS+ host



When an OLIM is installed in the host Stinger unit, you can create profiles that are associated with the Compact Remote units that are connected to it. These profiles in the management interface of the host unit, allow the Stinger CR units and the Stinger host to be managed through the same interface. See Chapter 5 for detailed information about these profiles and the configuration of a hosted Stinger CR.

The type of optical network created by hosted Stinger Compact Remote units is illustrated in Figure 1-6.

Figure 1-6. Stinger CR units connected to a host Stinger unit



For detailed physical information about the Stinger OLIM, see the *Stinger optical line interface module (OLIM) guide*.

Preparing to Install the CR Unit

2

Installation tools and equipment	2-1
Preventing static discharge damage	2-2
Unpacking the Stinger Compact Remote	2-4
Verifying the hardware	2-5
Checking modules and chassis	2-6

Installation tools and equipment

To install and configure the Stinger CR hardware and software, you need the following tools and equipment.

Physical installation:

- Antistatic wrist strap (Internal Lucent number: R-4987C)
- SC and LC fiber optic connector cleaner (Cletop, Optipop, or equivalent)
- Utility knife, or appropriate tool for striping wire insulation
- Screwdrivers
 - #1 cross-recess (phillips)
 - 1/8-inch flathead
 - 3/16-inch flathead
 - SSTMM 14 (for tamper proof screw removal)
- Wrenches and sockets
 - 3/8-inch wrench or socket
 - 7/16 inch wrench or socket
 - 1 inch open end wrench
 - 7/16 standard hex key (can wrench or thin-wall socket for enclosure door latches)
- *(Optional)* 10 inch tongue & groove (channel lock) pliers



Caution Using channel lock pliers can produce metal debris that may create an electrical and physical hazard. Carefully remove any metal debris produced by using channel lock pliers.

- A drill with the following bits:
 - 5/8 inch (15.9mm) drill bit for pole mounting holes up to 20 inches (50.8cm) deep.
 - 5/16 inch (7.5mm) drill bit
 - Hammer
 - Center punch
 - For cabinet mounting: 3/4 inch and 1 inch knock out punches (Greenlee)
 - (Optional) Small probe or jeweler's screwdriver (to set the chassis ID DIP switch)
- TAOS Configuration:
- A serial or network connection from a console terminal to the host unit to configure the lines of the Stinger CR
 - ASCII or VT100 console terminal (Internal Lucent number: ITE 6938) or equivalent with the following setup:
 - 9600 bps
 - Direct connection
 - 8 data bits
 - No parity
 - 1 stop bit
 - No flow control
 - RS-232 straight-through modem cable for connecting the console terminal or equivalent to the unit (Internal Lucent number: ITE-6801 List 22)

Preventing static discharge damage

Modules and semiconductor devices in general can be easily and permanently damaged due to electrostatic discharge during installation or removal. A person walking across a floor can generate electrostatic voltages in excess of 5000V. Although you might not notice a discharge of less than 3500V, discharges below 100V can damage semiconductor components.

You can destroy a component without noticing any electrostatic discharge. Because these discharges have very little current, they are harmless to people.

To prevent damage to components from electrostatic discharge, always follow the proper guidelines for equipment handling and storage.

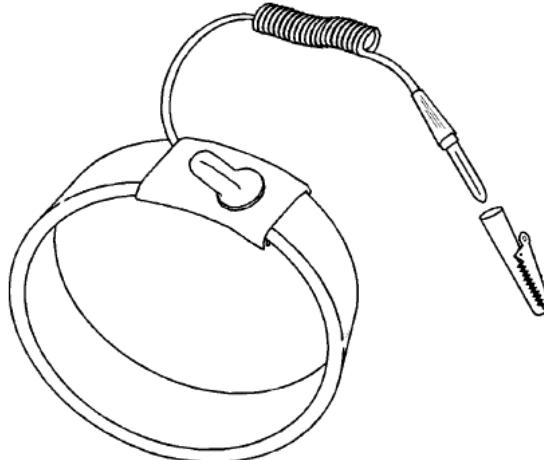
Use a wrist strap

To reduce the static potential on your body by proper grounding, wear an approved antistatic wrist strap (Figure 2-1) when installing, removing, or handling modules, or while handling any Lucent device containing semiconductor components.



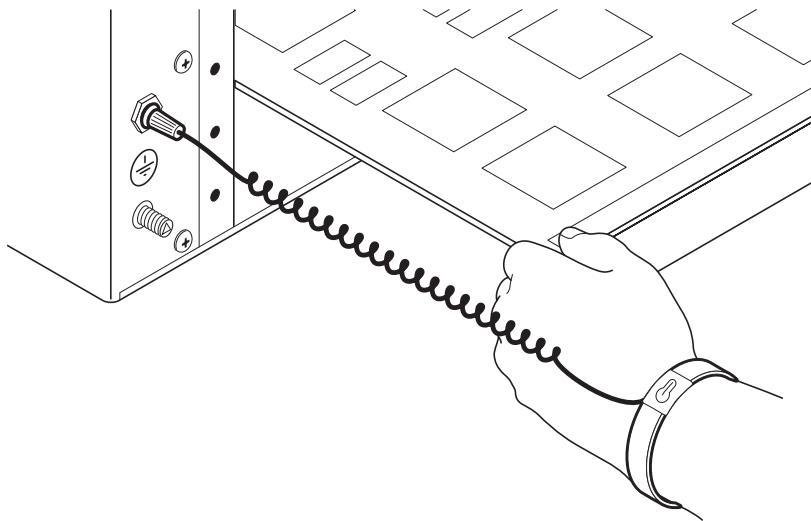
Caution Correct use of an approved antistatic wrist strap is the only reliable way to prevent damage to components by electrostatic discharge from your body

Figure 2-1. Wrist grounding strap



To minimize entanglement, right-handed people can wear the strap on the left hand. Plug the other end of the wrist strap into the grounding jack provided on most Lucent products, as shown in Figure 2-2. (See Figure 2-4 on page 2-6 for the location of ESD grounding point on the Stinger CR.)

Figure 2-2. Wrist strap plugged into a grounding jack



If a grounding jack is not available, use an alligator clip to connect the strap to electrical ground.

Use the following two simple tests to verify that the wrist strap is functioning properly:

- Measure the resistance between the wrist strap and its grounding plug. Overall resistance between these two points must be approximately 1 megohm. If it is not, replace the strap.
- Physically examine the strap for visible damage. If you see any damage, replace the strap.

Remove plastics from your work area

Work areas must be kept clear of common plastics, such as the following items:

- Polystyrene packing containers
- Clear plastic bags
- Plastic drinking cups
- Food wrappers
- Clear cellophane tape

These types of common plastic materials can carry a static charge that is not easily discharged to ground and must not make direct contact with modules or any other solid state components.

Store components properly

Protect modules immediately after removal from a chassis by placing them in their original factory packing materials. Storage in approved antistatic packaging is acceptable when factory packaging is unavailable.



Caution Never place unprotected modules directly on ungrounded metal shelving or on ungrounded carts without insulating surfaces.

Unpacking the Stinger Compact Remote

The unit is delivered with the Stinger CR chassis installed in its integrated outdoor enclosure. It may be shipped with all the ordered modules installed, or with filler-blanks in the slots of the chassis card-cage. The unit is delivered in a protective shipping carton attached to a wooden pallet with screws and L-brackets.

Before you remove the Stinger CR unit from the shipping carton and delivery pallet, check for damage. If you see any damage, follow the instructions described in your product warranty.

Due to the large size and weight of a fully configured unit, Lucent Technologies recommends moving the unit to the installation site *before* unpacking it from the shipping carton.



Warning A bare Stinger CR unit in its enclosure with its power supply, fans, and cables weighs up to 121 pounds (54.885kg). This weight does not include protection elements, LIMs, LPMs, or the COP. See "Weight and lifting requirements" on page D-6 for detailed weight information.

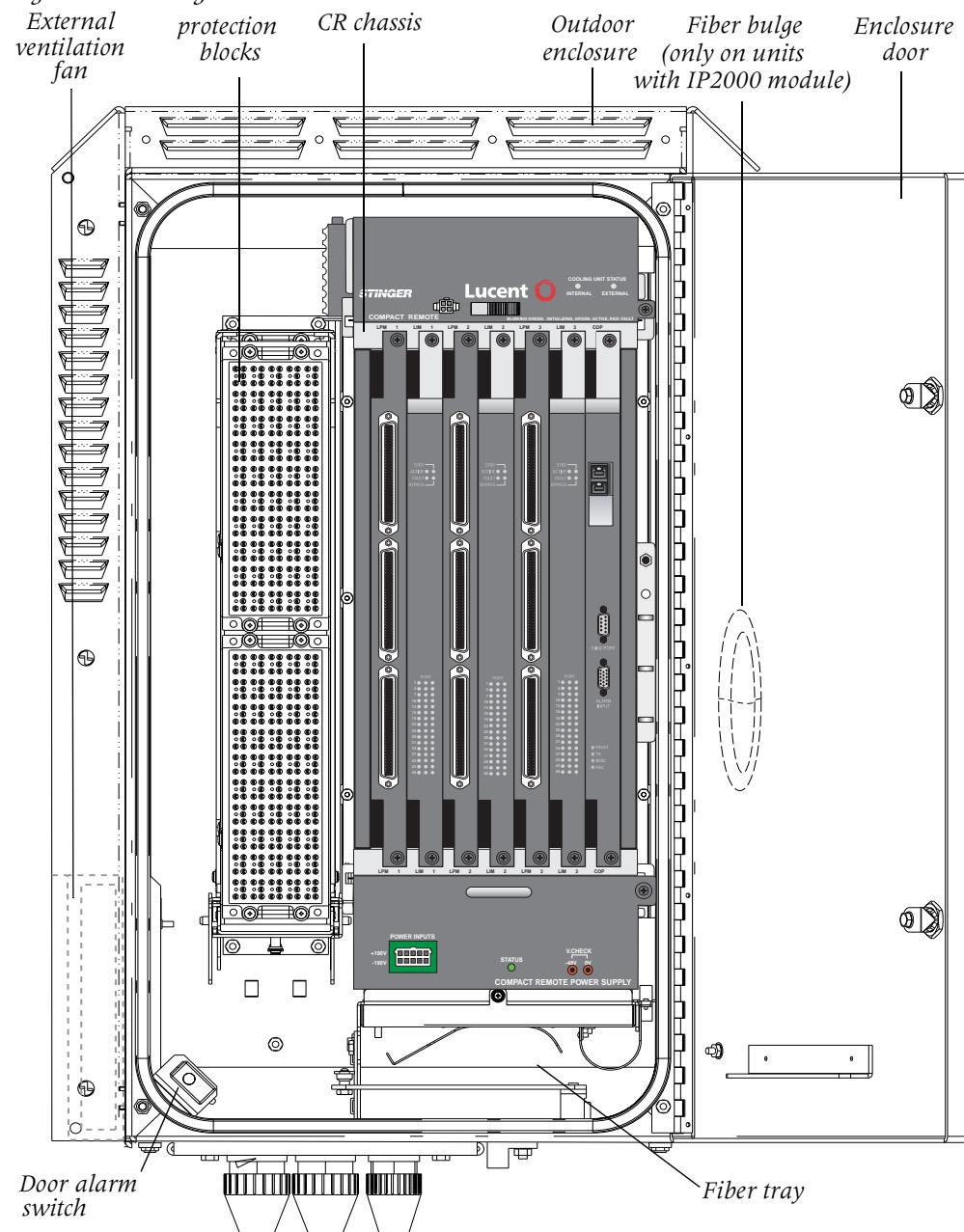
To unpack the unit:

- 1** Lift and remove the carton from the shipping pallet and remove all enclosed packing materials. Save the packing materials in case you need to repack the unit later.
- 2** Verify that the contents of the carton match the items listed on the packing slip (see "Verifying the hardware" on page 2-5).
- 3** Remove the bolts from the L-brackets on the delivery pallet.
- 4** Carefully remove the unit from the pallet.

Verifying the hardware

The Stinger CR card cage chassis is delivered in its outdoor enclosure with protection blocks installed. The cabling, power supply, cooling unit and other modules may be installed prior to shipment, or may be installed on location. Open the enclosure door to verify that the unit is configured as ordered. Figure 2-3 illustrates the primary components of the Stinger CR enclosure.

Figure 2-3. Stinger CR enclosure details



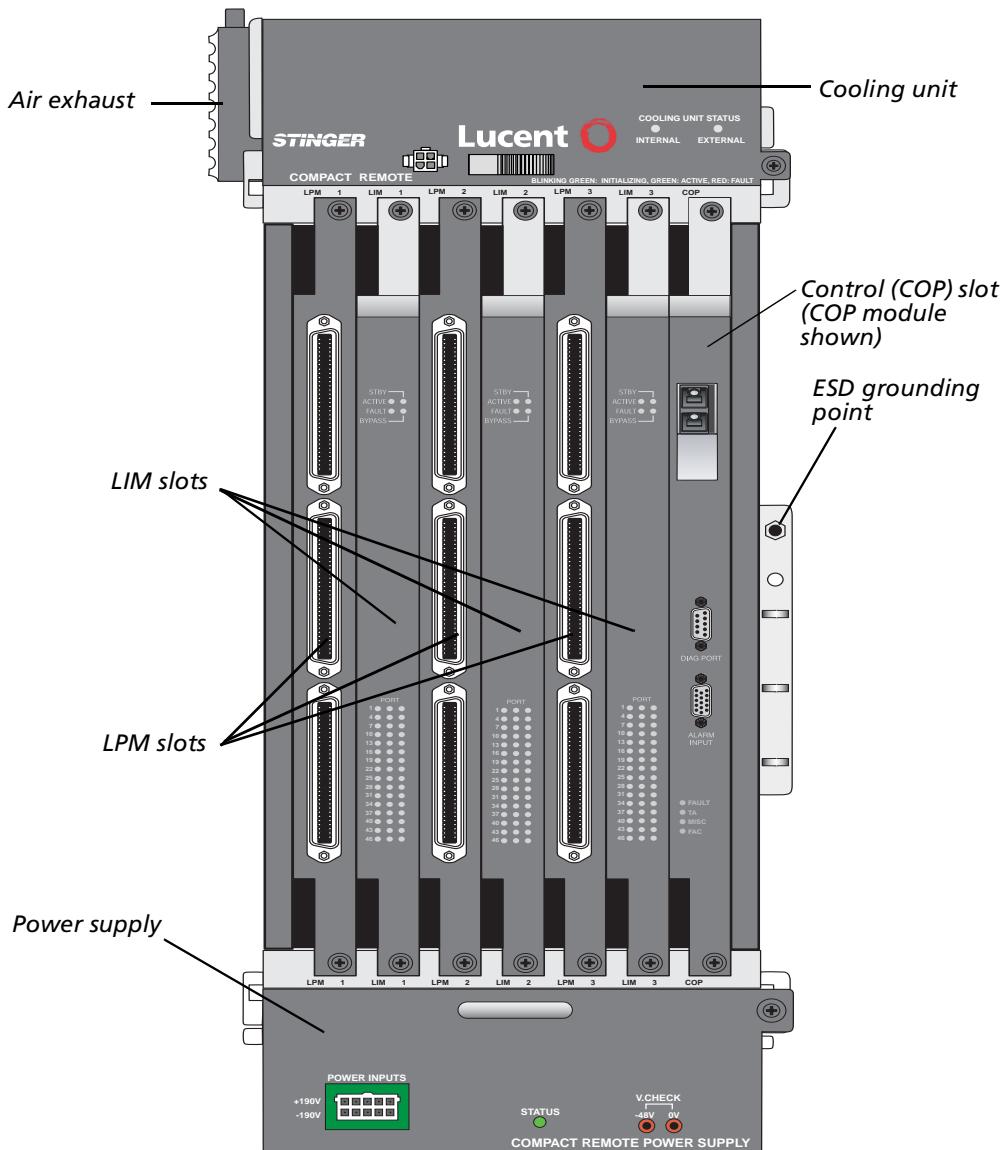
Checking modules and chassis

The Stinger Compact Remote has a backplane design that enables the installation and removal of all major circuit packs and modules in the front of a unit. Figure 2-4 shows the front slots of a Stinger Compact Remote chassis, equipped for hosted operation with a COP and three sets of RLIMs and LPMs. Your unit may be equipped with different modules depending upon its application.



Caution Wear an antistatic wrist strap before handling any of the unit components. If the chassis is mounted in a grounded frame, this can be connected to the electrostatic discharge (ESD) grounding jack (banana jack), located at right side of the chassis (Figure 2-4).

Figure 2-4. Front view of a Stinger Compact Remote chassis





Caution Stinger Compact Remote enclosures are produced in three colors, light gray, brown, and green. Because of the heat dissipation characteristics, the maximum operating temperature for brown enclosures is 104°F (+40°C). Also, green enclosures equipped with an IP2000 module must not contain more than two sets of LIM/LPM modules in environments where ambient temperatures exceed 104°F (+40°C).



Caution Slots that are not occupied by modules must be masked with blank covers to ensure proper air flow through the unit.

Checking modules in the control (COP) slot

The vertical slot on the right side in front of the unit is the control slot (see Figure 2-4). This slot contains the module that controls the backplane and coordinates the function of the local hardware. The circuit pack or module installed in this slot also determines whether the unit operates in stand-alone or hosted mode.

The control module

The Stinger CR unit operates in stand-alone mode with a control module (STGRRT-CM-A) installed in the control slot. The control module provides a TAOS management interface that can be accessed directly from a serial console, or remotely from a network connection. All configuration parameters for the unit and the lines to which it is connected can be accessed and set through this interface. Configuration settings for the unit are retained in the control module and can be saved onto PCMCIA cards that are plugged into the control module.

The 10/100 Ethernet port supports an administrative connection to a management network. It is not intended to carry end-user traffic.

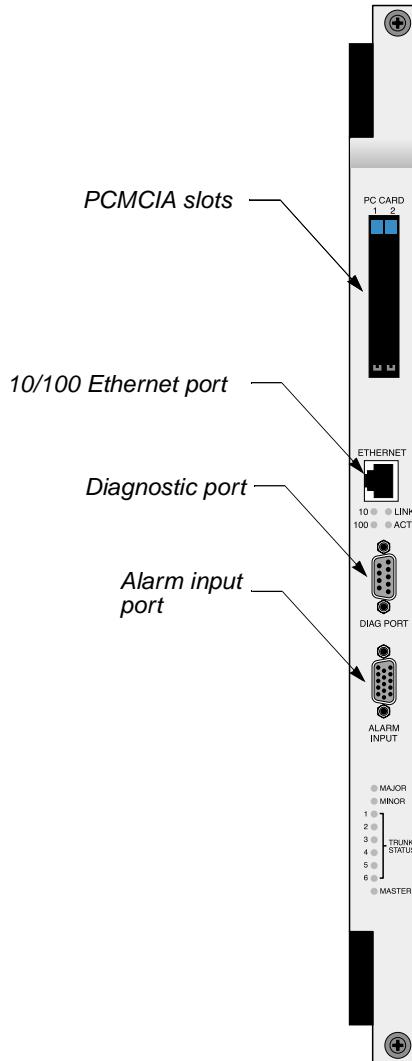
Control module interfaces

Figure 2-5 shows the location of the 10/100 Ethernet port, serial diagnostic port, alarm input port, and Personal Computer Memory Card International Association (PCMCIA) slots on a control module for the Stinger Compact Remote unit.

Preparing to Install the CR Unit

Checking modules and chassis

Figure 2-5. Stinger Compact Remote control module interfaces



The IP2000

The Stinger CR unit operates in stand-alone mode with an IP2000 module (STGRRT-CM-IP2000-F) installed in the COP slot. The IP2000 provides a TAOS management interface that can be accessed directly from a serial console, or remotely from a network connection. All configuration parameters for the unit and the lines to which it is connected can be accessed and set through this interface. Configuration settings for the unit are retained in the control module and can be saved onto PCMCIA cards that are plugged into the IP2000.

The IP2000 also supports a fiber-based Gigabit Ethernet (GigE) interface, with a modular Small Form Factor Pluggable (SFP) transceiver. This interface can be configured to carry network traffic for end-users that are connected to the Stinger CR

unit. Complete information about configuring the IP interfaces of the IP2000 module is contained in the *IP2000 Configuration Guide*.

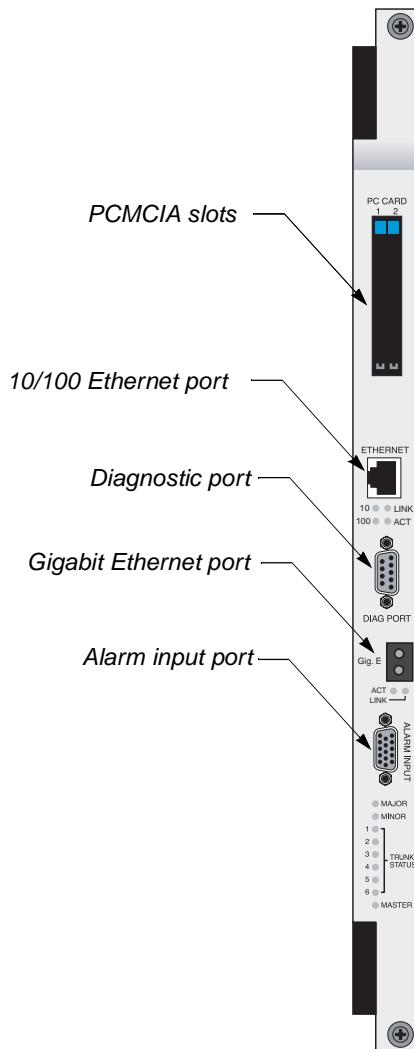


Note Units manufactured and equipped for stand-alone operation with an IP2000 module have a modified enclosure door. This door is manufactured with a 0.5 inch (1.3cm) bulge in the door at the location of the fiber connector on the IP2000. This bulge allows space for the curvilinear guide fiber cable to physically route the fiber light guides downward (see Figure 2-3 on page 2-5 and Figure 3-14 on page 3-20).

IP2000 interfaces

Figure 2-6 shows the location of the Gigabit Ethernet port, 10/100 Ethernet port, serial diagnostic port, alarm input port, and Personal Computer Memory Card International Association (PCMCIA) slots on a control module for the Stinger Compact Remote unit. Details about interfaces and hardware specifications for the IP2000 module are contained in the *IP2000 Configuration Guide*.

Figure 2-6. The IP2000 module



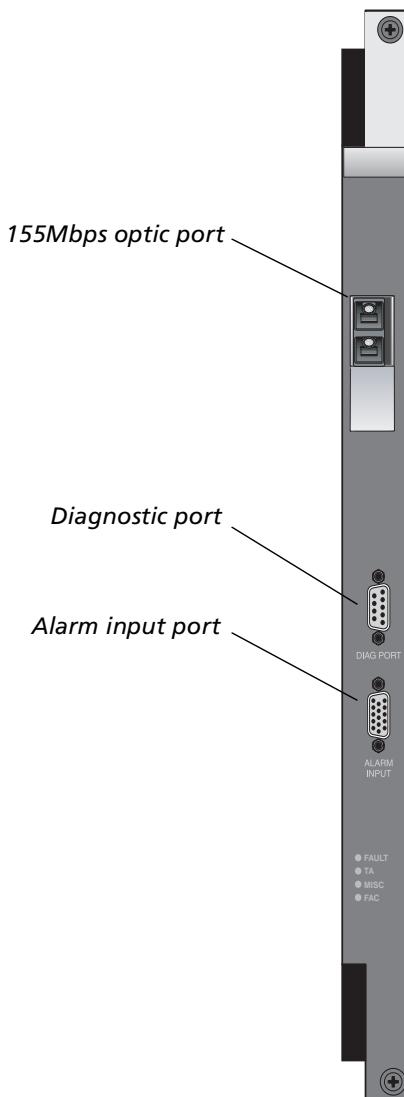
The COP

The Stinger Compact Remote operates in the hosted mode with a COP. Unlike the IP2000 module that supports standalone operation, the COP does not provide a local management interface for configuration of the unit. It depends upon a 155Mbps optical link to a host Stinger unit for configuration and management. This optical link, located on the COP, also carries network traffic for DSL users that are connected to the Compact Remote unit.

COP interfaces

Figure 2-7 shows the location of the 155Mbps optical port, serial diagnostic port, and alarm input port on a COP. On units that are shipped with the COP installed, the diagnostic port is not used.

Figure 2-7. Control and optics pack



Unlike standalone control modules or IP2000 modules, the COP does not store local configuration information in onboard flash memory. Configuration information for the Compact Remote unit and its modules is stored in the PCMCIA cards and the onboard nonvolatile RAM (NVRAM) of the control module in the host Stinger unit.

Checking the LIMs

Two types of LIMs can be used in the Stinger CR unit. ADSL LIMs support connections to individual DSL end-users. A T1 LIM provides bandwidth to support upstream network connections when the Stinger CR is equipped with a standard control module.

Line interface modules are installed in slots in the front of the chassis labeled LIM 1, LIM 2, and LIM 3. All LIMs connect to their respective line facilities through an associated line protection module (LPM) that is located in the slot to the immediate left of the LIM. The LPM slots are labeled LPM 1, LPM 2, and LPM3. Slots that are not occupied by modules must be masked with blank covers to ensure proper air flow through the unit.

In hosted operation, or standalone operation with an IP2000 module in the control (COP) slot, all three LIM slots can hold ADSL LIMs. In standalone operation, with a control module in the COP slot, one LIM slot must contain a T1 module to provide bandwidth for an upstream connection.

48-port ADSL LIM

The 48-port low power ADSL LIM (STGRCR-LIM-AP-48) has been designed to meet the power and heat specifications of the Stinger CR unit. These LIMs support end-user connections to the Stinger CR unit for stand-alone and hosted operations. The 48-port low-power LIM is shown in Figure 2-8.



Caution Other Stinger ADSL LIMs are not supported in the Stinger CR chassis and may result in excessive temperatures within the unit.



Note Detailed physical and configuration information for the 48-port low power ADSL LIM is included in the *Stinger ADSL Annex-A LIM Guide for LIMs with ADSL2+ Capability*.

Preparing to Install the CR Unit

Checking modules and chassis

Figure 2-8. The 48-port low-power LIM



The T1-IMA LIM

Two T1-IMA LIMs are available. One module supports up to 8 T1 connections (STGRRT-LIM-T1-8), the other module supports up to 24 T1 connections (STGRRT-LIM-T1-24). Both modules support UNI and PNNI ATM connections. Under a special software license from Lucent Technologies, these modules also support inverse multiplexing for ATM (IMA). For complete hardware specifications and information about configuring the T1 module, see the *Stinger T1 and E1 Modules Guide*.

The T1 module is shown in Figure 2-9.

Figure 2-9. The T1-IMA LIM (24-port version)



Checking the LPMs

Each LIM installed in the unit must have a corresponding LPM in the adjacent slot to the left of the LIM. Slots that are not occupied by modules must be masked with blank covers to ensure proper air flow through the unit. The LPMs provide the actual connection points to the physical line facilities.

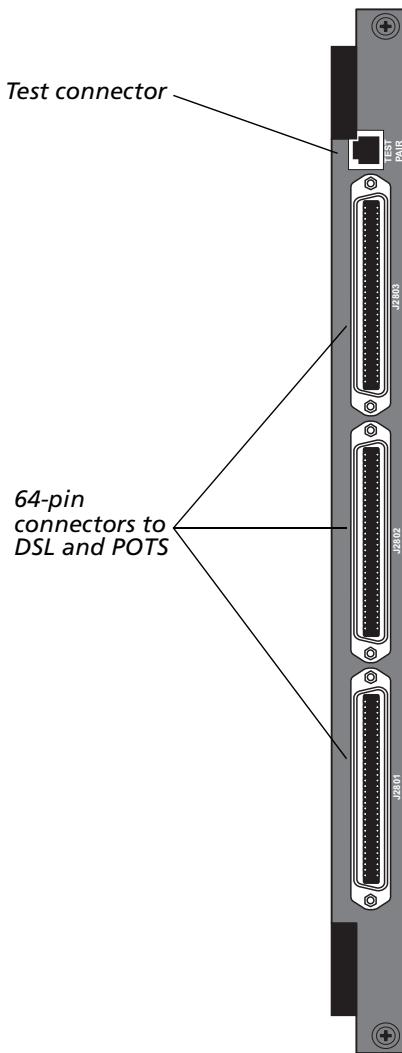
The 48-port LPM with splitters (STGRCR-LPM2-48-S) is designed for use with 48-port low-power LIM in the Stinger CR. It provides connection points for coupling analog voice service onto the subscriber facilities that carry the DSL service.

The 48-port LPM with splitters can also be used to provide the physical connection points for connecting an adjacent T1/IMA LIM to its line facilities. When used with a T1/IMA LIM, the 48-port LPM with splitters provides 4-wire connections for the T1 ports supported by the T1/IMA LIM. Specific information about making 2-wire ADSL and POTS connections, or 4-wire T1 connections to the 48-port LPM with splitters is contained in the Appendix C, "Cables and Connectors."

Preparing to Install the CR Unit

Checking modules and chassis

Figure 2-10. The 48-port LPM with splitters



Checking the cooling unit

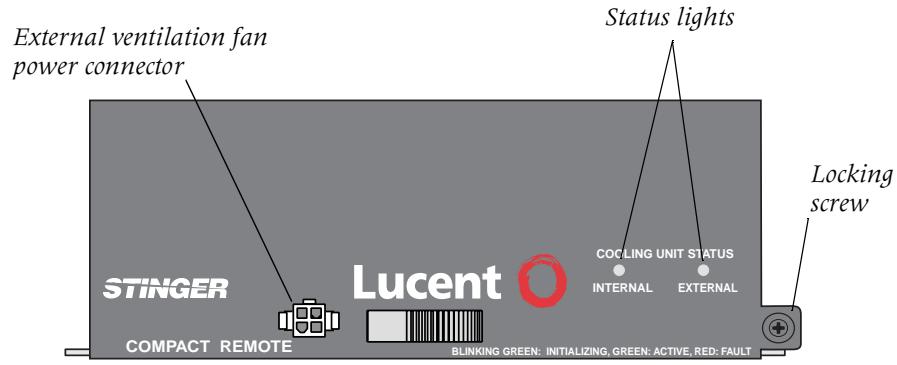
The cooling unit is installed at the top of the CR chassis. It uses an internal fan to circulate air past components in the Stinger CR and provides power for a external ventilation fan in the side of the outdoor enclosure. Heat is removed by air circulation and dissipated through the enclosure.



Note Check the power connector for the external ventilation fan to verify that it has not become loose during shipping, and is not disturbed during installation.

The Stinger CR cooling unit is shown in Figure 2-11.

Figure 2-11. The Stinger CR cooling unit

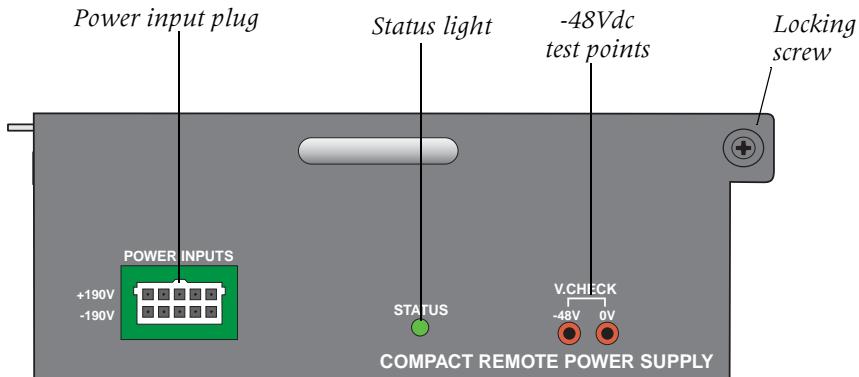


Checking the power supply

The Stinger CR power supply is installed at the bottom of the CR chassis. The power supply accepts +190Vdc and -190Vdc from the central office over multiple pairs of copper telecommunications facilities. This is converted within the power supply into the -48Vdc required to power the Stinger CR.

