

**Lucent Technologies**  
Bell Labs Innovations



# **Stinger<sup>®</sup> Compact Remote**

IP DSLAM Getting Started Guide

Part Number: 363-217-015R9.10.0  
Issue 3  
For software version 9.10.0  
December 2006


**Copyright © 2005, 2006 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](mailto: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](http://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 online documentation library at <http://www.lucent.com/support>.

#### **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](mailto: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
<b>About This Guide .....</b>	<b>i-xv</b>
What is in this guide .....	xv
What you should know .....	xv
Documentation conventions .....	xvi
Stinger documentation set.....	xvii
<b>Chapter 1 Introduction to the Stinger Compact Remote .....</b>	<b>1-1</b>
Stinger Compact Remote IP DSLAM description .....	1-1
Operational overview .....	1-1
Stinger Compact Remote hardware .....	1-1
Stinger Compact Remote card cage chassis .....	1-2
Card-cage modular components .....	1-4
Host hardware .....	1-4
IP control module .....	1-5
Gigabit Ethernet OLIM .....	1-5
<b>Chapter 2 Preparing to Install the Unit.....</b>	<b>2-1</b>
Installation safety .....	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 .....	2-3
Store components properly .....	2-3
Unpacking the Stinger Compact Remote IP DSLAM .....	2-4
Verifying the hardware .....	2-4
Checking modules and chassis .....	2-7
Checking the COP.....	2-8
The COP .....	2-8
COP interfaces .....	2-8
Checking the LIMs.....	2-9
Checking the LPMs.....	2-11
Checking the cooling unit.....	2-12
Checking the power supply .....	2-12
The $\pm 190$ Vdc power supply.....	2-12
The power filter .....	2-13

**Chapter 3 Compact Remote Enclosure and Component Installation .....3-1**

Introduction ..... 3-1

Before you begin ..... 3-1

Stinger CR enclosure mounting hardware ..... 3-2

    Pole mounting hardware ..... 3-3

    Cabinet mounting hardware ..... 3-4

    Pedestal mounting hardware ..... 3-6

    Inside rack mounting hardware ..... 3-7

Mounting the enclosure on a pole ..... 3-8

    Center-mounting the enclosure on a pole ..... 3-9

    Side-mounting the enclosure on a pole ..... 3-12

Mounting the enclosure on a wiring cabinet ..... 3-14

    Prepare the cabinet and install the mounting bracket ..... 3-14

    Mounting the enclosure ..... 3-15

Route and connect the fibers and ground cable inside the enclosure ..... 3-16

Routing the cables out of the enclosure ..... 3-17

    Routing the cables for cabinet mounting ..... 3-17

    Routing the cables for pole mounting ..... 3-18

Grounding the enclosure ..... 3-20

    Inspecting and replacing the door gasket ..... 3-20

Installing and replacing Stinger Compact Remote components ..... 3-22

    Slot numbering and module placement ..... 3-22

    GE-COP installation and replacement ..... 3-23

        Removing the GE-COP module from the COP slot ..... 3-23

        Installing a module in the COP slot ..... 3-23

    Installing and replacing LIMs ..... 3-24

        Installing a LIM ..... 3-24

        Replacing a LIM ..... 3-25

    Installing and replacing LPMs ..... 3-26

        Installing an LPM ..... 3-26

        Replacing an LPM ..... 3-26

    Replacing the chassis cooling module ..... 3-28

    Replacing the external cooling unit ..... 3-29

    Replacing the power supply ..... 3-31

Physical connections to the Stinger Compact Remote unit ..... 3-32

    Connections to the GE-COP ..... 3-33

        Gigabit Ethernet ports ..... 3-34

        Diagnostic port ..... 3-35

        Alarm input port ..... 3-35

    Connections to the LPMs ..... 3-36

        Connecting the LPM ..... 3-36

        Routing the LPM connector cables ..... 3-37

Turning on power to a Stinger Compact Remote unit ..... 3-38

Status lights ..... 3-40

    GE-COP status lights ..... 3-40

    LIM status lights ..... 3-42

    Internal cooling unit status lights ..... 3-43

    Power supply status lights ..... 3-44

What's next ..... 3-44

**Chapter 4 Hosted System Configuration .....4-1**

---

Elements of the hosted system architecture.....	4-1
Enabling GE-OLIM ports and configuring port usage .....	4-2
Enabling GE-OLIM ports .....	4-3
Configuring GE-OLIM port usage.....	4-3
Configuring GE-OLIM trunk ports 9 and 10 .....	4-4
Configuring an IP routed interface for a GE-OLIM trunk port .....	4-4
Configuring a routed VLAN interface for a GE-OLIM trunk port .....	4-5
Enabling IP multicast on a GE-OLIM trunk port .....	4-6
Configuring GE-OLIM trunk port link aggregation .....	4-6
Benefits of link aggregation .....	4-6
Configuration overview.....	4-7
Settings in the Ether-Group profile.....	4-7
Virtual Ethernet profile settings .....	4-8
Settings in Ethernet profiles for the physical GigE ports.....	4-9
LACP profile settings .....	4-11
Sample link aggregation configuration.....	4-11
Configuring a routed VLAN that uses the aggregated bandwidth.....	4-12
Configuring an MBONE interface on the aggregated trunk ports.....	4-12
LACP implementation details .....	4-13
Enabling host communication to remote shelves .....	4-14
Configuring the host system to operate in master mode.....	4-14
Configuring remote shelf settings.....	4-14
Overview of profile settings.....	4-14
Sample <b>remote-shelf-config</b> configuration .....	4-16
Enabling GE-OLIM CR port link aggregation.....	4-17
CAC bandwidth checks for guaranteed connections .....	4-17
Sample configuration enabling link aggregation .....	4-18
Configuring remote shelf validation (optional) .....	4-20
Setting the chassis ID on a remote shelf .....	4-20
Configuring remote shelf validation on the host system .....	4-22
Configuring subscriber connections .....	4-23
Enabling remote shelf RLIM interfaces.....	4-24
VLAN bridging (1:1) connection with CM egress .....	4-25
VLAN stacking connection with CM egress .....	4-26
Routed VLAN on a GE-OLIM trunk port with a PPPoE routed connection ....	4-27
Bridged IP routing (BIR) connections on RLIMs for multicast traffic only.....	4-29
ATM circuit between an RLIM port and a host trunk port.....	4-31
<b>Chapter 5 Hosted System Management.....</b>	<b>5-1</b>
Hosted system distributed multicast mechanism .....	5-1
Required setting on the master CM.....	5-1
Distributed multicast domains .....	5-2
Internal fast-forwarding interfaces .....	5-2
MBONE and multicast client interactions on FFW interfaces .....	5-2
What happens when a CPE joins a multicast group .....	5-3
What happens when a CPE leaves a multicast group .....	5-4
Displaying multicast information.....	5-4
Displaying FFW interface information.....	5-5
Slot-based address assignment for PPPoE connections .....	5-7
Overview of profile settings.....	5-7
Sample slot-based address configuration using the global router.....	5-9

IP filters for RLIM data connections .....	5-11
Current limitations on filtering RLIM connections .....	5-11
Sample input IP filtering on an RLIM connection .....	5-12
Administrative tools for hosted environments.....	5-13
Viewing the <b>remote-shelf-stat</b> profile.....	5-13
Using the <b>remoteself</b> command .....	5-15
Displaying traffic statistics.....	5-16
Opening a session to the RLIM, GE-OLIM, or GE-COP .....	5-17
Displaying statistics for terminating AAL5 connections.....	5-17
Displaying statistics for ATM traffic.....	5-19
Displaying statistics for bridged connections .....	5-20
Displaying statistics for distributed multicast traffic .....	5-20
LACP-related diagnostics.....	5-21
<b>Appendix A Stinger CR Intended Use.....</b>	<b>A-1</b>
User line interfaces .....	A-1
GE-COP interfaces.....	A-1
<b>Appendix B The Host Stinger GE-OLIM.....</b>	<b>B-1</b>
Introducing the Stinger GE-OLIM.....	B-1
Installing a GE-OLIM .....	B-2
Making connections to a GE-OLIM.....	B-3
Interpreting GE-OLIM status lights .....	B-4
GE-OLIM specifications.....	B-5
Configuring a Stinger GE-OLIM.....	B-6
<b>Appendix C Cables and Connectors .....</b>	<b>C-1</b>
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-7
Cable stub connections to protection blocks.....	C-15
Cable and protection associations .....	C-16
Power cables and connections.....	C-17
±190Vdc connections through the protection blocks .....	C-17
-48Vdc Power connections .....	C-19
Chassis door alarm connections .....	C-20
Door alarm for hosted operation .....	C-20
Enclosure cable exit points.....	C-20
Optical Gigabit Ethernet connectors .....	C-21
SFP modules .....	C-21
Optical connectors.....	C-21
<b>Appendix D Safety-Related Electrical, Physical, and Environmental Information .</b>	

**D-1**

Safety Instructions.....D-1  
     Stinger CR, ±190 V dc Models Important Safety Instructions .....D-1  
     Stinger CR, ±190 V dc Models Important Safety Instructions .....D-1  
     Stinger CR, -48 V dc Models Important Safety Instructions.....D-4  
     Stinger CR, (Indoor Cabinet) -48 V dc Models Important Safety Instructions..D-5  
 Electrical and electronic information .....D-7  
 Protection block elements .....D-8  
 Laser safety.....D-9  
     Laser classifications .....D-9  
     Laser warning instructions .....D-10  
     Laser warning labels .....D-10  
     Handling optical fibers .....D-11  
         Routing and connecting .....D-11  
         Splicing.....D-11  
         Cleaning optical connectors and couplings .....D-11  
 Safety certifications .....D-12  
 Physical specifications .....D-12  
 Site specifications .....D-13  
     Operating environment .....D-13  
 Weight and lifting requirements .....D-13

**Appendix E Replacing a Door Assembly on a Deployed Stinger CR .....E-1**

Replacing a compact remote door ..... E-1  
     Before you begin..... E-1  
     Replacing the damaged door ..... E-1

**Appendix F Upgrading Stinger Compact Remote.....F-1**

Retrofit Kit..... F-1  
     Torque Requirement..... F-4  
         Using torque wrenches for retrofit ..... F-4  
         Retrofit without torque wrenches..... F-5  
 Using Retrofit to Upgrade Compact Remote ..... F-5  
     Guidelines ..... F-5  
     Installing retrofit kit..... F-5

**Appendix G Card Cage Rack Mount System (CCRMS).....G-1**

CCRMS .....G-1  
     CCRMS Installation .....G-3  
         Replacing the air filter.....G-4  
         Replacing the fan.....G-4  
         Power filter .....G-4  
         Grounding .....G-5  
         ESD Jacks .....G-6  
 Site specifications .....G-6  
     Operating environment .....G-6  
     Space requirements .....G-7  
     Lifting requirements .....G-7  
 Additional brackets in CCRMS for stress prevention .....G-8  
     Installing the additional brackets.....G-9

**Index ..... Index-1**

---

# Tables



Table 3-1	Stinger Compact Remote mounting hardware .....	3-2
Table 3-2	Connectors for modules in the COP slot .....	3-34
Table 3-3	Number of pairs for providing power.....	3-39
Table 3-4	Status lights on the COP module .....	3-41
Table 3-5	ADSL 48-port Annex A LIM status lights .....	3-42
Table 3-6	Cooling unit status light .....	3-43
Table 4-1	Elements of a hosted Compact Remote IP DSLAM system.....	4-2
Table 4-2	GE-OLIM port function with this software version .....	4-3
Table 4-3	Validation ID DIP switch setting values .....	4-21
Table 4-4	Subscriber connection types.....	4-23
Table 5-1	FFW interfaces registered as multicast backbone or multicast client	5-2
Table B-1	GE-OLIM status lights .....	B-5
Table B-2	OLIM specifications .....	B-5
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-7
Table C-4	Tip/Ring connections to protection blocks 2, 4, and 6 .....	C-11
Table C-5	OSP cable binders, pairs, and protection block connections .....	C-16
Table C-6	Wiring connection from the power stub.....	C-18
Table C-7	Wire and pin assignments for -48Vdc cabling.....	C-19
Table C-8	SFP module information .....	C-21
Table D-1	Stinger electronic and electrical specifications .....	D-7
Table D-2	Approved Plug-in 5-pin Protectors.....	D-8
Table D-3	Laser classifications .....	D-9
Table D-4	Stinger CR physical specifications .....	D-12
Table D-5	Stinger CR site specifications.....	D-13
Table E-1	Compact Remote Door Torque Requirements .....	E-4
Table F-1	Contents of Retrofit kit:.....	F-3
Table F-2	Torque Requirements.....	F-4
Table G-1	Card Cage Rack Mount System parts .....	G-3
Table G-2	Minimum ground wire sizes .....	G-6
Table G-3	Site specifications .....	G-6
Table G-4	CCRMS Installation weight details.....	G-7



---

# Figures



Figure 1-1	The Stinger Compact Remote IP DSLAM.....	1-2
Figure 1-2	Stinger Compact Remote IP DSLAM card-cage .....	1-3
Figure 1-3	GE-OLIMs installed in a Stinger FS+ host.....	1-6
Figure 2-1	Wrist grounding strap .....	2-2
Figure 2-2	Wrist strap plugged into a grounding jack .....	2-3
Figure 2-3	Stinger Compact Remote IP DSLAM enclosure details .....	2-5
Figure 2-4	Phase 2 : Stinger CR ATM DSLAM enclosure details.....	2-6
Figure 2-5	Front view of a Stinger Compact Remote IPDSLAM chassis .....	2-7
Figure 2-6	Control and optics pack.....	2-9
Figure 2-7	The 48-port IP ADSL2+ LIM .....	2-10
Figure 2-8	The 48-port LPM with splitters .....	2-11
Figure 2-9	The Stinger Compact Remote cooling unit .....	2-12
Figure 2-10	The Stinger Compact Remote $\pm 190$ Vdc power supply.....	2-13
Figure 2-11	The Stinger Compact Remote power filter -48Vdc power supply ...	2-13
Figure 3-1	Pole mounting hardware.....	3-4
Figure 3-2	Cabinet side-mounting hardware .....	3-5
Figure 3-3	Cabinet rear-mounting hardware .....	3-6
Figure 3-4	Pedestal mounting kit hardware .....	3-7
Figure 3-5	Side rack mounting brackets.....	3-8
Figure 3-6	Lag bolt tab adjustment.....	3-9
Figure 3-7	Top and bottom pole mounting bolts.....	3-10
Figure 3-8	Attaching the Stinger enclosure rear mount hanger bracket.....	3-11
Figure 3-9	Side mounting bracket conversion.....	3-13
Figure 3-10	Enclosure fiber tray details.....	3-16
Figure 3-11	Interchangeable 45° cable duct and blocking plate.....	3-18
Figure 3-12	Cable duct and block plate configuration.....	3-18
Figure 3-13	Cable cover assembly screws.....	3-19
Figure 3-14	Enclosure grounding connector .....	3-20
Figure 3-15	Enclosure door gasket .....	3-21
Figure 3-16	Slot labeling on the Stinger Compact Remote IP DSLAM chassis...	3-22
Figure 3-17	Removing a GE-COP module from the COP slot .....	3-23
Figure 3-18	Installing a GE-COP module in the COP slot .....	3-24
Figure 3-19	Removing LPMs .....	3-27
Figure 3-20	Removing the cooling module .....	3-28
Figure 3-21	Replacing the external cooling unit .....	3-30
Figure 3-22	Removing the power supply .....	3-32
Figure 3-23	Connectors for the GE-COP .....	3-33
Figure 3-24	Gigabit Ethernet optical connection to the GE-COP .....	3-35
Figure 3-25	Connecting an LPM.....	3-37
Figure 3-26	LPM connector cable routing .....	3-38
Figure 3-27	GE-COP status lights .....	3-40

---

Figure 3-28	48-port IP ADSL2+ LIM status lights .....	3-42
Figure 3-29	The Stinger Compact Remote cooling unit .....	3-43
Figure 3-30	The Stinger Compact Remote ±190Vdc power supply.....	3-44
Figure 4-1	Hosted Compact Remote IP DSLAM architecture.....	4-1
Figure 4-2	Chassis validation ID DIP switches.....	4-21
Figure 4-3	Setting the Validation ID DIP switch.....	4-22
Figure 4-4	Bridging one PVC to one VLAN on IP2100 Gigabit Ethernet ports.	4-25
Figure 4-5	Bridging a PVC to an NSP VLAN (stacked VLANs) .....	4-26
Figure 4-6	A routed PPPoE connection with an upstream routed VLAN interface...	4-27
Figure 4-7	BIR connection for multicast video traffic.....	4-29
Figure 5-1	FFW interfaces on multicast-capable modules.....	5-2
Figure 5-2	Two IGMP Join requests for the same multicast group .....	5-3
Figure 5-3	Two IGMP Join requests for the same multicast group .....	5-4
Figure 5-4	Example of a PPPoE session on a DSL interface.....	5-9
Figure 5-5	PPPoE client with a filtered upstream traffic stream.....	5-12
Figure B-1	GE-OLIM interface applications .....	B-2
Figure B-2	Optical connection to a GE-OLIM.....	B-3
Figure B-3	GE-OLIM status lights .....	B-4
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	Phase 2: Protection block assembly.....	C-5
Figure C-5	Protection block port assignments.....	C-6
Figure C-6	Protection plug orientation example.....	C-7
Figure C-7	Stub cables for connection to the protection blocks.....	C-16
Figure C-8	Protection block power connectors.....	C-18
Figure C-9	-48Vdc stub-ended power cable.....	C-19
Figure C-10	-48Vdc power supply cable .....	C-19
Figure C-11	Door alarm connectors on the Stinger CR chassis .....	C-20
Figure C-12	Optical Connectors.....	C-21
Figure D-1	UL60950-21 .....	D-3
Figure D-2	Warning labels for identification of Class 1 laser devices.....	D-11
Figure E-1	Replacing a door assembly on a deployed Stinger CR .....	E-2
Figure E-2	Label for serialized number.....	E-3
Figure E-3	Blank label portion on the new door .....	E-3
Figure F-1	Retrofit Kit Parts.....	F-2
Figure F-2	Screws with captive washers.....	F-6
Figure F-3	Protection block assembly .....	F-7
Figure F-4	Captive knobs.....	F-8
Figure F-5	Male-Male standoffs.....	F-9
Figure F-6	Male-Female standoffs .....	F-9
Figure F-7	Male-Male standoffs.....	F-10
Figure F-8	Securing male-male standoffs .....	F-11
Figure F-9	Sliding in the duct, transition.....	F-12
Figure F-10	Fan lights.....	F-12
Figure G-1	Card Cage Rack Mount System parts.....	G-2
Figure G-2	CCRMS grounding options .....	G-5
Figure G-3	Additional brackets in CCRMS for stress prevention .....	G-8

---

# 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 Internet Protocol DSL Access Multiplex (IP DSLAM) unit:

- Physical installation of a Stinger Compact Remote IP DSLAM unit
- Physical installation and connection of components
- Physical configuration of a Stinger Compact Remote IP DSLAM as a remotely hosted unit
- Configuration of a Stinger host to utilize a hosted Stinger Compact Remote IP DSLAM

This guide also provides Stinger Compact Remote IP DSLAM technical specifications and an operational overview of the Stinger Compact Remote IP DSLAM. 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 IP DSLAM units running software version 9.8 or later. The Stinger Compact Remote IP DSLAM is not supported by earlier software releases.



**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:

<b>Convention</b>	<b>Meaning</b>
Monospace text	Represents text that appears on your computer’s screen, or that could appear on your computer’s screen.
<b>Boldface monospace text</b>	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.)
Press Enter	Means press the Enter or Return key or its equivalent on your computer.

<b>Convention</b>	<b>Meaning</b>
 <b>Note</b>	Introduces important additional information.
 <b>Caution</b>	Warns that a failure to follow the recommended procedure could result in loss of data or damage to equipment.
 <b>Warning</b>	Warns that a failure to take appropriate safety precautions could result in physical injury.
 <b>Warning</b>	Warns of danger of electric shock.