The Stinger CR power supply is shown in Figure 2-12.

Figure 2-12. The Stinger CR power supply



CR Enclosure and Component Installation

3

Before you begin	3-1
Stinger CR Installation	3-1
Installation and replacement of Stinger CR components.....	3-7
Physical connections to the Stinger CR unit	3-18
Turning on power to a Stinger CR unit	3-25
Status lights	3-26
What's next	3-32

Before you begin

Verify that you have completed the following tasks:

- Located all necessary hardware and tools are at the installation site
- Unpacked the Stinger unit
- Checked the module configuration in the unit



Warning Before installing the Stinger hardware, be sure to read the safety instructions in the *Edge Access and Broadband Access Safety and Compliance Guide*. See Appendix D, "Safety-Related Electrical, Physical, and Environmental Information," for information specific to your product.

Stinger CR Installation

The Stinger Compact Remote is delivered in its integrated outdoor enclosure. All ordered components may be installed prior to shipment or installation of components may be done on-location. The enclosure is available with mounting hardware for different mounting options:



Warning The weight and position of the components within the enclosure might make the enclosure awkward or unstable. Take all necessary precautions to anchor the enclosure securely before installation. For detailed weight information see "Weight and lifting requirements" on page D-6.

To install the Stinger Compact Remote enclosure you must perform the tasks:

- Attach the appropriate Stinger CR mounting hardware to the outdoor cross-connect cabinet, pedestal, or pole.
- Prepare cables and cable routes. (Drill pass-through holes, using the appropriate template, for cabling into an outdoor cabinet, or make cabling provisions for poll mounting.)
- Mount the Stinger CR enclosure to the bracket.
- Route and connect cabling for telecommunication facilities and power to the Stinger CR.

Mounting hardware

The Stinger CR enclosure can use integrated mounting brackets for mounting the unit on a pole, pedestal, or the side of an installed outdoor wiring cabinet. These brackets attach to vented covers on the side of the enclosure that allow air flow around the Stinger CR enclosure. A protective cover for the cables at the bottom of the enclosure is also included. The mounting bracket assemblies for these mounting options are shown in Figure 3-1, Figure 3-2, and Figure 3-3.

Figure 3-1. Stinger CR enclosure side mounting bracket assemblies

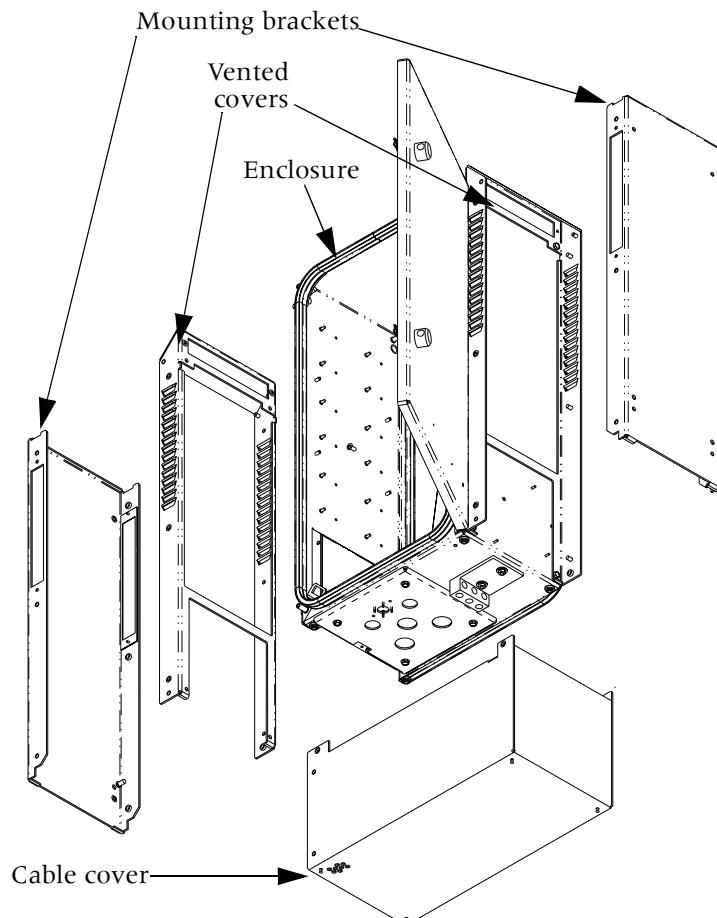


Figure 3-2. Stinger CR enclosure pedestal mounting bracket assemblies

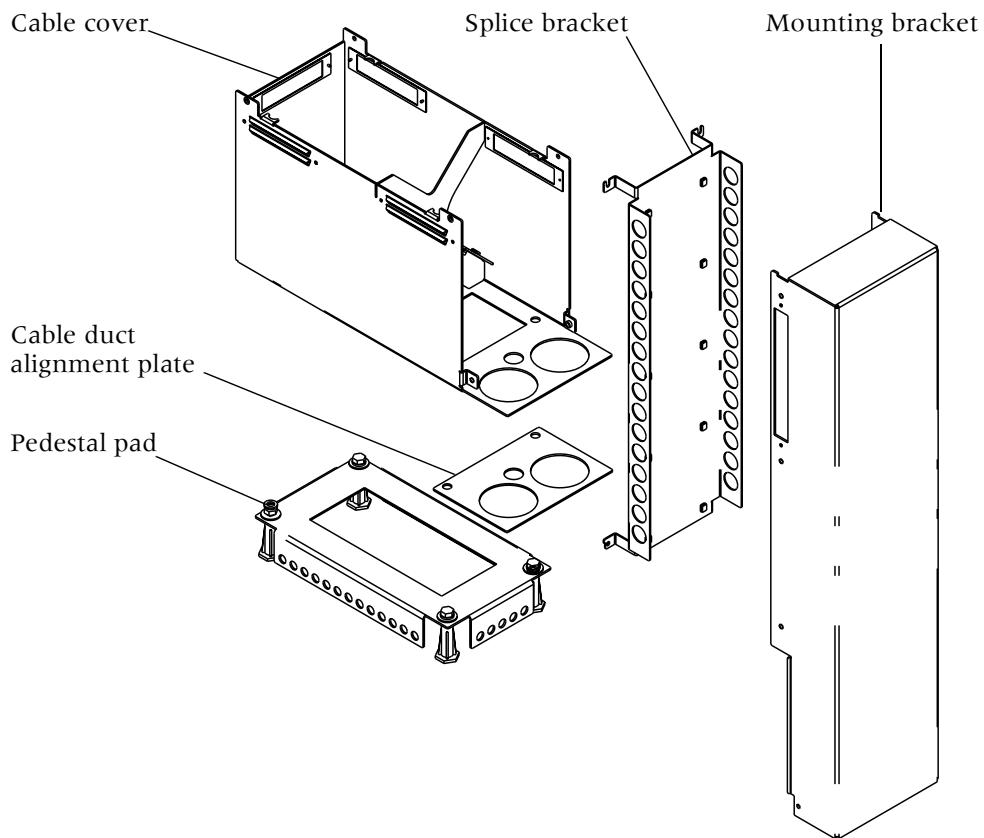
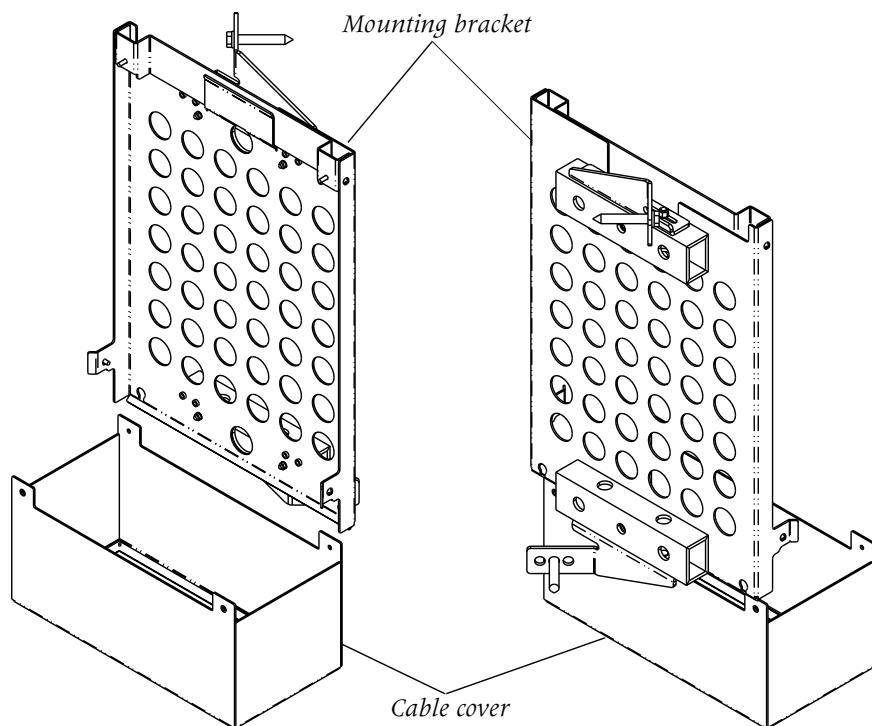


Figure 3-3. Stinger CR enclosure pole mounting bracket assemblies



Attaching the Stinger CR mounting bracket to a cabinet

An existing wiring cabinet must be carefully prepared for mounting a Stinger CR. Follow all local safety practices and guidelines in performing this work to avoid injury and the interruption of existing service.

Preparing the cabinet

You may use the following general procedure to install the mounting brackets.

- 1 Pre-position the mounting template that is shipped with the Stinger CR to verify that all holes can be drilled without damaging existing cables or hardware behind the mounting surface.
- 2 Mark the location of each hole and create an indentation in the center of each location with a center punch.
- 3 Use a 5/16 inch (7.5mm) drill bit to drill the four mounting holes for the CR mounting bracket.



Caution Metal debris from drilling can create an electrical hazard. Capture or clean and remove any debris created by drilling the mounting holes.

- 4 Place a washer on each mounting bolt and then press the four hex-head bolts through the holes so that the threaded portion is extended for the CR mounting bracket.
- 5 Align the holes in the CR mounting bracket with the extended ends of the mounting bolts.
- 6 Use a hex-head wrench to turn the bolts, screwing them into the mounting holes on the CR mounting bracket.

Preparing the cable pass-through holes

Installation on an outdoor cabinet requires a total of six pass-through holes for cables from the Stinger CR unit. Three holes are 3/4 inch in diameter, three holes are 1 inch in diameter. These holes were marked with the template in the previous process and should be drilled before installing the Stinger CR enclosure on the mounting bracket.

- 1 Drill a pilot hole at the center point for each pass-through hole marked previously.
- 2 Use knock-out tools to cut the holes.
- 3 Inspect each hole to verify that it is cleanly cut and free of metal burrs.
- 4 Install weather tight connectors in each of the pass-through holes.

Mounting the enclosure

The mounting bracket has two shoulder pins near the top of the bracket. These pins help support and position the enclosure to align the mounting holes with those of the mounting bracket and install the permanent one-way mounting screws are installed. Follow all local safety practices and guidelines and use the following general procedure to mount the enclosure.

- 1 Remove the cable shroud from the bottom of the enclosure.
- 2 Carefully lift to position the enclosure onto the two shoulder pins of the mounting bracket.

- 3 Align the six mounting points (three in front, and three in back) of the enclosure with the mounting holes in the bracket.
- 4 Use a flat-head screwdriver to install six permanent one-way screws to secure the enclosure.



Note Do not use power tools to install the one-way screws. When these screws are installed with a common screwdriver, they may be removed with the special SSTM 14 tool. If you install the one-way screws with a power tool, they can only be removed by drilling them out. This will damage the threads in the mounting bracket and enclosure.



Warning When one-way screws are removed or loosened with the special SSTM14 tool, sharp metal edges are created on the screw head that can result in injury. Follow local guidelines to replace one-way screws after loosening or removal.

Route and connect the cables

The Stinger CR unit has three cables that must be routed into the cross-connect cabinet from the three sets of protection blocks in the chassis. These cables are approximately 25 feet in length, and end in stubs. They pass through the three 3/4-inch (19mm) diameter holes. Optical cables, and cables for power and ground pass through the two 3/4-inch (19mm) holes. Specific information about cable pairs, binders, and their relationship to the circuits from the Stinger LPMs is described in Appendix C, "Cables and Connectors."

Pass all cables through the watertight seals. (See "Enclosure cable exit points" on page C-19 for the locations of the watertight fittings on the bottom of the enclosure.) Leave one loop of cable within the cable shroud below the unit when the mounting bracket is attached to the left side of the enclosure. This service loop allows slack for cable movement for maintenance access from below to the external cooling fan in the left side of the enclosure.

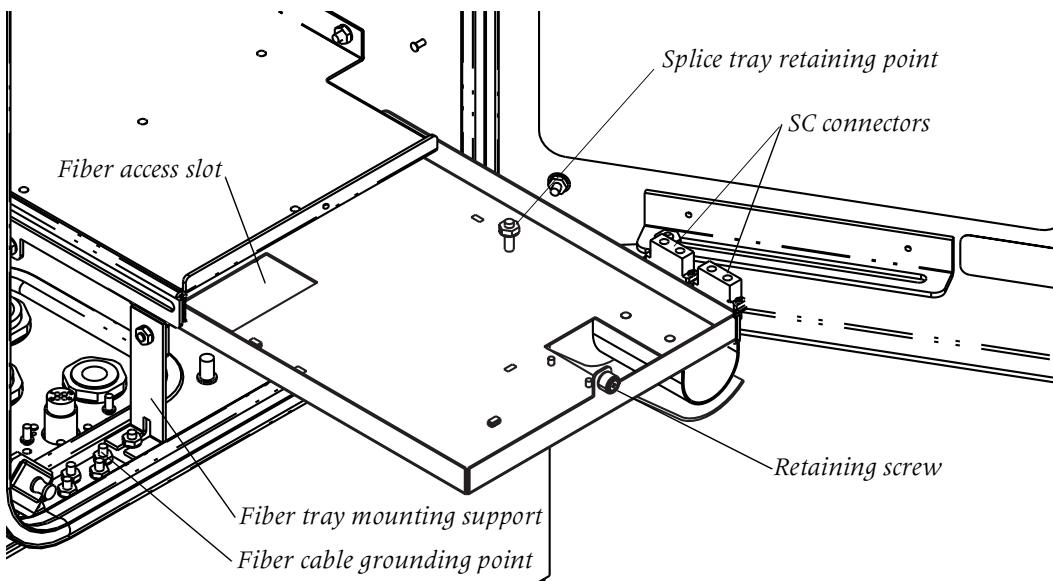


Note When side-mounting the enclosure, the left side is the preferred location of the mounting bracket.

Route and connect the fibers

Use the following procedure to route the fiber cable into the Stinger CR enclosure.

- 1 Feed the fiber cable through the watertight fitting on the bottom of the enclosure. (See "Enclosure cable exit points" on page C-19 for the locations of the watertight fittings on the bottom of the enclosure.)
- 2 Securely tighten the water tight fitting by hand.
- 3 Install a cable shield grounding harness to the fiber optic cable inside the enclosure.
- 4 Attach the ground cable from the grounding harness to the grounding point on the right side of the grounding bar located at the lower left side of the enclosure (see Figure 3-4).

Figure 3-4. Enclosure fiber tray details

Use the following procedure to route and connect the fiber optics within the enclosure.

- 1 Loosen the retaining screw on the fiber tray and slide the fiber tray forward.
- 2 Feed the fiber from the fiber cable up through the access slot near the back of the fiber tray.



Caution To avoid damage to the fiber, be sure to route the fiber behind the left front mounting support for the fiber tray before feeding it up through the fiber access slot.

- 3 Splice the fiber you are installing to the fiber that is provided from the bottom of the SC connectors on the fiber tray.
- 4 Secure the splice and excess fiber in a fiber splice tray (purchased separately) and attach the splice tray to the fiber tray at the splice tray retaining point.
- 5 Remove the SC connectors from the mating sleeve on the fiber tray, clean and reinsert them



Note Clean the fiber optic connectors in accordance with the following specifications.

- GR - 326 (Reliability requirements for single mode fiber optic connectors)
 - EIA/TIA 455 specifications:
 - 13A (insertion)
 - 34 (optical insertion loss)
 - 171 (optical reflectance)
 - Lucent specification X-21329
- 6 Remove the fiber jumper from its plastic bag and clean the fiber connectors.
 - 7 Remove dust covers from the top of the SC connectors. Insert the SC connector on one end of the fiber jumper into the SC mating sleeve on the fiber tray.

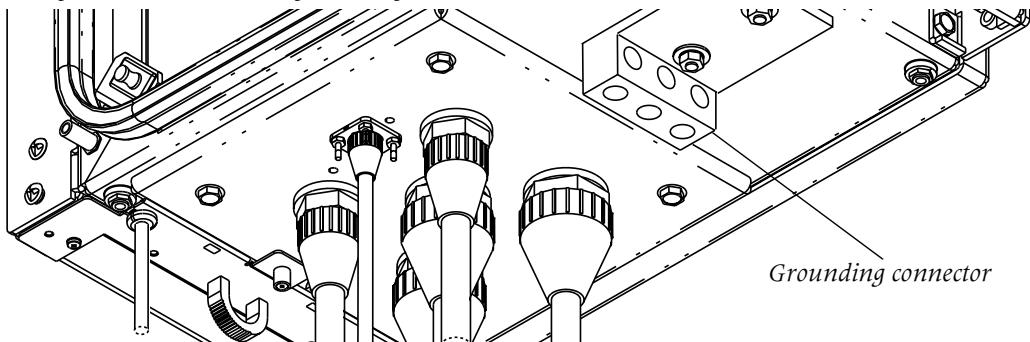
- 8 Run the fiber jumper through the guides on the right side of the card cage and insert the LC connector on this jumper into the connector on module in the COP slot.
- 9 Slide the fiber tray back into the chassis and tighten the retaining screw.

Grounding the enclosure

The cabinet grounding system is designed to protect personnel from shock hazards, and to protect the equipment from power transients caused by lighting and other sources. In addition the cabinet grounding system helps to prevent electronic noise from entering or radiating from the cabinet.

Before applying power to the CR, the enclosure must be connected to an earth ground. A grounding connector is provided at the base of the cabinet for this purpose (see Figure 3-5). This connector is capable of terminating 3 2-AWG grounding wires. In most areas two 8-foot grounding rods are sufficient. In areas of high lightning activity or low ground conductivity, additional grounding rods or a grounding ring should be used to increase the effectiveness of the grounding system. You must verify that the connections to the grounding rods are in accordance with NEC, UL, and any local safety codes that apply. The resistance of these grounding connections must be no more than 25 Ohms.

Figure 3-5. Enclosure grounding connector



Installation and replacement of Stinger CR components

The Stinger CR unit design enables you to install, remove, and replace some modules without shutting the unit off. However, you can turn off power to the unit as a precaution, if the unit is not currently providing service.



Warning Before installing your Stinger unit, be sure to read the safety instructions in the *Edge Access and Broadband Access Safety and Compliance Guide*. For information specific to your unit, see Appendix D, "Safety-Related Electrical, Physical, and Environmental Information," in this guide.



Warning If power to the unit is not turned off, an electrical energy hazard is present within the card cage and behind the cooling unit. Remove all metallic objects from hands and wrist to prevent bridging of live contact points.



Caution Wear an antistatic wrist strap before handling any of the unit components.

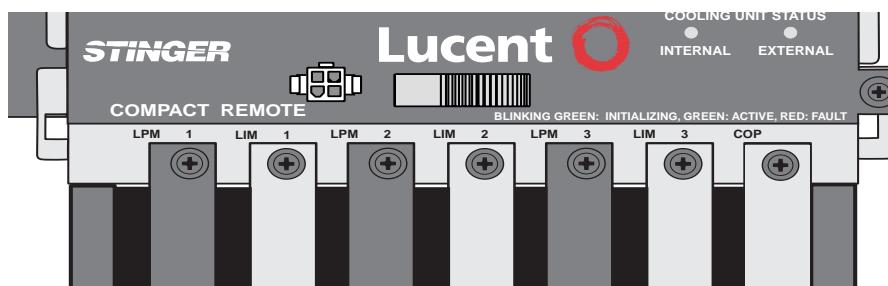
Slot numbering and module placement

Figure 3-6 shows the stenciling at top of the slots in a Stinger CR chassis. This identifies the locations for up to three LIMs, their associated LPMs, and the module in the COP slot.

Each of the LIMs that are installed in a Stinger CR unit are identified in the command interface by their physical location. The shelf designation of units operating in stand-alone mode is always 1 (one). So, units operating in stand-alone mode identify LIMs by their slot position in shelf 1. For example, the TAOS command interface on a stand-alone Stinger CR unit identifies the LIM in slot 1 as {shelf-1 slot-1 0}.

A hosted Stinger CR has a shelf number assigned to it in the command interface of the host unit. LIMs in a hosted Stinger CR are identified in the command interface of the host unit by their slot position in that shelf. For example, the TAOS command interface on the host unit identifies the LIM in slot 1 of a Stinger CR unit that has been designated shelf 5 as {shelf-5 slot-1 0}. (For details about assigning shelf numbers in the host command interface, see Chapter 5.)

Figure 3-6. Slot labeling on the Stinger CR chassis



Module installation and replacement for the COP slot



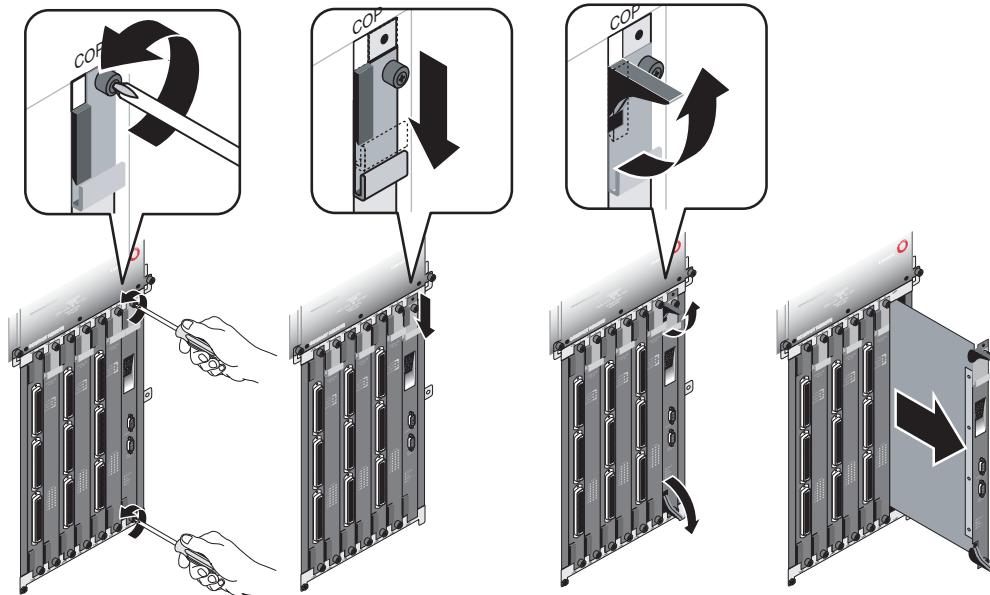
Caution The module in the COP slot controls operations on the local chassis. Removal of the module in the COP slot will cause an immediate failure of an operating Stinger CR unit. Before removing or replacing the module in the COP slot, perform a normal shut down of the unit and remove power from the Stinger CR.

Removing a module from the COP slot

To remove a COP, IP2000, or control module from the COP slot:

- 1 Put on the antistatic wrist strap, as recommended in "Preventing static discharge damage" on page 2-2, and connect it an electrical ground.
- 2 Turn off power to the unit.
- 3 Using a number 2 Phillips screwdriver, loosen the thumbscrews located on the top and bottom of the module, as shown in Figure 3-7. Other screwdrivers might damage the screw heads.

Figure 3-7. Removing a module from the COP slot



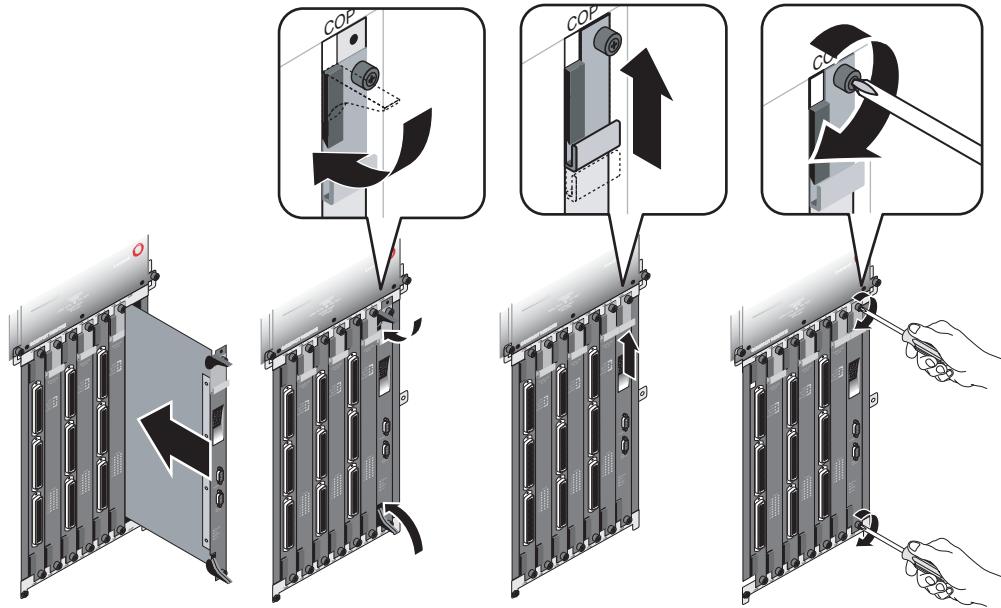
- 4 Slide the ejector lock at the top of the module down to access the top card ejector. This puts the module into a reset state.
- 5 Lift the top and bottom card ejectors simultaneously to remove the module from the unit.
- 6 Carefully slide the module out of the chassis, and place it into an antistatic container.

Installing a module in the COP slot

To install a COP, IP2000, or control module in the COP slot:

- 1 Put on the antistatic wrist strap, as recommended in “Preventing static discharge damage” on page 2-2, and connect it to an electrical ground.
- 2 Align the replacement module with the card guide and carefully slide the module into the unit, as shown in Figure 3-8.

Figure 3-8. *Installing a module in the COP slot*



- 3 Depress the card ejectors simultaneously to seat the module into the midplane.
- 4 Slide the card ejector lock up.
- 5 Using a number 2 Phillips screwdriver, tighten the two thumbscrews.
- 6 Restore power to the unit.
- 7 Verify that the FAULT LED on the COP lights while the system is booting and then turns off. If the FAULT LED remains lit, it indicates a problem with the unit.

Installing and replacing LIMs

Physical installation and replacement of an LIM are similar procedures to the installation and replacement of a module in the COP slot. Refer to the illustration in Figure 3-8, if necessary.



Note LIMs installed in a hosted Stinger CR are referred to as RLIMs because of their remote function in the CR chassis. This is a only a term of reference, related to the implementation of the LIM in a hosted Stinger CR, it does not identify a different type of module.

Installing a LIM

To install a LIM:

- 1 Put on the antistatic wrist strap, as recommended in “Preventing static discharge damage” on page 2-2, and connect it to an electrical ground.
- 2 Remove the blank slot cover on the desired slot on the front of the unit. (See “Installation and replacement of Stinger CR components” on page 3-7.)
- 3 Align the LIM with the card guides and carefully slide the module into the unit.



Caution To avoid damage, insert the LIM slowly. Keep the connector and components on the LIM being inserted away from components on adjacent LIMs

and LPMs. Do not force the card. Once the card has engaged its bus connector, press firmly to be sure it is fully seated.

- 4 Depress the ejectors simultaneously.
- 5 Slide the card ejector lock up.
- 6 Using a number 2 Phillips screwdriver, secure the LIM by tightening the thumbscrews.
- 7 If necessary, if all other installation tasks are complete, including the installation of an associated LPM, turn on power to the Stinger unit.
- 8 Wait several minutes and then verify the behavior of the status lights on the LIM to verify its operational status.

For status light information, see “LIM status lights” on page 3-30 or the module guide for the LIM you are installing.

Replacing a LIM



Caution Lucent Technologies recommends setting the administrative status of the LIM to Down (through the command-line interface) before replacing the module. When a LIM is removed, all its ports and circuits are terminated, and data loss might occur. For instructions on changing a LIM’s state to Down and then back to Up, see the *Stinger Administration Guide*.

Refer to the illustration in Figure 3-7 on page 3-9, if necessary.

To replace a LIM:

- 1 Put on the antistatic wrist strap, as recommended in “Preventing static discharge damage” on page 2-2, and connect it to an electrical ground.
- 2 Using a number 2 Phillips screwdriver, loosen the top and bottom thumbscrews attaching the module to the unit.
- 3 Slide the ejector lock located at the top of the RLIM down to disconnect the module from the network.
- 4 Lift the top and bottom card ejectors simultaneously to remove the module from the unit. Lift both ejectors simultaneously to avoid damage to the module.
- 5 Carefully slide the LIM out of the unit and place it into an antistatic container.
- 6 Align the LIM with the card guides and carefully slide the module into the unit.



Caution To avoid damage, insert the LIM slowly. Keep the connector and components on the LIM being inserted away from components on adjacent LIMs and LPMs. Do not force the card. Once the card has engaged its bus connector, press firmly to be sure it is fully seated.

- 7 Depress the ejectors simultaneously.
- 8 Slide the card ejector lock up.
- 9 Using a number 2 Phillips screwdriver, secure the module into the unit by tightening the thumbscrews on the LIM.
- 10 Wait several minutes and then verify the behavior of the status lights on the LIM to verify its operational status.

For status light information, see “LIM status lights” on page 3-30, or the module guide for the LIM you are installing.

Installing and replacing LPMs

Installation and replacement of line protection modules (LPMs) is similar to the procedure for LIMs, except that the top ejector levers are not protected by ejector locks.

Openings for unused LPM slots are protected by blank covers. A companion LPM must be installed for each LIM.

Installing an LPM

To install an LPM:

- 1 Put on the antistatic wrist strap, as recommended in "Preventing static discharge damage" on page 2-2, and connect it to an electrical grounding point.
- 2 Remove the blank filler module covering the LPM's slot.
- 3 Align the LPM with the card guides and gently slide the LPM into the unit.
- 4 Using a number 2 Phillips screwdriver, secure the module into the unit by tightening the thumbscrews on the LPM.
- 5 Connect the cables as described in "Connections to the LPMs" on page 3-24.

Replacing an LPM

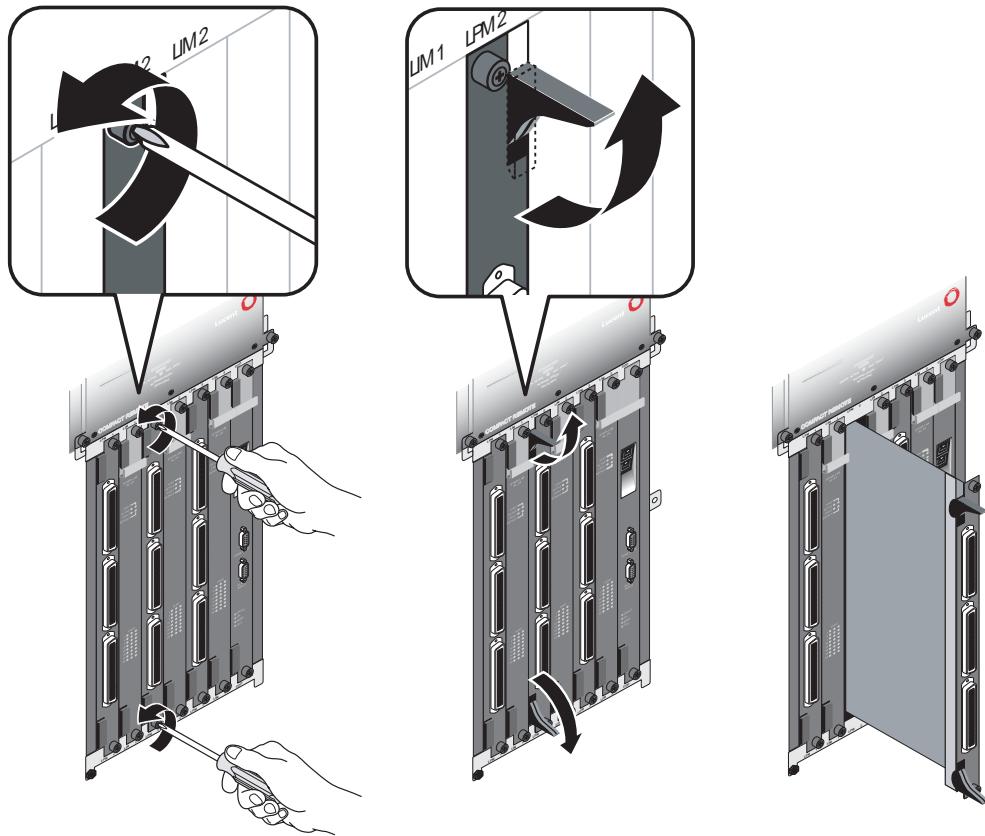


Caution Any circuits running through the LPM are interrupted when it is removed, which can result in data loss. Lucent Technologies recommends setting the associated LIM's administrative status to Down before removing the LPM from the unit. For instructions on changing a LIM's state to Down and then back to Up, see the *Stinger Administration Guide*.

To replace an LPM:

- 1 Put on the antistatic wrist strap, as recommended in "Preventing static discharge damage" on page 2-2, and connect it to an electrical ground.
- 2 Carefully unhook the cable ties connecting the cables and connectors from the card.
- 3 Using a number 2 Phillips screwdriver, loosen the top and bottom thumbscrews attaching the module to the unit, as shown in Figure 3-9.

Figure 3-9. Removing LPMs



- 4 Lift the top and bottom card ejectors simultaneously to remove the module from the unit. Lift both ejectors simultaneously to avoid damage to the module.
- 5 Carefully slide the LPM out of the unit and place it into an antistatic container.
- 6 Align the new or replacement LPM with the card guides and carefully slide the module into the unit. Press firmly to be sure it has engaged the midplane connectors.
- 7 Depress the ejectors simultaneously.
- 8 Using a number 2 Phillips screwdriver, secure the module into the unit by tightening the thumbscrews on the LPM.
- 9 Reconnect the cables, as described in “Connections to the LPMs” on page 3-24.

Replacing the chassis cooling module

It is not necessary to remove power to replace the cooling module. However, the cooling module must be replaced as quickly as possible to avoid overheating other modules in the unit. Unpack the replacement cooling module unpacked so that it is ready for installation before removing the cooling module being replaced.

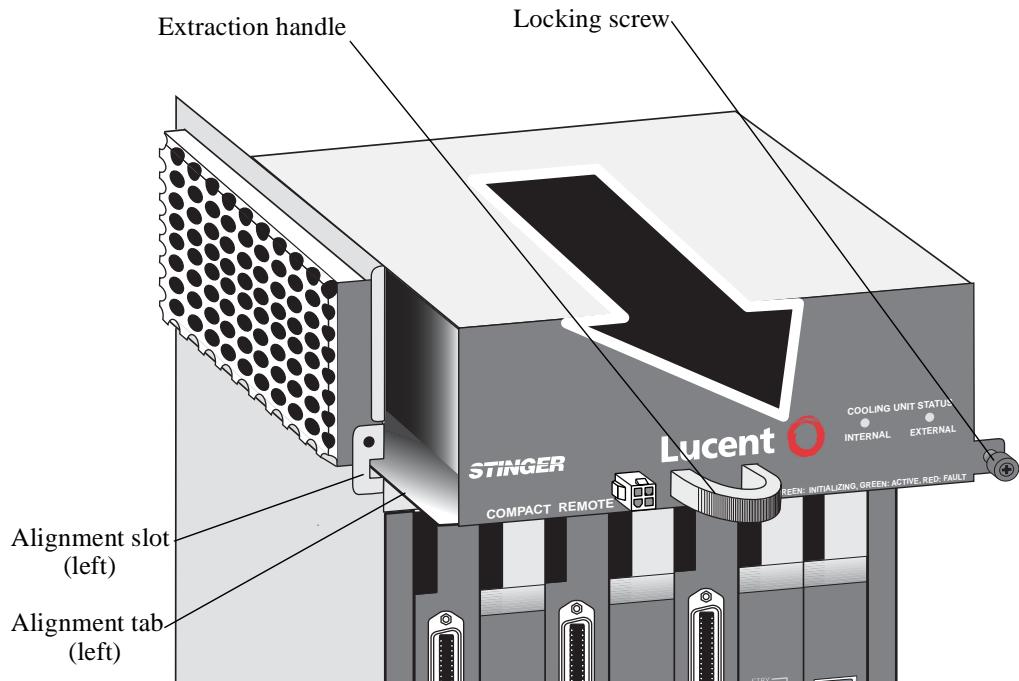


Warning Moving fan blades in the cooling module may cause injury to fingers. Do not completely remove the cooling module until the internal fan has stopped moving, as detailed in step 3 and step 4 below.

Use the following procedure to replace the cooling unit of a Stinger Compact Remote unit.

- 1 Remove the connector for the chassis external cooling fan from its power connection on the cooling module.
- 2 Fully loosen the locking screw on the lower right side of the front of the cooling module
- 3 Grasp the extraction handle on the cooling module and pull only enough to separate the module from its power connector in the back of the mounting bay.
- 4 Wait several seconds until the internal fan in the cooling module has stopped moving. Then slide the cooling module out of its mounting, as shown in Figure 3-10.

Figure 3-10. Removing the cooling module



- 5 Quickly install the replacement cooling module by aligning the tabs formed by the lower surface of the cooling module with the slots on each side of the chassis (left alignment tab and slot shown in Figure 3-10).
- 6 Gently slide the cooling module straight into the chassis until the connector on the back of the cooling module makes contact with the connector in the back left side of the cooling module bay.
- 7 Reattach the connector for the external cooling fan to its power connection on the cooling module.
- 8 Press the cooling module firmly into place until it is fully seated
- 9 Fully tighten the locking screw on the lower right side of the front of the cooling module.

Replacing the external cooling fan

The Stinger CR enclosure has an external cooling fan that circulates air through the ventilation panels that surround the enclosure. Power for this fan is provided from the cooling module in the Stinger CR chassis within the enclosure. The cable that provides this power connects inside the enclosure to a pass-through connector in the bottom of the enclosure. The power connector for the cooling fan connects to this pass-through connector within the cable guard beneath the enclosure.



Warning Moving fan blades in the external cooling fan may cause injury to fingers. Do not remove the external cooling fan until its blades have stopped moving, as detailed in the following procedure.

Use the following procedure to replace the cooling unit of a Stinger Compact Remote unit.

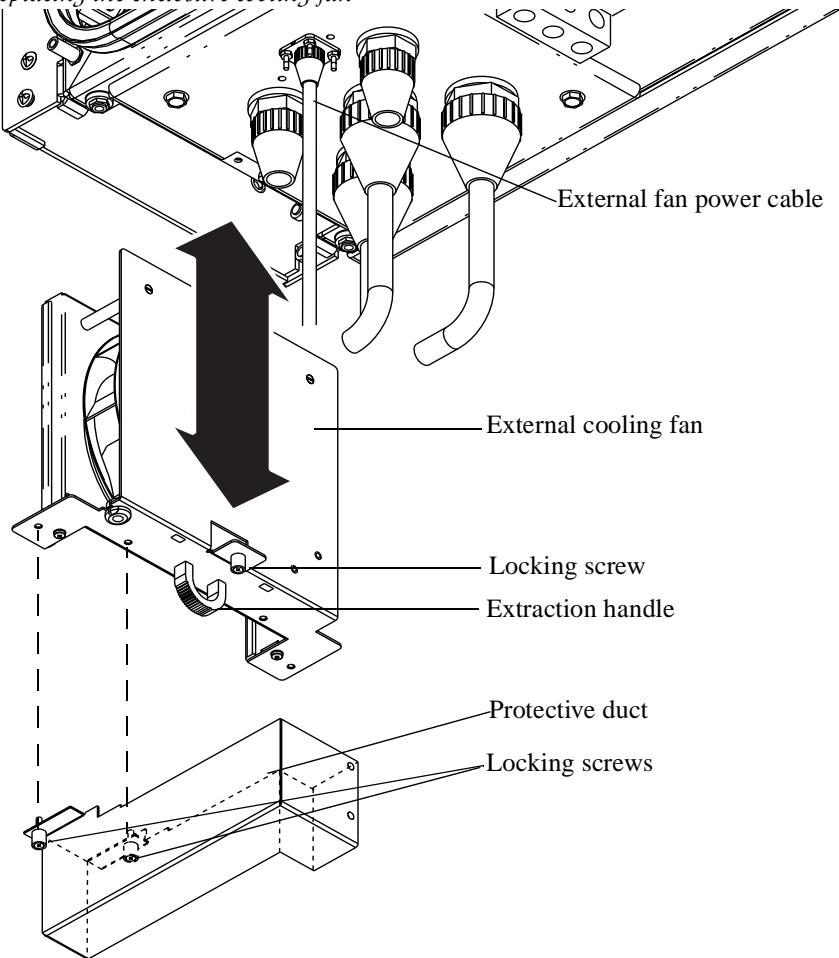
- 1 Remove the connector for the external cooling fan from its power connection on the cooling module inside the enclosure.



Note This will ensure that the fan blades of the external cooling fan are not moving during replacement.

- 1 Remove the cable cover below the enclosure.
- 2 Fully loosen the locking screw for the external cooling fan.
- 3 Grasp the extraction handle on the external cooling fan and pull to remove it from its mounting.
- 4 Unscrew and remove the external cooling fan power cable, shown in Figure 3-11, from the pass-through connector below the enclosure.
- 5 Remove the external cooling fan from the enclosure and place it on a flat work surface.
- 6 Fully loosen the locking screws on the protective duct below the cooling fan (see Figure 3-11) and remove the protective duct.

Figure 3-11. Replacing the enclosure cooling fan



- 7 Transfer the protective duct to the new fan unit and secure it by tightening the locking screws.
- 8 Reattach the power cable to the pass-through connector on the bottom of the enclosure.
- 9 Align the external cooling fan as shown in Figure 3-11, and slide it into the chassis until the locking screw makes contact with the bottom of the enclosure.
- 10 Fully tighten the locking screw.
- 11 Replace the cable cover on the bottom of the enclosure.

Use the following procedure to restore power to the external fan, and synchronize it with the internal fan in the cooling module.

- 1 Fully loosen the locking screw for the cooling module, containing the internal fan. (See Figure 3-10 on page 3-14)
- 2 Grasp the extraction handle on the cooling module and pull only enough to separate the module from its power connector in the back of the mounting bay.
- 3 Reattach the power cable for the external cooling fan to its power connection on the cooling module.

- 4 Press the cooling module firmly into place until it is fully seated
- 5 Fully tighten the locking screw on the lower right side of the front of the cooling module.

Replacing the power supply

Before removing the power supply for the Stinger CR, be sure that the unit has been properly shut down, and that the ± 190 Vdc source voltage has been disconnected.

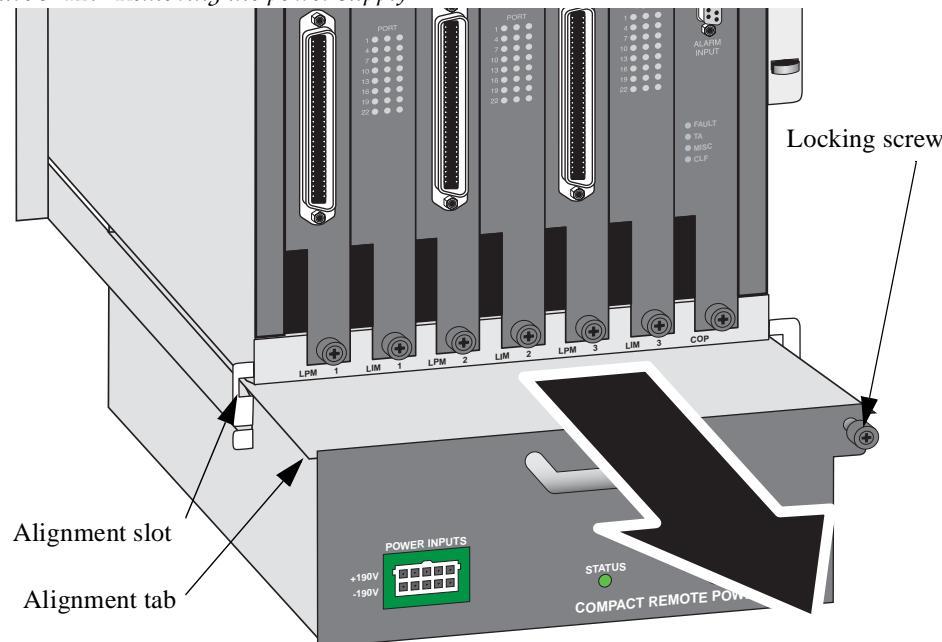


Note When removing the power supply, disconnect the ± 190 Vdc power input connector before loosening the locking screw. When installing the power supply, tighten the locking screw before connecting the power input connector.

Use the following procedure to replace the power supply of a Stinger Compact Remote unit.

- 1 Disconnect the ± 190 Vdc power connector from the power supply.
- 2 Fully loosen the locking screw on the upper right side of the front of the power supply and pull it straight out of its mounting bay as shown in Figure 3-10.

Figure 3-12. Removing the power supply



- 3 Install the replacement power supply by aligning the tabs formed by the upper surface of the power supply with the slots on each side of the chassis (left alignment tab and slot shown in Figure 3-12).
- 4 Gently slide the power supply straight into the chassis until the connector on the back of the power supply makes contact with the connector in the back of the power supply bay.
- 5 Firmly press the power supply firmly into place until it is fully seated
- 6 Fully tighten the locking screw on the upper right side of the front of the power supply.

- 7 Reconnect the ± 190 Vdc power input connector.

Physical connections to the Stinger CR unit

Information and illustrations here show how the DSL subscriber lines, and the analog voice facilities are connected to the LPMs and how to make connections to an IP2000, control module, or COP module in the COP slot.

Connections to modules in the COP slot

The COP module supports hosted operation of the Stinger CR unit. Both the IP2000 and control modules support stand-alone operation. However, all modules that are installed in the COP slot share some common connectors. The Figure 3-13 and table identify the connectors that are present on these modules.

Figure 3-13. Connectors for modules in the COP slot

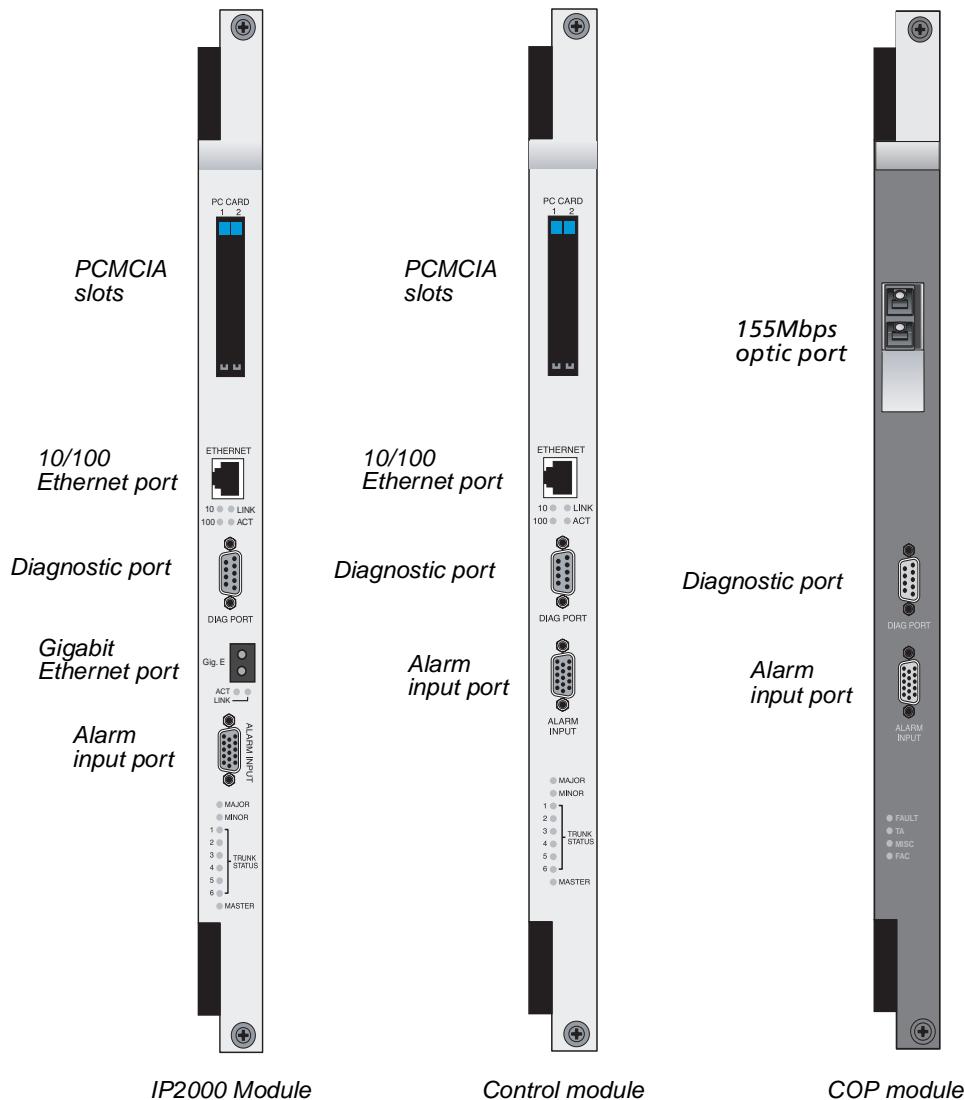


Table 3-1. Connectors for modules in the COP slot

Connector	Function	IP2000	Control module	COP module
PCMCIA slot	Holds PCMCIA cards for storage of configuration settings and software	Yes	Yes	No
Gigabit Ethernet port	High bandwidth connection for end-user traffic	Yes	No	No
155Mbps optical port	High bandwidth connection for end-user traffic and management information	No	No	Yes
10/100 Ethernet port	Low bandwidth connection to management network	Yes	Yes	No
Diagnostic port	Serial connection for management console	Yes	Yes	Yes (unused)
Alarm input port	Connections to monitor the status of up to seven external alarm A special cable, required with the IP2000 module, monitors the enclosure door alarm through the Alarm port. (See, "Door alarm connection for stand-alone operation" on page C-18.)	Yes	Yes	Yes

PCMCIA slot

This slot is supported on the IP2000 module and control module. It holds PCMCIA cards that can store configuration information and software for the Stinger unit.

You remove the PCMCIA cards by pushing the square, flat black buttons at the bottom of each PCMCIA card to eject it. After a card is removed, make sure it remains guarded against static discharge.

You install the PCMCIA cards by aligning the card edge with the slot guides, and pushing the card in until the black ejector button pops up.

Gigabit Ethernet port

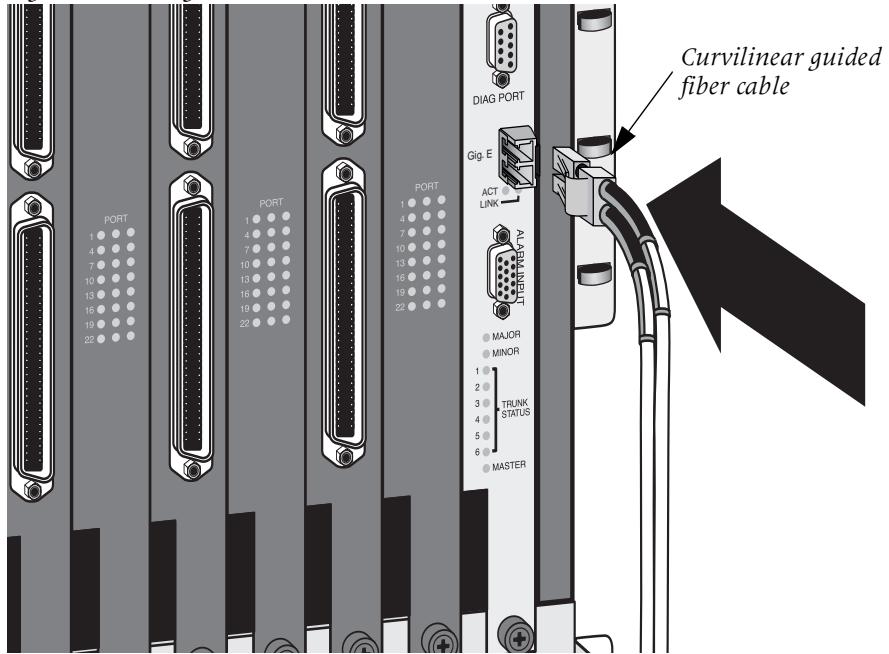
This port supported on the IP2000 module. It provides a gigabit Ethernet connection for end-user traffic, and can be used for administrative access. Stinger CR units that are equipped with an IP2000 module have an enclosure door that accommodates the optical fiber connection to the IP2000 (see Figure 1-3 on page 1-4). The special

CR Enclosure and Component Installation

Physical connections to the Stinger CR unit

curvilinear guided fiber cable, shipped with units that are equipped with IP2000 modules, must be used. This connection is shown in Figure 3-14.

Figure 3-14. Gigabit Ethernet connection to IP2000 module.



155Mbps optical port

This port is supported on the COP module. A 155Mbps optical connection to the COP requires duplex small form factor (LC) fiber optic cable.



Caution: Bind excess cable lengths in a figure-eight pattern. Do not wind excess cable into circular coils.

Note: Clean any fiber optic cables prior to connecting them.

To connect the optical jumper in the Stinger CR unit from the fiber tray to COP, align the latch on the LC connector head of the jumper with the latching point on the side of the LC connector in the COP and carefully insert the head of the jumper into the connector on the COP, as shown in Figure 3-15.

Figure 3-15. 155Mbps optical connection to the COP

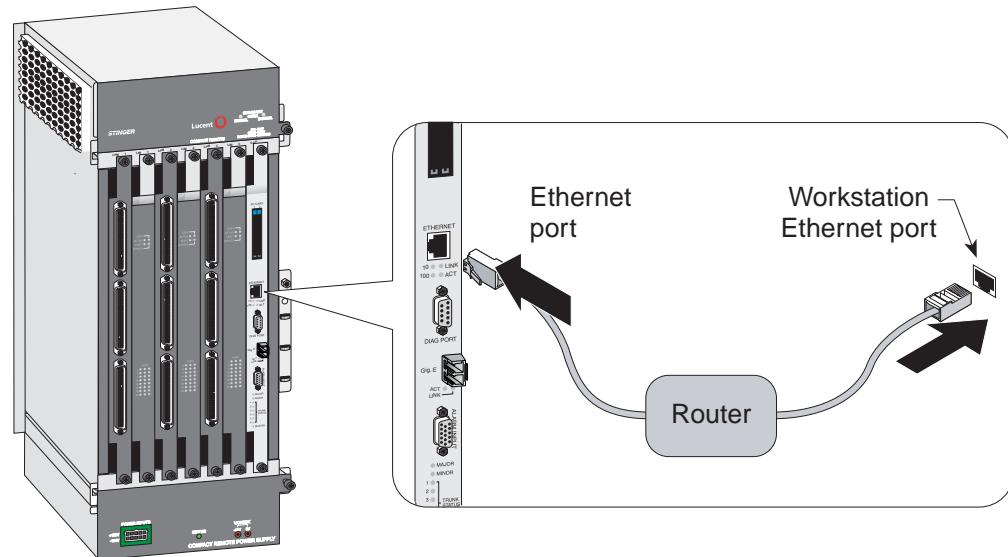


10/100 Ethernet port

This port is supported on the IP2000 module and control module. This port can connect the Stinger CR unit through an Ethernet network or, with an Ethernet turnover cable, directly to an administrative workstation. The IP address of the Stinger CR unit must be configured and the unit must be connected to an Ethernet network, or workstation before this port can be used.

Figure 3-16 shows an Ethernet network connection from the Stinger unit to a management workstation.

Figure 3-16. Ethernet connection



CR Enclosure and Component Installation

Physical connections to the Stinger CR unit

To connect a management workstation to the Stinger unit using an indirect Ethernet connection:

- 1 Connect one end of the Ethernet cable to the Ethernet RJ-48 port on the control module.
- 2 Connect the other end of the Ethernet cable to the local LAN.
- 3 Ensure that the management workstation has connectivity to the LAN on which the unit resides.
- 4 Ensure the Ethernet transceivers are connected properly to the network.

Diagnostic port

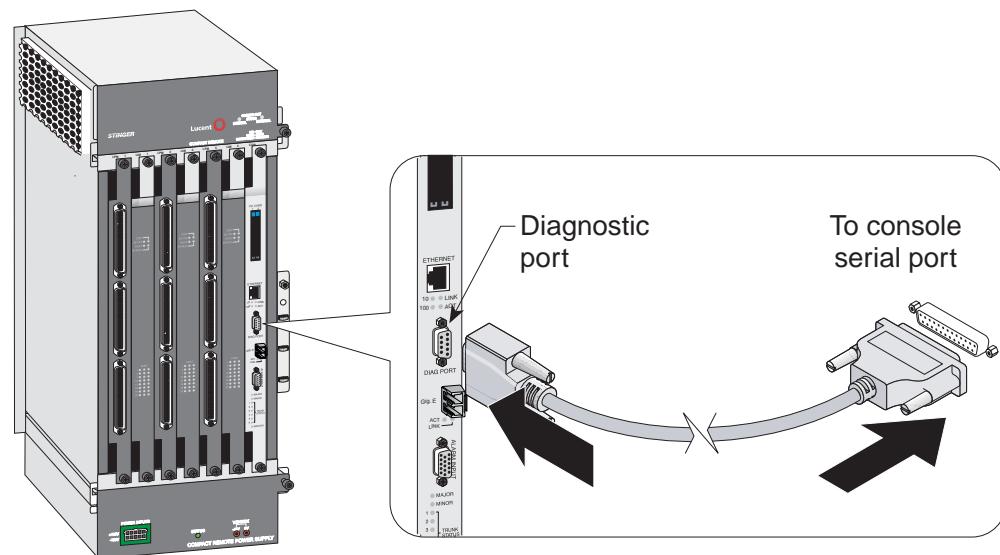
This port is present on the COP, IP2000, and control modules. However, it is only used to access the local command interface for configuration and management on stand-alone Stinger CR units, using the IP2000 module or control module.



Note This interface is not used on Stinger CR units that are being installed with a COP for hosted operation. The TAOS software installed on these units is set to operate the unit in hosted mode by default. Additional configuration of the ADSL lines and ATM connection is accomplished from the host unit.

Figure 3-17 shows a serial connection from a console terminal to the Diagnostic port of an IP2000 module in a Stinger CR unit.

Figure 3-17. Serial management connection for a stand-alone Stinger CR



To connect a console terminal to a Stinger CR unit, connect one end of a shielded straight-through cable to the diagnostic port (DIAG PORT) on the IP2000 or control module. Then connect the other end of the cable to the serial port on the console device.

The diagnostic port on the IP2000 or control module consists of a female DB-9 connector. Examine the serial connector of your PC or dumb terminal to ensure that your shielded straight-through cable has the proper connectors. If needed, you can use DB-9-to-DB-25 converters or gender converters to complete this connection.

See “Diagnostic port and cable pinouts” on page C-1 for detailed information about the pinouts on the console serial port.

Alarm input port

This port is present on the COP, IP2000, and control modules. The DB-15 connector can accept connections to monitor the alarm status of up to seven external devices. In stand-alone Stinger CR units with an IP2000 module or control module, a connection to this port is used to monitor the enclosure door alarm. In these units, a special cable connects the switch for the enclosure door alarm to pins one and two of this port.



Note In hosted Stinger CR units, the door alarm switch is connected directly to the door alarm pins on the chassis card-cage, behind the cooling module. The ALARM port of the COP module is not used to monitor the door alarm. (see “Chassis door alarm connections” on page C-18.)

Alarm connections for monitoring multiple external alarms

The ALARM port of an IP2000 or control module can be used to monitor multiple devices. The connection for each external device consists of a pair of 24-gauge to 28-gauge connectors. One connector supplies ground, and the other senses the status of the remote alarm by applying 3.3Vdc, which draws less than 10mA of current through the closed contacts of the alarm relay on the remote device. For the complete pinout arrangement of the DB-15 connector, see “Alarm input port pinouts” on page C-2.



Note This capability is generally not used on Stinger CR installations.

Alarm connection for monitoring the enclosure door alarm

When the Stinger CR is configured as a stand-alone unit with an IP2000 module or control module, a connection to the ALARM port is used to monitor the enclosure door alarm. A special cable, provided with the unit, connects the enclosure door alarm switch to pins one and two of this port. For additional cable details, see “Door alarm connection for stand-alone operation” on page C-18.

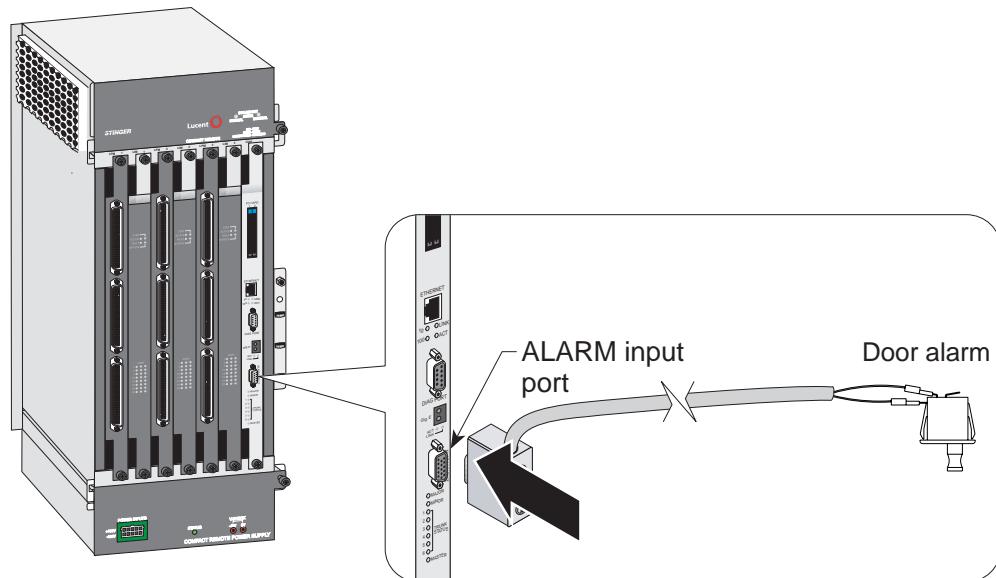
To connect to the enclosure door alarm:

- Connect The male DB-15 connector of the Stinger CR stand-alone door alarm cable to the ALARM port connector of the IP2000 or control module.
- On the opposite end of the cable, connect the spade connectors on the white and black wires to the corresponding spade terminals on the door alarm micro switch, as shown in Figure 3-18.