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

- *Stinger IP Control Module Configuration Guide*. For Stinger systems with an IP2000 or IP2100 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 IP DSLAM description . . . . .	1-1
Stinger Compact Remote hardware . . . . .	1-1
Host hardware . . . . .	1-4

## Stinger Compact Remote IP DSLAM description

The Stinger Compact Remote IP DSLAM is a temperature-hardened unit that can be installed outdoors, close to subscriber locations. Power can be provided over dedicated copper telecommunications facilities from the central office or a local power source. It is configured to function as a hosted optical network unit (ONU) that can provide subscriber data service, including VOIP telephony and digital video service. The Stinger Compact Remote IP DSLAM unit uses Gigabit Ethernet connections internally and for the connection to its host unit to provide multiple high-bandwidth services.

## Operational overview

The Stinger Compact Remote IP DSLAM is equipped with a Gigabit Ethernet control and optics pack (GE-COP). This circuit pack provides the hardware to control the operation of components in the local chassis, and two Gigabit Ethernet optical ports for connections to a host Stinger unit. Management and configuration for the Stinger Compact Remote IP DSLAM is handled through the TAOS management interface on the host Stinger unit.

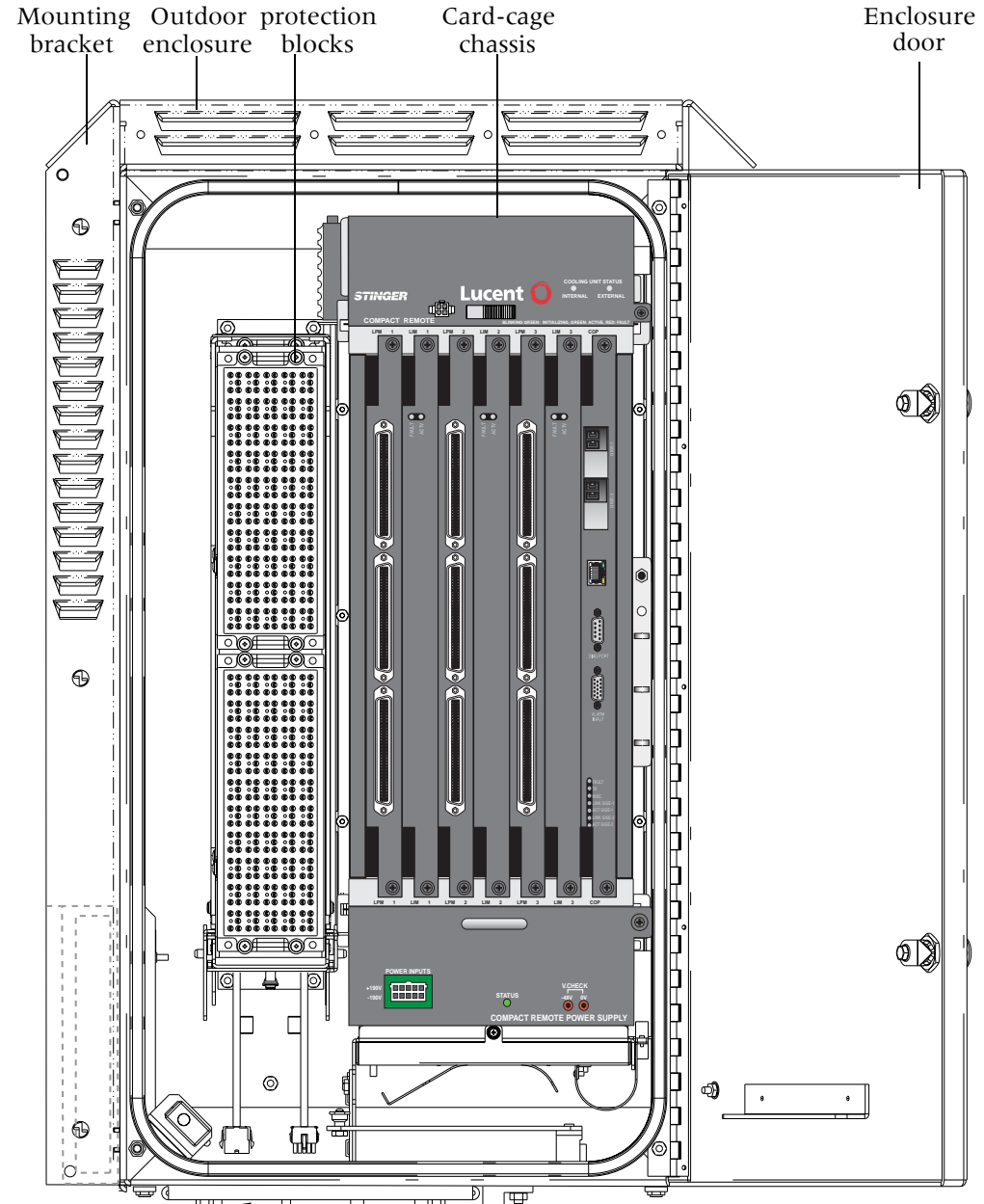
Subscriber DSL lines are physically terminated on the Stinger Compact Remote chassis. However, these lines appear as connection endpoints within the TAOS management interface for the host Stinger unit. Their configuration is also handled through the host management interface.

## Stinger Compact Remote hardware

The Stinger Compact Remote IP DSLAM unit, shown in Figure 1-1, consists of a card-cage chassis in an integrated outdoor enclosure. The unit is designed for installation in outdoor locations to bring DSL digital services close to customer locations. The enclosure is pre-wired with protection blocks for the copper telecommunications facilities, and provides an operating environment that can tolerate temperatures between -40°F (-40°C) and 114.8°F (+46°C). (For more environmental information, see “Operating environment” on page D-13.) The

card-cage chassis accommodates modular circuit packs, a cooling unit, and a power supply.

*Figure 1-1. The Stinger Compact Remote IP DSLAM*

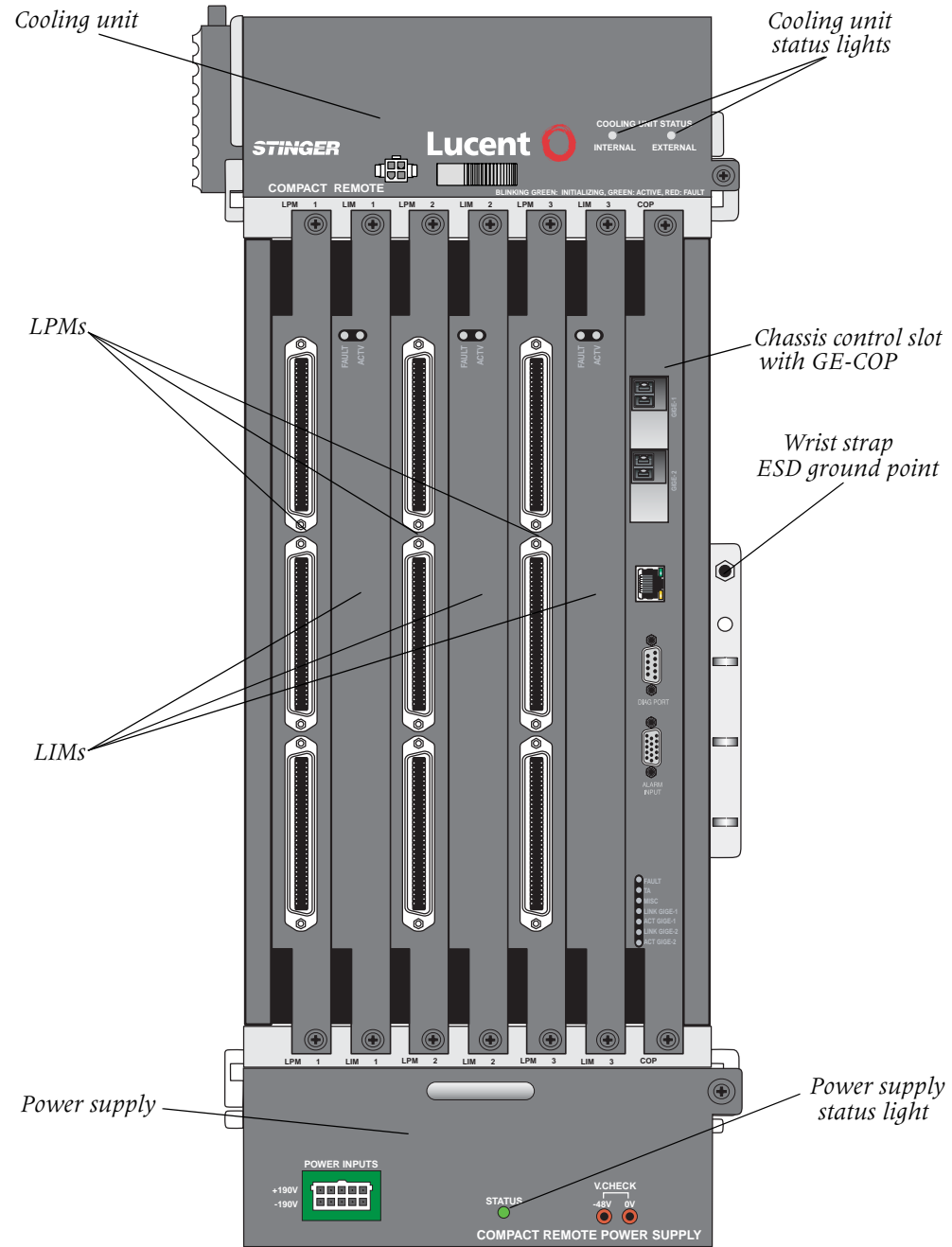


## **Stinger Compact Remote card cage chassis**

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

card cage, and a power supply is installed in a bay at the bottom of the card cage. These components are illustrated in Figure 1-2.

Figure 1-2. Stinger Compact Remote IP DSLAM card-cage



## Card-cage modular components

Each of the replaceable modular components support different capabilities.

- **The GE-COP**—The GE-COP is a specialized control and optics module that controls the operation of the unit. It contains controller hardware similar to that in control modules on larger Stinger units but the local management interface is not used for system configuration. It provides two Gigabit Ethernet optical interfaces that can be used to link the Stinger Compact Remote unit to a specialized Gigabit Ethernet optical line interface module (GE-OLIM) installed in a host Stinger unit. The port labeled GIGE-1 carries end-user traffic and a control link for management of the Compact Remote IP DSLAM unit. A second Gigabit Ethernet port, labeled GIGE-2 provides optional support for additional bandwidth for end-user traffic.
- **ADSL/ADSL2+ RLIMs**—The Stinger Compact Remote IP DSLAM requires specialized IP line interface modules (IP LIMs) that support the internal Ethernet architecture of the unit. Other LIMs cannot be used in this unit. The internal interfaces of these LIMs are configured to provide service for individual DSL subscriber lines. LIMs installed in a Stinger Compact Remote IP DSLAM unit are referred to as remote line interface modules (RLIMs), because they are accessed remotely, through the management interface of the host unit, for configuration and maintenance.
- **Line protection modules (LPMs)**—The LPMs provide protection for the unit from transient conditions on the subscriber lines and the facilities to the central office. LPMs with splitters, designed for the Stinger Compact Remote IP DSLAM, combine analog voice service from the central office and DSL service from the Stinger IP DSLAM on the same pair of wires to the subscriber.
- **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 Compact Remote IP DSLAM. The cooling unit also monitors, controls, and provides power to an external ventilation fan, mounted in the side of the enclosure.
- **Power supply**—Two different power supplies are available for the Stinger Compact Remote IP DSLAM.
  - **±190Vdc Power supply**—This power supply converts +190Vdc and -190Vdc provided from the central office into -48Vdc needed to operate the Stinger Compact Remote IP DSLAM.
  - **-48Vdc Power supply**—This power supply supports the use of native -48Vdc needed to operate the Stinger Compact Remote IP DSLAM.

## Host hardware

A Stinger FS+ unit must be properly equipped to act as a host for a Stinger Compact Remote IP DSLAM unit. It must be controlled by an IP2100 IP control module, or two IP2100 modules can be installed for redundancy. The host Stinger FS+ must contain one or more Gigabit Ethernet OLIMs (GE-OLIMs).

## IP control module

The Stinger FS+ host unit must be equipped with an IP2100 IP control module. The Gigabit Ethernet ports on this module can be used to support IP connections for high speed data and VOIP connections for end users.

## Gigabit Ethernet OLIM

A host Stinger FS+ unit must have a GE-OLIM installed to terminate a link from the GE-COP in a Stinger Compact Remote IP DSLAM unit. Stinger Compact Remote IP DSLAM units depend on a Gigabit Ethernet optical link to a host Stinger from the GIGE-1 port of the GE-COP for a configuration and control link. Each GE-OLIM in a host unit contains six Gigabit Ethernet optical interfaces that support these connections.

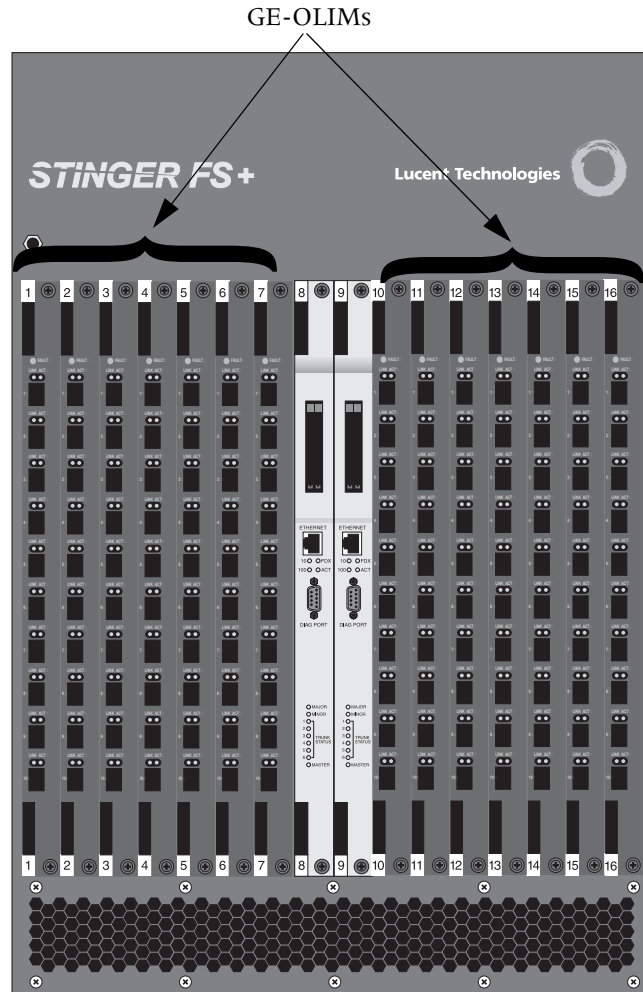
A GE-OLIM can support connections for up to six hosted Stinger Compact Remote IP DSLAM units with one link per unit, or up to three Stinger Compact Remote IP DSLAM units with two links per unit. A Stinger host can support up to a total of 42 remote Stinger Compact Remote IP DSLAM units.

The GE-OLIM also provides two Gigabit Ethernet trunk ports that can be used for “upstream” connections to a transport network. The trunk ports support high-speed digital video transmission from an upstream transport network. Two additional Gigabit Ethernet ports on the module are reserved for future use.

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

Figure 1-3 shows a Stinger FS+ with GE-OLIMs installed.

Figure 1-3. GE-OLIMs installed in a Stinger FS+ host



In the host Stinger unit, you can create profiles that are associated with the Compact Remote IP DSLAM units that are connected to it. These profiles, in the management interface of the host unit, allow the Stinger Compact Remote IP DSLAM units and the Stinger host to be managed through the same interface. See Chapter 4, “Hosted System Configuration,” for detailed information about these profiles and the configuration of the hosted Stinger Compact Remote IP DSLAM.

For detailed physical information about the Stinger GE-OLIM, see the Appendix B, “The Host Stinger GE-OLIM.”

---

# Preparing to Install the Unit

# 2

Installation safety . . . . .	2-1
Installation tools and equipment . . . . .	2-1
Preventing static discharge damage . . . . .	2-2
Unpacking the Stinger Compact Remote IP DSLAM . . . . .	2-4
Verifying the hardware. . . . .	2-4
Checking modules and chassis. . . . .	2-7

## Installation safety

Only trained and qualified personnel should perform installation and maintenance of the Stinger Compact Remote IP DSLAM. All work should be done in compliance with local safety guidelines and installation procedures. This unit contains sharp edges, moving fan blades, and electrical voltages that can cause injury to personnel, and damage to the Stinger hardware. You should read Appendix D, “Safety-Related Electrical, Physical, and Environmental Information” before installing a Stinger Compact Remote IP DSLAM unit.

## Installation tools and equipment

To install and configure the Stinger Compact Remote IP DSLAM 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 stripping wire insulation
- Standard screwdriver set, wrenches, and drills
- *(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.

- 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

## 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.

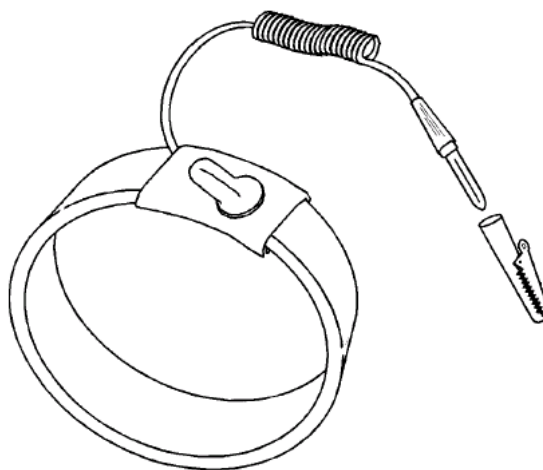
### Use a wrist strap

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.



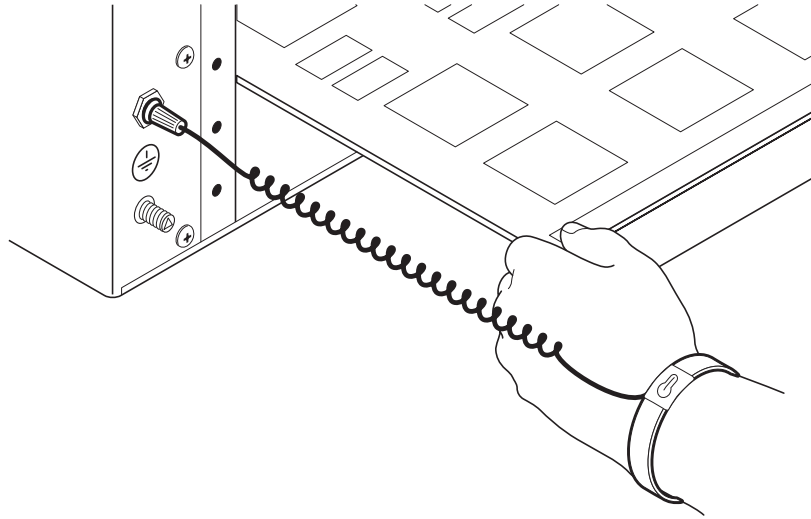
**Caution** Correct use of an approved antistatic wrist strap is the only reliable way to prevent damage to components by electrostatic discharge from your body

*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 as shown in Figure 2-2. (See Figure 2-5 on page 2-7 for the location of ESD grounding point on the Stinger Compact Remote IP DSLAM.)

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 IP DSLAM

The unit is delivered with the Stinger Compact Remote IP DSLAM 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 plastic or wooden pallet with screws and L-brackets.

Before you remove the Stinger Compact Remote IP DSLAM 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 Compact Remote IP DSLAM unit in its enclosure with its power supply, fans, and cables weighs up to 155 pound (70kg). This weight does not include protection elements, LIMs, LPMs, or the COP. See “Weight and lifting requirements” on page D-10 for detailed weight information.