CR Enclosure and Component Installation

Physical connections to the Stinger CR unit

Figure 3-18. Connecting the door alarm to the ALARM input port



The alarm relays of external devices can be either normally opened or normally closed. The Stinger unit can be configured to sense an alarm condition for the opening of a normally closed relay, or the closing of a normally open relay. For information on the configuration of these see "Alarm input port pinouts" on page C-2.

Connections to the LPMs

The LPMs connect their associated LIMs to physical line facilities. In the Stinger CR, the LPMs are connected directly to three sets of protection blocks located to the left of the Stinger chassis in the enclosure.

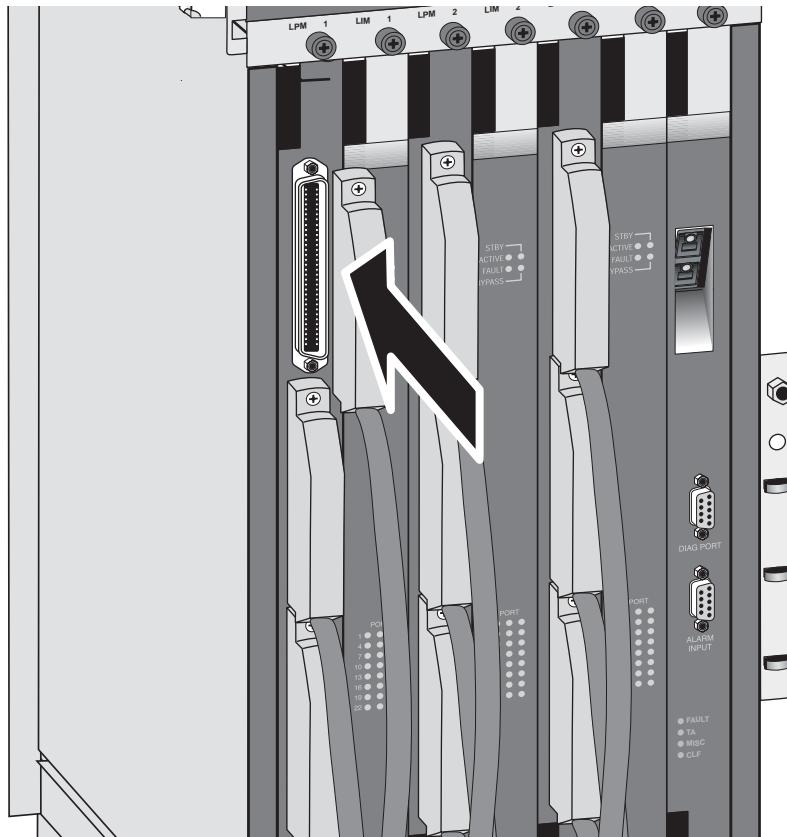
The 48-port LPMs with splitters also connect to facilities providing analog voice service (dial tone) from the central office. The integrated splitters combine analog and DSL data service on a single copper pair for delivery to the subscriber. For specific information connections from the LPMs, through the protection blocks, and to the copper telecommunication facilities, see "Stinger CR cabling for the 48-port LPM with splitters" on page C-2.

Connecting the LPM

The 48-port LPM with splitters is designed to provide access to subscriber facilities for DSL service and connection points for analog voice service. The splitters in this unit allow both services to be combined on the same subscriber facilities. Information about LPMs that are used with other Stinger units is provided in the Getting Started Guide for each unit. Additional details about the connection points for the 48-port LIM with splitters is provided in "Stinger CR cabling for the 48-port LPM with splitters" on page C-2.

Connections to the 48-port LPM with splitters are shown in Figure 3-19.

Figure 3-19. Connecting an LPM



To connect the cables to the 64-pin connectors on an LPM:

- 1 Beginning with the bottom connector, carefully insert the head of the cable into the connector on the LPM, as shown in Figure 3-19.
- 2 Press the connector firmly into place until it is fully seated.
- 3 Using a number 1 cross-recess (Phillips) screwdriver tighten the lock screws at the top and bottom of the connector.
- 4 Move up to the next connector and repeat step 1 through step 3 until the top connector on the LPM has been installed.



Note See “Stinger CR cabling for the 48-port LPM with splitters” on page C-2 for pinout information and wiring details.

Turning on power to a Stinger CR unit



Warning Use appropriate caution when handling the ± 190 Vdc power connections. A hazard for electrical shock exists in spite of the protection provided by ground fault interrupters (GFIs) in the central office and 100W power limit of the lines.

Power is provided from an Argus CSM-36-BC power supply in the central office over multiple pairs of copper telecommunications wire. Three to five ± 190 Vdc power sources are required to power each Stinger CR. The number of power sources

required to provide power depends upon the loop resistance of the available copper telecommunication facilities, as shown in the following table.

Table 3-2. Number of pairs for providing power

Number of power sources	Loop resistance
3	190 Ohms or less
4	191-515 Ohms
5	516-685 Ohms



Caution Do not turn on power to a Stinger CR unit without a COP, IP2000, or control module installed in the chassis. Starting up a unit without a COP, IP2000, or control module installed can damage hardware components.

All Stinger CR status lights momentarily turn ON just after startup, except as noted below for the COP, IP2000, and control modules.

Status lights

The status lights on the modules in the Stinger CR unit indicate the operating status of each module.



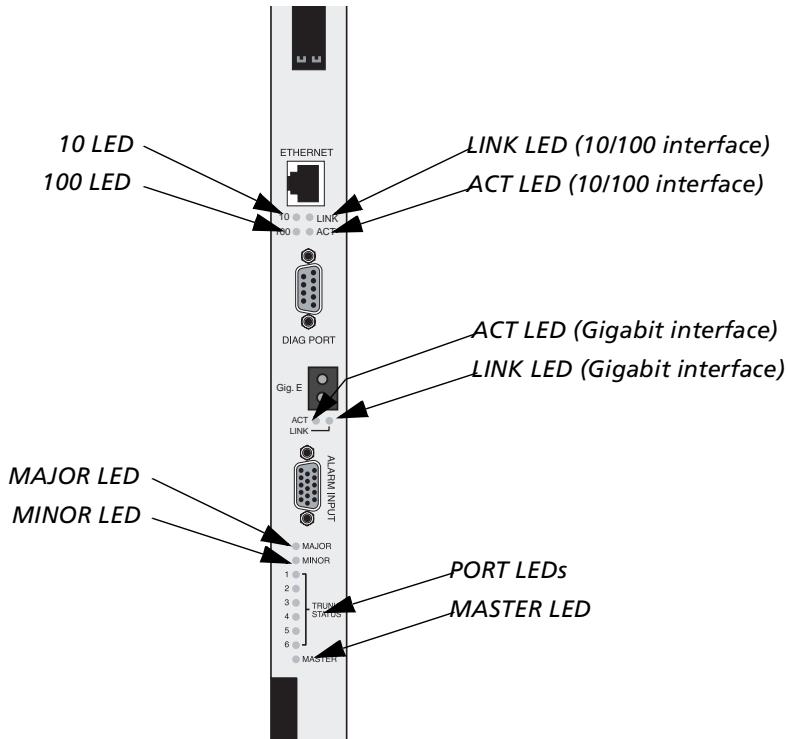
Note For information about status lights on the OLIM in the host Stinger unit, see “Interpreting OLIM status lights” on page B-2.

IP2000 and control module status lights

All IP2000 and control module status lights, except the MASTER light, momentarily turn ON just after startup, and all six TRUNK STATUS lights turn OFF. After the system starts up, each light indicates status information as described in Figure 3-3.

Figure 3-20 shows the locations of the status lights on an IP2000. The locations on a control module are similar, except that the control module does not have a gigabit Ethernet interface and its associated lights.

Figure 3-20. IP2000 status lights



The FAULT LED momentarily turns ON just after startup. After the system starts up, each light monitors a state as described in Table 3-3.

Table 3-3. Status lights on the IP2000 module

Status light	Color	Condition	Indicates
10	Green	On	A 10Mbps network has been detected on the 10/100 Ethernet interface.
100	Green	On	A 100Mbps network has been detected on the 10/100 Ethernet interface.
LINK	Green	On	A good physical link to a router or other Ethernet device has been detected on the associated 10/100 or gigabit Ethernet interface. Note The gigabit interface and its LINK light are only present on the IP2000 module.
ACT	Green	On	Traffic has been detected on the associated 10/100 or gigabit Ethernet interface. Note The gigabit interface and its ACT light are only present on the IP2000 module.

CR Enclosure and Component Installation

Status lights

Table 3-3. *Status lights on the IP2000 module (continued)*

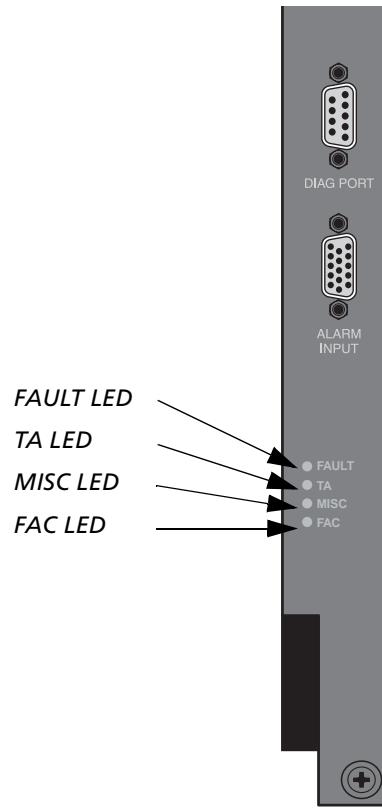
Status light	Color	Condition	Indicates
MAJOR	Red	ON or blinking	A major alarm condition has been detected. For information about configuring major alarms, see the Stinger Administration Guide. The MAJOR status light turns ON at startup. It then blinks slowly while the IP2000 or control module runs its POST in the boot loader. It continues to blink while the module loads its operational code from the PCMCIA flash card. It stops blinks and remains OFF when the code is loaded successfully and POST is completed. If the MAJOR status light continues to blink, it indicates a failure.
MINOR	Red	On	A minor alarm condition has been detected. For information about configuring minor alarms, see the Stinger Administration Guide. The MINOR status light is ON at startup. It remains ON until the IP2000 or control module passes all POST tests. It then stays OFF until a minor alarm occurs. If the IP2000 or control module fails POST, the MINOR status light remains ON.
TRUNK STATUS	Green	ON	<i>Not used on the Stinger CR.</i> Indicates that the corresponding port on a trunk module is fully operational.
MASTER	Green	ON	Indicates that this IP2000 or control module is the master (primary) chassis controller. (Always ON in the Stinger CR.)

COP status lights

On the COP, the FAULT status light turns ON briefly at startup. If the MAJOR status light remains on, or turns on during operation of the unit, it indicates a failure.

Figure 3-21 shows the locations of the COP status lights.

Figure 3-21. COP status lights



The FAULT LED momentarily turns ON just after startup. After the system starts up, each light monitors a state as described in Table 3-3.

Table 3-4. Status lights on the COP module

Status light	Color	Condition	Indicates
FAULT	Red	ON	The system is booting or the system is in a failure mode.
TA	Green	ON	A test relay has been operated on an LPM to test the copper ADSL facilities.
MISC	Yellow	ON	The COP has detected a relay closure on one of the seven pairs connected to the ALARM connector.
FAC	Green	ON	The optical connection for the COP is operating properly.
	Yellow	ON	The optical connection for the COP has failed.

LIM status lights

Several status lights on the front panel of the LIM ADSL low-power 48-port LIM indicate the status of the module and its ports. Figure 3-22 shows the front panel and status lights of the ADSL low-power 48-port LIM. The front panel of the T1-IMA LIM has identical lights, except that there are fewer port status lights.

Figure 3-22. ADSL 48-port low-power LIM



All status lights illuminate briefly upon startup or restart, then remain dark until the module passes its power-on self test (POST). When the module passes the POST and becomes operational, the ACTIVE light illuminates. It is the only light that is on during normal operation.

Table 3-5 explains the ADSL 48-port status lights.

Table 3-5. ADSL 48-port Annex A LIM status lights

Light	Color	Indication
STBY	Orange	The module is a designated spare. The control module switches traffic to the module if one of the other modules fails.
ACTIVE	Green	The module or port is fully operational and no errors have been detected.
FAULT	Orange	The module failed to pass its POST.
BYPASS	Orange	The module is in bypass mode. (The module redundancy feature is activated.)
PORt	Green	The local and remote ends of the physical line have achieved frame synchronization, and the local end of the link has achieved cell delineation. If the light is not illuminated, the port is inactive.

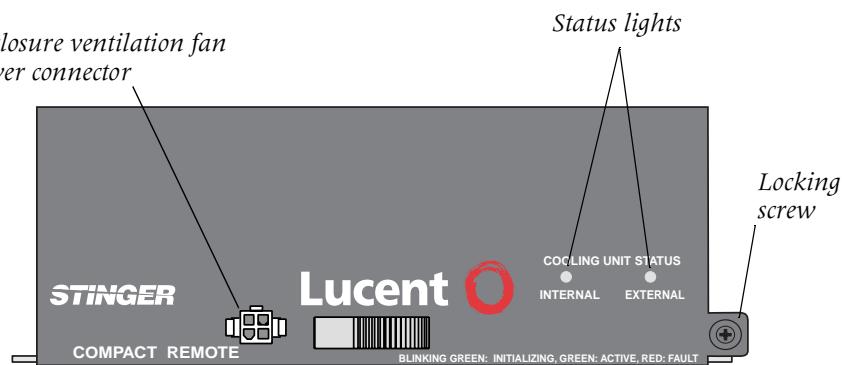


Note Detailed physical and configuration information for the 48-port low power ADSL LIM is included in the *Stinger ADSL Annex-A LIM Guide for LIMs with ADSL2+ Capability*.

Cooling unit status lights

The Stinger CR cooling unit is shown in Figure 3-23.

Figure 3-23. The Stinger CR cooling unit



The Stinger CR cooling unit has two status lights on the front to indicate the operating status of the cooling unit and the enclosure ventilation fan. The status indicated by these lights is described in Table 3-6.

Table 3-6. Cooling unit status light

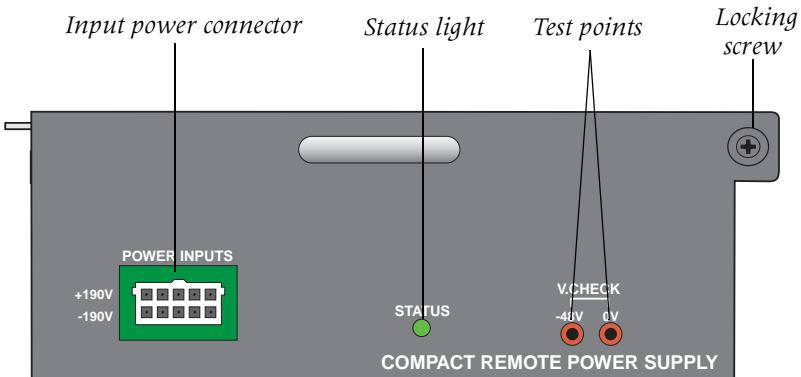
Condition	Indicates
On green	The fan has power.
On red	The fan is in a fault state.
Blinking green	The fan is initializing.

Power supply status lights

When lit, the power supply status light indicates that it is providing -48Vdc power to the Stinger CR unit. You can use the test points to measure the -48Vdc output and verify that it is within tolerance ($\pm 10\%$).

The Stinger CR power supply is shown in Figure 3-23.

Figure 3-24. The Stinger CR power supply



What's next

When you finish physically installing the Stinger CR unit you can proceed to the next chapter.

Initial Stand-alone Configuration

Basic configuration overview	4-1
Administrative connections	4-2
Logging into the IP2000 or control module	4-4
Restricting administrative access	4-5
Providing a basic system IP configuration	4-7

Basic configuration overview

The module in the COP slot controls the local operation of the Stinger CR unit. In hosted mode a COP module is installed in this location and configuration is performed on the host unit, not locally. In stand-alone mode an IP2000 or control module is installed in this location and basic configuration is performed on the management interface of the Stinger CR unit. This stand-alone configuration provides the unit with network connectivity for complete and ongoing configuration and management.

In stand-alone operation, the IP2000 or control module manages and boots the LIMs, maintains a central repository of the unit's configuration, performs call control and processing operations, and manages all centralized functions, such as SNMP access or communication with a RADIUS server.

Basic configuration of an IP2000 or control module includes the following tasks:

- Connecting a console workstation to the serial port on the IP2000 or control module in the Stinger CR unit
- Logging into the Stinger unit
- Changing default security settings to protect the unit
- Configuring IP to make the system accessible by Telnet, SNMP, and Ping



Note Complete information about configuration of the IP2000 module to support termination and aggregation of RFC 2684 Asynchronous Transfer Mode (ATM) PVCs, IGMP multicast v1/v2 and IEEE 802.1Q tagged virtual local area networks (VLANs), is contained in the *Stinger IP2000 Configuration Guide*.

Administrative connections

The serial port of an IP2000 or control module is used to perform initial stand-alone configuration of the Stinger CR from a console device. The Stinger CR can then be administered remotely by Telnet or SNMP.

Remote administrative access depends upon an IP network connection to the Stinger CR. This connection can be made through a dedicated administrative network, connected directly to the 10/100 Ethernet port of the IP2000 or control module. An administrative IP connection can also be established through the network supported by the Gigabit Ethernet port found only on the IP2000 module. The following information describes these physical connections.

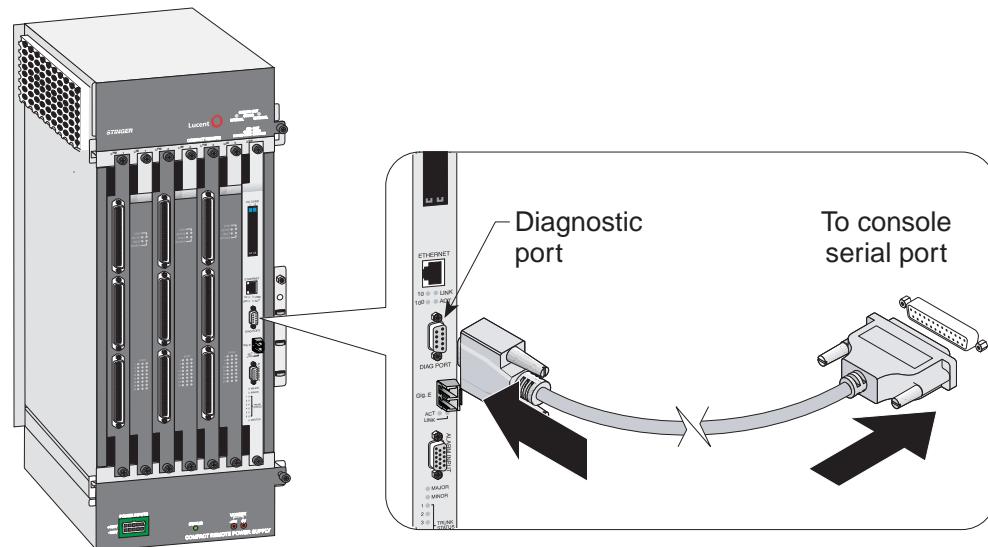
Serial connection to a console

Figure 4-1 shows a cable connection from a Stinger CR unit to a console terminal.



Note Although an IP2000 module is depicted, the same connection is made to a control module in the same way. For connector details, see “Control module interfaces” on page 2-7, and “IP2000 interfaces” on page 2-9.

Figure 4-1. Serial management connection to a Stinger CR unit



To connect the console terminal to the Stinger CR unit, connect one end of a shielded straight-through cable to the diagnostic port (DIAG PORT) on the IP2000 or control module. Then connect the other end of the cable to the serial port on the console device.

The diagnostic port on the controlling module in the COP slot consists of a female DB-9 connector. Examine the serial connector of your PC or dumb terminal to ensure that your shielded straight-through cable has the proper connectors. If needed, you can use DB-9-to-DB-25 converters or gender converters to complete this connection.

See Appendix C, “Cables and Connectors,” for detailed information about the pinouts on the console serial port.

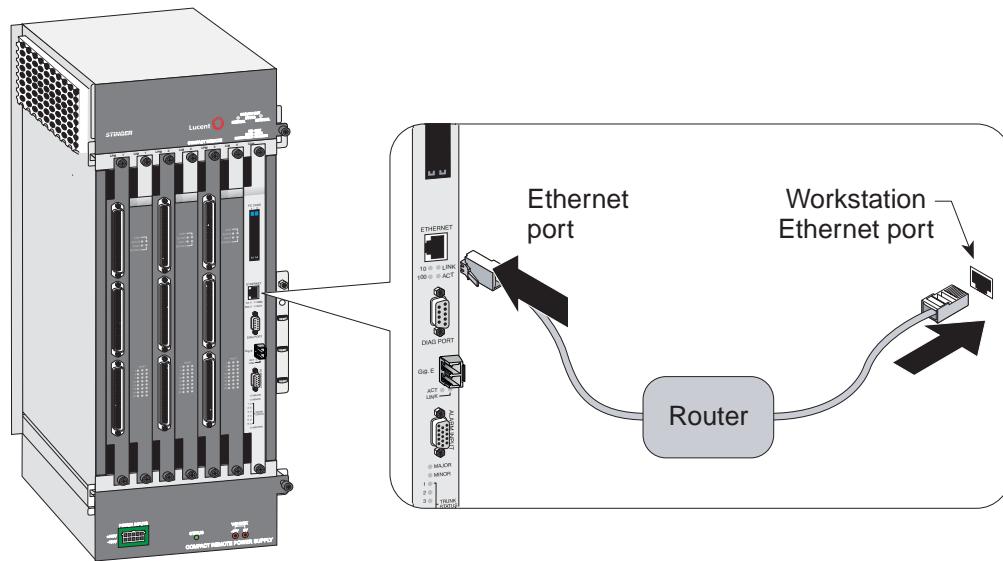
10/100 Ethernet connection to a workstation console

After the IP address for the 10/100 Ethernet port of a Stinger unit is configured, and the unit is connected to a 10/100 Ethernet network, an administrative Telnet connection can be established through the network. Figure 4-2 shows an Ethernet network connection from the Stinger CR unit to the management workstation.



Note Although an IP2000 module is depicted, the same connection is made to a control module in the same way. For connector details, see “Control module interfaces” on page 2-7, and “IP2000 interfaces” on page 2-9.

Figure 4-2. 10/100 Ethernet connection



To connect a management workstation to the Stinger CR unit using an indirect Ethernet connection:

- 1 Connect one end of the Ethernet cable to the Ethernet RJ-48 port on the IP2000 or control module.
- 2 Connect the other end of the Ethernet cable to the local LAN.
- 3 Ensure that the management workstation has connectivity to the LAN on which the unit resides.
- 4 Ensure the Ethernet transceivers are connected properly to the network.

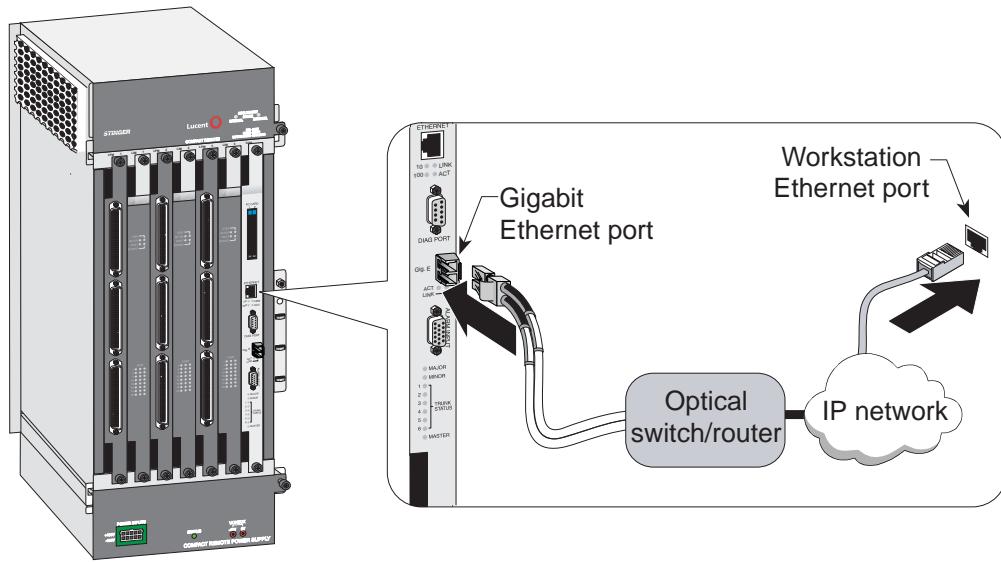
Gigabit Ethernet connection to a workstation console

After the IP address for the Gigabit Ethernet port of a Stinger unit is configured, and the unit is connected to a Gigabit Ethernet network, an administrative Telnet connection can be established through the network. Figure 4-2 shows an Ethernet network connection from the Stinger CR unit to the management workstation.

Initial Stand-alone Configuration

Logging into the IP2000 or control module

Figure 4-3. Gigabit Ethernet connection



To connect a management workstation to the Stinger CR unit using an indirect Ethernet connection:

- 1 Connect the optical fiber to the Gigabit Ethernet port on the IP2000 module.
- 2 Connect the other end of the optical fiber to an optical switch that provides access to the management network.
- 3 Ensure that the management workstation has connectivity to the management network on which the unit resides.
- 4 Ensure the Ethernet transceivers are connected properly to the network.

Logging into the IP2000 or control module

To configure the unit initially, or after clearing its NVRAM, you must connect a workstation to the serial port of the IP2000 or control module (labeled DIAG PORT). Then launch a communications program that supports terminal emulation. Make sure that the terminal emulation settings specify 9600bps, 8 data bits, 1 stop bit, and no parity or flow control.

The default settings for the serial port profile allow anyone connecting to it to access the system as the administrative (admin) user, without logging in or being authenticated. When you connect to an unconfigured Stinger unit to which power has been applied, you are presented with the prompt for the admin user:

```
admin>
```

After you have configured basic IP information, as described in “Providing a basic system IP configuration” on page 4-7, you can access the command-line interface of the Stinger CR unit by using Telnet from an IP host. Or, you can log in by using an SNMP management station from an IP host. These types of connections require that you authenticate a User profile and supply a password to acquire administrative permissions. During basic configuration, Lucent Technologies recommends that you also configure the serial port to require username and password authentication. For details about User profiles, see the *Stinger Administration Guide*.

Restricting administrative access

Each stand-alone Stinger CR unit is shipped from the factory with its security features set to defaults that allow you to easily access the unit so you can configure it without any restrictions. Before you bring the unit online, you must change the default security settings to protect the configured unit from unauthorized access.

Changing defaults for serial-port logins

The factory default setting for the serial interface of the IP 2000 or control module specifies that any connection to that interface will use the `admin` User profile. To help protect the system from unauthorized administrative access on the serial interface, change the following default setting:

```
[in SERIAL/{ shelf-1 control-module 2 }]
user-profile = admin
```

Parameter	Setting
User-Profile	Name of the User profile to be used for logins on the IP2000 module serial port. User profiles set permissions and other parameters for logins to the Stinger CR command-line interface. If no name is specified, the system prompts for both the name and password of a User profile, as it does for Telnet logins.

The TAOS software automatically creates a Serial profile for the serial interface of the IP2000 or control module. To list the Serial profiles, use the `Dir` command as follows:

```
admin> dir serial
13 01/25/2004 02:57:48 { shelf-1 first-control-module 2 }
```

To make serial logins more secure, modify the Serial profile to specify a null User profile name, as shown in the following example. Anyone trying to establish a connection through the serial port is then required to provide a username and password.

```
admin> read serial {1 8 2}
SERIAL/{ shelf-1 first-control-module 2 } read
admin> set user-profile =
admin> write
SERIAL/{ shelf-1 first-control-module 2 } written
```

Changing the default `admin` password

Because the `admin` User profile controls permissions that enable most levels of activity, access to that login must be carefully restricted. To protect the `admin` login, change its well-known default password the first time you log into the unit. Following is the password parameter, shown with its factory default setting:

Initial Stand-alone Configuration

Restricting administrative access

```
[in USER/admin]
password = "Ascend"
```

Parameter	Setting
Password	Text string of up to 20 characters, which must be entered by a user to log in with permissions authorized by the admin profile. The value is case sensitive.

You can specify any password up to 20 characters. All future logins governed by the admin User profile must provide the new password.

For example, the following commands change the admin password to x1!35DPG:

```
admin> read user admin
USER/admin read

admin> set password = x1!35DPG
admin> write
USER/admin written
```

When an administrator Telnets into the Stinger CR unit, the system prompts for the name and password of a User profile and authenticates the information before allowing the Telnet session. For example:

```
% telnet 1.1.1.1
Trying 1.1.1.1...
Connected to 1.1.1.1
Escape character is '^]'.

User: admin
Password: x1!35DPG
```

Setting a Telnet password

A Telnet password is a global, system-wide password required for Telnet logins to the unit. The Telnet password is requested before the system accepts the connection and prompts for the username. Following are the default parameters associated with Telnet logins to a Stinger CR unit:

```
[in IP-GLOBAL]
telnet-password = ""
user-profile = ""
```

Parameter	Setting
Telnet-Password	Text string of up to 20 characters, required from all users requesting a Telnet session. A user is allowed three attempts, with 60 seconds per attempt, to enter the correct password. A third unsuccessful attempt terminates the login process. The value is case sensitive.
User-Profile	Sets the name of a default User profile for authenticating all Telnet logins. If no name is specified, the system prompts the user to enter the name of a User profile.

For example, the following commands set the Telnet password to **dpg01!**:

```
admin> read ip-global
IP-GLOBAL read
admin> set telnet-password = dpg01!
admin> write
IP-GLOBAL written
```

When a Telnet password has been specified, the system requires a two-tier password authentication for Telnet logins, first the Telnet password, then the username and its associated password. For example:

```
% telnet 1.1.1.1
<stinger01> Enter Password: dpg01!
Trying 1.1.1.1...
Connected to 1.1.1.1
Escape character is '^]'.

User: admin
Password: *****
```

If the user enters an incorrect Telnet password, the system prompts again, allowing up to three attempts before timing out. If the user specifies the correct password, the connection is established and the user is prompted to enter the name and password of a valid User profile.

Providing a basic system IP configuration

To enable Telnet and SNMP access to the unit, and to allow connectivity between the unit and local IP hosts, you must assign IP addresses to the Stinger CR Ethernet ports and configure basic IP routing. A basic configuration for remote inband management can be saved in a special file called **default.cfg**. If the basic configuration is saved in this way, the system can restart with the configured remote management capability, even after nonvolatile memory has been cleared with the NVRAM command. For more information about retaining a configuration after clearing NVRAM, see the *Stinger Administration Guide*.

IP address syntax

The Stinger unit uses dotted decimal notation (not hexadecimal) for IP addresses. Netmask information is appended to the IP address after a forward slash (/).

Netmasks

If no netmask is specified, the unit uses a default mask based on the class of the IP address that is supplied. Table 4-1 shows address classes and the number of network bits in the default mask for each class.

Table 4-1. IP address classes and number of network bits

Class	Address range	Default network bits
Class A	0.0.0.0 through 127.255.255.255	8

Initial Stand-alone Configuration

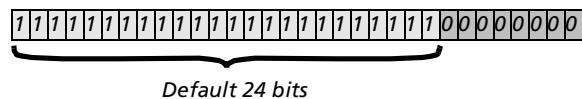
Providing a basic system IP configuration

Table 4-1. IP address classes and number of network bits (Continued)

Class	Address range	Default network bits
Class B	128.0.0.0 through 191.255.255.255	16
Class C	192.0.0.0 through 223.255.255.255	24

For example, a class C address, such as 198.5.248.40, has 24 network bits, leaving 8 bits for the host portion of the address. If no subnet mask is specified for a class C address, the Stinger unit uses the default mask of 24 bits, as shown in Figure 4-4.

Figure 4-4. Default netmask for class C IP address



By default, this address is displayed as 198.5.248.40/24.

Subnets

Subnets are permitted under the same syntax. A subnet address specifies a number of network bits that does not adhere to the Class A, B, or C network limits. For example, the following address specifies a 29-bit subnet:

```
ip-address = 198.5.248.40/29
```

In this address, 29 bits of the address are used to specify the network. The 3 remaining bits are used to specify eight addresses on the subnet. With 3 bits used to specify hosts on a 29-bit subnet, eight different bit combinations are possible. Of those eight possible host addresses, two are reserved:

000 — Reserved for the network (base address)

001

010

100

110

101

011

111 — Reserved for the broadcast address of the subnet

Note Early implementations of TCP/IP did not allow zero subnets (subnets with the same base address as a class A, B, or C network). For example, the subnet 192.32.8.0/30 was illegal because it had the same base address as the class C network 192.32.8.0/24, while the subnet 192.32.8.4/30 was legal. Modern implementations of TCP/IP support zero subnets, and the Stinger implementation of Routing Information Protocol (RIP) treats these subnets the same as any other network. Make sure that you treat zero subnets consistently throughout your network. Otherwise, you might encounter routing problems.

Table 4-2 shows subnet masks and prefix lengths for a class C network.

Table 4-2. Decimal subnet masks and prefix lengths

Subnet mask	Number of host addresses	Prefix length
255.255.255.0	254 hosts + 1 broadcast address, 1 network base address	/24
255.255.255.128	126 hosts + 1 broadcast address, 1 network base address	/25
255.255.255.192	62 hosts + 1 broadcast address, 1 network base address	/26
255.255.255.224	30 hosts + 1 broadcast address, 1 network base address	/27
255.255.255.240	14 hosts + 1 broadcast address, 1 network base address	/28
255.255.255.248	6 hosts + 1 broadcast address, 1 network base address	/29
255.255.255.252	2 hosts + 1 broadcast address, 1 network base address	/30
255.255.255.254	Invalid mask (no hosts)	/31
255.255.255.255	1 host—a host route	/32

The broadcast address of any subnet has the host portion of the IP address set to all 1s (ones). The network address (or base address) represents the network itself, because the host portion of the IP address is all 0s (zeros). For example, suppose that the Stinger configuration assigns the following address to a remote router:

198.5.248.120/29

The Ethernet network attached to that router has the following address range:

198.5.248.120 – 198.5.248.127

A host route is a special-case IP address with a prefix length of /32. For example:

198.5.248.40/32

Host routes are routes to a single host, rather than to a network or subnet. This is determined by the fact that a 32-bit netmask does not allow for any host addresses on the network, other than the single address that is specified. It is, in effect, a one-address subnet.

Assigning the Ethernet IP addresses

A Stinger CR unit creates an IP interface for each Ethernet port of the IP2000 or control module. Use the **Dir** command to list the IP interfaces, as follows:

```
admin> dir ip-interface
18 01/25/2004 16:36:32 { { any-shelf any-slot 0 } 0 }
29 01/25/2004 16:27:57 { { shelf-1 first-control-module 1 } 0 }
18 01/25/2004 23:53:47 { { shelf-1 first-control-module 2 } 0 }
```

Interface number 1 is the 10/100 Ethernet interface. Interface number 2 is the Gigabit Ethernet interface, which will only be seen if an IP2000 module is installed.



Note The IP-Interface profile with the zero index (the default `any-shelf` `any-slot` index) is used for a soft interface. The soft interface can be used to provide a common address for access to redundant IP2000 or control modules in systems that support redundant controlling modules.

The 10/100BaseT Ethernet interface

The 10/100Base T Ethernet interface can be configured to provide a separate connection to a dedicated administrative network. This is common for Stinger units in locations where there is access to a 10/100Base T administrative network.

In this example, the 10/100BaseT interface on the unit is assigned the IP address 1.1.1.1 with a 24-bit netmask:

```
admin> read ip-interface { { shelf-2 8 1 } 0 }
IP-INTERFACE/{ { shelf-1 first-control-module 1 } 0 } read
admin> set ip-address = 1.1.1.1/24
admin> write
IP-INTERFACE/{ { shelf-1 first-control-module 1 } 0 } written
```

After you assign IP addresses, you can verify that the Stinger unit is a valid IP host on its configured network by pinging other network hosts, as shown in the following example:

```
admin> ping 1.1.1.56
PING 1.1.1.56: 56 Data bytes
64 bytes from 1.1.1.56: icmp_seq=0 ttl=255 time=0 ms
64 bytes from 1.1.1.56: icmp_seq=3 ttl=255 time=0 ms
^C
--- 1.1.1.56: Ping statistics ---
2 packets transmitted, 2 packets received, 0% packet loss
round-trip min/avg/max = 0/0/0 ms
```

The IP2000 Gigabit Ethernet interface

In remote locations, where there is no access to a 10/100Base T Ethernet network, connection to an administrative network can be configured for the Gigabit Ethernet port.

In this example, the Gigabit Ethernet interface on the IP2000 is assigned the IP address 1.1.1.2 with a 24-bit netmask:

```
admin> read ip-interface { { shelf-1 8 2 } 0 }
IP-INTERFACE/{ { shelf-1 first-control-module 2 } 0 } read
admin> set ip-address = 1.1.1.2/24
admin> write
IP-INTERFACE/{ { shelf-1 first-control-module 2 } 0 } written
```

After you assign IP addresses, you can verify that the Stinger unit is a valid IP host on its configured network by pinging other network hosts, as shown in the following example:

```
admin> ping 1.1.1.56
PING 1.1.1.56: 56 Data bytes
64 bytes from 1.1.1.56: icmp_seq=0 ttl=255 time=0 ms
```

```
64 bytes from 1.1.1.56: icmp_seq=3 ttl=255 time=0 ms
^C
--- 1.1.1.56: Ping statistics ---
2 packets transmitted, 2 packets received, 0% packet loss
round-trip min/avg/max = 0/0/0 ms
```


Hosted System Configuration

5

Stinger CR configuration overview for hosted operation	5-1
Setting the chassis ID (optional)	5-1
Introduction to the host management interface	5-3
Configuring a hosted Compact Remote system	5-4
Traffic management in hosted Compact Remote systems	5-8
Working with the remote-shelf-config profile	5-11

Stinger CR configuration overview for hosted operation

Stinger Compact Remote configuration tasks for hosted operation include the following:

- Physical configuration of the chassis validation ID (optional)
- Configuration of the software parameters on the host Stinger unit to establish it as a host unit, enable communication with the remote Stinger CR units, and configure their lines (See “Configuring a hosted Compact Remote system” on page 5-4.)
- Defining ATM traffic contracts (See “Traffic management in hosted Compact Remote systems” on page 5-8.)
- Configuring connections, either locally or through RADIUS

Setting the chassis ID (optional)

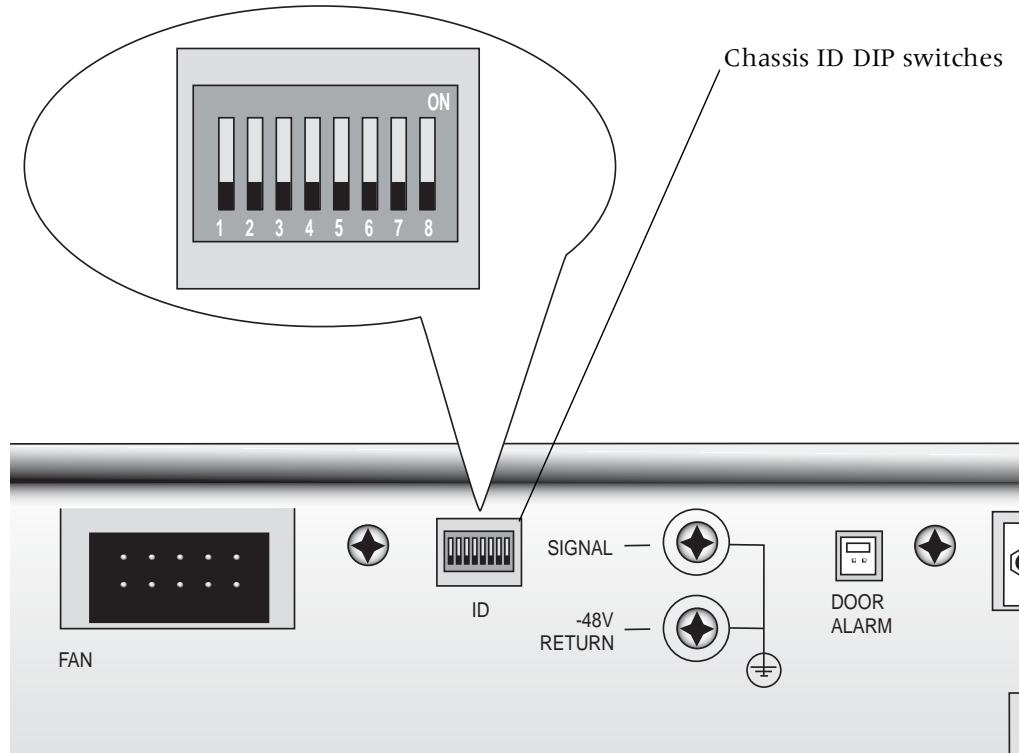
To avoid connecting a Stinger CR unit to the wrong OLIM port on the host, each Stinger CR chassis has a set of eight DIP switches that are used to configure an identification number between 0 and 255 for that chassis. The number configured with these switches can be compared with an identification number that is configured in software on the host Stinger unit. This comparison verifies that a specific Stinger CR chassis has been connected to a specific optical port of an OLIM on the host Stinger unit. Detection of the chassis ID can be enabled or disabled on the host Stinger unit.

The chassis ID DIP switches are located behind the cooling unit in the top rear area of the Stinger CR chassis, as shown in Figure 5-1.

Hosted System Configuration

Setting the chassis ID (optional)

Figure 5-1. Chassis validation ID DIP switches



Each DIP switch represents a single bit in an 8-bit ID number. The switches are configured to provide the binary equivalent of decimal values from 0 (all switches off) to 255 (all switches on). Valid Chassis ID numbers must be from 1 to 255. A chassis ID of 0 is not allowed.

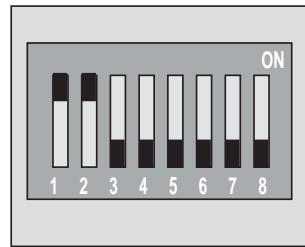
Each switch produces a binary 1, when it is set in the ON position. DIP switch number 1 sets the most significant bit in the binary number produced by these switches. The following table details the binary and decimal value for each of the individual DIP switches.

Table 5-1. Validation ID DIP switch setting values

Switch number	Value on	Value off (binary)	Value on (decimal)
1	1	0	128
2	1	0	64
3	1	0	32
4	1	0	16
5	1	0	6
6	1	0	4
7	1	0	2
8	1	0	1

The decimal value of validation ID is the total of all decimal values for DIP switches that are set to ON. For example, the binary 8-bit ID number created by setting only DIP switches 1 and 2 ON is 11000000. The decimal value of the validation ID produced by this setting is 192. This setting is shown in Figure 5-2.

Figure 5-2. Setting the Validation ID DIP switch



Use the following procedure to set the chassis validation ID DIP switch:

- 1 Verify that power has been removed from the Stinger CR unit.
- 2 Remove the Stinger CR cooling unit as described in “Replacing the chassis cooling module” on page 3-13.
- 3 Use a small probe or jewelers screwdriver to set the desired DIP switches.
- 4 Replace the Stinger CR cooling module as described in “Replacing the chassis cooling module” on page 3-13.

Introduction to the host management interface

All provisioning and management of a hosted Stinger CR is performed on the host. You can *telnet* to the host’s command-line interface through an Ethernet port, or via the ATM management connection over the host system’s trunk interface.

The look and feel of the host management interface is very similar to that of a stand-alone system, except that some commands require that you specify a shelf ID in the physical address of a slot or port. Also, the shelf ID displayed in the output of commands indicates the shelf numbers assigned to remote Stinger CR units. Some commands display extended information for multishelf system management. For details, see “Monitoring the status of remote shelves” on page 6-4.

The *show* command includes information about all shelves with an active control channels to the host. The following command output shows that in addition to the host shelf (shelf ID 1), shelf 2 has an active control channel to the host.

```
HOST> show
Shelf 1 ( master ):
Controller { first-control-module } ( PRIMARY ):
                                         Reqd  Oper  Slot Type
{ second-control-module }    UP    DOWN  ( SECONDARY )
{ shelf-1 slot-1 0 }        UP    UP    stngr-olim-card
{ shelf-1 trunk-module-+ }  UP    UP    oc12-atm-trunk-daughter-card
{ shelf-2 slot-2 0 }        UP    UP    stngr-48-gs-ads1-card
{ shelf-2 first-control+ }  UP    UP    crt-cm
```



Note All configuration profiles reside on and are accessible only on the host system.

You can also use the `open` command to access RLIMs directly from the host. Opening a session to the resources of another unit in the hosted system is useful for diagnosing error conditions, checking configurations, or performing certain maintenance functions, but it cannot be used to provision the hosted system. For example, the following command opens a session with the RLIM in slot 3 of remote shelf 2:

```
HOST>> open 2 3  
dads1-atm-24-2/3>
```

The `open` command can also be used on a remote shelf to open a session to the host. For example, a repair or maintenance technician working at a remote site can open a session to the host to inspect or change the configuration, run diagnostics, or perform certain maintenance functions. In addition, once a session is open to the host, an additional session can be opened from the host back to a remote LIM.

Configuring a hosted Compact Remote system

In a hosted system, the control module in the host is configured as the *host* controller and the remote shelves operate in *hosted* mode. The host controller uses some of the bandwidth of the 155Mbps optical link to a remote shelf for control messages to the remote system resources—for example, to set up virtual circuits, update or create profiles, and manage the remote LIMs (RLIMs). When a hosted COP receives control messages from the host controller, it acts as proxy for the host controller and forwards the messages to the proper RLIM.

The first steps in setting up a hosted system are to install the physical components and cables. For details about installation, see earlier chapters in this guide. Following the initial installation, the Compact Remote shelves come up in the hosted mode, ready to communicate with the master controller over the 155Mbps optical uplink. To configure the hosted system, you must complete the following steps:

- 1 Configure the host unit to operate in host mode, then reset the host unit.
- 2 Identify the remote shelves in the hosted system.
- 3 Enable RLIM and host trunk interfaces.
- 4 Provision virtual circuits.

Optionally, you can also configure CAC procedures for the hosted system, and remote shelf validation. For details, see “Traffic management in hosted Compact Remote systems” on page 5-8, and “Configuring shelf validation” on page 5-13.

Configuring the host system to operate in master mode

To configure the controller in the host Stinger to operate as the master controller, follow these steps:

- 1 If the host previously operated in standalone mode and does not already have a multishelf boot loader installed, you must first perform an upgrade. (See, “Typical hosted system upgrade procedure” on page 6-2, and “Hosted system upgrades that include bootloader code” on page 6-3.) The upgrade instructions in the release note for the new software version will contain additional details.

- 2 Enable master mode in the `system` profile. Following are the required commands:

```
HOST> read system  
HOST> set shelf-controller-type = master  
HOST> write -f
```

The master controller is always shelf 1.

If the system has `remote-shelf-config` profiles for remote shelves, it prevents you from changing the `shelf-controller-type` back to `standalone`. (To do so, you must delete all `remote-shelf-config` profiles.)

- 3 Reset the system.

After a unit's `shelf-controller-type` has been changed, it must be reset for the change to become effective.

Identifying the remote shelves

For each shelf you want to put into service, you need to create and enable a `remote-shelf-config` profile on the host system. The profiles are indexed by shelf ID, and are also accessible via SNMP.

When you enable a `remote-shelf-config` profile for a Compact Remote system, the `oc3-atm` profile for the associated OLIM port is automatically enabled as well. The enabled setting in the `oc3-atm` profile for an OLIM is read-only, and reflects the status of the enabled setting in the associated `remote-shelf-config` profile.

For example, the following steps show how to add a shelf identified as `shelf-7`, which is connected to port 5 of an OLIM in the host's slot 2:

- 1 Create a `remote-shelf-config` profile and assign it a unique shelf number.

```
HOST> new remote-shelf-config  
HOST> set remote-shelf-id = shelf-7
```
- 2 Specify the OLIM port to which the remote shelf is connected.

```
HOST> set host-port physical-address slot = slot-2  
HOST> set host-port physical-address item-number = 5
```
- 3 Enable the control channel to the remote shelf (and configure validation checking if appropriate) and save the profile. For information about validation, see "Configuring shelf validation" on page 5-13.

```
HOST> set enabled = yes  
HOST> set validation-config validation-enable = no  
HOST> write -f
```

- 4 Verify that the control channel is active and the host sees the remote shelf.

It may take up to several minutes to establish an active control channel. When the control channel becomes active, the `show` command output should include the remote shelf. For example:

```
HOST> show  
Shelf 1 ( master ):  
Controller { first-control-module } ( PRIMARY ):  
                                         Reqd  Oper  Slot Type  
{ second-control-module }    UP    DOWN  ( SECONDARY )  
{ shelf-1 slot-1 0 }          UP    UP    stngr-olim-card
```

```
{ shelf-1 trunk-module-+      UP      UP      oc12-atm-trunk-daughter-card
{ shelf-2 slot-2 0 }          UP      LOAD    stngr-48-gs-adsl-card
{ shelf-2 first-control+     UP      UP      crt-cm
```

First the remote shelf COP (crt-cm) is shown in the UP state, and then the host downloads the RLIM image. When the RLIM image has been loaded to the remote shelf, and the RLIM is initialized, the RLIM (stngr-48-gs-adsl-card) will also be in the UP state.

Enabling RLIM and host trunk interfaces

Before you can provision a virtual circuit between an RLIM interface and a host trunk interface, you must make sure that the interfaces are in the UP state. For example, the following steps enable an OC12 interface in the host system and an RLIM port on a remote shelf:

- 1 Enable the interfaces.

For example, the following commands enable a host trunk interface:

```
HOST> read sonet { 1 trunk-module-2 1 }
HOST> set enabled = yes
HOST> write -f
```

The following commands enable an RLIM interface on remote shelf 8, slot 2, port 1:

```
HOST> read a1-dmt { 8 2 1 }
HOST> set enabled = yes
HOST> write -f
```

- 2 Verify that the interfaces are in the UP state.

For example, the following command verifies the UP state of the OC12 interface:

```
HOST> atmtrunks -a
All OC12 ATM trunks:
          OC12 Lines      (dvOp  dvUpSt  dvRq      sAdm  nailg)
  Line    { 1 18 1 }      (Up      Assign   UP      UP      00851)
  ...

```

The next command verifies the UP state of the DSL interface on the remote shelf:

```
HOST> dmtal -u
In-Use DMT ADSL lines:
          (dvOp  dvUpSt  dvRq      sAdm  nailg)
  Line    { 8 2 1 }      (Up      Assign   UP      16101)
  ...

```



Note For complete details about configuring the interfaces on an RLIM, see the *Stinger ADSL Annex A Line Interface Module (LIM) Guide for LIMs with ADSL2+ Capability*. For complete information about configuring the interfaces on an OC12 trunk module, see the *Stinger OC12-ATM Trunk Module Guide*.

Provisioning a virtual circuit from a remote LIM

You use the same profiles and procedure for provisioning virtual circuits in a hosted system as you do on a standalone Stinger. For background information about provisioning virtual circuits, see the *Stinger ATM Configuration Guide*.

When a LIM is initially installed, its interfaces are assigned nailed group numbers using the default allocation shown in Table 5-2.

Table 5-2. Default allocation of unique nailed-group numbers to remote shelves

Shelf number	Default nailed-group range
1 (the host)	1..4000
2	4001..6000
3	6001..8000
4	8001..10000
...	...
25	50001..52000

These default nailed-group numbers can be obtained for any specific interface in the hosted system by using the `which` command. For example, the following command displays the nailed-group number of the RLIM interface on shelf 8, slot 2, port 1:

```
admin> which -n { 8 2 1 }
Nailed group corresponding to port { shelf-8 slot-2 1 } is 16101
```

The following commands provision an ATM circuit from that RLIM DSL interface to a host OC12 interface:

```
HOST> new connection
HOST> set station = pvc-8-2-1
HOST> set atm-options nailed-group = 16101
HOST> set atm-options vci = 55
HOST> set atm-connect-options nailed-group = 851
HOST> set atm-connect-options vci = 55
HOST> write -f
```

You can use standard ATM-related commands, such as `atmvcx` or `atmvcl`, to display connection information in hosted systems. For details, see the *Stinger Administration Guide*. For example, the following command displays information about virtual circuits on shelf 8:

```
HOST> atmvcx -sh 8
Low                                         High
Profile      Kind Intf|Sh|S1|Port|VPI|VCI|Oper  Intf|Sh|S1|Port|VPI|VCI|Oper
                                         Permanent VC X-Connects:
                                         pvc-8-2-1  pvc  13  1  18  1    0  55  up      821  8  2  1    0  55  up
```

Traffic management in hosted Compact Remote systems

In a hosted Compact Remote system, the total amount of LIM bandwidth varies when remote shelves are added or removed. To accommodate this environment, ATM parameters previously located in the `atm-config` profile have been relocated in the `system` or `slot-static-config` profiles, and the `atm-config` profile has been deprecated. A `slot-static-config` profile is created dynamically for an RLIM when the associated `remote-shelf-config` profile is created (written).



Note The system provides a seamless upgrade from earlier releases by relocating existing configurations from the deprecated `atm-config` profile to their new locations, as shown in Table 5-3. The parameters still work as described in the *Stinger ATM Configuration Guide* and *Stinger Reference*.

Table 5-3. New locations for traffic management settings

Deprecated configuration settings	Replacement configuration settings
<code>[in ATM-CONFIG:slot-vpi-vci-range]</code> <code>slot-vpi-vci-range[N]</code>	<code>[in SLOT-STATIC-CONFIG/{ shelf-M slot-N 0 }]</code> <code>vpi-vci-range</code>
<code>[in ATM-CONFIG]</code> <code>cac-preference</code>	<code>[in SYSTEM]</code> <code>cac-preference</code>
<code>[in ATM-CONFIG:bandwidth-config[N]]</code> <code>allow-max-up-stream-bandwidth</code> <code>allow-guaranteed-up-stream-bandwidth</code>	<code>[in SLOT-STATIC-CONFIG/{ shelf-M slot-N 0 }]</code> <code>allow-max-up-stream-bandwidth</code> <code>allow-guaranteed-up-stream-bandwidth</code>
<code>[in ATM-CONFIG:lim-cac-config[N]]</code> <code>enable</code> <code>over-subscription</code>	<code>[in SLOT-STATIC-CONFIG/{ shelf-M slot-N 0 }]</code> <code>port-cac-enable</code> <code>port-cac-oversubscription</code> <code>slot-cac-enable (New)</code> <code>slot-cac-oversubscription (New)</code>
<code>[in ATM-CONFIG:traffic-shapers[N]]</code> <code>enabled</code> <code>bit-rate</code> <code>peak-rate</code> <code>max-burst-size</code> <code>aggregate</code> <code>priority-number</code>	<code>[in SYSTEM:traffic-shapers[N]]</code> <code>enabled</code> <code>bit-rate</code> <code>peak-rate</code> <code>max-burst-size</code> <code>aggregate</code> <code>priority-number</code>

slot-level LIM CAC default behavior

Because upstream data in a hosted system converges at an OLIM slot, slot-level LIM-side CAC is enabled by default via the `slot-cac-enable` parameter. This parameter is found in TAOS 9.6.0 and later versions. LIM port CAC, which operates only at provisioning time, is configured separately and is disabled by default.



Note LIM slot CAC applies to all LIM slots in the host, not just to the OLIM slots. However, only the OLIM aspects of this feature are described in the next section.

Hosted system bandwidth and CAC calculations

For a general description of CAC and how the system uses guaranteed bandwidth values for CAC purposes, see the *Stinger ATM Configuration Guide*. For details about each CAC setting, see the *Stinger Reference*.

Following are the LIM and trunk CAC parameters, shown with default settings:

```
[in SLOT-STATIC-CONFIG/{ shelf-M slot-N 0 }]
allow-guaranteed-up-stream-bandwidth = 42500
port-cac-enable = no
port-over-subscription = 10
slot-cac-enable = yes
slot-over-subscription = 10

[in HIGH-SPEED-SLOT-STATIC-CONFIG/{ shelf-1 trunk-N 1 }:trunk-cac-config[1]]
enable = yes
over-subscription = 10
```

Parameter	Setting
allow-guaranteed-up-stream-bandwidth	Guaranteed upstream bandwidth. The system uses this value for CAC purposes. For information about allocating LIM bandwidth, see the <i>Stinger ATM Configuration Guide</i> .
port-cac-enable	Enable/disable CAC on the LIM's ports.
port-over-subscription	Factor (from 0 to 10,240) by which a LIM port allows oversubscription to the port PHY bandwidth. A value of zero disables port CAC.
slot-cac-enable	Enable/disable CAC on the LIM slot. Slot-level CAC is enabled by default with this new setting.
slot-over-subscription	Factor (from 0 to 10,240) by which a LIM slot allows oversubscription to its provisioned guaranteed upstream bandwidth. A value of zero disables slot CAC.
enable	Enable/disable CAC on the trunk port. Trunk port CAC is enabled by default.
over-subscription	Factor (from 0 to 10,240) by which a trunk port allows oversubscription to its PHY bandwidth.

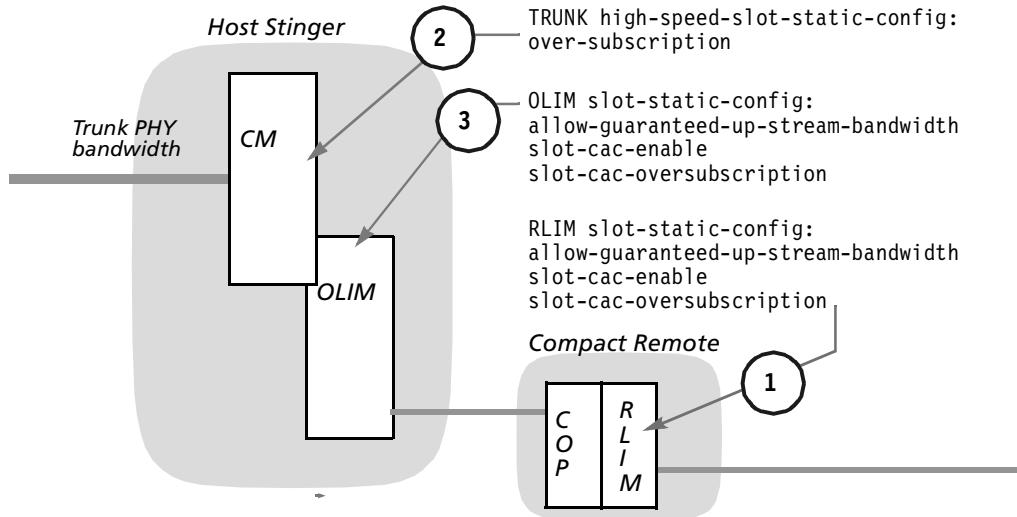
With the default CAC configuration, for an RLIM-to-trunk PVC connection request, the system performs bandwidth calculations in the sequence shown in Figure 5-3:

- 1 RLIM slot bandwidth
- 2 Trunk port bandwidth
- 3 OLIM slot bandwidth

Hosted System Configuration

Traffic management in hosted Compact Remote systems

Figure 5-3. Slot-level CAC bandwidth calculations performed with default settings

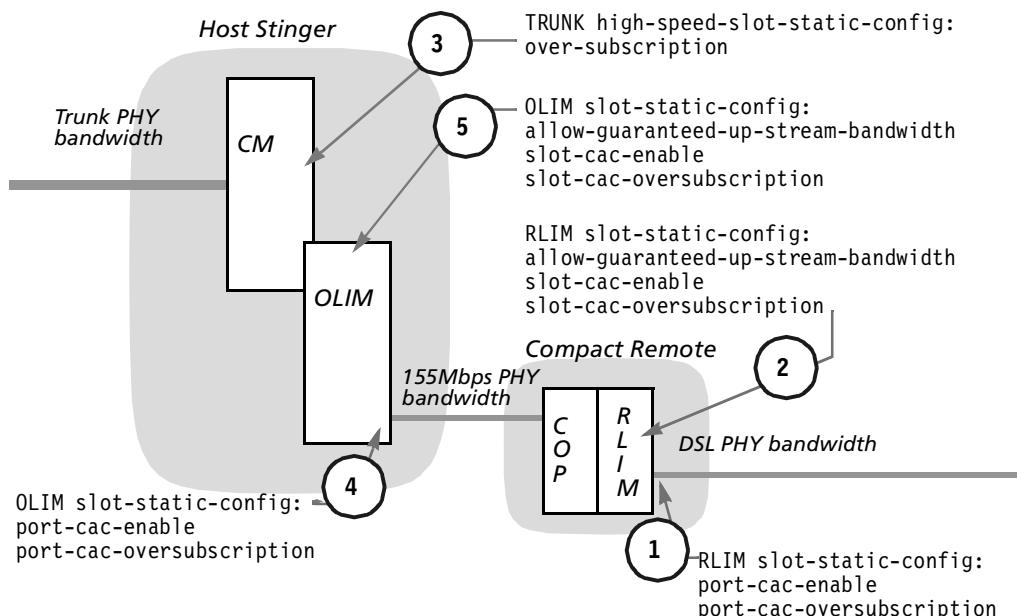


LIM port CAC is disabled by default. To enable it, you must set `cac-preference` to `provisioning-time` system-wide. For details, see the *Stinger ATM Configuration Guide*.

In addition, you must configure the LIM's `slot-static-config` profile by setting `port-cac-enable` to yes, with a nonzero value for `port-over-subscription`.

When port-level CAC is enabled, the system performs two additional CAC calculations before allowing a connection to be provisioned. The port-level CAC sequence is shown in Figure 5-4. If sufficient bandwidth is not available at any one of the calculation points, the connection profile cannot be written.

Figure 5-4. Port-level CAC sequence (performed only at provisioning time)



Upstream traffic shaping in a hosted system

The system shapes traffic in the transmit output direction at the maximum line rate of the host trunk port and at the maximum line rate of each optical interface of every remote COP in the hosted system. The line rate is not configurable for these interfaces. Virtual path shaping, which enables traffic shaping control on a per-VPI basis, can be configured and applied only at the host trunk ports.

For OLIM interfaces and LIM interfaces in the host, and RLIM interfaces in remote shelves, the `allow-max-up-stream-bandwidth` setting provides a configurable maximum line rate for upstream traffic.