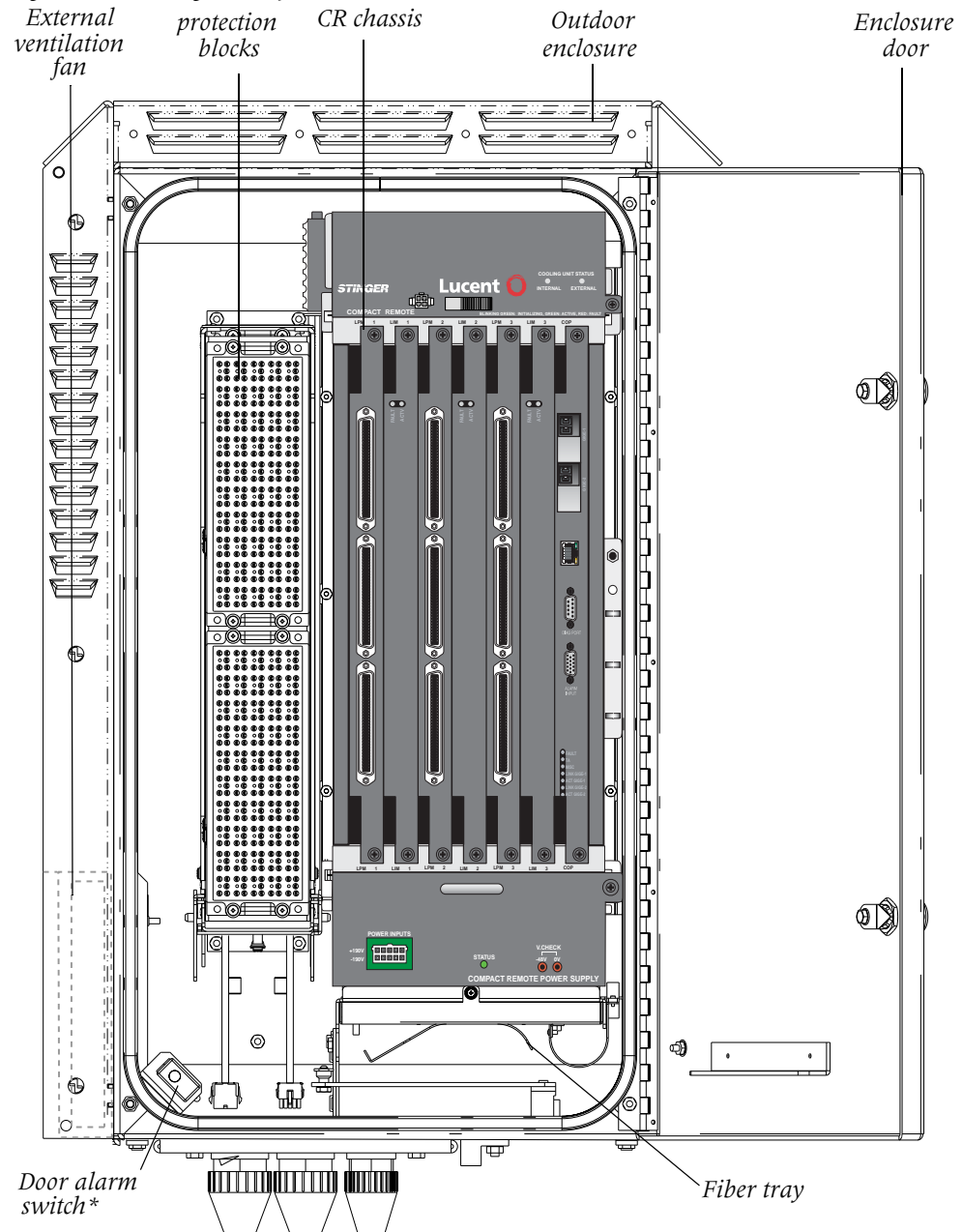
To unpack the unit:

- 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 2-4).
- 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 Compact Remote IP DSLAM card cage chassis is delivered in its outdoor enclosure with the cables, power supply, and fans. The protection blocks are not delivered with the system. 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 Compact Remote IP DSLAM enclosure.

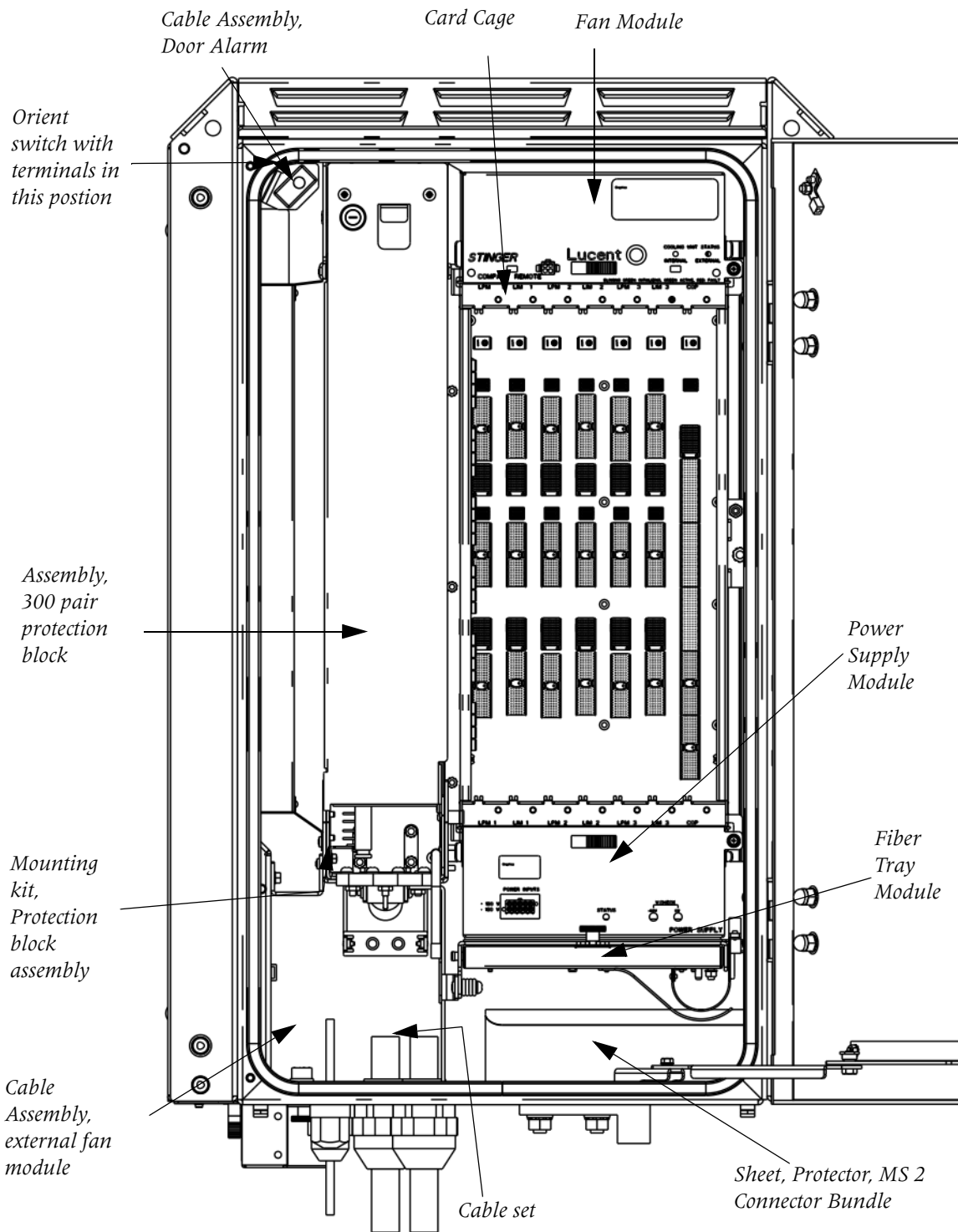
Figure 2-3. Stinger Compact Remote IP DSLAM enclosure details



\* To deactivate the door alarm, when the door is open for service, pull out the alarm switch plunger. Closing the door returns this switch to normal operation.

**Preparing to Install the Unit**  
Verifying the hardware

Figure 2-4. Phase 2 : Stinger CR ATM DSLAM enclosure details



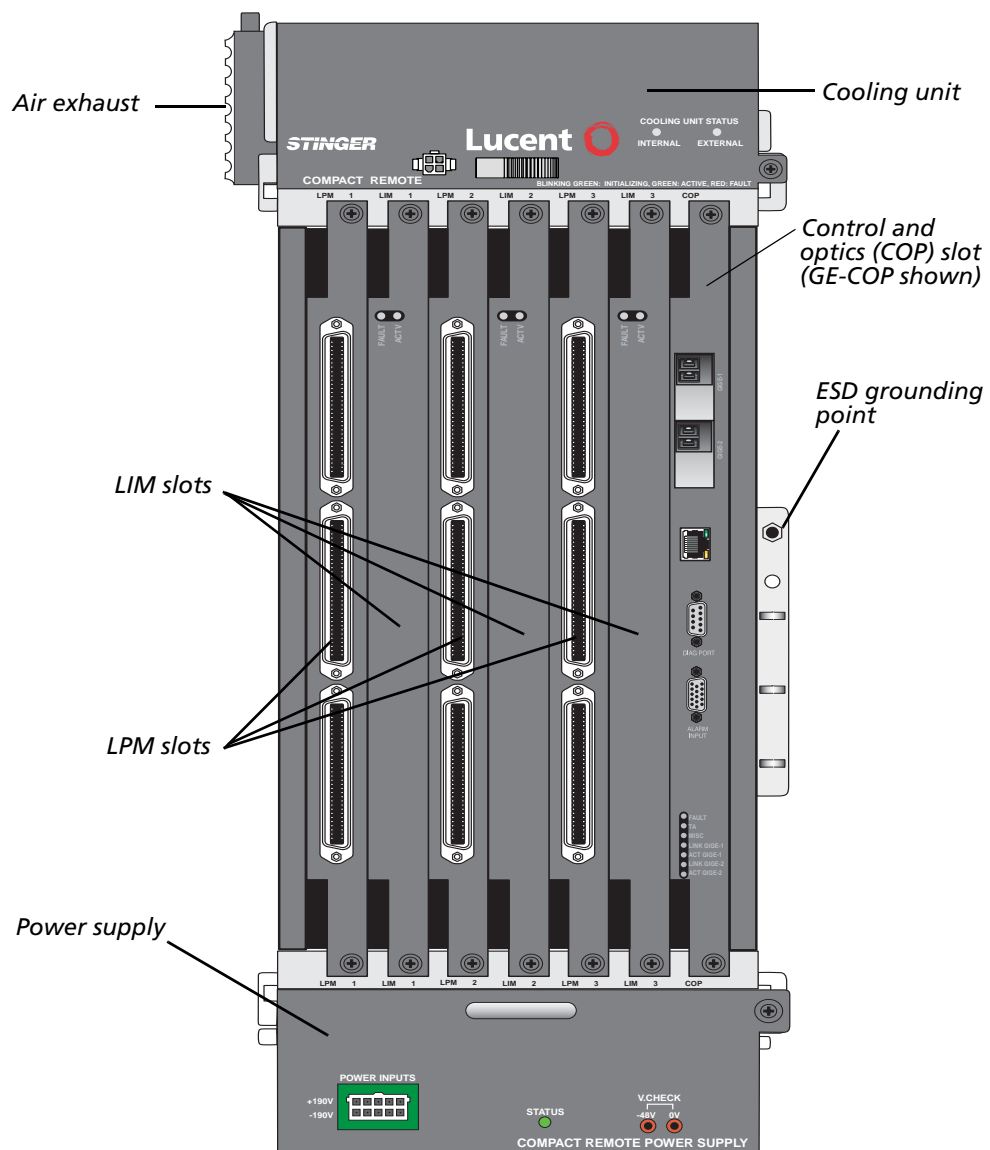
## Checking modules and chassis

The Stinger Compact Remote IPDSLAM has a backplane design that enables the installation and removal of all major circuit packs and modules in the front of a unit. Figure 2-5 shows the front slots of a Stinger Compact Remote IPDSLAM chassis, equipped with a GE-COP and three sets of RLIMs and LPMs.



**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 2-5).

Figure 2-5. Front view of a Stinger Compact Remote IPDSLAM chassis



**Caution** For the blank circuit packet slots that are not occupied by modules, use airdam modules to ensure proper air flow through the unit.

You can either use the power supply or the power filter.

## **Checking the COP**

The vertical slot on the right side in front of the unit is the control slot (see Figure 2-5). This slot contains the module that controls the backplane and coordinates the function of the local hardware.

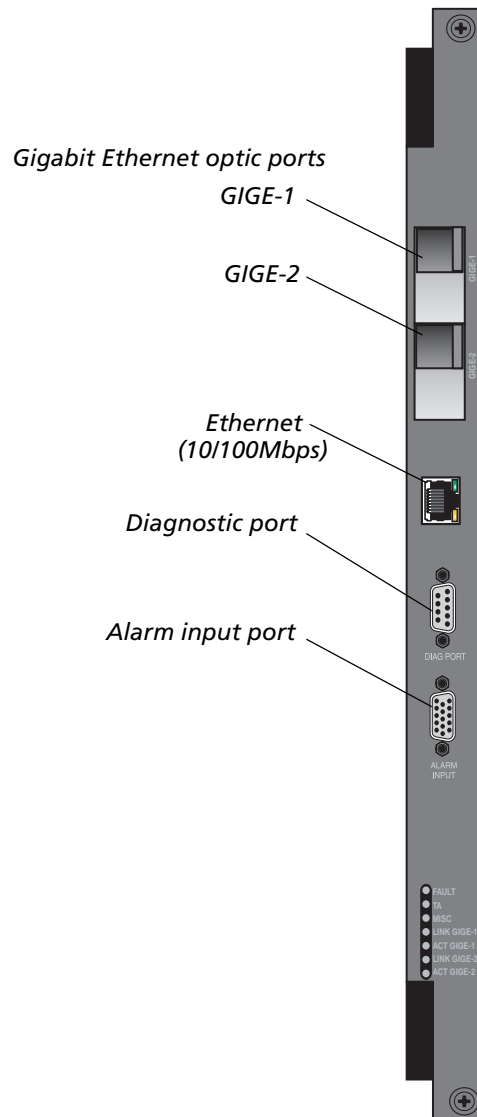
### **The COP**

The Stinger Compact Remote IPDSLAM requires a Gigabit Ethernet COP. The serial interface on this GE-COP is not used for configuration of the unit. It depends upon a Gigabit Ethernet optical link to a host Stinger unit for configuration and management. This optical link is provided by the interface labeled GIGE-1. This link also carries network traffic for end users that are connected to the Compact Remote unit. A second Gigabit Ethernet interface, labeled GIGE-2, provides an optional connection for second link for additional end-user bandwidth.

### **COP interfaces**

Figure 2-6 shows the location of the Gigabit Ethernet optical ports, serial diagnostic port, 10/100Mbps Ethernet port, and alarm input port.

Figure 2-6. Control and optics pack



Unlike standard control 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 IP2100 module in the host Stinger unit.

## Checking the LIMs

The Stinger Compact Remote IP DSLAM unit uses a 48-port IP ADSL2+ LIM (STGRCR-ELIM-AP-48) that is designed to operate across the internal bus of the unit at higher rates than other LIMs. Other LIMs are not supported for use in the Stinger Compact Remote IP DSLAM unit.

The LIMs 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.

The 48-port IP ADSL2+ LIM (STGRCCR-ELIM-AP-48) has been designed to meet the power and heat specifications of the Stinger Compact Remote IP DSLAM unit. The 48-port IP ADSL2+ LIM is shown in Figure 2-7.



**Caution** Other Stinger ADSL LIMs are not supported in the Stinger Compact Remote IP DSLAM and may also result in excessive temperatures within the unit.

*Figure 2-7. The 48-port IP ADSL2+ LIM*

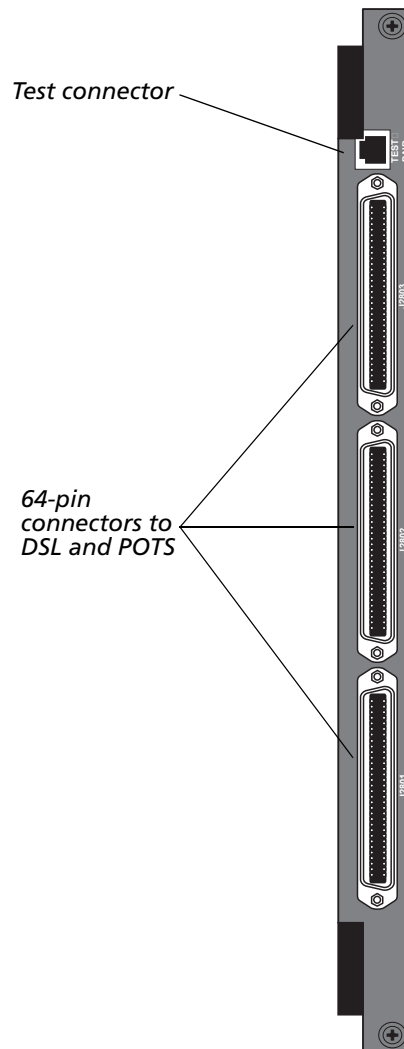


## Checking the LPMs

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 (STGRRCR-LPM2-48-S) is designed for use with the 48-port IP ADSL2+ LIM in the Stinger Compact Remote IP DSLAM. It provides connection points for coupling analog voice service onto the subscriber facilities that carry the DSL service. Specific information about making 2-wire ADSL and POTS connections to the 48-port LPM with splitters is contained in the Appendix C, “Cables and Connectors.”

Figure 2-8. The 48-port LPM with splitters



## Checking the cooling unit

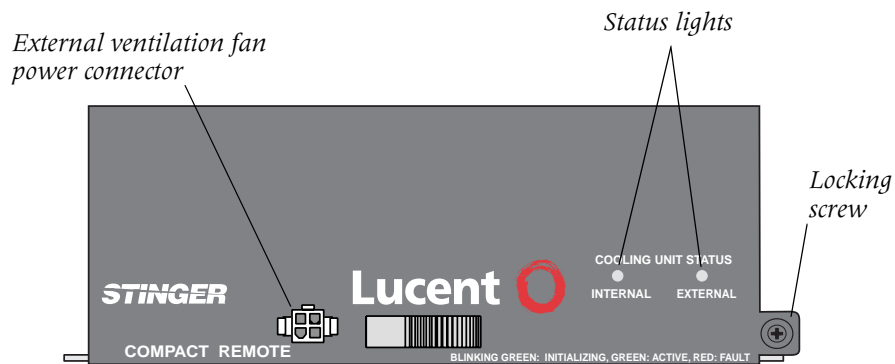
The cooling unit used in the Stinger Compact Remote IP DSLAM is identical to the cooling unit used in the Stinger Compact Remote ATM DSLAM unit. It is installed at the top of the Compact Remote chassis. It uses an internal fan to circulate air past components in the chassis and provides power for an external ventilation fan in the side of the outdoor enclosure. Heat is removed from the enclosure by air circulation and dissipation 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 Compact Remote cooling unit is shown in Figure 2-9.

Figure 2-9. The Stinger Compact Remote cooling unit



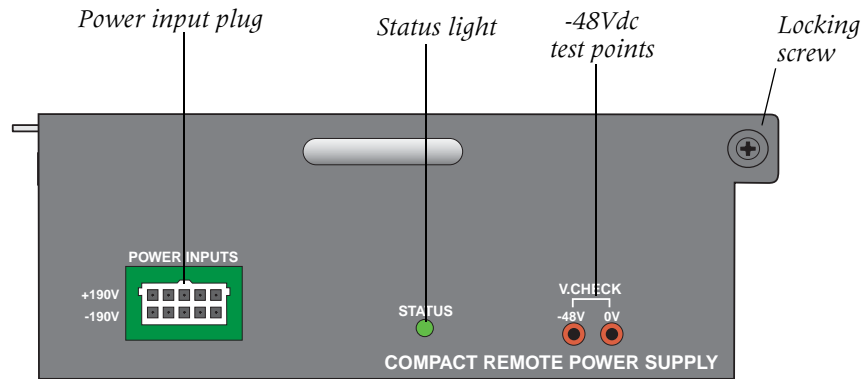
## Checking the power supply

Power supplies used in the Stinger Compact Remote IP DSLAM are identical to power supplies used in the standard ATM-based Stinger Compact Remote unit. The Stinger Compact Remote power supply is installed at the bottom of the chassis. Two types of power supplies are available. One type accepts +190Vdc and -190Vdc from the central office over multiple pairs of copper telecommunications facilities. The type other accepts -48Vdc over a single pair of 18 AWG wires that are routed into the cabinet separately from the copper telecommunications facilities.

### The $\pm 190$ Vdc power supply

The Stinger Compact Remote  $\pm 190$ Vdc 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 Compact Remote. The  $\pm 190$ Vdc power supply is shown in Figure 2-10.

Figure 2-10. The Stinger Compact Remote  $\pm 190\text{Vdc}$  power supply

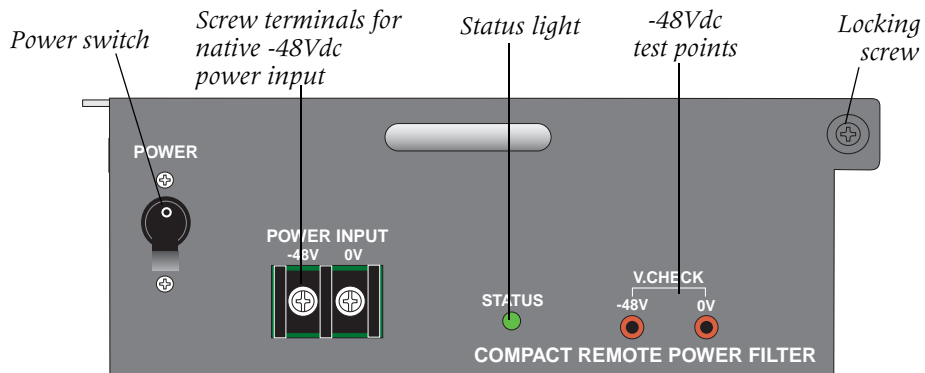


## The power filter

The Stinger Compact Remote power filter (-48Vdc power supply) regulates and filters native -48Vdc to power the unit.

The Stinger Compact Remote power filter (-48Vdc power supply) is shown in Figure 2-11.

Figure 2-11. The Stinger Compact Remote power filter -48Vdc power supply





---

# Compact Remote Enclosure and Component Installation

# 3

Introduction . . . . .	3-1
Before you begin . . . . .	3-1
Stinger CR enclosure mounting hardware . . . . .	3-2
Mounting the enclosure on a pole . . . . .	3-8
Mounting the enclosure on a wiring cabinet . . . . .	3-14
Route and connect the fibers and ground cable inside the enclosure . . . . .	3-16
Routing the cables out of the enclosure . . . . .	3-17
Grounding the enclosure . . . . .	3-20
Installing and replacing Stinger Compact Remote components . . . . .	3-22
Physical connections to the Stinger Compact Remote unit . . . . .	3-32
Turning on power to a Stinger Compact Remote unit . . . . .	3-38
Status lights . . . . .	3-40
What's next . . . . .	3-44

## Introduction

This section describes the hardware that is available for mounting the Stinger Compact Remote in different locations. The installation process for the two most common locations, pole mounting and cabinet mounting, are also described, along with instructions for installing and replacing the components of the Stinger Compact Remote.

## Before you begin

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

- Locate all necessary hardware and tools at the installation site
- Unpack the Stinger unit
- Attach the appropriate Stinger CR mounting hardware to the outdoor cross-connect cabinet, pedestal, pole, or rack.

- Prepare cables and cable routes. (Drill pass-through holes, if required for cabinet mounting, using the appropriate template, or make cabling provisions for pole mounting.)
- Mount the Stinger CR enclosure to the mounting hardware.
- Route and connect cabling for telecommunication facilities and power to the Stinger CR.



**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.



**Warning** Before making connections, ensure that the bare conductors are coated with an appropriate antioxidant compound. Before connecting, all mounting hardware such as unplated connectors, braided strap, and bus bars must be brought to a bright finish and then coated with an antioxidant.

## Stinger CR enclosure mounting hardware

Depending on the local environment, the Stinger Compact Remote enclosure can be mounted in the following ways:

- On a standard telephone utility pole—The enclosure can be mounted on a standard telephone utility pole in a center-mount or side-mount configuration.
- On a concrete pad—A concrete pad can be poured, and the enclosure can be mounted on the pad using the pedestal mount kit.
- On an outdoor wiring cabinet—The rear or side of the enclosure can be mounted to an outdoor wiring cabinet.
- In an equipment rack—The enclosure can be installed in an equipment rack, in a central office, or local equipment hut.

Several different mounting kits can be ordered with the hardware to support these types of installations. These kits, with their Comcodes, are identified and described in Table 3-1.

*Table 3-1. Stinger Compact Remote mounting hardware*

<b>Comcode</b>	<b>Description</b>	<b>Includes</b>
300715547	Pole mount kit: center mount (rear) or side mount	Pole mount brackets, center (rear) mounting bracket, hanger, lag bolts, cable cover, and screws
109579813	Pole mount kit: side mount only	Pole mount brackets, lag bolts, cable cover, and screws
300716735	Pedestal mount kit	All components of 300719564 and 300719572

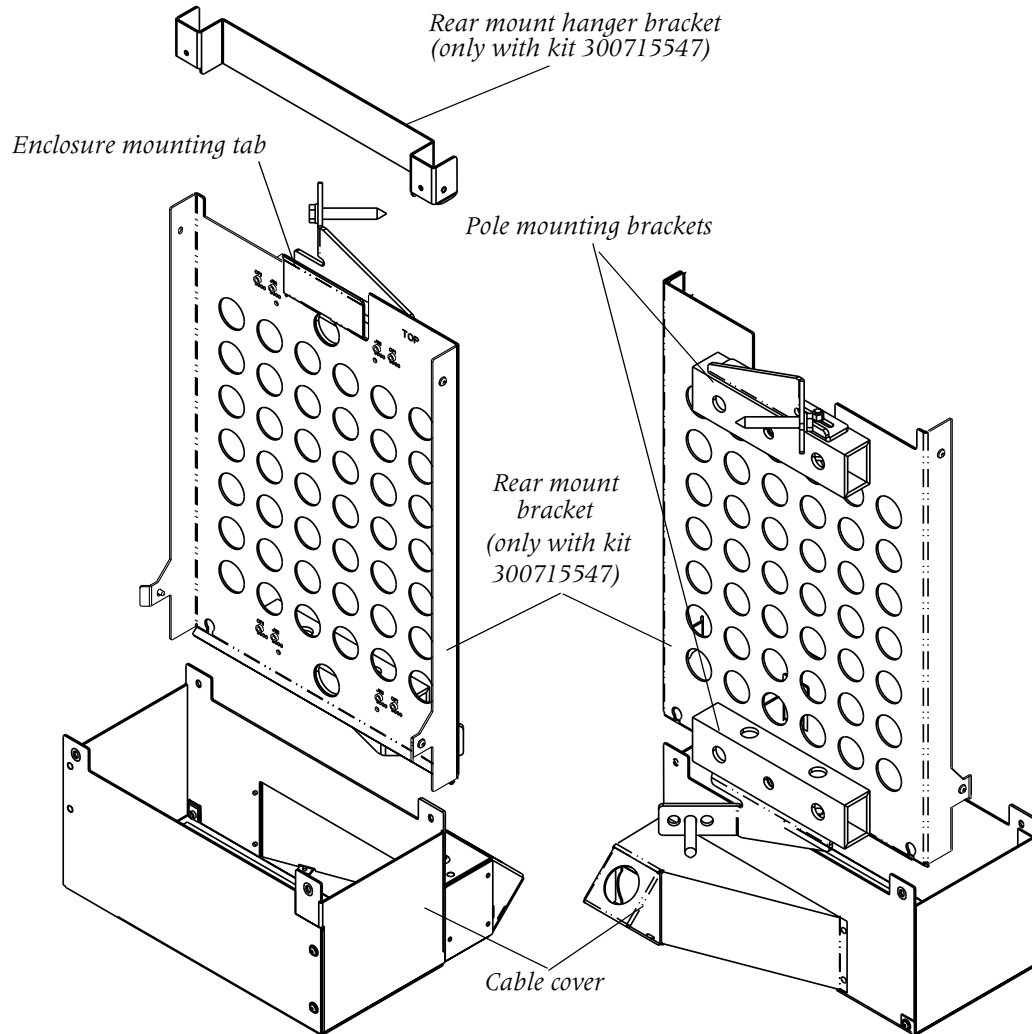
*Table 3-1. Stinger Compact Remote mounting hardware (continued)*

<b>Comcode</b>	<b>Description</b>	<b>Includes</b>
300719564	Pedestal mount kit: cable and splice hardware	Splice cover, splice holder bracket, cable cover for pedestal mount, and screws
300719572	Pedestal mount kit: pad hardware	Pedestal bracket, duct alignment plate, outrigger mounting brackets, and anchor bolts
300716743	JWI (jumper wire interface) cabinet rear mount kit	Rear mounting bracket, hanger, cable cover, cable cover extension, and screws
300716750	OPI (outside plant interface) cabinet rear mount kit	Rear mounting bracket, hanger, cable cover, and screws
300716727	JWI/OPI kit: side mount cable cover	Side-mount cable cover and screws
109567164	Inside rack mount kit	Side brackets for rack mounting, screws, nuts, and washers

## Pole mounting hardware

Figure 3-1 illustrates the pole mounting hardware that is included with kits 300715547 and 109579813

Figure 3-1. Pole mounting hardware



## Cabinet mounting hardware

The Stinger Compact Remote can be side-mounted or rear-mounted to a wiring cabinet. It is side-mounted with the integrated mounting brackets on the enclosure shown in Figure 3-2. A cable cover for this installation is provided with kit #300716727.



**Note** There is a ventilation fan on the left side of the enclosure. When possible, mount right side of enclosure to left side of a wiring cabinet. This provides better access to the ventilation fan for service.

Kit 300716750 provides the rear mount hanger bracket, rear mount bracket, and cable cover for rear-mounting the enclosure to an wiring cabinet.

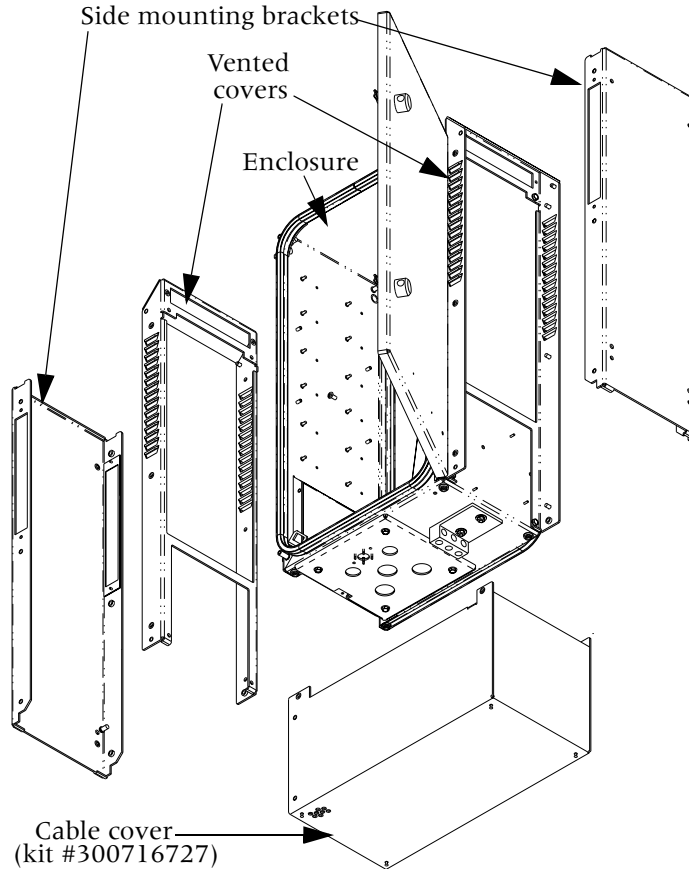


**Note** Kit 300716743 is available for customers using a JWI cabinet. It also includes a cable cover extension for rear-mounting the enclosure to a this type of cabinet. The hardware provided by these kits is illustrated in Figure 3-3.

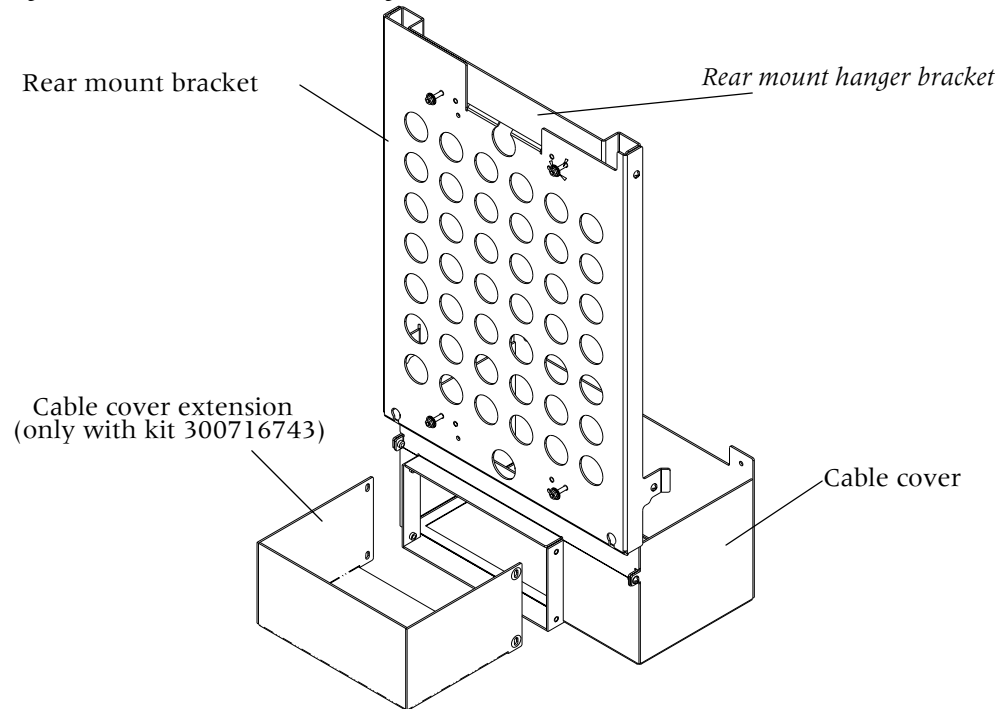


**Note** The actual supplied equipment might have visual differences as compared to the figures provided in this chapter.

Figure 3-2. Cabinet side-mounting hardware



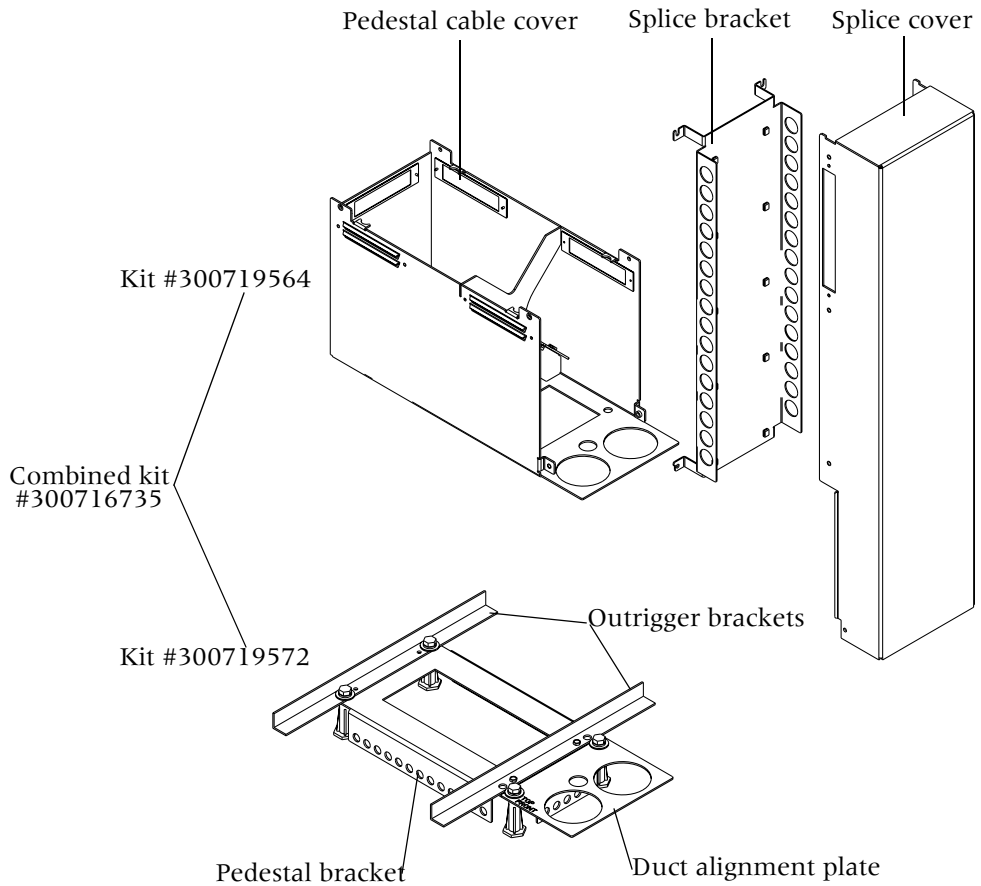
*Figure 3-3. Cabinet rear-mounting hardware*



## **Pedestal mounting hardware**

The Stinger Compact Remote can be mounted on an outside pedestal. The pedestal cable cover and splice cover hardware can be ordered in kit #300719564. The pedestal mounting hardware can be ordered in kit #300719572. These kits can also be ordered combined as kit #300716735. This hardware is shown in Figure 3-4.

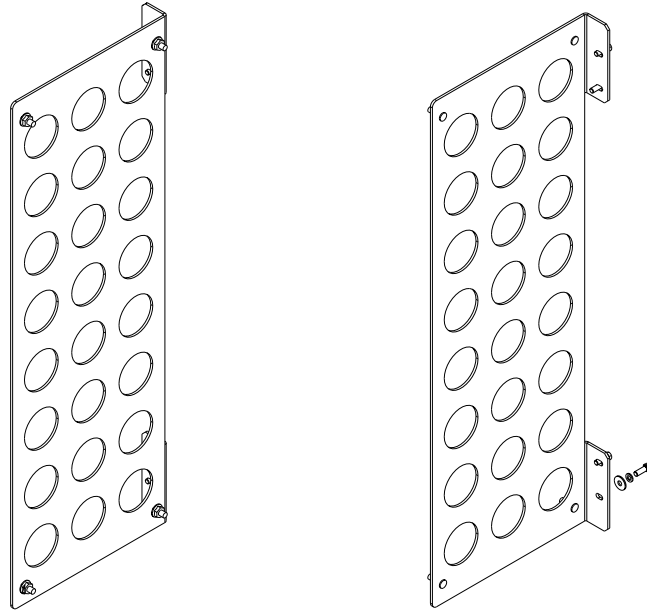
Figure 3-4. Pedestal mounting kit hardware



## Inside rack mounting hardware

Side rack mounting brackets can be attached to the enclosure for mounting in an equipment rack that has rails that are 23 inches apart, with 1.75in. hole spacing. These brackets are ordered with kit number 109567164, and are shown in Figure 3-5.

Figure 3-5. Side rack mounting brackets



The Stinger CR enclosure has integrated mounting brackets that are used for mounting the enclosure. These brackets attach to vented covers on the side of the enclosure. These mounting brackets are used with all kits except the pedestal mount kit.

## Mounting the enclosure on a pole

The Stinger Compact Remote ATM DSLAM is delivered in its integrated outdoor enclosure with all ordered components installed prior to shipment.



**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-13.

To install a Stinger Compact Remote enclosure on a pole, you need the following items:

- The Stinger Compact Remote enclosure
- The Stinger pole mounting hardware (see Figure 3-1 on page 3-4)
- 2 locally supplied pole mounting bolts, 5/8in. in diameter, with a 15/16in. hexagonal head, and a threaded length that is at least 1.25 in. (3.175cm) greater than the diameter of the pole
- An antistatic wrist strap (Lucent number: R-4987C or equivalent) for handling components
- An electric drill
- A 5/16in. diameter drill bit with at a 10 inch extension.
- An 11/16 inch diameter drill bit, or a drill bit 0.625 to 0.7 in. (15.875mm to 17.78mm) in diameter, that is long enough to pass completely through the pole
- A 15/16 in. combination wrench

- A 15/16 in. socket with a 2 in. extension (min.) and handle.
- A 9/16 in. socket
- A 10 inch (25cm) tongue and groove (channel lock) pliers
- Safety screw driver for removal and installation of tribunal recessed head screws (Part number 29-99-183-22, available from Southco Inc., or equivalent)
- Phillips and slot screwdrivers

Follow all local safety practices and guidelines in performing this work to avoid injury and the interruption of existing service.

## Center-mounting the enclosure on a pole

To center-mount the rear of the enclosure to a pole, do not immediately remove the shipping brackets or pallet from the base of the enclosure. The shipping brackets can be used as handles to help lift and position the enclosure when mounting it. The pallet also protects the cables below the chassis until it is mounted on the pole.