Internal queue priorities on an OLIM

With this software version, the queueing mechanisms of both the remote COPs and the OLIM are internal. The system provides non-configurable default queues to maintain priority and preferred scheduling as appropriate for different traffic classes (CBR, rtVBR, and so forth).



Note The system creates `switch-config` profiles for each OLIM installed in the system. However, these profiles are read-only for the OLIM queues and shaping configurations.

LIM-trunk VP switching capacity via an OLIM

Up to a total of 59 LIM-to-trunk virtual path connections can be supported through an OLIM.

Working with the *remote-shelf-config* profile

The *remote-shelf-config* profile resides on the host for enabling control channel communications to remote shelves and (optionally) shelf validation. To identify a remote shelf as part of the hosted system, you must create a *remote-shelf-config* profile and assign a shelf ID that is unique within the system. For example:

```
HOST> new remote-shelf-config shelf-3
HOST> list
[in REMOTE-SHELF-CONFIG/shelf-3 (new)]
remote-shelf-id* = shelf-3
host-port = { { shelf-1 any-slot 0 } 0 }
name = ""
location = ""
enabled = no
remote-shelf-type = stngr-cr-3
validation-config = { yes 0 }
```

Overview of profile contents

Following are the parameters, shown with default settings, for enabling a remote shelf:

```
[in REMOTE-SHELF-CONFIG/""]
remote-shelf-id* = any-shelf
host-port = { { shelf-1 any-slot 0 } 0 }
name = ""
```

```
location = ""
enabled = no
remote-shelf-type = stngr-cr-3
validation-config = { stinger-defined 0 }
```

Parameter	Setting
remote-shelf-id	Remote shelf ID. The setting must be shelf-<i>N</i> , where <i>N</i> is from 2 to 46. Note Although shelf ID numbers may be assigned from 2 to 46, a maximum of 24 CR units are supported by a single Stinger host.
host-port:physical-address	Physical address of the OLIM port to which the remote shelf is linked.
shelf	Shelf ID of the host, which is always 1.
slot	Number of the slot housing the OLIM. The setting must be slot-<i>N</i> , where <i>N</i> is from 1 to 7, or from 10 to 16.
item	Port number on the OLIM, from 1 to 6.
logical-item	Currently, logical interfaces on OLIM ports is not supported.
name	Name of the remote shelf, up to 23 characters. You can use this field to specify a plain text name or a Common Location Language Identifier (CLLIT™) code to uniquely identify each remote shelf in a hosted system.
location	Location of the remote shelf, up to 83 characters. This field is used to specify the physical location of the remote shelf equipment.
enabled	Enables/disables the control channel between the host and remote shelf.
remote-shelf-type	Displays the type of remote shelf. This field is currently read-only. It must always display stngr-cr-3 for Compact Remote shelves.
validation-config	Remote shelf validation configuration. See "Configuring shelf validation" on page 5-13.

Minimal configuration for a remote shelf

For example, the following commands identify a remote shelf 7 connected to the third OLIM port in slot 1, and enable the control channel:

```
HOST> new remote-shelf-config shelf-7
HOST> set host-port physical-address slot = 1
HOST> set host-port physical-address item = 3
HOST> set enabled = yes
HOST> write -f
```

Specifying a remote shelf name and location

You can assign a name or CLLI code to uniquely identify each remote shelf, and specify the shelf's physical location to simplify maintenance procedures.

For example, the following commands specify a name and location for a Stinger Compact Remote:

```
HOST> new remote-shelf-config shelf-7
HOST> set host-port physical-address slot = 1
HOST> set host-port physical-address item = 3
HOST> set name = ZOWISAAASCR
HOST> set location = ZoowieIsland-Saskatchewan
HOST> set enabled = yes
HOST> write -f
```

Configuring shelf validation

Remote shelf validation provides a layer of error checking for indicating if a remote shelf is disconnected from one OLIM port and accidentally reconnected to the wrong OLIM port. This level of error checking is important especially when an OLIM is being replaced or when fibers are being rearranged at a fiber cross-connect panel.

When validation is enabled and a nonzero ID has been assigned in the *remote-shelf-config* profile, the host performs a comparison of the software ID setting and a binary validation ID set manually by using an 8-bit DIP switch on the backplane of the shelf. If the manual setting and the software ID setting do not match, the shelf does not come up as part of the hosted system, and the validation failure is recorded and reported.

The comparison occurs at the moment the control channel is established between the host and remote shelf. For example, it occurs when the remote shelf recovers from a reset or the optical link to the shelf recovers from a failure.

If the validation ID in *remote-shelf-config* is set to zero (the default), validation is not performed for the shelf, regardless of *validation-enable* settings.

If the validation ID in *remote-shelf-config* is set to a nonzero value, validation is performed if validation has been enabled for the shelf.

Following are the parameters for enabling shelf validation and specifying an ID:

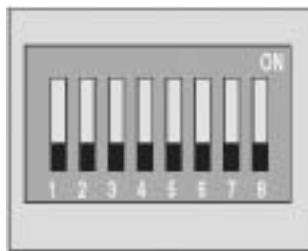
```
[in SYSTEM]
validation-enable = yes
[in REMOTE-SHELF-CONFIG/shelf-M:validation-config]
validation-enable = system-defined
validation-id = 0
```

Parameter	Setting
<code>validation-enable</code>	Enables/disables validation. For the system to perform ID comparison, validation must be enabled and <code>validation-id</code> must also have a nonzero value. In the <code>system</code> profile, valid values are <code>yes</code> and <code>no</code> . In the <code>remote-shelf-config</code> profile, following are valid values: <code>system-defined</code> Use the setting in the <code>system</code> profile to determine if validation is enabled for this shelf. <code>yes</code> Enable validation for this shelf. The <code>system</code> profile setting is not used. <code>no</code> Disable validation for this shelf. The <code>system</code> profile setting is not used.
<code>validation-id</code>	A validation ID, from 1 to 255, to compare against the DIP-switch setting of the remote shelf. With a zero value, the system does not perform validation. With a nonzero value, the system compares the value to the binary DIP-switch setting of the remote shelf. If the values do not match exactly, RLIM service in the remote shelf is disabled. If you specify a nonzero value, it must be unique within the hosted system. If you specify an ID that is already specified for another shelf, the system refuses to write the profile.

In Figure 5-5, the DIP switch is in its factory default setting, with all switches in the OFF (down) position. With the factory default setting, the binary value of the switches is 00000000. Position 1 is the most significant bit and position 8 is the least significant bit of the ID.

For information about setting the DIP switch on a remote shelf, see Chapter 4.

Figure 5-5. Factory-default validation ID setting on Compact Remote



If you set the switch 1 and switch 2 to the ON (up) position, the value of the validation ID becomes 11000000 binary (decimal 192).

The following commands set the host to validate this shelf this shelf with the number (192) that has been configured separately on the Stinger CR DIP switch:

```
HOST> read remote-shelf-config shelf-3  
HOST> set validation-config validation-id = 192  
HOST> write -f
```

This validation setting on the host Stinger is applied when the corresponding hosted Stinger CR unit is reset and the control link to the host unit is reestablished.



Caution Resetting the hosted Stinger unit will interrupt any traffic on the unit while it is restarting.

You may reset a hosted stinger unit with the **reset** command (see “Reset options for hosted systems” on page 6-3). The command shown in the following example will reset a hosted unit that is designated as shelf 3.

```
HOST> reset -s 3
```


Hosted System Management

6

Upgrading hosted system software.....	6-1
Monitoring remote LIMs and connections.....	6-3
Monitoring the status of remote shelves	6-4

This chapter describes some common administrative tasks and describes aspects specifically related to hosted systems. For general system management procedures, see the *Stinger Administration Guide*. For details about specific commands and profiles, see the *Stinger Reference*.

Upgrading hosted system software

To upgrade a hosted Compact Remote system, you must first upgrade the host's software by following the upgrade instructions for the new software version. For a typical upgrade, propagation of the new software to remote shelves can occur automatically, as described in "Typical hosted system upgrade procedure" on page 6-2. This section explains related issues.



Note Always check the specific upgrade instructions for a new software version. This section describes general procedure and requirements.

Required steps before initializing NVRAM in the host

Although you do not normally need to clear nonvolatile random-access memory (NVRAM) for an upgrade, if the upgrade requires this step, follow the instructions in this section.

Before you initialize the host system's NVRAM, you must save basic configuration settings to the `default.cfg` file in the system's flash memory, to enable the system to restore a minimal configuration. For background information about `default.cfg`, see the *Stinger Administration Guide*.



Caution For a hosted system, it's very important to save enough profile information in `default.cfg` to allow the master controller to restore the hosted system framework and recognize the remote shelves. Otherwise, when you load the saved configuration file after clearing NVRAM, the host will drop connection profiles with nailed groups that do not yet exist in the system.

To ensure that the system reestablishes all remote shelves and connections after its NVRAM has been initialized, follow these steps:

- 1 On the host, create a `default.cfg` file with minimal required profiles. For example:
`HOST> save flash 1/default.cfg -p remote-shelf-config system
ip-interface ip-route user`
- 2 Back up the system configuration that contains connection data for RLIMs. For example:
`HOST> save -a network 10.5.63.145 hostcr-config-0930`
- 3 Initialize NVRAM on the host.
`HOST> nvram -f`
- 4 After the host has reinitialized and reset, wait until it has recreated its `remote-shelf-config` and `slot-static-config` profiles.
The `slot-static-config` profiles for RLIMs are created dynamically when the corresponding `remote-shelf-config` profile is written.
- 5 Restore the system configuration containing RLIM connection data. For example:
`HOST> load config network 10.5.63.145 hostcr-config-0930`

Typical hosted system upgrade procedure

Software upgrades usually do not include new bootloader code. For an upgrade that introduces new operational code only, you can allow most of the upgrade procedure to occur automatically between the host and remote shelves.

Following is the general procedure for loading new operational software to host flash from a TFTP server on the network (10.5.63.145 in this example):

- 1 Load the new operational software to host flash:
`HOST> load tar network 10.5.63.145 stgrel.tar`
- 2 Reset the host.
`HOST> reset`

After you reset the host system, it communicates the version and size of its operational code to the remote shelves. When a remote COP detects a difference from its operational code, it downloads the new code from the host automatically.

During the download, the remote shelf COP displays a spinning clock at the console, and a NOTICE log message is displayed on the host. All CLI downloads also are blocked during the control channel loading from the host.

You do not need to reset each remote shelf separately. The system resets the remote COPs automatically when you allow the hosted system to upgrade its remote shelves automatically.



Note Before you reset the host, you can choose to manually load operational code to each remote shelf via the `loadslave` command, to slightly reduce service outage when upgrading. For details about `loadslave` command usage and options, see the *Stinger Reference*.

Hosted system upgrades that include bootloader code

If the new software version requires an upgrade of both the operational code and the bootloader, then in addition to loading the operational code, you must load both the host bootloader and Compact Remote bootloader to host flash. Because the host and the Compact Remote are different types of systems, they cannot share bootloader code.

For example, the following commands load the required software to host flash from a TFTP server on the network (10.5.63.145 in this example):

- 1 Load the new operational code to host flash:
HOST> load tar network 10.5.63.145 stgrel1.tar
- 2 Load the new host bootloader to host flash:
HOST> load boot-cm network 10.5.63.145 stgcmb2.bin
- 3 Load the Compact Remote bootloader to host flash:
HOST> load file network 10.5.63.145 crtcmb.bin

Then, *before resetting the host*, you must use the **loadslave** command to transfer the Compact Remote bootloader (crtcmb.bin) to all remote shelves. For details about the **loadslave** command, see the *Stinger Reference*.

After the transfer of crtcmb.bin to all remote shelves has completed, resetting the host completes the rest of the upgrade automatically, as described in “Typical hosted system upgrade procedure” on page 6-2.

Reset options for hosted systems

From the host, you can reset the host system only, a specific remote shelf, or the entire hosted system. If you use the **reset** command with no options, the default action is to reset all controllers in the hosted system. For example:

HOST> reset

To reset only the master controller (the controller in the host system), use the **-m** option:

HOST> reset -m

To reset a specific remote shelf, use the **-s** option and specify the shelf’s ID. For example, the following command resets shelf 3:

HOST> reset -s 3

Monitoring remote LIMs and connections

Some Stinger administrative commands have been modified to support a shelf-specific option, to allow you to focus on a particular remote shelf rather than obtain a large output for all interfaces or connections in the hosted system. Where appropriate, output of these commands now shows the shelf number, along with slot and port.

Displaying RLIM status

The following new options have been added to Stinger commands for monitoring LIMs, to specify a shelf, or a shelf and slot combination on the command line:

-sh shelf
-s1 shelf slot

These options are not order-dependent, they can appear before or after other options when entering the following commands:

- **ds1lines**
- **dmtalds1lines**
- **hds121ines**
- **sds1lines**
- **shds1lines**
- **vds1lines**

Displaying shelf-specific ATM connection and signaling information

The following new option has been added to commands for monitoring ATM connection and signaling details:

-sh shelf

The following ATM-related commands have been extended to display information about remote shelves in a hosted system:

- **atmvcl**
- **atmvpl**
- **atmvcx**
- **atmvpx**
- **spvcc**
- **spvpc**
- **spvcshow**
- **atmsig**

You can also specify a shelf number with the existing **-s** (slot), **-p** (port), or **-d** (details) options to these commands. If no shelf number is specified, shelf 1 is assumed. For example, the following command shows PVC cross-connects on shelf 2, slot 1:

```
HOST> atmvcx -s 2 1
          Low                               High
Profile    Kind Intf|Sh|S1|Port|VPI|VCI|Oper  Intf|Sh|S1|Port|VPI|VCI|Oper
          Permanent VC X-Connects:
pvc-2-1-1    pvc  11   1  17 1    0   1005 up    311  2   1   1    0   35  up
pvc-2-1-8    pvc  11   1  17 1    0   902  up    318  2   1   8    0   35  up
```

Monitoring the status of remote shelves

The **remote-shelf-stat** profile resides on the host for monitoring remote shelves. The **remoteshelf** command displays information about enabled remote shelves in the hosted system.

You can also set alarms and traps to notify an SNMP management station when certain conditions occur on a remote shelf.

Using the remote-shelf-stat profile

When the host detects an enabled remote shelf, the system creates a remote-shelf-stat profile for the shelf. For example:

```
HOST> dir remote-shelf-stat
0 08/27/2003 16:11:22 shelf-2
0 08/27/2003 16:17:39 shelf-3
0 08/27/2003 16:13:33 shelf-4
```

As with other stat profiles, the remote-shelf-stat profile is read-only, and maintains dynamic state information regarding the remote shelf. It is accessible by SNMP managers. Following are the read-only fields in a profile for shelf 3:

```
[in REMOTE-SHELF-STAT/shelf-3]
remote-shelf-id* = shelf-3
host-port = { { shelf-1 slot-1 3 } 0 }
remote-shelf-oper-state = remote-shelf-oper-state-up
name = ZOWISAAASCR
location = ZoowieIsland-Saskatchewan
internal-fan-unit-failed = no
external-fan-unit-failed = no
door-open = no
over-temperature = no
contact-closure = [ no no no no no no no ]
validation-status = { no 0 0 }

[in REMOTE-SHELF-STAT/shelf-3:host-port]
physical-address = { any-shelf any-slot 0 }
logical-item = 0

[in REMOTE-SHELF-STAT/shelf-3:contact-closure]
contact-closure[1] = no
contact-closure[2] = no
contact-closure[3] = no
contact-closure[4] = no
contact-closure[5] = no
contact-closure[6] = no
contact-closure[7] = no

[in REMOTE-SHELF-STAT/shelf-3:validation-status]
id-valid = no
validation-id-setting = 0
validation-id = 0
```

Parameter	Setting
remote-shelf-id	Shelf ID of the remote shelf represented in this profile.
remote-shelf-oper-state	The state of the remote shelf. The remote-shelf-state-change alarm will be raised when the operational state of the remote shelf goes from UP to DOWN or DOWN to UP state. The reason may be any one of the following values:
remote-shelf-oper-state-down	The remote shelf is down, a non-operational state.

Parameter	Setting
remote-shelf-oper-state-up	The remote shelf is operating normally.
remote-shelf-link-failed	Link failure was detected on the optic link connecting the Compact Remote to the OLIM.
remote-shelf-discovering	Remote shelf discovery in progress.
remote-shelf-discovery-up	Remote shelf discovered.
remote-shelf-ms-link-down	The logical control channel is down between this remote shelf and the host.
name	Name of the remote shelf as configured in the <code>remote-shelf-config</code> profile.
location	Location of the remote shelf as configured in the <code>remote-shelf-config</code> profile.
internal-fan-unit-failed	An alarm was received from the remote shelf fan to indicate a failure of the internal fan unit (yes or no).
external-fan-unit-failed	An alarm was received from the remote shelf fan to indicate a failure of the external fan unit (yes or no).
door-open	An alarm was received from the remote shelf fan to indicate that the door is open (yes or no).
over-temperature	An alarm was received from the remote shelf fan to indicate an over-temperature condition (yes or no).
contact-closure[N]	An array of 7 indexed parameters that indicate the contact closure state (yes if contact closure is detected) on the corresponding remote shelf.
host-port:physical-address	The physical address of the OLIM port to which the remote shelf is linked.
validation-status	Validation status of the remote shelf.
id-valid	Indicates whether the <code>validation-id</code> setting in the <code>remote-shelf-config</code> profile matches the validation ID specified by the remote shelf's DIP-switch setting.
validation-id-setting	The disabled value indicates that no validation was performed. A true setting indicates that validation was done, and the software validation ID setting matched the DIP switch setting. A false setting indicates that validation was done, and the software validation ID setting did not match the DIP switch setting.
validation-id-setting	The physical validation ID set by DIP switches on the remote shelf (from 0 to 255). This value is read from the remote shelf.

Parameter	Setting
validation-id	The validation ID specified in the remote-shelf-config profile. This value is compared against the validation-id-setting from the remote shelf to determine the validation result, which is shown in the id-valid field.

Using the remoteself command

A new remoteself command displays information about enabled remote shelves. It uses the following syntax on a hosted system:

```
HOST> help remoteself
usage: remoteShelf -[s|o] <param>
remoteShelf with no options, show all configured remote shelves
remoteShelf -s <shelf> show detailed information for a single remote shelf
remoteShelf -o <slot> show all remote shelves associated with a given OLIM
slot
```

For example, the following command shows details about remote shelf 2:

```
HOST> remoteself -s 2
Shelf: 2
Shelf Name: ZOWISAAASCR
Shelf Location: ZoowieIsland-Saskatchewan
Shelf Type: 3 slot Compact Remote
Host Port: {{ 1 5 2 } 0 }
Admin State: Enabled
Oper State: OPER_Down
Up Count: 0
Last Up Time: Tue Sep 16 10:08:51 2003
Last down Time: Tue Sep 16 10:08:45 2003
```

If you specify a nonexistent shelf number, the host returns the information that the shelf does not exist in the hosted system. For example:

```
HOST> remoteself -s 5
Remote shelf 5 does NOT exist!
```

The following command shows which shelves are connected to an OLIM in slot 5:

```
HOST> remoteself -o 5
Shelf Name AdminState OperState host-port up-count
2 ZOWISAAASCR Enabled OPER_Down {{ 1 5 2 } 0 } 0
```

Without any options, the command displays all configured remote shelves:

```
HOST> remoteself
Shelf Name AdminState OperState host-port up-count
2 ZOWISAAASCR Enabled OPER_Down {{ 0 0 0 } 0 } 0
```

Raising and clearing alarm events in a hosted system

Alarms triggered by events on remote shelves operate within the existing profile-based alarm infrastructure, which is described in the *Stinger Administration Guide*. If you configure an alarm to be active by setting its value to yes, an action is triggered and volatile profiles are updated. An emergency level log message is generated whenever the alarm is raised or cleared.

Configuring alarms for remote shelves

The following parameter, shown with its default setting, determines the scope of an alarm event in a hosted system:

```
[in ALARM/""]  
physical-address = { any-shelf any-slot 0 }
```

The default setting represents all remote shelves in the hosted system. To specify an alarm event that will be triggered only when it occurs on the host itself, specify shelf 1. For example:

```
HOST> set physical-address shelf = shelf-1
```

To configure an alarm for a specific remote shelf, specify the ID of that shelf. For example, to configure an alarm for shelf 2:

```
HOST> set physical-address shelf = shelf-2
```

An alarm profile specific to a remote shelf is deleted if the `remote-shelf-config` profile for that shelf is deleted, and the corresponding alarms are cleared.

Remote shelf alarm events

Following are events related to Compact Remote shelves:

Table 6-1. Compact Remote alarm events

Alarm event definition	Event on remote shelf that triggers alarm
remote-shelf-state-change	The remote shelf changes state. The new status is shown in the <code>remote-shelf-oper-state</code> setting of the <code>remote-shelf-stat</code> profile.
line-state-change	A change has been detected in the state of a DSL line on the remote shelf.
slot-state-change	A change has been detected in the state of a card in the designated slot of the remote shelf.
fan-failure	A sensor on the remote shelf indicates failure of the internal fan unit. The failed status is shown in the <code>internal-fan-unit-failed</code> setting of the <code>remote-shelf-stat</code> profile.
external-fan-failure	A sensor on the remote shelf indicates failure of the external fan unit. The failed status is shown in the <code>external-fan-unit-failed</code> setting of the <code>remote-shelf-stat</code> profile.
input-relay-closed	Contact-closure sensors on the remote shelf indicate closure. The status is shown in the <code>contact-closure[N]</code> setting of the <code>remote-shelf-stat</code> profile.
input-relay-open	Contact-closure sensors on the remote shelf indicate loss of contact closure. The status is shown in the <code>contact-closure[N]</code> setting of the <code>remote-shelf-stat</code> profile.

Table 6-1. Compact Remote alarm events

Alarm event definition	Event on remote shelf that triggers alarm
over-temperature-relay	A temperature sensor on the remote shelf indicates an over-temperature condition. The status is shown in the over-temperature setting of the remote-shelf-stat profile.
door-open	A sensor on the remote shelf indicates that the door has been opened. The status is shown in the door-open setting of the remote-shelf-stat profile.

Sample alarm for remote shelf 3 state change

The following commands set an alarm for a change in status of shelf 3:

```
HOST> new alarm shelf-3
HOST> set enabled = yes
HOST> set event = remote-shelf-state-change
HOST> set physical-address shelf = shelf-3
HOST> write -f
```

If the alarm is triggered (for example, if shelf 3 becomes unavailable), an emergency log message is displayed. For example:

```
LOG emergency, Shelf 1, Controller-1, Time: 14:26:35--
Wed Sep 17 14:26:35 2000 - ALARM: Remote Shelf { 3 } Alarm is: Active
```

The following alarm command shows that an alarm has been set and the remote shelf is down:

```
HOST> alarm -s
      Type          Address      State
      Remote Shelf Down    { 3 }      Active
```

When the shelf changes state again, for example, when it comes up or is disabled in the remote-shelf-config profile, the alarm is cleared. for example:

```
LOG emergency, Shelf 1, Controller-1, Time: 14:28:16--
Wed Sep 17 14:28:16 2000 - ALARM: Remote Shelf { 3 } Alarm is: Cleared
```

```
HOST> alarm -s
      Type          Address      State
```

Sample alarm for input-relay closure status on any remote shelf

The following commands configure an alarm for input-relay closure on any remote shelf in a hosted system:

```
HOST> new alarm closed
HOST> set enabled = yes
HOST> set event = input-relay-closed
HOST> write -f
HOST> new alarm open
HOST> set enabled = yes
```

```
HOST> set event = input-relay-open
```

```
HOST> write -f
```

If one of the alarms is triggered, the alarm action takes effect, and the `remote-shelf-stat` profile is updated. In addition, the status is accessible in the output of the `alarm -s` command. For example, the following output shows contact closure on shelf 2:

```
HOST> alarm -s
```

Type	Address	State
Input Relay Closed	{ 2 0 1 }	Active
Input Relay Closed	{ 2 0 2 }	Active
Input Relay Closed	{ 2 0 3 }	Active
Input Relay Closed	{ 2 0 4 }	Active
Input Relay Closed	{ 2 0 5 }	Active
Input Relay Closed	{ 2 0 6 }	Active
Input Relay Closed	{ 2 0 7 }	Active

Sample alarm for internal fan failure on shelf 2

The next commands set an alarm for failure of the internal fan unit on shelf 2:

```
HOST> new alarm fan
```

```
HOST> set enabled = yes
```

```
HOST> set event = fan-failure
```

```
HOST> set physical-address shelf = shelf-2
```

```
HOST> write -f
```

If the alarm is triggered, the alarm action takes effect, and the `remote-shelf-stat` profile is updated. In addition, the status is accessible in the output of the `alarm -s` command. For example:

```
HOST> alarm -s
```

Type	Address	State
Fan Failure	{ shelf - 2 }	Active

Enabling traps for remote-shelf events

When you have configured a trap profile to generate a trap protocol data unit (PDU) on detection of a certain event, if the event occurs, the system sends a PDU to a specified SNMP station. For hosted systems, the host sends trap PDUs generated by any shelf in the system. For background information about traps, see the *Stinger Administration Guide*.

Trap optimization

To streamline the number of traps generated by remote shelves, you can enable trap optimization. Trap optimization behavior depends on the settings of the following parameters, shown with default values:

```
[in TRAP/""]
trap-optimization-enabled = no
slot-enabled = no
linkdown-enabled = yes
```

```
linkup-enabled = yes
ascend-link-down-trap-enabled = no
ascend-link-up-trap-enabled = no
```

To fully enable trap optimization, set all these fields to yes. For example:

```
HOST> read trap dsl-snmp
HOST> set trap-optimization-enabled = yes
HOST> set slot-enabled = yes
HOST> set ascend-link-down-trap-enabled = yes
HOST> set ascend-link-up-trap-enabled = yes
HOST> write -f
```

The following trap optimizations are made:

- LinkUp and LinkDown traps are not generated unless `ascend-link-down-trap-enabled` and `ascend-link-up-trap-enabled` are set to no.
- AscendLinkUp traps are not generated in the case of slots coming up and system reset. In these cases, the `ascendLinkUp` trap will not be sent for 120 seconds after the slot comes up.
- AscendLinkDown traps are not generated in the case of slots going down.
- The `sysSlotStateChange` trap is generated only for the slot status changes to `operStateDown` or `operStateUp`. The trap is not sent for other intermediate states such as `operStateLoading` and `operStatePost`.
- If `trap-optimization-enabled` is set to yes but `slot-enabled` is set to no, the system generates `ascendLinkDown` and `ascendLinkUp` traps for each line when a slot changes state, and does not generate the `sysSlotStateChange` trap.

Modified traps to include shelf numbers

Several traps have been modified to include the value of the shelf number along with the slot index for events such as a card reset, slot state change, system clock change, flash state change, CAC failure, or ATM OAM loopback time-out. In addition, new traps have been introduced for events and state changes on remote shelves.

Enabling remote shelf watchdog warning traps

To enable the system to send traps related to sensors on remote shelves, the following parameters must be set to yes (their default value):

```
[in TRAP/""]
remote-shelf-enabled = yes
watchdog-warning-enabled = yes
```

Remote shelf watchdog profiles are created and deleted on the host depending on the operational state of the `remote-shelf-stat` profile for that shelf. These profiles are indexed using the `shelf-number` \times 1000 + the unit value on the remote shelf. For example, 4001 = 4 \times 1000 + 1.

For example:

```
HOST> dir watchdog
31 11/05/2003 21:29:06 { fan fantray 1 }
31 11/05/2003 21:29:06 { fan fantray 2 }
31 11/05/2003 21:29:06 { fan fantray 3 }
```

```
24 11/06/2003 00:22:27 { fan fantray 4001 }
33 11/06/2003 00:24:08 { relay cm-input-relay 4001 }
33 11/06/2003 00:22:27 { relay cm-input-relay 4002 }
33 11/06/2003 00:22:27 { relay cm-input-relay 4003 }
33 11/06/2003 00:22:27 { relay cm-input-relay 4004 }
33 11/06/2003 00:22:27 { relay cm-input-relay 4005 }
33 11/06/2003 00:22:27 { relay cm-input-relay 4006 }
33 11/06/2003 00:22:27 { relay cm-input-relay 4007 }
37 11/05/2003 21:29:07 { cbus shelf-controller 0 }
40 11/06/2003 00:22:27 { over-temperature cm-input-relay 4001 }
34 11/06/2003 00:22:27 { external-fan cm-input-relay 4001 }
26 11/06/2003 00:22:27 { door cm-input-relay 4001 }
```

The next commands configure a trap profile to support these watchdog warnings on a remote shelf, to be sent to an SNMP station at IP address 10.10.10.1:

```
HOST> new trap 10.10.10.1
HOST> set host-address = 10.10.10.1
HOST> set alarm-enabled = yes
HOST> set remote-shelf-enabled = yes
HOST> set watchdog-warning-enabled = yes
HOST> write -f
```

Stinger CR Intended Use

A

User line interfaces	A-1
COP interfaces	A-1
IP2000 interfaces	A-2

The Stinger CR unit is a remote Stinger unit that operates in hosted mode to extend the capability of a host Stinger DSL ATM switch. It provides DSL connections for individual users that are too far from the Stinger host to be directly connected to it.

Users connect to the Stinger CR over DSL lines supported by line interface modules (LIMs) that are installed in the Stinger CR unit. Every Stinger CR unit contains a special COP module that controls the operation of the unit and provides an OC3 link to the host Stinger unit. The physical interfaces on the unit provide DSL or ATM network connections to digital lines, and a serial connection for configuration and administration, an OC3 optical port, and an interface for monitoring the alarm status of other devices.

User line interfaces

The 48-port low-power ADSL LIM designed for use with the Stinger Compact Remote allow users to connect to the Stinger unit over DSL lines supporting the following DSL protocols:

- G.992.3 Annex A (G.dmt.bis)
- G.992.4 Annex A (G.lite.bis)
- G.992.5 Annex A (G.adsl2plus)

User connection to each LIM is provided through an associated line protection module (LPM).

COP interfaces

The COP is equipped with the following interfaces:

- A DB-9 female connector for an RS-232 serial connection, with the following default settings:
 - 9600bps
 - Direct connection
 - 8 data bits

- No parity
- 1 stop bit
- No flow control
- A DB-9 female connector for alarm monitoring connections.
- A duplex LC connector for optical connection.

IP2000 interfaces

The IP2000 is equipped with the following interfaces:

- A DB-9 female connector for an RS-232 serial connection, with the following default settings:
 - 9600bps
 - Direct connection
 - 8 data bits
 - No parity
 - 1 stop bit
 - No flow control
- A DB-9 female connector for alarm monitoring connections (revision 2 control modules).
- An RJ-45 connector for a 10/100BaseT Ethernet connection.
- An RJ-11 connector for the optional internal modem.
- A PCMCIA interface, designed to accept PCMCIA flash-memory cards. Other PCMCIA devices are not supported.
- A duplex LC connector for optical connection.

Control module interfaces

The control module is equipped with the following interfaces:

- A DB-9 female connector for an RS-232 serial connection, with the following default settings:
 - 9600bps
 - Direct connection
 - 8 data bits
 - No parity
 - 1 stop bit
 - No flow control
- A DB-9 female connector for alarm monitoring connections (revision 2 control modules).
- An RJ-45 connector for a 10/100BaseT Ethernet connection.
- An RJ-11 connector for the optional internal modem.
- A PCMCIA interface, designed to accept PCMCIA flash-memory cards. Other PCMCIA devices are not supported.