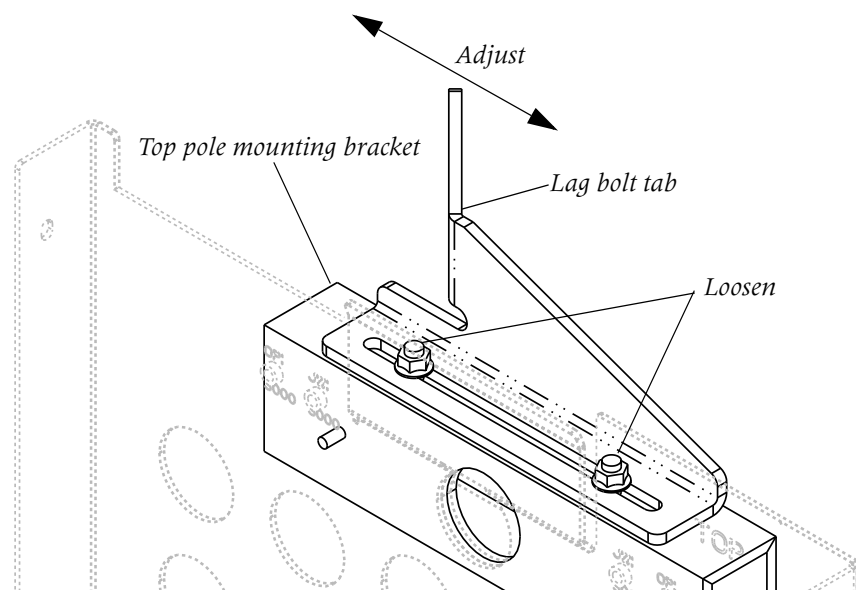
You may use the following procedure to center-mount (rear-mount) the enclosure to a pole.



**Note** These instructions assume that the pole is vertical. On poles that lean more than 2°, additional precautions must be taken to be sure that the mounting bolts are centered through the pole, and that the pole does not obstruct the enclosure cable duct.

- 1 Use a 9/16 in. combination wrench or socket with a 6 in. extension and handle to loosen the two nuts that secure the lag bolt tabs on the top and bottom pole mounting brackets. The top bracket is shown in Figure 3-6. (These tabs must be loose so that you can adjust them to the diameter of the pole when you install the hardware. The tabs will be secured after the hardware is mounted on the pole.)

Figure 3-6. Lag bolt tab adjustment

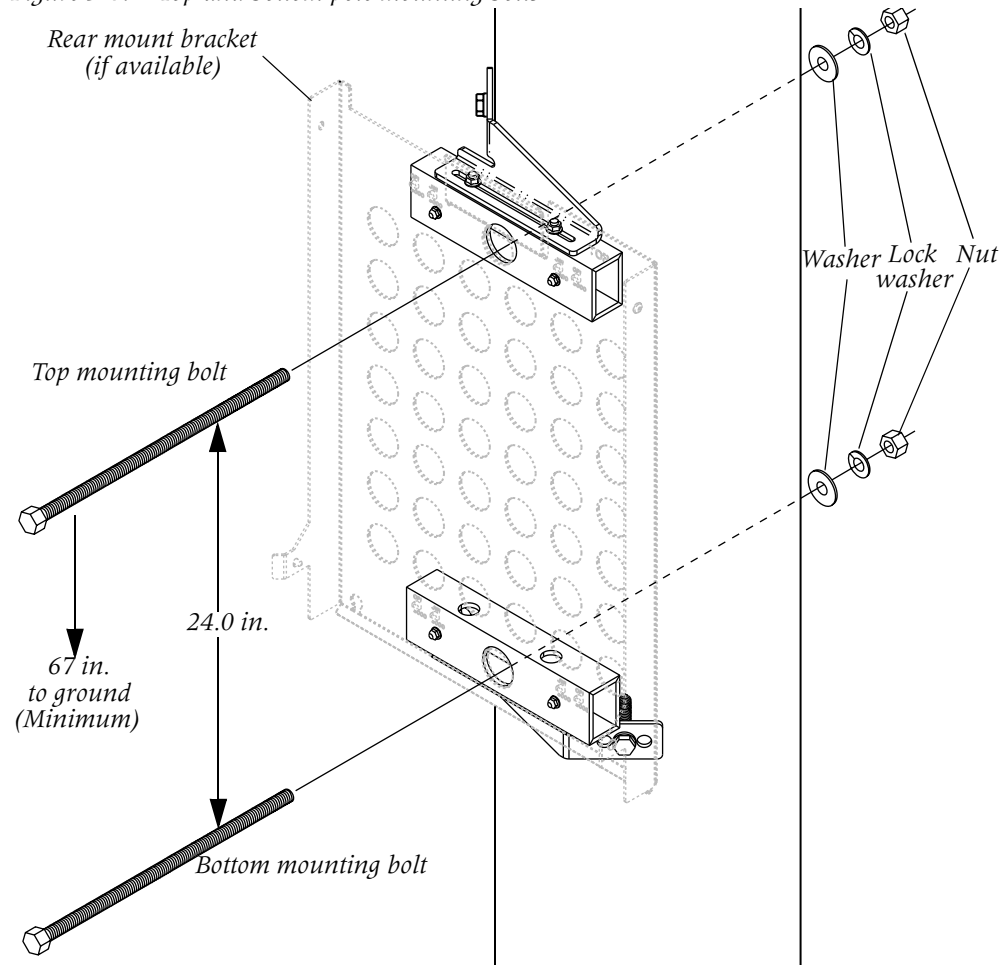


## Compact Remote Enclosure and Component Installation

### Mounting the enclosure on a pole

- 2 Position the mounting hardware against the pole so that the center mounting bolt hole of the top pole mounting bracket is centered on the pole at least 67 inches (1.7 meters) above the ground (see Figure 3-7). Mark the location for the top mounting bolt hole on the pole and use an 11/16in. drill bit, or a drill bit that is 0.625in. to 0.7in. (15.875mm to 17.78mm) in diameter, to drill the hole for the top mounting bolt through the center of the pole.

Figure 3-7. Top and bottom pole mounting bolts



- 3 Use the top mounting bolt to temporarily install the mounting hardware on the pole. Allow the hardware to hang vertically and mark the location for the lower mounting bolt on the pole.
- 4 Remove the mounting hardware from the pole and drill the hole for the lower mounting bolt. Then permanently mount the hardware, using the top and bottom mounting bolts.



**Note** The threaded end of the bolt should extend at least 1 inch beyond the back of the pole.

- 5 Place washers and nuts on the threaded ends of the two bolt ends and use a 15/16in. combination wrench to tighten the nuts until the washers begin to become concave into the pole.



**Note** While tightening the nut on the threaded end of the bolt, hold the bolt head with a 15/16in. socket with a 2in. extension (min.) and handle.

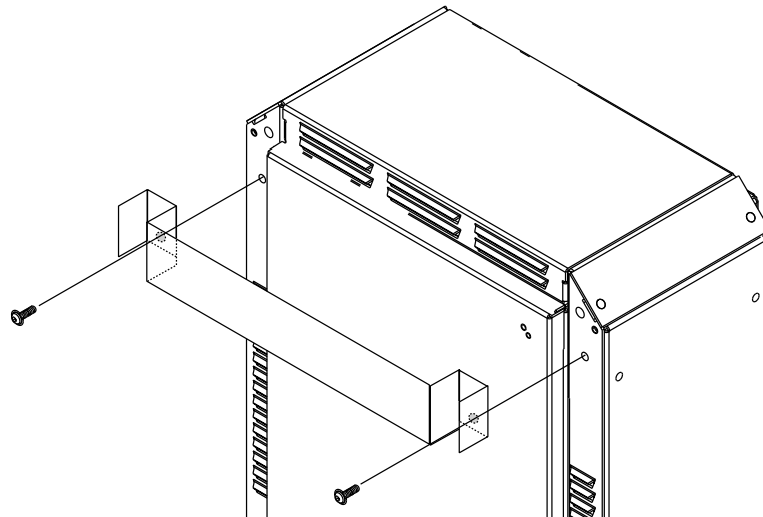
- 6 Slide the lag bolt tabs on each of the pole mounting brackets so that the tabs are in contact with the pole. Then use a 9/16in. socket to tighten the two nuts on each mounting bracket that hold the lag bolt tabs in place (see Figure 3-6 on page 3-9).
- 7 Of the three lag bolt holes, select the one that is in direct contact with the pole. Drill into the pole through this lag bolt hole to a depth of at least 4 inches with a 5/16in. drill bit. Or, you can use a drill bit with the smallest diameter between 0.3in. and 0.4in. that allows the lag bolts to be threaded into the pole without excessive force.



**Note** A cut-out area on left side of the top edge of the rear mount bracket provides access for drilling the upper lag bolt hole with a drill bit that has an extension at least 10 inches long. If a drill bit with an extension of this length is not available, the rear mount bracket must be removed from the pole mounting brackets to drill the upper lag bolt hole.

- 8 Install the lag bolts with a 5/16in wrench.
- 9 Attach rear mount hanger bracket to the back of the Stinger Compact Remote chassis, as shown in Figure 3-8.

Figure 3-8. Attaching the Stinger enclosure rear mount hanger bracket



- 10 Lift the chassis so that the hanger bracket on the back of the chassis is over the mounting tab on the top of the rear mount bracket plate (see Figure 3-1 on page 3-2). Then carefully lower the enclosure until it is hanging from this tab. This tab will temporarily support the enclosure while it is being secured.
- 11 Remove the bolts that hold the shipping brackets to the bottom of the chassis and remove the shipping brackets.

- 12 Align the two holes on each side of the chassis with the holes in the pole mounting hardware and install the bolts to secure the chassis on the mounting hardware.

### Side-mounting the enclosure on a pole

The exterior ventilation covers on each side of the chassis have mount points and can also serve as side mounting brackets for the chassis. Follow all local safety practices and guidelines and use the following general procedure to mount the enclosure.

- 1 Use a 9/16 in. combination wrench or socket with a 6 in. extension and handle to loosen the two nuts that secure the lag bolt tabs on the top and bottom mounting brackets. The top bracket is shown in Figure 3-6 on page 3-9.
- 2 Mark the location of the top mounting bolt hole in the center of the pole, at least 67 inches (1.7 meters) above the ground. Use an 11/16in. drill bit, or a drill bit that is 0.625in. to 0.7in. (15.875mm to 17.78mm) in diameter, to drill the hole for the top mounting bolt through the center of the pole.
- 3 If a rear mount bracket is available, use the top mounting bolt to temporarily install it and the pole mounting brackets, as shown in Figure 3-7 on page 3-10. Allow the hardware to hang vertically and mark the location for the lower mounting bolt on the pole.



**Note** If a rear mount bracket is not available, mark the location for the center of the lower mounting bolt hole exactly 24.0 inches below the center of the top bolt hole.

- 4 Mount the upper and lower pole mounting brackets, using the top and bottom mounting bolts.



**Note** The threaded end of the bolt should extend at least 1 inch beyond the back of the pole.

- 5 Place washers and nuts on the threaded ends of the two bolt ends and use a 15/16in. combination wrench to tighten the nuts until the washers begin to become concave into the pole.



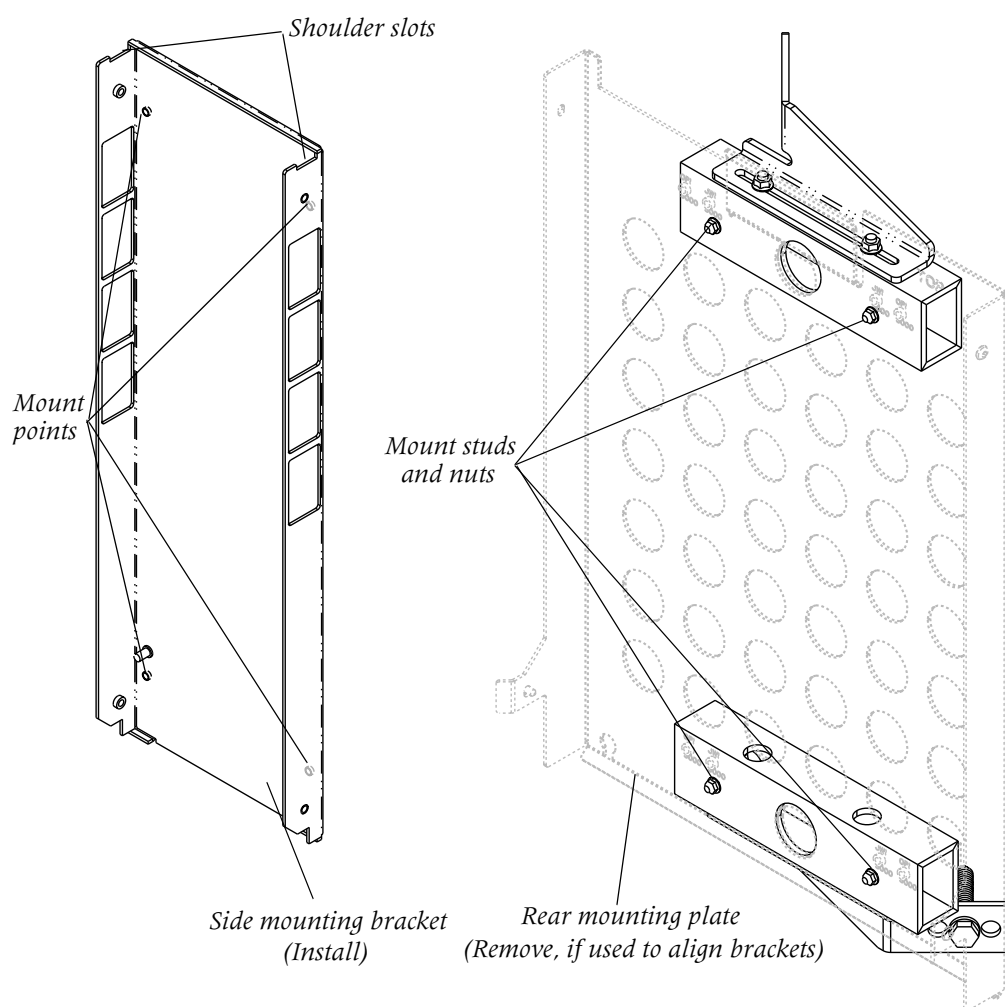
**Note** While tightening the nut on the threaded end of the bolt, hold the bolt head with a 15/16in. socket with a 2in. extension (min.) and handle.

- 6 Slide the lag bolt tabs on each of the mounting brackets so that the tabs are in contact with the pole. Then use a 9/16in. socket to tighten the two nuts on each mounting bracket that hold the lag bolt tabs in place (see Figure 3-6 on page 3-9).
- 7 Of the three lag bolt holes, select the one that is in direct contact with the pole. Drill into the pole through this lag bolt hole to a depth of at least 4 inches with a 5/16in. drill bit. Or, you can use a drill bit with the smallest diameter between 0.3in. and 0.4in. that allows the lag bolts to be threaded into the pole without excessive force.
- 8 Install the lag bolts with a 5/16in wrench.
- 9 Carefully lay the Stinger Compact Remote chassis onto its side so that the side that will be mounted against the pole is facing up. Remove the side mounting bracket from this side.

- 10 Remove the four plastic plugs that fill the mounting points on the side mounting bracket. If needed, a small screwdriver can be used to help remove the plugs.
- 11 Place the side mounting bracket on the pole mounting brackets, so that the four studs that supported the mounting plate are inserted into the mounting points in the side mounting bracket. Reinstall the nuts on these studs to secure the ventilation cover on the pole mounting brackets.

**Note** The side mounting bracket has two shoulder slots on the top of each side. Pins in the inside half of the vented cover, still installed on the chassis, rest in these slots to help support and position the enclosure while aligning the mounting holes on the ventilation covers to secure the enclosure.

Figure 3-9. Side mounting bracket conversion



- 12 Carefully lift the enclosure and position the two shoulder pins in the inside ventilation cover that is attached to the enclosure into the shoulder slots on the sides of the exterior ventilation cover that is mounted on the pole mounting brackets.
- 13 To secure the chassis, align the four mounting points (two on each side) of the unit and install the mounting bolts in the ventilation covers.

## Mounting the enclosure on a wiring 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.

To install a Stinger Compact Remote enclosure on a pole, you need the following items:

- The Stinger enclosure and appropriate mounting kit
- A hammer
- An antistatic wrist strap (Lucent number: R-4987C or equivalent) for handling components
- A center punch
- An electric drill
- A 5/16 inch (7.5mm) drill bit
- A 3/4 inch (19mm) metal hole saw
- A knock-out punch (Greenlee)
- A 10 inch (25cm) tongue and groove (channel lock) pliers
- Safety screw driver for removal and installation of trilobular recessed head screws (Part number 29-99-183-22, available from Southco Inc., or equivalent)
- Three 1 inch liquid tight strain relief fitting (Bell SAP 233536 NM)
- Three 3/4 inch liquid tight strain relief fitting (Bell SAP 595613 NM)

### Prepare the cabinet and install the mounting bracket

Installation on an outdoor cabinet requires a total of four mounting holes and six pass-through holes for cables from the Stinger CR unit. The mounting holes are 5/16 inch (7.5mm) in diameter. Three of the cable holes are 3/4 inch in diameter, and three holes are 1 inch in diameter. These holes are marked with a template that is supplied with the mounting kit.

If you are side-mounting the enclosure, you must remove the integrated side-mounting bracket from the enclosure before beginning (see Figure 3-2 on page 3-5). If you are rear mounting the enclosure, you must install the enclosure hanger on the enclosure before beginning (see Figure 3-8 on page 3-11).

You may use the following general procedure to prepare the cabinet and install the mounting bracket.

- 1 Pre-position the mounting template that is shipped with the mounting kit to verify that all holes can be drilled without damaging existing cables or hardware behind the mounting surface.
- 2 Mark the location of each mounting hole and cable pass-through hole and create an indentation in the center of each location with a center punch.



**Note** To protect them from damage during drilling, verify that no cables or wires are routed near the locations where holes will be drilled.

- 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.
- 7 Drill a pilot hole at the center point for each pass-through hole marked previously.
- 8 Use knock-out tools to cut the three holes 1 5/16 inches in diameter for the outside plant cables.
- 9 Use knock-out tools to cut the three holes 1 1/8 inches in diameter for the fiber, ground, and power cables.
- 10 Inspect each hole to verify that it is cleanly cut and free of metal burrs.
- 11 Install liquid-tight strain-relief fittings (customer provided) in each of the pass-through holes and tighten them with the channel-lock pliers.

## Mounting the enclosure

The side-mount mounting bracket has two shoulder slots near the top of the bracket, similar to those shown in Figure 3-9 on page 3-13. These slots accept pins on the side ventilation cover of the enclosure to help support and position the enclosure while aligning the mounting holes in the side ventilation cover with those of the mounting bracket.

The rear-mount bracket has a tab that supports a hanger that is installed on the chassis (see Figure 3-3 on page 3-6). The tab supports the chassis while aligning the mounting holes on the bracket with those on the sides of the enclosure.

Follow all local safety practices and guidelines and use the following general procedure to mount the enclosure.

- 1 Remove the cable cover from the bottom of the enclosure.
- 2 If side-mounting—Carefully lift to position the pins on the ventilation cover of the enclosure onto the two shoulder slots of the mounting bracket. Allow the weight of the enclosure to be supported on the shoulder slots.  
If rear-mounting—Carefully lift and position the enclosure hanger over the enclosure mounting tab on the mounting bracket. Allow the weight of the enclosure to be supported by the mounting tab.
- 3 Align the six mounting points (three in front, and three in back) for side mounting, or four mounting points (two on each side) for rear mounting) on the enclosure with the mounting holes in the bracket.
- 4 Use a safety screw driver (Part number 29-99-183-22, available from Soothed Inc., or equivalent) to install six tribural recessed head screws to secure the enclosure.

## Compact Remote Enclosure and Component Installation

Route and connect the fibers and ground cable inside the enclosure



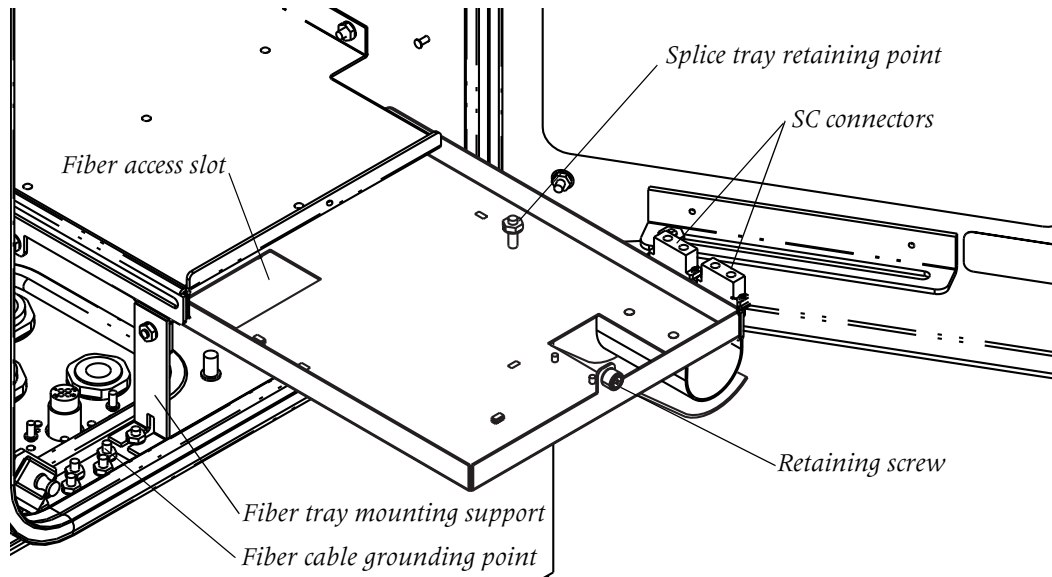
**Warning** Early models of the Stinger Compact Remote were installed with one-way screws. If one-way screws are being removed or loosened with an SSTM14 tool, sharp metal edges are created on the screw head that can result in injury. After loosening or removal. Follow local guidelines when replacing one-way screws with tribunal recessed head screws.

## Route and connect the fibers and ground cable inside the enclosure

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-20 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 3-10).

Figure 3-10. 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.



**Note** The ends of all fiber connectors are delivered clean, polished, and protected. When handling them during connection take care to not touch, contaminate, or damage the fiber ends. If the fiber ends must be cleaned or restored, it should be done 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
- 5 Remove the fiber jumper from its plastic bag. Remove dust covers from the top of the SC connectors on the fiber tray. Insert the SC connector on one end of the fiber jumper into the SC mating sleeve on the fiber tray.
  - 6 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.
  - 7 Slide the fiber tray back into the chassis and tighten the retaining screw.

## Routing the cables out of the enclosure

Cables are routed differently, depending on the way in which the enclosure is mounted. Routing information for pole mounting and cabinet mounting are described here. Local conditions should be taken into consideration, and local procedures should be followed when using the predeclares described here, or when mounting the enclosure in other situations.

### Routing the cables for cabinet mounting

The Stinger CR unit has three outside plant cables that must be routed into the 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 1 inch (25.4mm) weather tight connectors installed in the 1 5/16 inch holes in the cabinet.

The optical cables, and the cables for power and ground pass through the three 3/4-inch (19mm) weather tight connectors installed in 1 1/8 inch the 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."

- 1 Place a 1 inch (25.4mm) weather-tight compression fitting, along with its associated flat nylon washer and rubber bushing, on each of the outside plant cables.
- 2 Place 3/4 inch (19mm) weather-tight compression fittings, along with their associated flat nylon washer and rubber bushing, on the fiber, power, and ground cables.

## Compact Remote Enclosure and Component Installation

### Routing the cables out of the enclosure

- 3 Pass the cables through the weather-tight connectors on the wiring cabinet, as described above step number one.
- 4 When mounting the left side of the enclosure to the wiring cabinet, adjust the cables to leave a service loop approximately 12 inches in diameter below the unit. 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.

- 5 Tighten the compression fitting on each of the cables to make a weather-tight seal.

## Routing the cables for pole mounting

When pole mounting The Stinger Compact Remote unit, all OSP, fiber, and power cables are routed through a 45° cable duct on the cable cover below the enclosure. The cable cover is partially disassembled to make this process easier. While it is disassembled, the cable cover can be configured for centered)-mounted or side-mounted enclosures by changing the positions of the 45° cable duct and a blocking plate. The 45° cable duct and block plate each have threaded studs in identical patterns, as shown in Figure 3-11. A ground cable is routed through a separate hole in the cable cover near the duct, as shown in Figure 3-12.

Figure 3-11. Interchangeable 45° cable duct and blocking plate

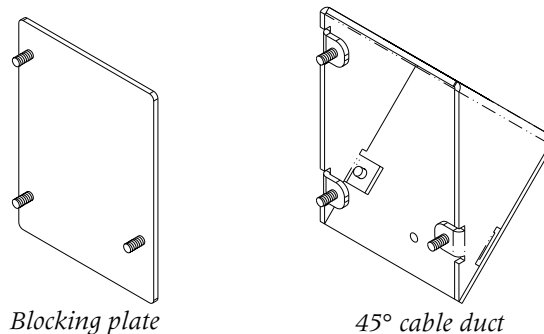
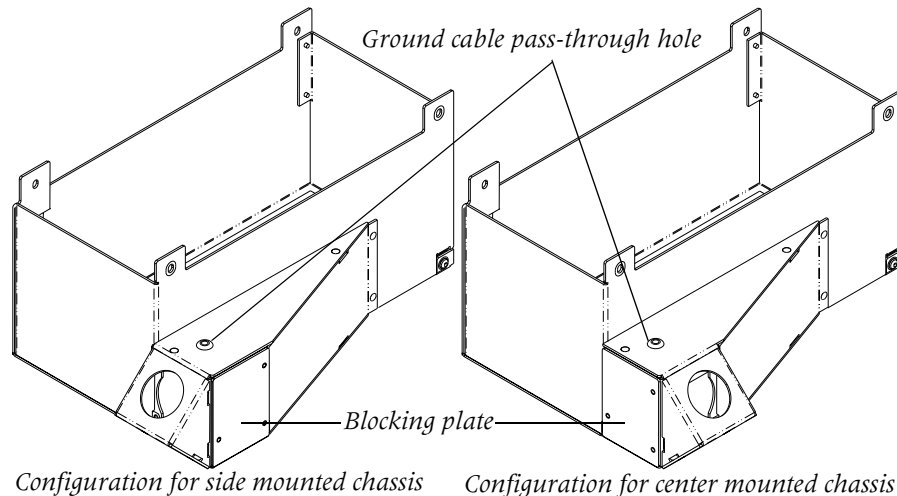


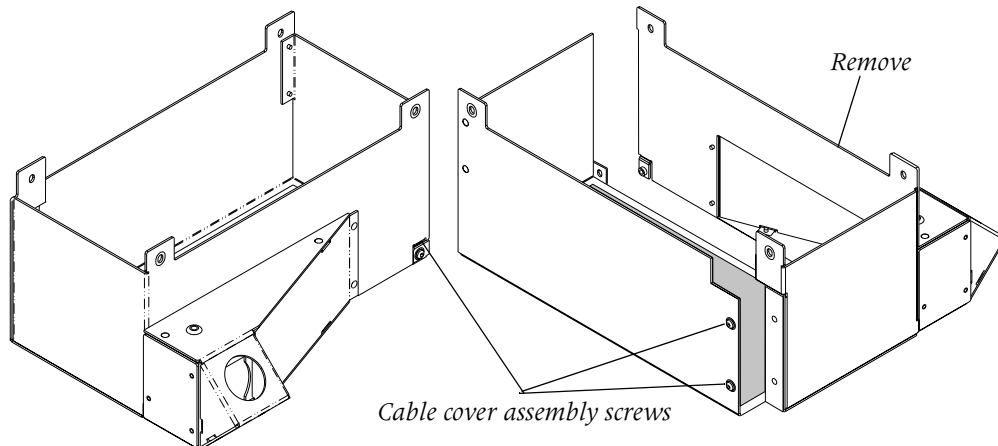
Figure 3-12. Cable duct and block plate configuration



To route the cable up the pole for splicing and connection:

- 1 Remove the 45° cable duct by removing the three nuts that secure it inside the cable cover. Set this piece aside.
- 2 If necessary, remove the three nuts that secure the blocking plate and reinstall it as shown in Figure 3-12, so that it matches with the way in which the enclosure is mounted on the pole.

Figure 3-13. Cable cover assembly screws



- 3 Remove the three screws shown in Figure 3-13, and remove the 2 sides of the cable cover with the cable duct from the remainder of the cover.



**Note** The cable cover is partially disassembled to make cable routing easier, and reassembled onto the Stinger Compact enclosure.

- 4 Thread the subscriber cables, power cable, and fiber cable(s) through the opening in the cable cover where the cable duct will be attached. Then attach the two sides of the cable cover to the bottom of the enclosure with the cable duct in the rear of the enclosure.
- 5 Insert the cable ends in the 45° cable duct and slide the duct along the cables until it meets the partial cable cover, mounted on the enclosure.



**Note** The cables are a tight fit through the 45° cable duct. To make it easier to slide the duct along the cables, make sure that the cables are aligned along their entire length and do not cross or wrap around one another. If needed, you may temporarily wrap tape around the cable bundle at intervals to keep the cables in alignment. Remove the tape after installing the cable duct.

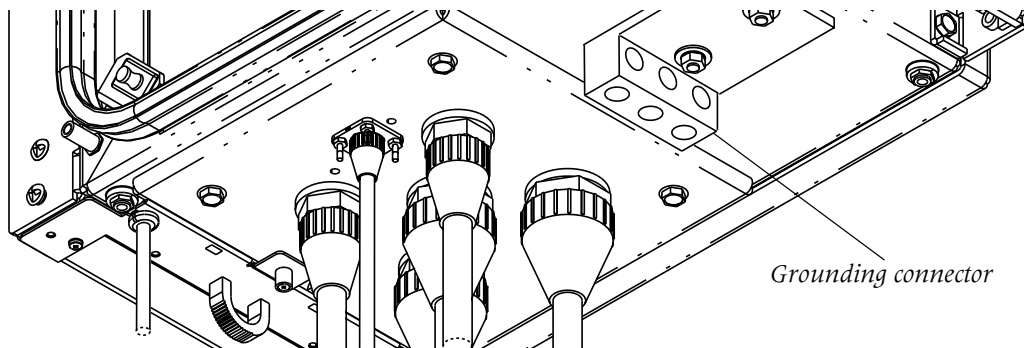
- 6 Position the 45° cable duct on the cable cover, and secure it with the three nuts removed in step 1.
- 7 Feed the ground cable through the pass-through hole in the cable vent (see Figure 3-12 on page 3-18) and attach it to electrical ground.

## 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 lightning 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 Compact Remote unit, 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 3-14). 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 3-14. Enclosure grounding connector



## Inspecting and replacing the door gasket

The enclosure is equipped with a gasket that is located on a flange surrounding the opening for the door. If this gasket is damaged, excessive moisture may enter the cabinet and damage the Stinger Compact Remote components.

Examine the gasket for any cuts, cracks, tears, or deformations. If any of these conditions are observed, the gasket must be replaced to insure a proper seal around the door.



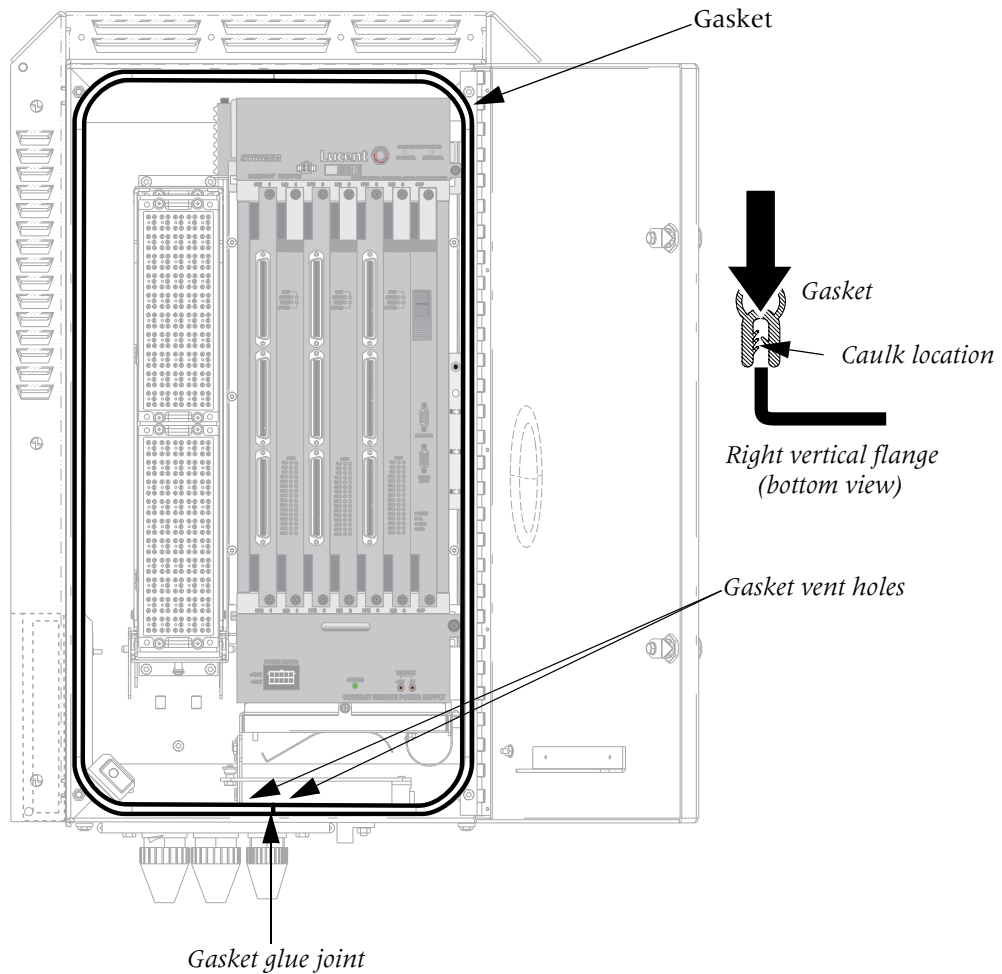
**Note** The gasket is manufactured with two small round holes located on either side of the gasket glue joint near the center of the bottom horizontal flange. These are gasket vent holes, and do not indicate that replacement of the gasket is required.

Use the following procedure to replace the door gasket.

- 1 Order a factory prepared replacement door gasket (order number 848915625), and have it available for installation.
- 2 Remove the old gasket material from the door flange by pulling it away from the flange. To do this, pull one portion of the gasket away from the flange (i.e. one corner), and work around the door opening until the entire gasket is removed.
- 3 Remove as much residual caulking material as possible from the perimeter of the door flange.

- 4 Position the replacement gasket so that the vent holes and the gasket glue joint are located in the center of the bottom horizontal door flange (see Figure 3-15).
- 5 Press the gasket onto the door flange. Apply pressure around the entire door flange to install the gasket evenly and completely. Use a soft rubber mallet to tap the gasket into place.
- 6 Apply a thin bead of caulk (General Electric RTV 108 caulk or equivalent) to the outside perimeter border of the gasket, where the flange enters the gasket (see Figure 3-15).

Figure 3-15. Enclosure door gasket



## Installing and replacing Stinger Compact Remote components

The Stinger Compact Remote 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.



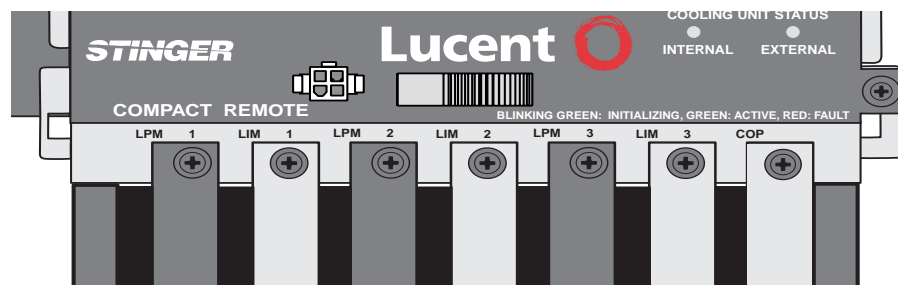
**Caution** Wear an antistatic wrist strap before handling any of the unit components.

### Slot numbering and module placement

Figure 3-16 shows the stenciling at top of the slots in a Stinger Compact Remote IP DSLAM chassis. This identifies the locations for up to three LIMs, their associated LPMs, and GE-COP module in the COP slot.

A Stinger Compact Remote IP DSLAM has a shelf number assigned to it in the command interface of the host unit. LIMs in a hosted Stinger Compact Remote IP DSLAM 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 Compact Remote IP DSLAM 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 3-16. Slot labeling on the Stinger Compact Remote IP DSLAM chassis



## GE-COP installation and replacement



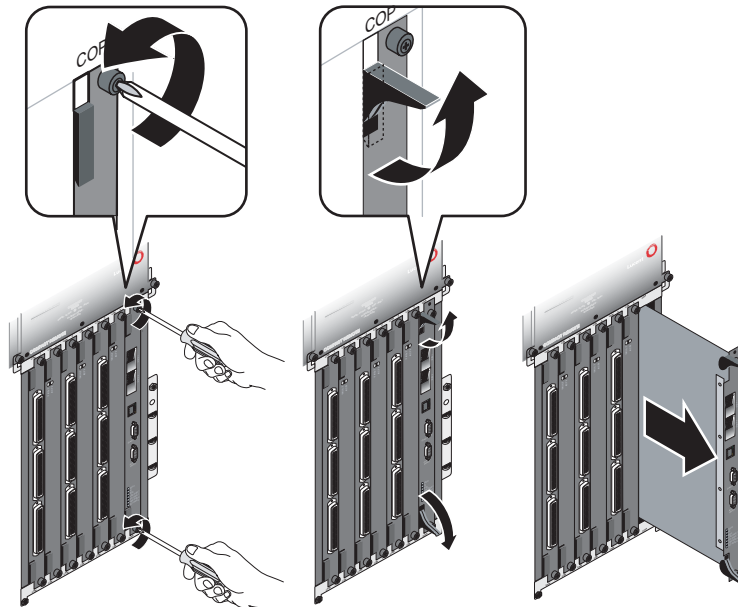
**Caution** The Gigabit Ethernet control and optics module in the COP slot controls operations on the local chassis. Removal of this module will cause an immediate failure of an operating Stinger Compact Remote IP DSLAM unit. Before removing or replacing the GE-COP, perform a normal shut down and remove power from the unit.

### Removing the GE-COP module from the COP slot

To remove a GE-COP 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 3-17. Other screwdrivers might damage the screw heads.

Figure 3-17. Removing a GE-COP module from the COP slot



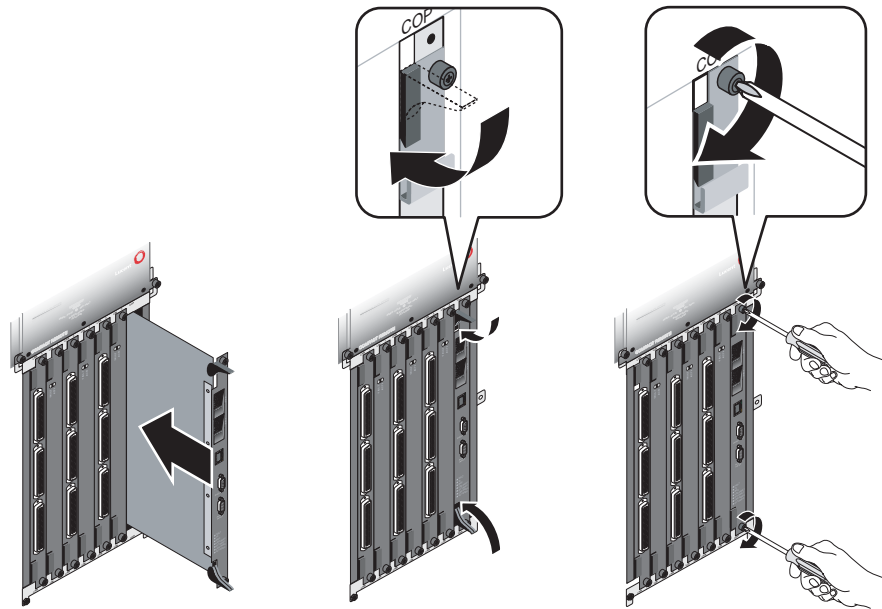
- 4 Lift the top and bottom card ejectors simultaneously to remove the module from the unit.
- 5 Carefully slide the module out of the chassis, and place it into an antistatic container.