The Host Stinger OLIM

**B**

Introducing the Stinger OLIM	B-1
Installing an OLIM	B-1
Interpreting OLIM status lights	B-2
OLIM specifications	B-3
Configuring a Stinger OLIM	B-4

The optical line interface module (OLIM) provides six 155.52-Mbps fiber optic interfaces for connections between a Stinger host unit and up to six hosted Stinger Compact Remote units acting as remote shelves.

Introducing the Stinger OLIM

Each 155Mbps optical connection to an OLIM carries user data traffic and control channel data from a hosted Stinger Compact Remote unit. The control channel data integrates the configuration and management of hosted Stinger CR units into the TAOS interface of the host Stinger unit. The hosted units are configured in the TAOS interface of the host Stinger as remote shelves.

Installing an OLIM

A host Stinger unit can support up to 24 hosted Stinger CR units with four fully utilized OLIMs or a greater number of partially utilized OLIMs. The procedure for installing an OLIM in the host Stinger chassis is identical to the installation procedure for any other LIM. See the *Getting Started Guide* for the host Stinger unit for detailed LIM installation instructions.

After installing the OLIM and connecting the optical links to the COPs of Stinger Compact Remote units, you verify the status of the card and its connections by checking the status lights.

Interpreting OLIM status lights

The OLIM has status lights that indicate the overall status of the card and each of its six optical interfaces. Figure B-1 shows the Stinger OLIM.

Figure B-1. the Stinger OLIM



Table B-1 lists the OLIM status light indications.

Table B-1. OLIM status lights

Light	Color	Indication
Fault	Red	At startup—the card is performing its POST test. During operation—the card has failed.
FAC 1 through FAC 6	Green	The associated interface 1 through 6 is operating properly
	Yellow	The associated interface 1 through 6 is not connected or the connection has failed
	Off	The associated interface 1 through 6 is not configured for a hosted Stinger CR unit

OLIM specifications

The Stinger OLIM provides up to six 155.52-Mbps ports for optical connections. Table B-2 lists Stinger OLIM specifications.

Table B-2. OLIM specifications

Category	Specifications
Physical dimensions	Height: 15 inches (38.1 cm). Width: 1.06 inches (2.69 cm). Depth: 9 inches (22.8 cm). Weight: 4 pounds (1.8 kg).
Power requirements	24.24 W.
Ambient temperature range	-40°C to 46°C (-40°F to 114.8°F)
Operating humidity	0% to 90%, noncondensing.
Agency approvals	Electromagnetic Emissions Certifications: FCC Part 15 Class A, and CISPR Class A.
Physical connectors	LC small form factor connector. (For connector details, see “Optical connectors” on page C-20.)
Physical interfaces	Six UNI 3.0/3.1 cell-bearing 155.52-Mbps ports (optical).
Maximum modules	Four fully utilized per unit, or up to 24 active connections to Stinger Compact Remote hosted units.

Table B-2. OLIM specifications (Continued)

Category	Specifications
Signal distance/levels (single-mode laser optics)	Medium-Reach: <ul style="list-style-type: none">■ Up to 15 kilometers (9.3 miles).■ TX power: -15dBm to -8dBm.■ RX Sensitivity: -8dBm, -28dBm.■ Nominal wavelength: 1310 nanometers.
Minimum bend radius	3 inches (7.62 cm).

Configuring a Stinger OLIM

Each OLIM supports six 155.52 Mbps-interfaces, and each interface connects to one Stinger Compact Remote hosted unit. After installation of the OLIM in a host Stinger unit, it is only necessary to identify the remote shelves that will be connected to it and the ports to which they will be connected. It is not necessary to configure specific parameters of the optic interfaces on the OLIM.

See Chapter 5 for detailed information about identifying remote shelves on the Stinger host and associating them with the optical interfaces on the OLIM.

Cables and Connectors



Diagnostic port and cable pinouts	C-1
Alarm input port pinouts	C-2
Stinger CR cabling for the 48-port LPM with splitters	C-2
Protection block power connections	C-17
Chassis door alarm connections	C-18
Enclosure cable exit points	C-19

Diagnostic port and cable pinouts

The diagnostic port uses a standard DB-9 female connector that conforms to the EIA RS-232 standard for serial interfaces. Table C-1 applies to all Stinger CR units that use the diagnostic port of the module in the COP slot for initial configuration.

Table C-1. Control port and cable pinouts

DB-9 pin number	RS-232 signal name	Function	I/O
1	DCD	Data Carrier Detect	O
2	RD	Serial Receive Data	O
3	SD	Serial Transmit Data	I
4	DTR	Data Terminal Ready	I
5	GND	Signal Ground	
6	DSR	Data Set Ready	O
7	RTS	Request to Send	I
8	CTS	Clear to Send	O

Cables and Connectors

Alarm input port pinouts

Table C-1. Control port and cable pinouts (Continued)

DB-9 pin number	RS-232 signal name	Function	I/O
9*	RI	Ring Indicator	O

*. Pin 9 is not active. (Ring Indication signal not supplied.)

Alarm input port pinouts

The ALARM port on the module in the COP slot consists of a DB-15 female connector that can monitor up to 7 external alarm conditions. This connector provides seven pairs of pins that can be connected to the alarm relays of up to seven external devices. Operation or nonoperation of the relays or switches associated with these connections is sensed by the TAOS software, based on continuity or lack of continuity between the pair of pins to which it is connected.

The sensing connections apply 3.3Vdc at less than 10mA through the closed contacts of the remote relay or switch. The cable associated with this connector must consist of 24-gauge to 28-gauge conductors.

Stinger CR units that are equipped with an IP2000 or control module for stand-alone operation are also equipped with a cable that attaches the ALARM port directly to the enclosure door alarm switch. This cable uses the first pair of pins on the ALARM port to detect the condition of the door alarm switch.

Table C-2 provides the pinouts for the DB-15 alarm input port.

Table C-2. Alarm input pinouts

Alarm Number	Sensing Connection	Ground Connection
Alarm 1*	Pin 1	Pin 2
Alarm 2	Pin 3	Pin 4
Alarm 3	Pin 5	Pin 6
Alarm 4	Pin 7	Pin 8
Alarm 5	Pin 10	Pin 11
Alarm 6	Pin 12	Pin 13
Alarm 7	Pin 14	Pin 15

*. Dedicated to the enclosure door alarm on stand-alone Stinger CR units.

Stinger CR cabling for the 48-port LPM with splitters

The cabling for the 48-port LPM with splitters extends the POTs and DSL connections from the LPM through protection blocks in the enclosure to three cable stubs. The

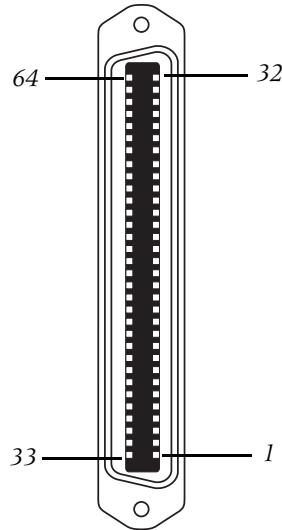
protection blocks protect the Stinger hardware from voltage spikes and transient conditions on the copper facilities that could damage the Stinger hardware.

The following information details the association between the connection points of circuits on each LPM, and their location on the protection blocks. It also details the termination of circuits from the protection blocks on the three cable stubs that exit the Stinger CR enclosure.

LPM connectors

The 48-port LPM with splitters has three 64-pin connectors, labeled P2801, P2802, and P2803. This connector is detailed in Figure C-1.

Figure C-1. LPM 64-pin connector



On each LPM, the bottom connector (P2801) provides 32 connections for subscriber voice-over-DSL connections. The top connector (P2803) provides 32 connections for analog POTS service from the telephone switch. The connector in the middle (P2802) provides the remaining 16 voice-over-DSL and 16 POTS connections.

LPM connections and protection blocks

There are three pairs of protection blocks in the Stinger CR enclosure. Each pair of protection blocks is pre-wired with three 64-pin connectors for connection to one of the LPMs in the Stinger CR card cage.

LPM cables

Each pair of protection blocks has a set of three cables for connection to the 64-pin connectors on an LPM. These cables and connectors are illustrated in Figure C-2.

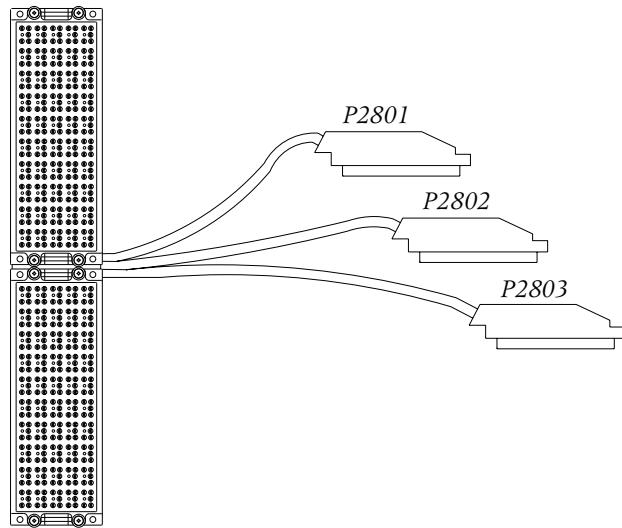


Note Figure C-2 is not an exact representation of the length or position of the cables connected to the protection blocks.

Cables and Connectors

Stinger CR cabling for the 48-port LPM with splitters

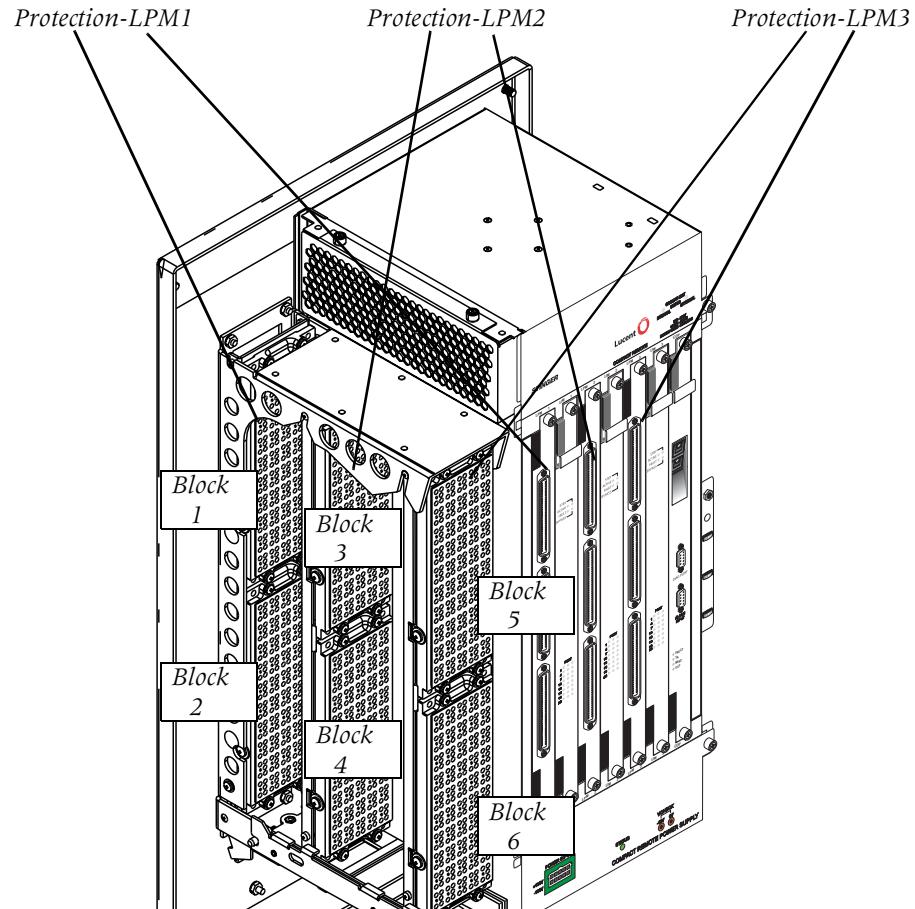
Figure C-2. Protection block cables



LPM to protection block associations

Each LPM is associated with a different pair of protection blocks as indicated in Figure C-3 and Figure C-4.

Figure C-3. LPMs and related protection blocks





Note The protection blocks pairs are articulated so that protection blocks P5/P6 and P3/P4 can be rotated down and toward the enclosure opening to provide access to all three pairs of protection blocks. See instructions on the enclosure door for details.

Protection block Port numbering vs. TAOS port indexing

Each LIM/LPM pair supports 48 ports. These ports are referred to by the TAOS software as ports 1 through 48 indexed by the shelf and slot in which the LIM that supports these ports is installed. The TAOS software refers to these ports as {shelf-n slot-1 1} through {shelf-n slot-1 48}. Lines through P1 and P2 are identified by TAOS as ports {shelf-n slot-1 1} through {shelf-n slot-1 48}. Lines through P3 and P4 are identified by TAOS as ports {shelf-n slot-2 1} through {shelf-n slot-2 48}. Lines through P5 and P6 are identified by TAOS as ports {shelf-n slot-3 1} through {shelf-n slot-3 48}.

An illustration on the enclosure door shows the ports for all three slots numbered continuously on the protection blocks. Figure C-4 shows this port numbering system. Protectors shown as IN are associated with pairs that bring analog POTS service into the Stinger CR from the central office. Protectors shown as OUT are associated with the pairs that carry combined ADSL/POTS service to individual subscribers.

Figure C-4. Protection block port assignments

LPM 1
LPM 2
LPM 3

P1
P3
P5

P2
P4
P6

IN
IN
IN

1
11
21
31
41

2
12
22
32
42

3
13
23
33
43

4
14
24
34
44

5
15
25
35
45

6
16
26
36
46

7
17
27
37
47

8
18
28
38
48

9
19
29
39
PWR

10
20
30
40
PWR

IN
IN
IN
IN
IN

49
59
69
79
89

50
60
70
80
90

51
61
71
81
92

52
62
72
82
92

53
63
73
83
93

54
64
74
84
94

55
65
75
85
95

56
66
76
86
96

57
67
77
87
PWR

58
68
78
88
NC

IN
IN
IN
IN
IN

97
107
117
127
137

98
108
118
128
138

99
109
119
129
139

100
110
120
130
140

101
111
121
131
141

102
112
122
132
142

103
113
123
133
143

104
114
124
134
144

105
115
125
135
NC

106
116
126
136
NC

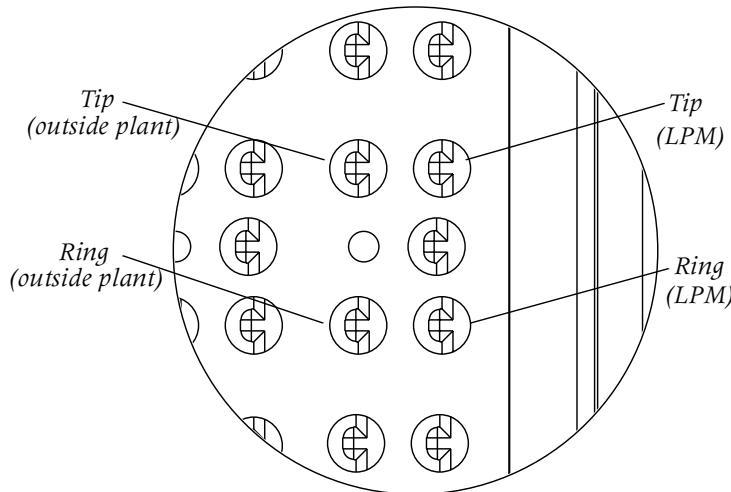
Cables and Connectors

Stinger CR cabling for the 48-port LPM with splitters

Protector orientation details

The cables from the LPMs connect to the protected (inside) side of the protection blocks. Another group of cables connect the unprotected (outside) side of the protection blocks to the copper facilities. The tips and rings of the outside plant cables and the LPM cables terminate on the protection plugs of the protection blocks as shown in Figure C-5.

Figure C-5. Protection plug orientation example



For information about the type of protection elements that should be installed, see “Protection block elements” on page D-2.

Connection block LPM cable associations

Each pair of protection blocks have similar cable connections to an LPM in the Stinger unit. The connection of the LPM connectors P2801, P2802, and P2803 to the protection blocks is described in Table C-3 and Table C-4.

LPM connections for the top protection block (blocks 1, 3, and 5) are detailed in Table C-3. When a T1/IMA LIM is installed in one of the LIM slots, up to 24 4-wire ports are supported and mapped as shown. The numbering for protectors on P1, P3, and P5 corresponds to the protector numbering in Figure C-4 on page C-5.

Table C-3. Tip/Ring connections to protection blocks 1, 3, and 5

P1 (LPM 1)	P3 (LPM 2)	P5 (LPM 3)	LPM connector	Pin No.	LPM 2-wire ports	LPM 4-wire ports
1T	49T	97T	P2801	33	1T(ADSL)	1T(XMT)
1R	49R	97R	P2801	1	1R(ADSL)	1R(XMT)
2T	50T	98T	P2801	34	2T(ADSL)	1T(RCV)
2R	50R	98R	P2801	2	2R(ADSL)	1R(RCV)
3T	51T	99T	P2801	35	3T(ADSL)	2T(XMT)

Table C-3. Tip/Ring connections to protection blocks 1, 3, and 5 (Continued)

P1 (LPM 1)	P3 (LPM 2)	P5 (LPM 3)	LPM connector	Pin No.	LPM 2-wire ports	LPM 4-wire ports
3R	51R	99R	P2801	3	3R(ADSL)	2R(XMT)
4T	52T	100T	P2801	36	4T(ADSL)	2T(RCV)
4R	52R	100R	P2801	4	4R(ADSL)	2R(RCV)
5T	53T	101T	P2801	37	5T(ADSL)	3T(XMT)
5R	53R	101R	P2801	5	5R(ADSL)	3R(XMT)
6T	54T	102T	P2801	38	6T(ADSL)	3T(RCV)
6R	54R	102R	P2801	6	6R(ADSL)	3R(RCV)
7T	55T	103T	P2801	39	7T(ADSL)	4T(XMT)
7R	55R	103R	P2801	7	7R(ADSL)	4R(XMT)
8T	56T	104T	P2801	40	8T(ADSL)	4T(RCV)
8R	56R	104R	P2801	8	8R(ADSL)	4R(RCV)
9T	57T	105T	P2801	41	9T(ADSL)	5T(XMT)
9R	57R	105R	P2801	9	9R(ADSL)	5R(XMT)
10T	58T	106T	P2801	42	10T(ADSL)	5T(RCV)
10R	58R	106R	P2801	10	10R(ADSL)	5R(RCV)
11T	59T	107T	P2801	43	11T(ADSL)	6T(XMT)
11R	59R	107R	P2801	11	11R(ADSL)	6R(XMT)
12T	60T	108T	P2801	44	12T(ADSL)	6T(RCV)
12R	60R	108R	P2801	12	12R(ADSL)	6R(RCV)
13T	61T	109T	P2801	45	13T(ADSL)	7T(XMT)
13R	61R	109R	P2801	13	13R(ADSL)	7R(XMT)
14T	62T	110T	P2801	46	14T(ADSL)	7T(RCV)
14R	62R	110R	P2801	14	14R(ADSL)	7R(RCV)
15T	63T	111T	P2801	47	15T(ADSL)	8T(XMT)
15R	63R	111R	P2801	15	15R(ADSL)	8R(XMT)
16T	64T	112T	P2801	48	16T(ADSL)	8T(RCV)

Cables and Connectors*Stinger CR cabling for the 48-port LPM with splitters*

Table C-3. Tip/Ring connections to protection blocks 1, 3, and 5 (Continued)

P1 (LPM 1)	P3 (LPM 2)	P5 (LPM 3)	LPM connector	Pin No.	LPM 2-wire ports	LPM 4-wire ports
16R	64R	112R	P2801	16	16R(ADSL)	8R(RCV)
17T	65T	113T	P2801	49	17T(ADSL)	9T(XMT)
17R	65R	113R	P2801	17	17R(ADSL)	9R(XMT)
18T	66T	114T	P2801	50	18T(ADSL)	9T(RCV)
18R	66R	114R	P2801	18	18R(ADSL)	9R(RCV)
19T	67T	115T	P2801	51	19T(ADSL)	10T(XMT)
19R	67R	115R	P2801	19	19R(ADSL)	10R(XMT)
20T	68T	116T	P2801	52	20T(ADSL)	10T(RCV)
20R	68R	116R	P2801	20	20R(ADSL)	10R(RCV)
21T	69T	117T	P2801	53	21T(ADSL)	11T(XMT)
21R	69R	117R	P2801	21	21R(ADSL)	11R(XMT)
22T	70T	118T	P2801	54	22T(ADSL)	11T(RCV)
22R	70R	118R	P2801	22	22R(ADSL)	11R(RCV)
23T	71T	119T	P2801	55	23T(ADSL)	12T(XMT)
23R	71R	119R	P2801	23	23R(ADSL)	12R(XMT)
24T	72T	120T	P2801	56	24T(ADSL)	12T(RCV)
24R	72R	120R	P2801	24	24R(ADSL)	12R(RCV)
25T	73T	121T	P2801	57	25T(ADSL)	13T(XMT)
25R	73R	121R	P2801	25	25R(ADSL)	13R(XMT)
26T	74T	122T	P2801	58	26T(ADSL)	13T(RCV)
26R	74R	122R	P2801	26	26R(ADSL)	13R(RCV)
27T	75T	123T	P2801	59	27T(ADSL)	14T(XMT)
27R	75R	123R	P2801	27	27R(ADSL)	14R(XMT)
28T	76T	124T	P2801	60	28T(ADSL)	14T(RCV)
28R	76R	124R	P2801	28	28R(ADSL)	14R(RCV)
29T	77T	125T	P2801	61	29T(ADSL)	15T(XMT)

Table C-3. Tip/Ring connections to protection blocks 1, 3, and 5 (Continued)

P1 (LPM 1)	P3 (LPM 2)	P5 (LPM 3)	LPM connector	Pin No.	LPM 2-wire ports	LPM 4-wire ports
29R	77R	125R	P2801	29	29R(ADSL)	15R(XMT)
30T	78T	126T	P2801	62	30T(ADSL)	15T(RCV)
30R	78R	126R	P2801	30	30R(ADSL)	15R(RCV)
31T	79T	127T	P2801	63	31T(ADSL)	16T(XMT)
31R	79R	127R	P2801	31	31R(ADSL)	16R(XMT)
32T	80T	128T	P2801	64	32T(ADSL)	16T(RCV)
32R	80R	128R	P2801	32	32R(ADSL)	16R(RCV)
33T	81T	129T	P2802	33	33T(ADSL)	17T(XMT)
33R	81R	129R	P2802	1	33R(ADSL)	17R(XMT)
34T	82T	130T	P2802	34	34T(ADSL)	17T(RCV)
34R	82R	130R	P2802	2	34R(ADSL)	17R(RCV)
35T	83T	131T	P2802	35	35T(ADSL)	18T(XMT)
35R	83R	131R	P2802	3	35R(ADSL)	18R(XMT)
36T	84T	132T	P2802	36	36T(ADSL)	18T(RCV)
36R	84R	132R	P2802	4	36R(ADSL)	18R(RCV)
37T	85T	133T	P2802	37	37T(ADSL)	19T(XMT)
37R	85R	133R	P2802	5	37R(ADSL)	19R(XMT)
38T	86T	134T	P2802	38	38T(ADSL)	19T(RCV)
38R	86R	134R	P2802	6	38R(ADSL)	19R(RCV)
39T	87T	135T	P2802	39	39T(ADSL)	20T(XMT)
39R	87R	135R	P2802	7	39R(ADSL)	20R(XMT)
40T	88T	136T	P2802	40	40T(ADSL)	20T(RCV)
40R	88R	136R	P2802	8	40R(ADSL)	20R(RCV)
41T	89T	137T	P2802	41	41T(ADSL)	21T(XMT)
41R	89R	137R	P2802	9	41R(ADSL)	21R(XMT)
42T	90T	138T	P2802	42	42T(ADSL)	21T(RCV)

Cables and Connectors

Stinger CR cabling for the 48-port LPM with splitters

Table C-3. Tip/Ring connections to protection blocks 1, 3, and 5 (Continued)

P1 (LPM 1)	P3 (LPM 2)	P5 (LPM 3)	LPM connector	Pin No.	LPM 2-wire ports	LPM 4-wire ports
42R	90R	138R	P2802	10	42R(ADSL)	21R(RCV)
43T	91T	139T	P2802	43	43T(ADSL)	22T(XMT)
43R	91R	139R	P2802	11	43R(ADSL)	22R(XMT)
44T	92T	140T	P2802	44	44T(ADSL)	22T(RCV)
44R	92R	140R	P2802	12	44R(ADSL)	22R(RCV)
45T	93T	141T	P2802	45	45T(ADSL)	23T(XMT)
45R	93R	141R	P2802	13	45R(ADSL)	23R(XMT)
46T	94T	142T	P2802	46	46T(ADSL)	23T(RCV)
46R	94R	142R	P2802	14	46R(ADSL)	23R(RCV)
47T	95T	143T	P2802	47	47T(ADSL)	24T(XMT)
47R	95R	143R	P2802	15	47R(ADSL)	24R(XMT)
48T	96T	144T	P2802	48	48T(ADSL)	24T(RCV)
48R	96R	144R	P2802	16	48R(ADSL)	24R(RCV)
PWR	PWR	NC	NA	NA		
PWR	PWR	NC	NA	NA		
PWR	NC	NC	NA	NA		
PWR	NC	NC	NA	NA		

LPM connections for the bottom protection block of each pair (blocks 2, 4, and 6) are detailed in Table C-4. The numbering for protectors on P2, P4, and P6 corresponds to the protector numbering in Figure C-4 on page C-5.

Table C-4. Tip/Ring connections to protection blocks 2, 4, and 6

P2 (LPM 1)	P4 (LPM 2)	P6 (LPM 3)	LPM connector	Pin No.	LPM connection
1T	49T	97T	P2803	33	1T(POTS)
1R	49R	97R	P2803	1	1R(POTS)
2T	50T	98T	P2803	34	2T(POTS)
2R	50R	98R	P2803	2	2R(POTS)

Table C-4. Tip/Ring connections to protection blocks 2, 4, and 6 (Continued)

P2 (LPM 1)	P4 (LPM 2)	P6 (LPM 3)	LPM connector	Pin No.	LPM connection
3T	51T	99T	P2803	35	3T(POTS)
3R	51R	99R	P2803	3	3R(POTS)
4T	52T	100T	P2803	36	4T(POTS)
4R	52R	100R	P2803	4	4R(POTS)
5T	53T	101T	P2803	37	5T(POTS)
5R	53R	101R	P2803	5	5R(POTS)
6T	54T	102T	P2803	38	6T(POTS)
6R	54R	102R	P2803	6	6R(POTS)
7T	55T	103T	P2803	39	7T(POTS)
7R	55R	103R	P2803	7	7R(POTS)
8T	56T	104T	P2803	40	8T(POTS)
8R	56R	104R	P2803	8	8R(POTS)
9T	57T	105T	P2803	41	9T(POTS)
9R	57R	105R	P2803	9	9R(POTS)
10T	58T	106T	P2803	42	10T(POTS)
10R	58R	106R	P2803	10	10R(POTS)
11T	59T	107T	P2803	43	11T(POTS)
11R	59R	107R	P2803	11	11R(POTS)
12T	60T	108T	P2803	44	12T(POTS)
12R	60R	108R	P2803	12	12R(POTS)
13T	61T	109T	P2803	45	13T(POTS)
13R	61R	109R	P2803	13	13R(POTS)
14T	62T	110T	P2803	46	14T(POTS)
14R	62R	110R	P2803	14	14R(POTS)
15T	63T	111T	P2803	47	15T(POTS)
15R	63R	111R	P2803	15	15R(POTS)

Cables and Connectors

Stinger CR cabling for the 48-port LPM with splitters

Table C-4. Tip/Ring connections to protection blocks 2, 4, and 6 (Continued)

P2 (LPM 1)	P4 (LPM 2)	P6 (LPM 3)	LPM connector	Pin No.	LPM connection
16T	64T	112T	P2803	48	16T(POTS)
16R	64R	112R	P2803	16	16R(POTS)
17T	65T	113T	P2803	49	17T(POTS)
17R	65R	113R	P2803	17	17R(POTS)
18T	66T	114T	P2803	50	18T(POTS)
18R	66R	114R	P2803	18	18R(POTS)
19T	67T	115T	P2803	51	19T(POTS)
19R	67R	115R	P2803	19	19R(POTS)
20T	68T	116T	P2803	52	20T(POTS)
20R	68R	116R	P2803	20	20R(POTS)
21T	69T	117T	P2803	53	21T(POTS)
21R	69R	117R	P2803	21	21R(POTS)
22T	70T	118T	P2803	54	22T(POTS)
22R	70R	118R	P2803	22	22R(POTS)
23T	71T	119T	P2803	55	23T(POTS)
23R	71R	119R	P2803	23	23R(POTS)
24T	72T	120T	P2803	56	24T(POTS)
24R	72R	120R	P2803	24	24R(POTS)
25T	73T	121T	P2803	57	25T(POTS)
25R	73R	121R	P2803	25	25R(POTS)
26T	74T	122T	P2803	58	26T(POTS)
26R	74R	122R	P2803	26	26R(POTS)
27T	75T	123T	P2803	59	27T(POTS)
27R	75R	123R	P2803	27	27R(POTS)
28T	76T	124T	P2803	60	28T(POTS)
28R	76R	124R	P2803	28	28R(POTS)

Table C-4. Tip/Ring connections to protection blocks 2, 4, and 6 (Continued)

P2 (LPM 1)	P4 (LPM 2)	P6 (LPM 3)	LPM connector	Pin No.	LPM connection
29T	77T	125T	P2803	61	29T(POTS)
29R	77R	125R	P2803	29	29R(POTS)
30T	78T	126T	P2803	62	30T(POTS)
30R	78R	126R	P2803	30	30R(POTS)
31T	79T	127T	P2803	63	31T(POTS)
31R	79R	127R	P2803	31	31R(POTS)
32T	80T	128T	P2803	64	32T(POTS)
32R	80R	128R	P2803	32	32R(POTS)
33T	81T	129T	P2802	49	33T(POTS)
33R	81R	129R	P2802	17	33R(POTS)
34T	82T	130T	P2802	50	34T(POTS)
34R	82R	130R	P2802	18	34R(POTS)
35T	83T	131T	P2802	51	35T(POTS)
35R	83R	131R	P2802	19	35R(POTS)
36T	84T	132T	P2802	52	36T(POTS)
36R	84R	132R	P2802	20	36R(POTS)
37T	85T	133T	P2802	53	37T(POTS)
37R	85R	133R	P2802	21	37R(POTS)
38T	86T	134T	P2802	54	38T(POTS)
38R	86R	134R	P2802	22	38R(POTS)
39T	87T	135T	P2802	55	39T(POTS)
39R	87R	135R	P2802	23	39R(POTS)
40T	88T	136T	P2802	56	40T(POTS)
40R	88R	136R	P2802	24	40R(POTS)
41T	89T	137T	P2802	57	41T(POTS)
41R	89R	137R	P2802	25	41R(POTS)

Cables and Connectors

Stinger CR cabling for the 48-port LPM with splitters

Table C-4. Tip/Ring connections to protection blocks 2, 4, and 6 (Continued)

P2 (LPM 1)	P4 (LPM 2)	P6 (LPM 3)	LPM connector	Pin No.	LPM connection
42T	90T	138T	P2802	58	42T(POTS)
42R	90R	138R	P2802	26	42R(POTS)
43T	91T	139T	P2802	59	43T(POTS)
43R	91R	139R	P2802	27	43R(POTS)
44T	92T	140T	P2802	60	44T(POTS)
44R	92R	140R	P2802	28	44R(POTS)
45T	93T	141T	P2802	61	45T(POTS)
45R	93R	141R	P2802	29	45R(POTS)
46T	94T	142T	P2802	62	46T(POTS)
46R	94R	142R	P2802	30	46R(POTS)
47T	95T	143T	P2802	63	47T(POTS)
47R	95R	143R	P2802	31	47R(POTS)
48T	96T	144T	P2802	64	48T(POTS)
48R	96R	144R	P2802	32	48R(POTS)
PWR	NC	NC	P2802	NA	
PWR	NC	NC	P2802	NA	
PWR	NC	NC	P2802	NA	
PWR	NC	NC	P2802	NA	

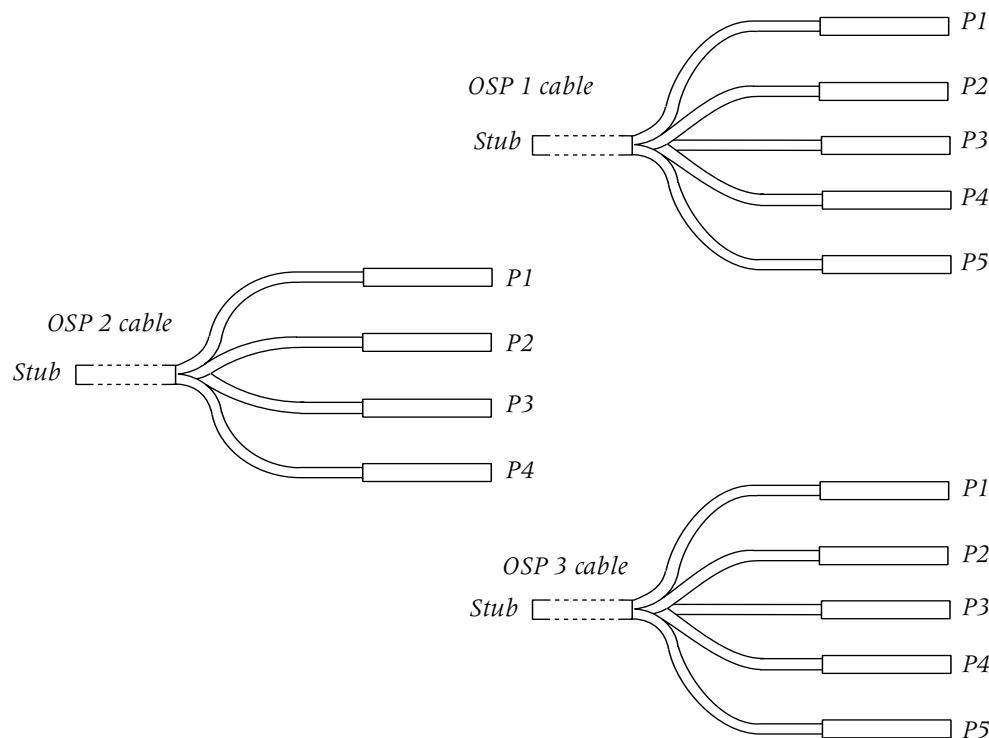
Cable stub connections to protection blocks

Four connectors on the back of each pair of protection blocks provide access to the unprotected (outside) side of the protection blocks. Circuits from the three pairs of connections blocks are terminated on three cable stubs.