### Installing a module in the COP slot

To install a GE-COP 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 3-18.

Figure 3-18. Installing a GE-COP module in the COP slot



- 3 Depress the card ejectors simultaneously to seat the module into the midplane.
- 4 Using a number 2 Phillips screwdriver, tighten the two thumbscrews.
- 5 Restore power to the unit.
- 6 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 3-18, if necessary.



**Note** LIMs installed in a hosted Stinger Compact Remote are referred to as RLIMs because of their remote function in the Compact Remote chassis. This is only a term of reference, related to the implementation of the LIM in a hosted Stinger Compact Remote, 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 “Installing and replacing Stinger Compact Remote components” on page 3-22.)

- 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 Using a number 2 Phillips screwdriver, secure the LIM by tightening the thumbscrews.
- 6 If necessary, if all other installation tasks are complete, including the installation of an associated LPM, turn on power to the Stinger unit.
- 7 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 3-42 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 removing 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 3-17 on page 3-23, 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 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.
- 4 Carefully slide the LIM out of the unit and place it into an antistatic container.
- 5 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.

- 6 Depress the ejectors simultaneously.
- 7 Using a number 2 Phillips screwdriver, secure the module into the unit by tightening the thumbscrews on the LIM.
- 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 3-42, 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.

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 3-36.

### Replacing an LPM

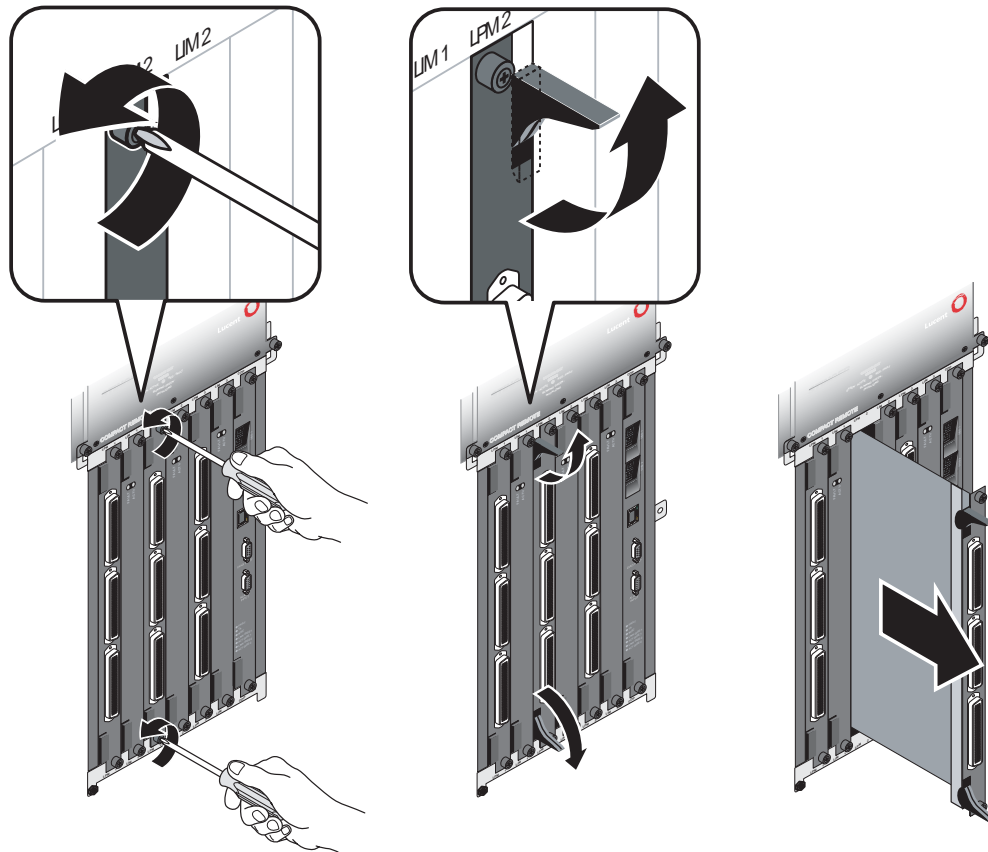


**Caution** Any circuits running through the LPM are interrupted when it is removed, which can result in data loss. Lucent Technologies recommends setting the associated LIM’s administrative status to Down before removing the LPM from the unit. For instructions on changing a LIM’s state to Down and then 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 3-19.

Figure 3-19. 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 3-36.

## 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.

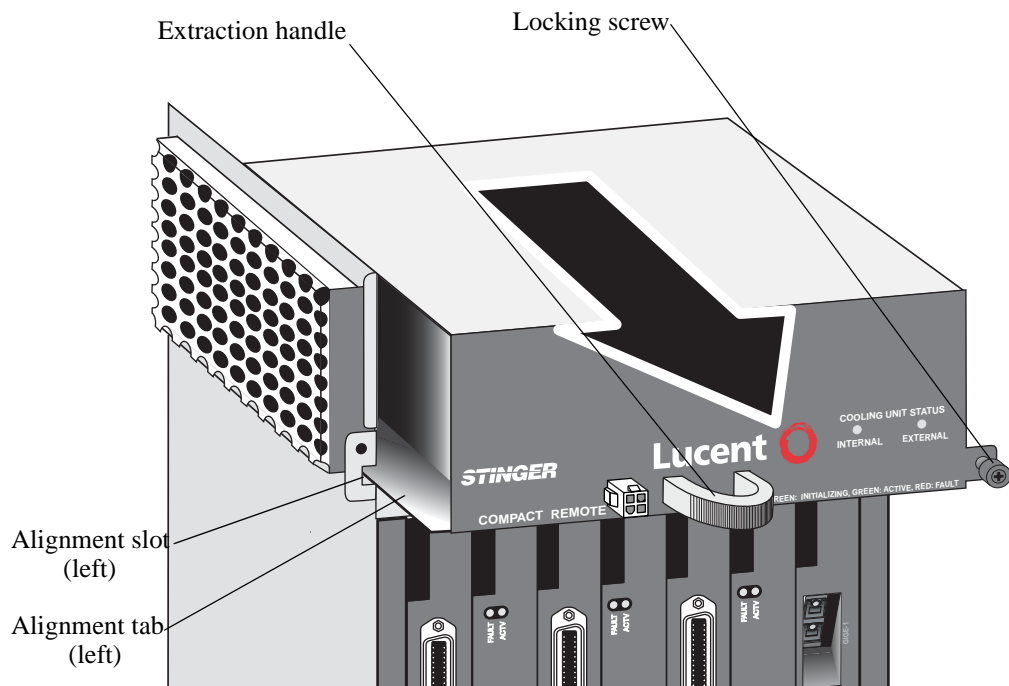


**Warning** Moving fan blades in the cooling module may cause injury to fingers. Do not completely remove the cooling module until the internal fan has stopped moving, as detailed in step 3 and step 4 below.

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

- 1 Remove the connector for the chassis external cooling unit 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 3-20.

*Figure 3-20. 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 3-20).

- 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 unit 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 unit

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

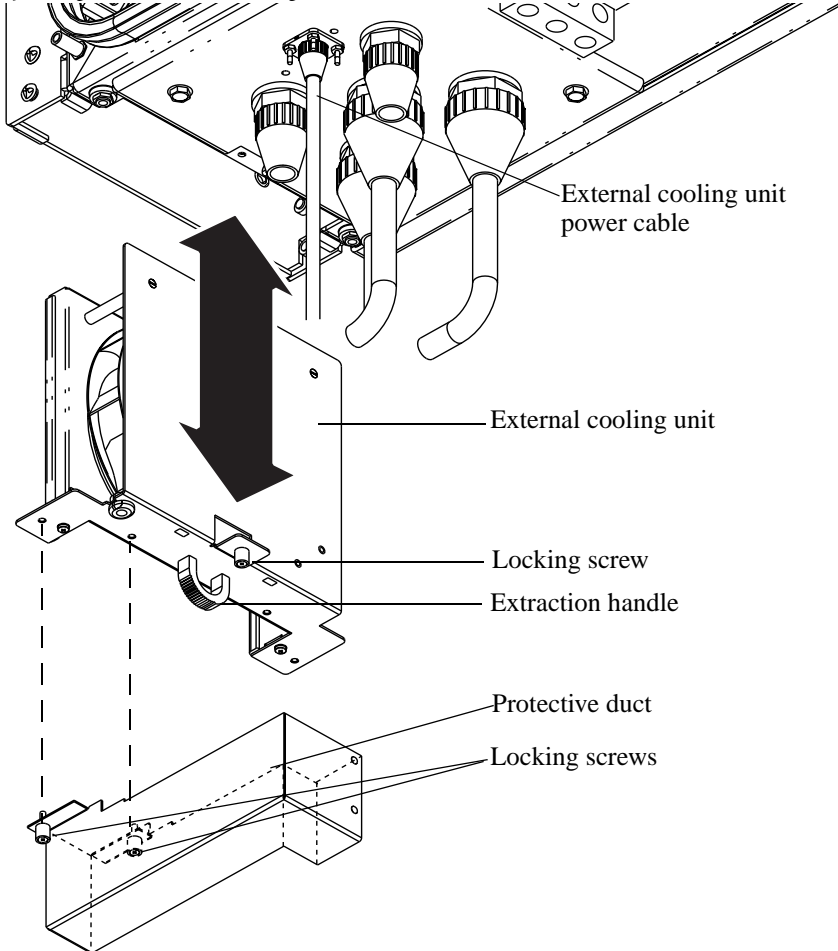


**Warning** Moving fan blades in the external cooling unit may cause injury to fingers. Do not remove the external cooling unit until its fan blades have stopped moving, as detailed in the following procedure.

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

- 1 Fully loosen the locking screws on the protective duct below the external cooling unit (see Figure 7) and remove the protective duct.

Figure 3-21. Replacing the external cooling unit



**Note** New versions of the units have a single knurled knob in the front and a keyhole/pin at the rear. Remove the single knurled knob and disengage the keyhole/pin.

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



**Note** This ensures that the fan blades of the external cooling fan are not moving during replacement.

- 3 Remove the cable cover below the enclosure.
- 4 Fully loosen the locking screw for the external cooling unit.
- 5 Grasp the extraction handle on the external cooling unit and pull to remove it from its mounting.
- 6 Unscrew and remove the external cooling unit power cable, shown in Figure 7, from the pass-through connector below the enclosure.
- 7 Remove the external cooling unit from the enclosure and place it on a flat work surface.
- 8 Transfer the protective duct to the new fan unit and secure it by tightening the locking screws.

- 9 Reattach the power cable to the pass-through connector on the bottom of the enclosure.
- 10 Align the external cooling unit as shown in Figure 7, and slide it into the chassis until the locking screw makes contact with the bottom of the enclosure.
- 11 Fully tighten the locking screw.
- 12 Replace the cable cover on the bottom of the enclosure.

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

- 1 Fully loosen the locking screw for the internal cooling module. (See Figure 3-20 on page 3-28)
- 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 unit 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 Compact Remote, be sure that the unit has been properly shut down, and that the source voltage has been disconnected.



**Note** When removing the power supply, disconnect the power input connector ( $\pm 190\text{Vdc}$ ) or screw terminals ( $-48\text{Vdc}$ ) before loosening the locking screw. When installing the power supply, tighten the locking screw before connecting the power input connector.

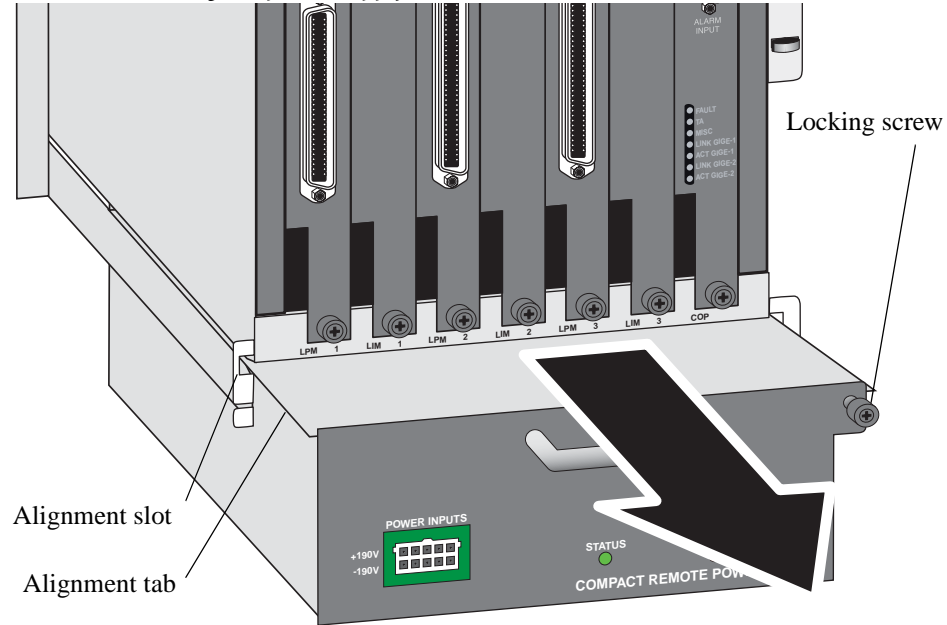
Use the following procedure to replace the power supply of a Stinger Compact Remote unit.

- 1 Disconnect the power input connector ( $\pm 190\text{Vdc}$ ) or screw terminals ( $-48\text{Vdc}$ ) 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 3-20.

## Compact Remote Enclosure and Component Installation

Physical connections to the Stinger Compact Remote unit

Figure 3-22. 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 3-22).
- 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 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 power input connector ( $\pm 190\text{Vdc}$ ) or screw terminals ( $-48\text{Vdc}$ ).

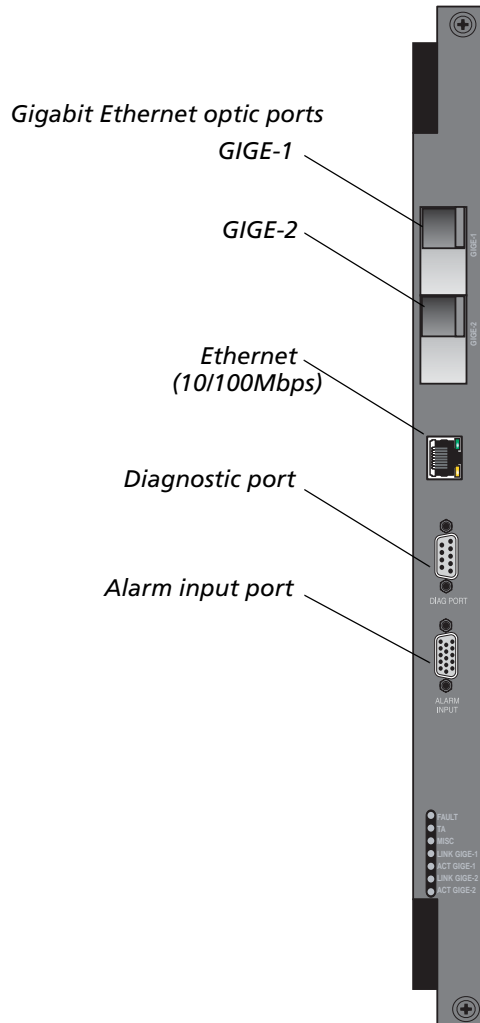
## Physical connections to the Stinger Compact Remote unit

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 a GE-COP module in the COP slot.

## Connections to the GE-COP

The GE-COP module supports hosted operation of the Stinger Compact Remote IP DSLAM unit. Figure 3-23 and Table 3-2 on page 3-34 identify the connectors that are present on this module.

Figure 3-23. Connectors for the GE-COP



*Table 3-2. Connectors for modules in the COP slot*

<b>Connector</b>	<b>Function</b>
Gigabit Ethernet ports	GIGE-1: Control channel connection and high bandwidth connection for end-user traffic  GIGE-2: Optional second high bandwidth connection for end-user traffic
10/100 Ethernet port	This port is not used on the hosted Compact Remote IP DSLAM.
Diagnostic port	Serial diagnostic connection for management console
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-20.)

## Gigabit Ethernet ports

These ports provide Gigabit Ethernet connections for end-user traffic, and a control channel from the host Stinger unit. These ports require duplex small form factor modules that provide LC fiber optic connections.



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

To connect the optical jumper in the Stinger Compact Remote unit from the fiber tray to the GE-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 GE-COP and carefully insert the head of the jumper into the connector on the GE-COP, as shown in Figure 3-24.

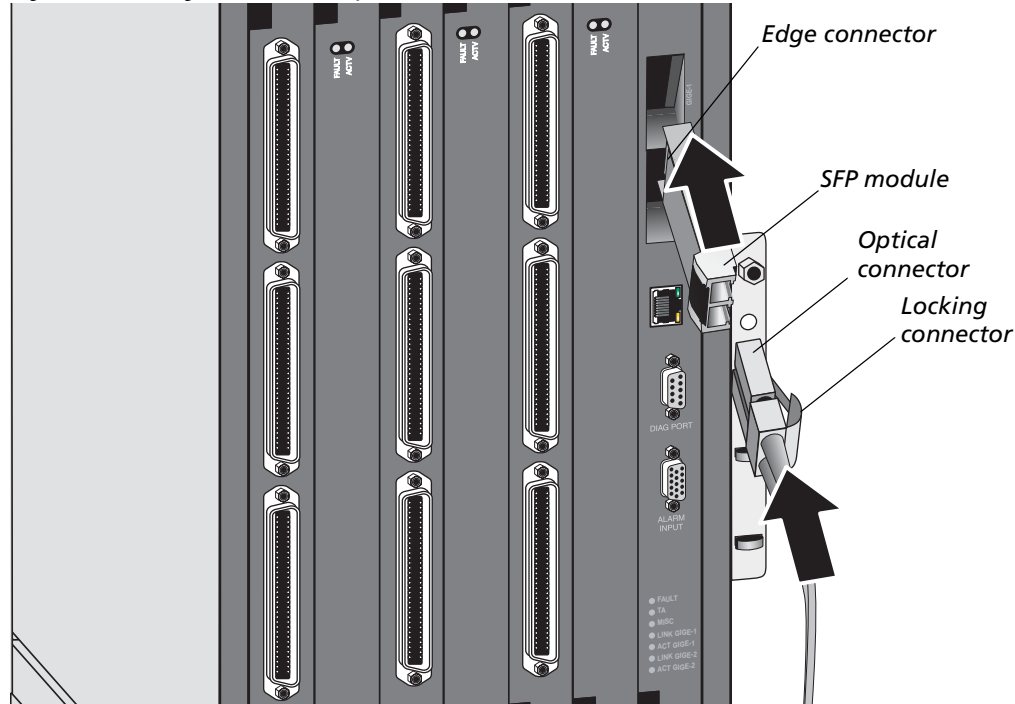


**Caution** Bind excess cable lengths in a figure-eight pattern. Do not wind excess cable into circular coils.

Use the following procedure to install and connect the SFP module in a GIGE port on the GE-COP module.

- 1** Align the SFP modules so the edge connector is visible on the left side. (See Figure 3-24.)
- 2** Slide the module into the port.
- 3** Press firmly to seat the SFP module.
- 4** Align the LC connector on optical cable so the locking connector is on the right. (See Figure 3-24.)
- 5** Slide the optical connector into the SFP module until the locking connector engages with a slight click.

Figure 3-24. Gigabit Ethernet optical connection to the GE-COP



### Diagnostic port

This port is present on the GE-COP. However, it is not used on Stinger Compact Remote IP DSLAM units. The TAOS software on these units is set to operate the unit in hosted mode and does not require that a terminal be connected to this interface. Configuration of the unit, the ADSL lines, and IP connections is accomplished from the host unit.

### Alarm input port

This port is present on the GE-COP. The DB-15 connector can accept connections to monitor the alarm status of up to seven external devices.



**Note** In hosted Stinger Compact Remote 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-20.)

### Alarm connections for monitoring multiple external alarms

The ALARM port of the GE-COP 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-3.

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

## **Compact Remote Enclosure and Component Installation**

*Physical connections to the Stinger Compact Remote unit*

---

opening of a normally closed relay, or the closing of a normally open relay. For information on their configuration see “Alarm input port pinouts” on page C-3.