Note The three cables that terminate at these stubs are each unique. The OSP1 and OSP3 cables have five connectors. The OSP2 cable has four connectors. These cables must be correctly connected across the four connectors on the back of each of the protection blocks.

Figure C-6. Stub cables for connection to the protection blocks



Cable and protection associations

The Stub cables are identified as OSP 1, OSP 2, and OSP 3. The cables connectors on these cables are labeled P1 through P4 or P5, depending on the cable. The connections on the protection blocks for these connectors are also labeled OSP 1, OSP 2, OSP 3, and OSP 4. Use the color codes, labeling on the cables, and the information in Table C-5 to connect the proper connector from the OSP cables to the proper OSP connector on the protection blocks.

Table C-5. OSP cable binders, pairs, and protection block connections

Cable	Binder	Pairs	Cable	Protection	Protection	LPM/	2-wire	4-wire
			Connector	Connector block	block	LIM	Circuits	Circuits
OSP 1	Blue	1-25	P1	2	OSP 3	1	POTS 1-25	NA
OSP 1	Orange	1-23	P2	2	OSP 4	1	POTS 26-48	NA

Cables and Connectors

Stinger CR cabling for the 48-port LPM with splitters

Table C-5. OSP cable binders, pairs, and protection block connections (Continued)

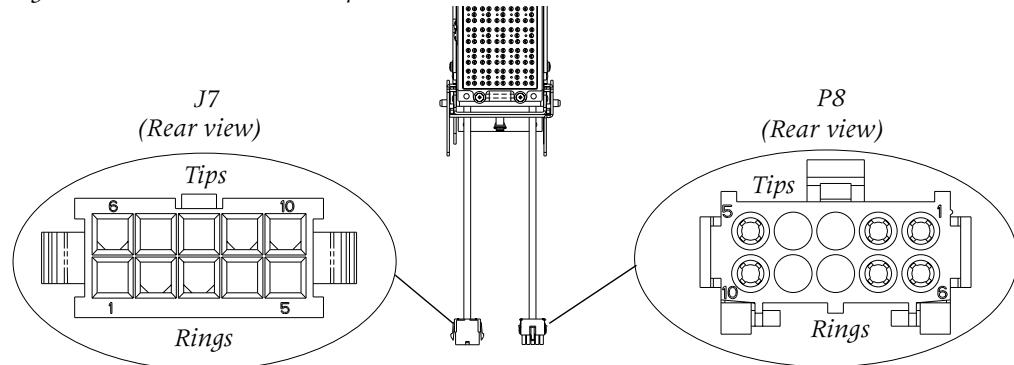
Cable	Binder	Pairs	Cable Connector	Protection block	Protection block Connector	LPM/ LIM No.	2-wire Circuits	4-wire Circuits
OSP 1	Orange	24-25	P3	4	OSP 3	2	POTS 1-2	NA
OSP 1	Green	1-23	P3	4	OSP 3	2	POTS 3-25	NA
OSP 1	Green	24-25	P4	4	OSP 3	2	POTS 26-27	NA
OSP 1	Brown	1-21	P4	4	OSP 4	2	POTS 28-48	NA
OSP 1	Brown	22-25	P5	6	OSP 3*	3	POTS 1-4	NA
OSP 2	Blue	1-21	P1	6	OSP 3*	3	POTS 5-25	NA
OSP 2	Blue	22-25	P2	6	OSP 4	3	POTS 26-29	NA
OSP 2	Orange	1-19	P2	6	OSP 4	3	POTS 30-48	NA
OSP 2	Green	1-21	P3	5	OSP 1*	3	ADSL 5-25	T1 3-12 & T1 13 XMT only
OSP 2	Green	22-25	P4	5	OSP 2*	3	ADSL 26-29	T1 13 RCV only T1 14 T1 15 XMT only
OSP 2	Brown	1-19	P4	5	OSP 2	3	ADSL 30-48	T1 15 RCV only T1 16-24
OSP 3	Blue	1-25	P1	1	OSP 1	1	ADSL 1-25	T1 1-12 & T1 13 XMT only
OSP 3	Orange	1-23	P2	1	OSP 2	1	ADSL 26-48	T1 13 RCV only & T1 14-24
OSP 3	Orange	24-25	P3	3	OSP 1	2	ADSL 1-2	T1 1
OSP 3	Green	1-23	P3	3	OSP 1	2	ADSL 3-25	T1 2-13 & T1 13 XMT only
OSP 3	Green	24-25	P4	3	OSP 2	2	ADSL 26-27	T1 13 RCV & T1 14 XMT
OSP 3	Brown	1-21	P4	3	OSP 2	2	ADSL 28-48	T1 14 RCV only & T1 15-24
OSP 3	Brown	22-25	P5	5	OSP 1*	3	ADSL 1-4	T1 1 & 2

*. Four connectors are combined to form two pairs of back-to-back connectors. Connector P5 for cable OSP 1 and connector P1 for cable OSP 2 connect on top of each other on connector OSP 3 of connection block 6 for LPM3. Connector P3 for cable OSP 2 and connector P5 for cable OSP 3 connect on top of each other on connector OSP 1 of connection block 5 for LPM3.

Protection block power connections

The ± 190 Vdc power is supplied from the central office over multiple pairs of telecommunications wires and terminated on a power stub connector labeled P7. A 10-pin Molex connector, labeled J7, connects this voltage to the outside plant tips and rings of five connection points on the protection blocks. The tips and rings on the other side of the protection block are wired to a 10-pin Tyco connector, labeled P8. This connector plugs into the front of the Stinger CR power supply. Figure C-7 shows the power connections through the protection blocks.

Figure C-7. Protection block power connectors



The wiring connections from the power stub through the connection blocks is detailed in the following table Table C-6.

Table C-6. Wiring connection from the power stub

P7 Color (power stub)	P7/J7 Pins	J7 Color	Protection Block	Protection Location	P8 Color	P8 Pins
Slate/White	1	Brown	P3	49R	Blue	6
Brown/White	2	Slate	P2	50R	Orange	7
Green/White	3	Brown	P2	49R	Blue	8
Orange/White	4	Slate	P1	50R	Orange	9
Blue/White	5	Brown	P1	49R	Blue	10
White/Slate	6	Violet	P3	49T	White	1
White/Brown	7	Violet	P2	50T	White	2
White/Green	8	Violet	P2	49T	White	3
White/Orange	9	Violet	P1	50T	White	4
White/Blue	10	Violet	P1	49T	White	5

Chassis door alarm connections

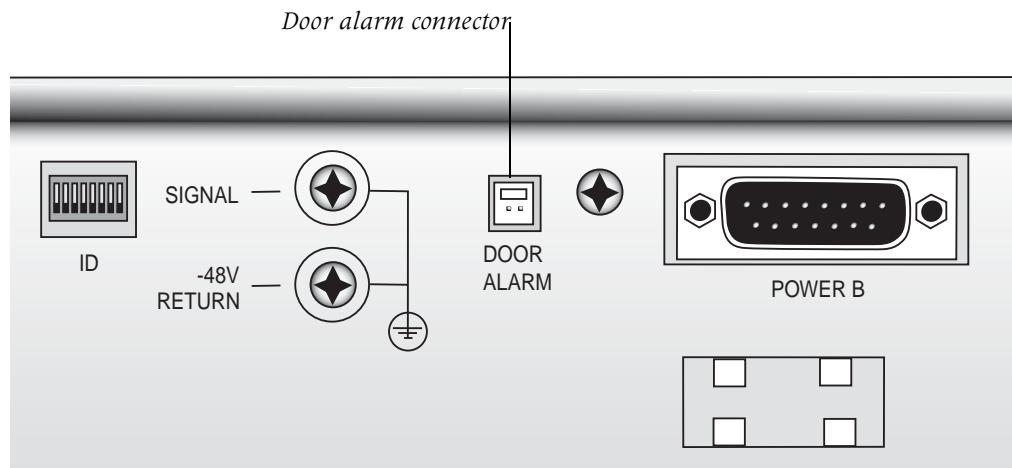
The door alarm for Stinger CR units operating in the hosted mode is connected directly to the card cage and monitored through the TAOS software on the host Stinger unit.

The door alarm for Stinger CR units operating in the stand-alone mode is connected directly to the ALARM port of the IP2000 or control module that controls the unit and monitored through the TAOS software in that module.

Door alarm for hosted operation

The door alarm switch is located in the lower left corner of the Stinger CR enclosure door opening. (See Figure 2-3 on page 2-5.) On Stinger CR units operating in hosted mode, the black and white wires from this switch connect to a pair of pins on the Stinger CR chassis, behind the cooling unit. The location of this connector is shown Figure C-8 on page C-18

Figure C-8. Door alarm connectors on the Stinger CR chassis



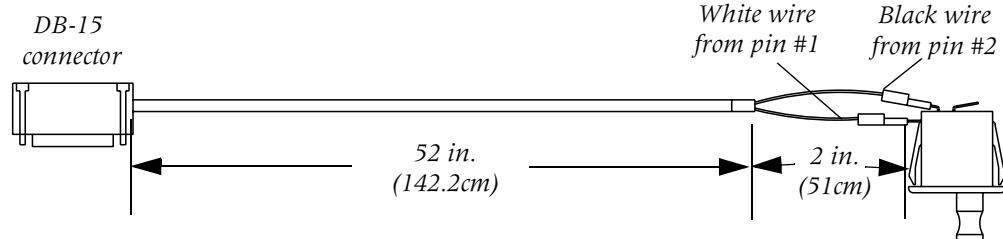
Note On Stinger CR units that operate in the stand-alone mode, the door alarm switch is connected to pins one and two of the ALARM port on the IP2000 or control module (see “Alarm input port pinouts” on page C-2).

Door alarm connection for stand-alone operation

A Stinger CR functioning as a stand-alone unit with an IP2000 or control module uses the first set of connections (pins 1 and 2) on the ALARM connector of the IP2000 or control module to monitor the enclosure door alarm. (See, “Alarm connection for monitoring the enclosure door alarm” on page 3-23). A special cable

connects the door alarm for the enclosure to the ALARM connector of the IP2000 or control module. This cable is illustrated in Figure C-9.

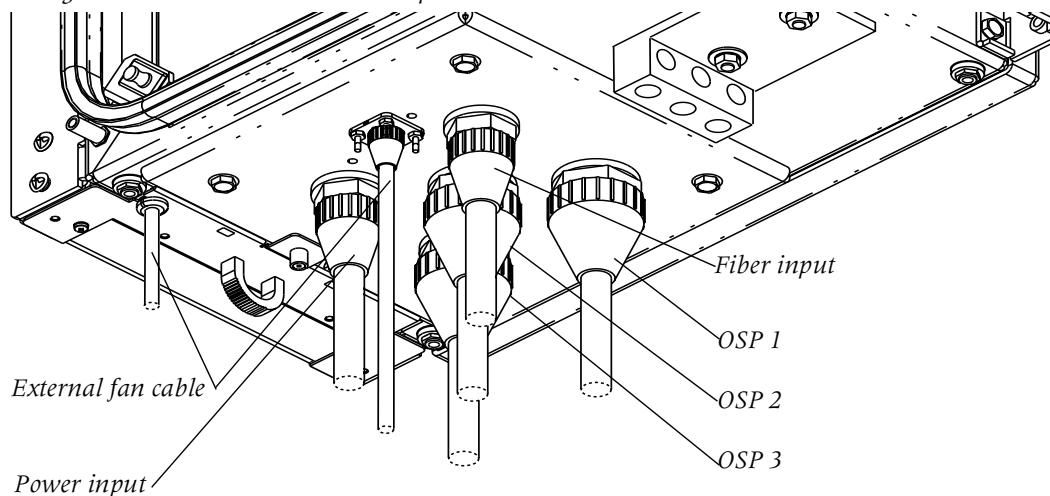
Figure C-9. Door alarm cable for stand-alone operation



Enclosure cable exit points

All cables and fiber that connect to the Stinger CR enter the enclosure through the bottom of the unit. Figure C-10 identifies each of these cables.

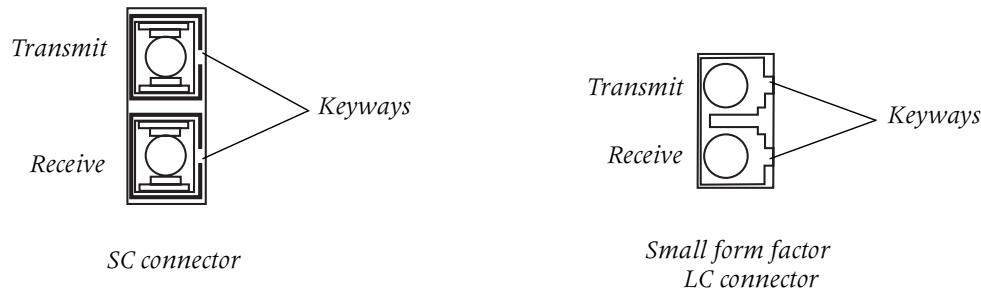
Figure C-10. Enclosure cable exit points



Optical connectors

Stinger OC3-ATM trunk modules use SC optical connectors. Other modules, including the OC12-ATM, COP, and OLIM use LC small form factor connectors. The keyways and the transmit/receive orientation of these connectors are illustrated in Figure C-11.

Figure C-11. Optical connectors



Safety-Related Electrical, Physical, and Environmental Information

D

Electrical and electronic information	D-1
Laser safety	D-2
Safety certifications	D-5
Physical specifications	D-5
Site specifications	D-6
Weight and lifting requirements	D-6

See the *Edge Access and Broadband Access Safety and Compliance Guide* for safety instructions and country-specific information.

Warning Before installing your Stinger unit, be sure to read the *Edge Access and Broadband Access Safety and Compliance Guide*.



Electrical and electronic information

The Stinger CR unit is nominally powered from an Argus CSM36-BC power source. Table D-1 describes Stinger CR electronic and electrical specifications.

Table D-1. Stinger electronic and electrical specifications

Application	Specification
Input voltage	±190Vdc (must be from an Argus CSM36-BC power supply)
Input power	260 watts (W) maximum
Connection	5-pair wire stub
Certification	Telcordia GR-487-CORE Telcordia GR-1089-CORE, Issue 3, October 2002
EMI compliance	FCC Part 15 Class A ICES 003 Class A

Protection block elements

The proper protection elements must be installed in the protection blocks of the Stinger CR enclosure. Install protection elements in the protection blocks as follows:

- Pairs supplying power—Avaya 3B1EW 5-pin gas protector (Com. code 104410147), or equivalent.
- All other pairs—Avaya 3C1S 5-pin solid state protector (Com. code 105514756), or equivalent.

Laser safety

The Lucent Technologies Stinger Compact Remote unit is an FDA/CDRH Class I / IEC Hazard Level 1 system. Laser circuit packs for use in the Stinger CR are FDA Class I and IEC Hazard Level 1 devices.

Stinger circuit packs or modules that utilize laser radiation for optical transmission are Class 1 Optical Fiber Telecommunications laser products that comply with FDA/CDRH21 CFR 1040.10 and 1040.11. They meet the safety measures specified in the United States Food and Drug Administrations' Center for Devices and Radiological Health (FDA/CDRH) regulations and international standards IEC-60825 or DIN/EN 60825.

Potential dangers

Beware of the following potential sources of danger, that will remain despite all safety measures.

- Laser radiation from optical transmission systems is in a wavelength that is invisible to the human eye.
- Laser radiation can cause damage to skin and eyes.



Caution Although, at present, the transmit power for Class 1 lasers are below levels known to cause injury to the eye at distances greater than 250mm (10 Inches), direct exposure should always be avoided. Always observe the information listed below in "Laser warning instructions."

Laser classifications

The maximum output power of laser radiation depends on the type of laser diode used. The international standards IEC-60825 or DIN/EN 60825 define the maximum output power of laser radiation for each laser class in accordance with the wavelength.

Table D-2. Laser classifications

Laser class	Wavelength	Output power
1	1310nm	15.6mW (11.93dBm) maximum
	1550nm	10.0MW (10.0dBm) maximum
1M	1310nm	15.6—44.9mW (11.93—16.52dBm)
	1550nm	10.0—136.4mW (10.0—21.35dBm)

Table D-2. Laser classifications (Continued)

Laser class	Wavelength	Output power
3B	1310nm	44.9—500mW (16.52—26.99dBm)
	1550nm	136.4—500mW (21.35—26.99dBm)
4	1310nm	Greater than 500mW (26.99dBm)
	1550nm	Greater than 500mW (26.99dBm)

Laser warning instructions

In its normal operating mode, the Stinger Compact Remote unit is totally enclosed and presents no risk of eye injury. It is a laser Class 1/I product.

The lightguide cables that interconnect various components of a lightwave system can be disconnected or break, and may expose people to lightwave emission. Also, certain measures and service procedures may expose the technician to emission from the laser circuit pack or module during installation and servicing.

Observe the following instructions to avoid exposing yourself and others to risk:

- Do not look into the end of an exposed fiber or an open connector when the optical source is on. (Even though viewing Class 1 lasers at distances greater than 250mm (10 inches) will normally not cause eye injury.)
- Only authorized technicians, who have satisfactorily completed an approved training course are allowed to perform service, maintenance, and restoration activities on lightwave or lightguide facilities, or laser components. Untrained technicians must never perform these tasks.
- Read all related documentation and instructions before attempting to operate, install, or perform maintenance on any Stinger optical circuit packs or modules. Failure to follow instructions can result in exposure to dangerous radiation.
- Remove power from the optical source before disconnecting optical fibers, if the source is not a laser Class 1 product, or if the laser Class of the source is unknown.
- Never scan a fiber with an optical test set without verifying that all lightwave sources on the fiber are turned off or that the test set is specially approved for the test.
- When in doubt, verify that the optical source is switched off by measuring the optical output with an optical power meter.
- When fiber is disconnected from the COP or other optical component, always put a protective cup on the optical connectors of the fiber and the optical component.

Laser warning labels

The laser warning labels indicate the laser class and hazard level of laser radiation. The Stinger is classified as class 1/I unit. This means that, under normal operating conditions, all energized laser transmitting components are terminated on optical fibers that enclose the laser energy with the fiber sheath. Also, covers are in place over the circuit pack shelves.

The labels shown below are used to identify systems that belong to laser class 1.

Figure D-1. Warning labels for identification of Class 1 laser devices



Handling optical fibers

Never look into the end of an optical fiber or connector when the optical source is switched on. Always observe the laser warning instructions.

Routing and connecting

During installation, the optical connectors of the fibers and the Stinger circuit pack or module must be equipped with a protective cap until they are coupled. The fibers should be guided to the optical circuit pack or module using the special protective spiral wrap of the pigtail.



Caution Bending an optical fiber to a radius of less than 30mm, can cause the fiber to break or produce micro defects in the fiber. Micro defects can affect product safety, increase fiber attenuation, and reduce long term stability. Ensure that the bending radius of the fiber is not less than 30mm.

Splicing

Only trained personnel are allowed to cut and splice optical fibers. Always read and be sure that you understand all the instructions in the documentation related to splicing and cutting equipment. Before splicing, verify the fiber is disconnected from the optical component.

After completion, check every splice according to the instructions in the documentation related to splicing and cutting equipment.

Cleaning optical connectors and couplings

Before cleaning optical connectors, verify that the optical source is switched off. Never look into the end of an exposed fiber or optical connector when the optical source is switched on. Always observe the laser warning instructions.

Optical connectors should be cleaned if problems are encountered that indicate the connectors have an impurity. (For example, attenuation is beyond the maximum value permitted.)

To check for impurities (dust particles or other contamination), examine the connector face with a microscope that has an enlargement factor of 200. The physical geometry of the coupling does not allow it to be checked under a microscope. Visually check a coupling for residual impurities by holding it to light.

Prior to connection, verify that the optical connectors and couplings are free of impurities. You can clean the coupling with a pipe cleaner and isopropanol. Let the isopropanol on the connector coupling face evaporate completely by air-drying, or with the use of purified compressed air.

Safety certifications

The Stinger Compact Remote meets U.S. and Canadian UL specification 60950-1, First Edition.

Physical specifications

Table D-3 describes the Stinger CR physical specifications.

Table D-3. Stinger CR physical specifications

Specification	Description
ATM standards	ATM Forum UNI (Version 3.0 and Version 3.1), ATM Forum Interim Interswitch Signaling Protocol (IISP)
WAN interfaces	155.52Mbps optical
Physical characteristics	Basic unit includes one populated Stinger CR chassis (cooling fan module, control and optics pack, power supply, and three 48-port LIM/LPM pairs), in an outdoor chassis with protector blocks and cabling.
Enclosure size*	<p>Height (enclosure only): 30.1 inches (76.5cm) Height (overall): 40.5 inches (102.9cm)</p> <p>Depth (enclosure only): hosted units—11.5 inches (29.2cm) stand-alone units—12 inches (30.5cm)</p> <p>Depth (overall): 12.6 inches (32cm)</p> <p>Width (enclosure only): 16.2 inches (41.2cm) Width (overall): 20.5 inches (52cm)</p>
Unit weight	121 pounds (54.885kg) maximum (with fans, power supply, protections blocks, and cables)

*. The overall measurements include clearance for cabinet hardware, locking mechanism, ventilation shrouds, and cable cover.

Site specifications

Stinger units require a particular operating environment and minimum clearance for proper operation.

Operating environment

Table D-4 describes the environmental requirements for selecting an installation site for the Stinger CR hardware. The site requirements are based on Network Equipment Building System (NEBS) GR-63-CORE and GR-1089-CORE.

Table D-4. Stinger CR site specifications

Parameter	Requirement
Ambient operating temperature	Light gray enclosures (fully populated): -40°C to 46°C (-40°F to 114.8°F)
	Green enclosures with IP2000 modules and 2 LIM/LPM circuit packs (maximum): -40°C to 46°C (-40°F to 114.8°F)
	Brown or green enclosures (fully populated): -40°C to 40°C (-40°F to 104°F)
Relative humidity	10% to 95% (noncondensing)
Operating altitude	To 13,123 feet (4000 m)
Ambient storage temperature and humidity	-40°C to 85°C (-40°C to 140°F), 95% relative humidity
Storage altitude	-1,000 feet to +30,000 feet (-305m to 9150m)



Caution To avoid damage from condensation and regulate the internal temperature of the enclosure, power should be applied to the Stinger CR as soon as possible after installation.

Weight and lifting requirements

A fully loaded Stinger Compact Remote enclosure weighs approximately 160 pounds (72.575kg). For ease of installation the unit should be installed without its modular components in place. The following table will help you determine the weight of the unit you are installing.

Table D-5. Stinger CR weight details

Item	Weight
Bare system (includes card cage, solar shields, and protection blocks)	74 pounds (33.566kg)*
Cooling unit and enclosure fan	18 pounds (8.165kg)

Table D-5. Stinger CR weight details (Continued)

Item	Weight
Cables (with 20 foot external drops)	29 pounds (13.154kg)
LIMs	3.6 pounds (1.633kg) per LIM
LPMs	3.3 pounds (1.497kg) per LPM
COP	2.1 pounds (0.953kg)
Protection elements	10 pounds (maximum, fully equipped)

*. Add an additional 5 pounds (2.268kg) for enclosure JW1 2700.

Index

A

addresses, IP
assigning for Ethernet 4-9
syntax 4-7
admin login, recommended password change 4-5
administrative access, restricting 4-5
administrative connections 4-2
alarms 3-23
diagnostic 3-22
alarms
configuring for remote shelves 6-8
connector description C-2
input connector pinouts C-2
raising and clearing 6-7
altitude
operating D-6
storage D-6
ATM connection, displaying information 6-4
ATM, standards D-5

C

cables
diagnostic port C-1
power stub connections C-17
serial port C-1
CAC
calculations for host system bandwidth 5-9
default behavior 5-8
cautions about replacing modules 3-7
changing default logins 4-5
chassis ID
DIP switch location 5-1
commands
Dir 4-5
Read and Write 4-10
Set 4-10
configuration
basic IP 4-7

configuration for hosted operation 5-4
console terminal, connecting and setting up 4-2
cooling unit
checking 2-13
function 1-7
status lights 3-31, 3-32
COP
connecting 3-18
functions 1-7
installing and replacing 3-8
interfaces checking 2-10
status lights 3-28

D

DIAG PORT. *See* serial port
DIP switch
default ID setting 5-14
location for setting chassis ID 5-1

E

electrostatic discharge (ESD) jack 2-6
enclosure
illustrated 2-5
mounting 3-4
size D-5
environmental specifications D-6
ESD, grounding jack 2-6
Ethernet ports
IP addresses 4-9

F

fan status lights 3-31, 3-32

H

hardware, verifying configuration 2-5
high-speed-slot-static-config 5-9
host management interface 5-3
hosted operation
 configuration 5-4
 traffic management 5-8
 upstream traffic shaping 5-11
humidity requirement D-6

I

installation
 prerequisites 3-1
 required tools 2-1
intended use A-1
IP
 address syntax 4-7
 host routes 4-9
 minimal configuration 4-7
 subnet notation 4-9
IP2000
 basic configuration overview 4-1
 connecting 3-18
 control function defined 4-1
 functions 1-7
 installing and replacing 3-8
 interfaces checking 2-9
 logging into 4-4
 status lights 3-26
IP-Global profile 4-6
IP-Interface profile 4-9

L

LEDs. *See* status lights
LIM
 checking 2-11
 displaying remote status 6-3
 installing and replacing 3-10
 monitoring remote connections 6-3
LPM
 50-pin connector C-3
 checking 2-13
 connecting 3-24
 function 1-7
 installing and replacing 3-12

M

management interface, for hosted operation 5-3
modules, cautions about replacing 3-7
monitor-control, pinouts C-1

N

nailed-group number allocation 5-7
netmask 4-8
NVRAM
 host initialization 6-1

O

OLIM
 installation B-1
 overview B-1
 queue priorities 5-11
 specifications B-3
 status lights B-2

P

passwords
 changing defaults 4-5
 Telnet 4-6
PCMCIA cards
 described 2-11
pinouts
 alarm input C-2
 alarm input connector C-2
 monitor-control C-1
plug-in components
 cooling unit 1-7
 COP 1-7
 IP2000 1-7
 LPM 1-7
 power supply 1-7
 RLIM 1-7
power
 cable connections to power unit C-17
power supply
 checking 2-15
 function 1-7
powering up, described 3-25
preventing static discharge damage 2-2
profile
 remote-shelf-config 5-11
 remote-shelf-stat 6-4

validation-config 5-13

profiles

- IP-Global 4-6
- IP-Interface 4-9
- Serial 4-5
- User 4-5

protection blocks

- tip/ring orientation C-6

Q

queue priorities 5-11

R

remote shelves

- configuring alarms 6-8
- enabling traps 6-10
- identifying 5-5
- monitoring status 6-4

remote-shelf-config 5-11

- contents 5-11

remote-shelf-stat 6-4

RLIM

- function 1-7

S

security

- changing admin password 4-5
- changing default logins 4-5
- Telnet password 4-6

serial port

- restricting access 4-5

Serial profile 4-5

shelf validation

- configuration 5-13
- enabling 5-13

validation-config 5-13

Single-mode (OC3/STM)

- medium-reach B-4

size of enclosure D-5

slot numbering 3-8

specifications

- cable pinouts C-1
- electrical D-1
- environmental D-6
- physical D-5

startup sequence 3-25

static discharge damage 2-2

preventing 2-2

status lights

- COP 3-28
 - fan and cooling unit 3-31, 3-32
 - IP2000 3-26
 - OLIM B-2
- subnet mask 4-9
- subnet notation 4-9
- system software, upgrading 6-1

T

Telnet password 4-6

temperature

- operating D-6
- storage D-6

terminal emulation settings, required 2-2, 4-4

tools and equipment required for installation 2-1

traffic shaping 5-11

traps, enabling for remote shelf events 6-10

trunk interfaces

- CAC support 5-9

trunk interfaces, enabling 5-6

trunk-cac-config 5-9**U**

upgrading system software

- automatic procedure 6-2
- overview 6-1

use of wrist strap 2-2

user interface, terminal configuration for 2-2

User profile 4-5

V

virtual circuit provisioning 5-7

W

WAN interfaces supported D-5

weight of unit D-5

workstation, connecting 10/100 Ethernet 4-3

workstation, connecting gigabit Ethernet 4-3