### **Connections to the LPMs**

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

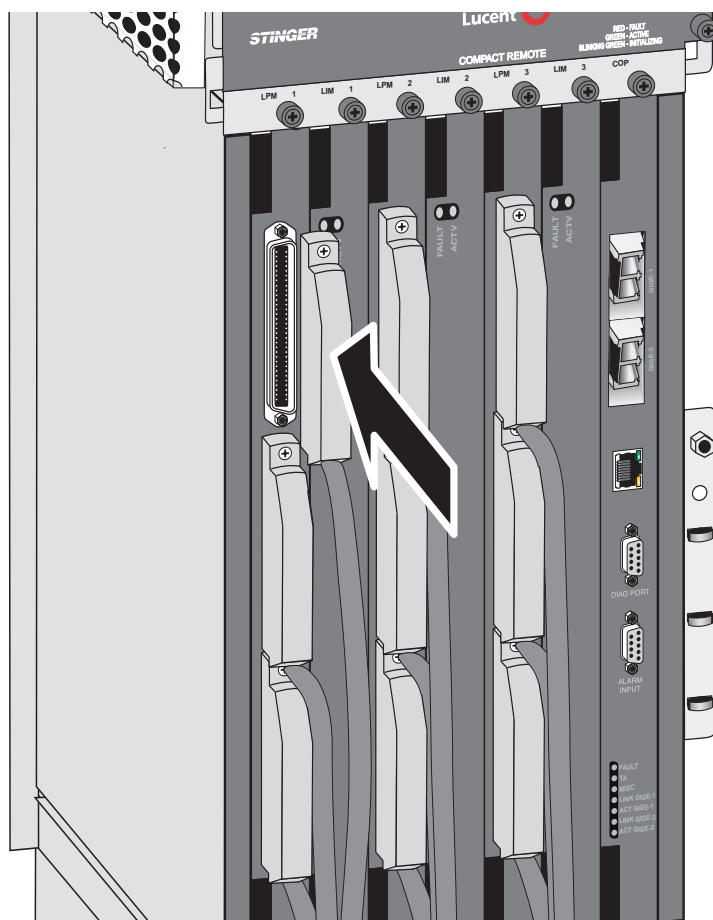
The 48-port LPMs with splitters also connect to facilities providing analog voice service (dial tone) from the central office. The integrated splitters combine analog and DSL data service on a single copper pair for delivery to the subscriber. For specific information connections from the LPMs, through the protection blocks, and to the copper telecommunication facilities, see “Stinger CR cabling for the 48-port LPM with splitters” on page C-3.

### **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-3.

Connections to the 48-port LPM with splitters are shown in Figure 3-25.

Figure 3-25. 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 3-25.
- 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-3 for pinout information and wiring details.

### Routing the LPM connector cables

Prior to closing the enclosure door, the cables from each of the LPM connectors must be routed to the side of the connectors.



**Caution** Any cable that remains over an LPM connector will prevent the enclosure door from closing properly, and may be damaged when attempting to close the door.

## Compact Remote Enclosure and Component Installation

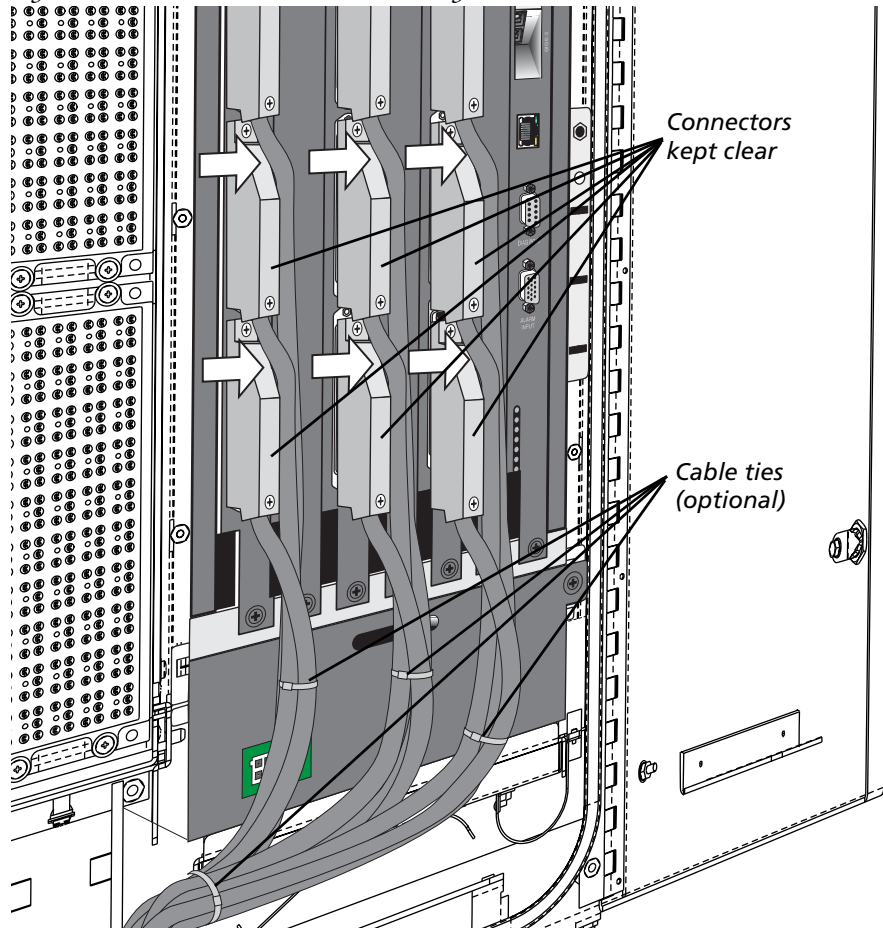
Turning on power to a Stinger Compact Remote unit

The cables from each of the LPM connectors must be routed to the right of any lower connectors, as shown in Figure 3-26, and routed in front of the adjacent LIM toward the bottom of the enclosure. The cables can be bundled together and maintained in place with four cinch-wrap cable ties below the LIM/LPM slots, as shown in Figure 3-26. The use of cable ties is optional, since they may obstruct replacement of the power supply.



**Caution** Any cable ties used must meet fire specification UL 94V-0.

Figure 3-26. LPM connector cable routing



## Turning on power to a Stinger Compact Remote unit



**Caution** Lucent Technologies does not recommend applying power to Stinger units that contain circuit packs (LIMs, TMs, LPMs, CLTs, etc.), if a control module is not installed in the chassis. If desired, power may be applied to Stinger units that are completely unpopulated and do not contain any circuit packs or control modules.



**Warning** Use appropriate caution when handling the  $\pm 190\text{Vdc}$  and  $-48\text{Vdc}$  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 for  $\pm 190\text{Vdc}$  operation is provided from an Argus CSM-36-BC power supply in the central office over multiple pairs of copper telecommunications wire. Three to five  $\pm 190\text{Vdc}$  power sources are required to power each Stinger Compact Remote. 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 3-3. Number of pairs for providing power*

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

For  $-48\text{Vdc}$  operation, you connect one pair of 19 AWG wires in the stub end of the power cable to a local  $-48\text{Vdc}$  power source. This cable terminates on a Tyco connector in the Compact Remote enclosure. A jumper cable connects between the Tyco connector and the power terminals on the  $-48\text{Vdc}$  power supply.

All Stinger Compact Remote 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 Compact Remote unit indicate the operating status of each module.

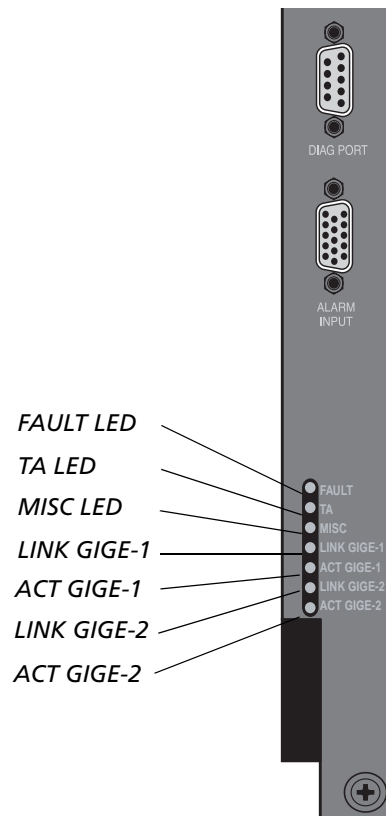


**Note** For information about status lights on the OLIM in the host Stinger unit, see “Interpreting GE-OLIM status lights” on page B-4.

## GE-COP status lights

There are seven status lights near the bottom of the front panel of the GE-COP. Figure 3-27 shows the locations of the COP status lights.

Figure 3-27. GE-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 3-4.

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	One of the following has occurred: The COP has detected a relay closure on one of the seven pairs connected to the ALARM connector. An internal or external fan failure has been detected. The enclosure door is open. <b>Note</b> When the door is opened for service, pull the door alarm switch plunger to deactivate this alarm indication. (See Figure 2-3 on page 2-5.)
LINK GIGE-1	Green	ON	The Gigabit Ethernet optical link is operating properly.
		OFF	The Gigabit Ethernet optical link has failed.
ACT GIGE-1	Green	ON	There is activity (data traffic) on the link.
LINK GIGE-2	Green	ON	The Gigabit Ethernet optical link is operating properly.
		OFF	The Gigabit Ethernet optical link has failed.
ACT GIGE-2	Green	ON	There is activity (data traffic) on the link.

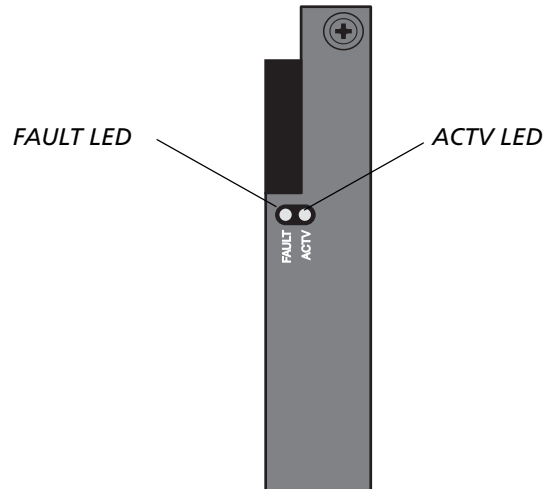


**Note** On early GE-COP modules, the ACT LED is lit whenever the link on that port is operating properly. This is the same indication displayed by the LINK LED.

## LIM status lights

The front panel of the 48-port IP ADSL2+ LIM has two status lights, located near the top of the panel, that indicate the status of the module. Figure 3-28 shows the location of the status lights on the 48-port IP ADSL2+ LIM.

Figure 3-28. 48-port IP ADSL2+ LIM status lights



Both 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 ACTV 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
ACTV	Green	The module or port is fully operational and no errors have been detected.
FAULT	Orange	The module failed to pass its POST.

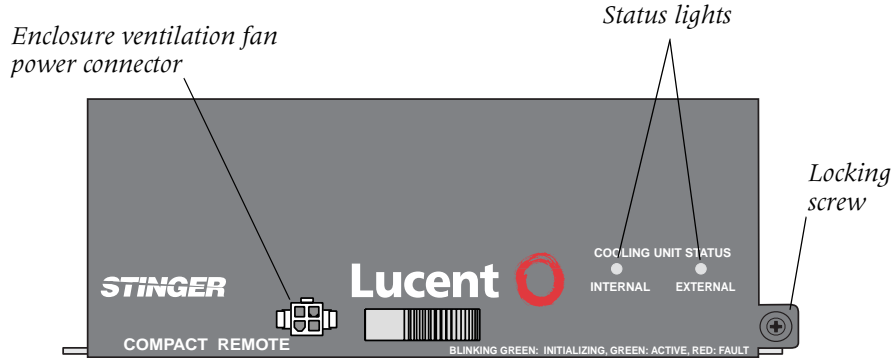


**Note** Detailed physical and configuration information for the 48-port IP ADSL2+ LIM is included in the *Stinger ADSL Annex-A LIM Guide for LIMs with ADSL2+ Capability*.

## Internal cooling unit status lights

The Stinger Compact Remote internal cooling unit is shown in Figure 3-29.

Figure 3-29. The Stinger Compact Remote cooling unit



The Stinger Compact Remote cooling unit has two status lights on the front panel to indicate the status of the fans in the internal and external cooling units. 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.

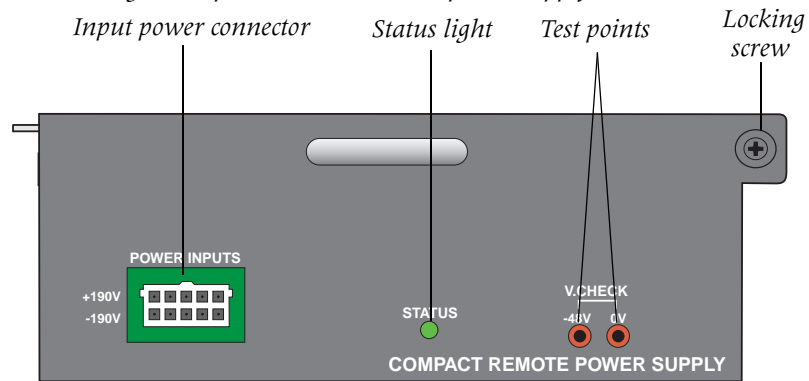
## Power supply status lights

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

The status lights for both the  $\pm 190$ Vdc power supply and the -48Vdc power supply are identical. The STATUS light is lit if the power supply is providing internal -48Vdc power for the unit.

The Stinger Compact Remote  $\pm 190$ Vdc power supply is shown in Figure 3-29.

Figure 3-30. The Stinger Compact Remote  $\pm 190$ Vdc power supply



## What's next

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

# Hosted System Configuration

# 4

Elements of the hosted system architecture. . . . .	4-1
Enabling GE-OLIM ports and configuring port usage . . . . .	4-2
Configuring GE-OLIM trunk port link aggregation . . . . .	4-6
Enabling host communication to remote shelves . . . . .	4-14
Enabling GE-OLIM CR port link aggregation. . . . .	4-17
Configuring remote shelf validation (optional) . . . . .	4-20
Configuring subscriber connections . . . . .	4-23

This chapter describes the basic configurations you must complete to enable and begin to use a Stinger Compact Remote IP DSLAM hosted system. In a hosted system, all provisioning and configuration occurs on the central Stinger FS+ host system.

## Elements of the hosted system architecture

A hosted Compact Remote IP DSLAM system consists of a central Stinger FS+ (the *host*) and up to 48 distributed Compact Remote shelves (*remote shelves*), as shown in Figure 4-1. For an overview of these elements, see Table 4-1 on page 4-2.

Figure 4-1. Hosted Compact Remote IP DSLAM architecture

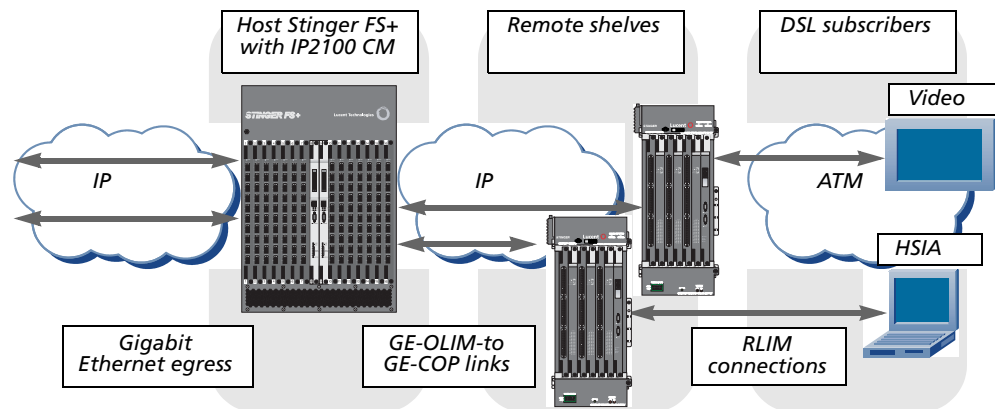


Table 4-1. Elements of a hosted Compact Remote IP DSLAM system

Element	Description
Host Stinger FS+ with IP2100 CM	<p>Performs all provisioning and management</p> <p>CM operates in <i>master mode</i>, with a high-bandwidth backplane interface and 2 Gigabit Ethernet (GigE) ports.</p> <p>Supports up to 14 GigE Optical LIMs (GE-OLIMs), or a mix of GE-OLIMs and other LIM types. Each GE-OLIM supports up to six GigE links to remote shelves, with up to two links to each shelf. Each GE-OLIM also supports two GigE trunk ports.</p>
Remote shelves	<p>Supports a GigE Control and Optics pack (GE-COP) operating in <i>slave mode</i>, which has GigE backplane data paths to the RLIMs and 2 GigE ports for uplinks to a host GE-OLIM.</p> <p>Provides access to up to 144 DSL subscribers via remote ADSL2+ IP LIMs (RLIMs).</p> <p>For details about the types of connections supported on RLIMs, see Table 4-4 on page 4-23.</p> <p>Trunk egress is provided only through the host system.</p>
DSL subscriber services over RLIM connections	<p>Multicast video (IPTV)</p> <p>Unicast video on demand (VoD)</p> <p>High-speed Internet access (HSIA)</p> <p>Voice over IP (VOIP/IP phone)</p>

## Enabling GE-OLIM ports and configuring port usage

The GE-OLIM provides ten GigE ports, which are used for connection to remote shelves and for trunking applications. The ports are labeled from 1 to 10, with 1 in the topmost vertical position.

When a GE-OLIM is installed in the host system, the system creates an ethernet profile for each GE-OLIM port, and one `ol im-port-usage` profile for the slot, to configure how each of the 10 ports will be used.

With the current software version, the `ol im-port-usage` profile provides a default static configuration for port usage. Future software versions will support dynamic configuration of GE-OLIM port usage.

## Enabling GE-OLIM ports

Unlike the Stinger Compact Remote ATM DSLAM, the GMAC interfaces in the Stinger Compact Remote IP DSLAM must be explicitly enabled before the port is available for use.

To use a GE-OLIM port in the IP DSLAM, you must first enable the physical interface in the ethernet profile. For example:

```
HOST-IP2100> read ethernet { 1 1 1 }
HOST-IP2100> set enabled = yes
HOST-IP2100> write -f
```

## Configuring GE-OLIM port usage

With this software version, the system maintains a fixed association between port and function, as shown in Table 4-2. With this fixed association, the default values of the profile apply.

*Table 4-2. GE-OLIM port function with this software version*

Port	Function
Ports 1-6	CR ports, for GigE links to remote shelves.
Ports 7-8	Reserved for future use.
Ports 9-10	Trunk ports, for direct access to an IP network. For example, a trunk port might provide access to an external video server on the network.

Following are the parameters, shown with default settings for a GE-OLIM in slot 1, in the olim-port-usage profile. Ports 7 and 8 are set to cascade, which is not currently supported. (These ports are reserved for future use.)

```
[in OLIM-PORT-USAGE/{ shelf-1 slot-1 0 }:olim-port-config]
olim-port-config[1] = { cr 0 0 }
olim-port-config[2] = { cr 0 0 }
olim-port-config[3] = { cr 0 0 }
olim-port-config[4] = { cr 0 0 }
olim-port-config[5] = { cr 0 0 }
olim-port-config[6] = { cr 0 0 }
olim-port-config[7] = { cascade 0 0 }
olim-port-config[8] = { cascade 0 0 }
olim-port-config[9] = { trunk 0 0 }
olim-port-config[10] = { trunk 0 0 }
[in OLIM-PORT-USAGE/{ shelf-1 slot-1 0 }:olim-port-config[1]]
port-function = cr
cascaded-port = 0
trunk-group = 0
```

Parameter	Setting
port-function	The function of the GE-OLIM port. Following are possible values:

<b>Parameter</b>	<b>Setting</b>
	cr                    Use the port for a GigE link to the Compact Remote shelf GE-COP. With this software, this is the required setting for ports 1 through 6.
	cascade              Use the port to connect to a trunk port of another GE-OLIM in a cascading configuration, to share trunk access. <i>Not currently supported.</i>
	trunk                 Use the port for trunk access to the IP network. With this software, this is the required setting for ports 9 and 10.
cascaded-port	On trunk ports only, this parameter can specify a cascade port on another GE-OLIM. This allows bidirectional traffic flow between the trunk port and the specified cascade port. The valid range is 0 (the default, which disables cascading) and 10. <i>Not currently supported.</i>
trunk-group	<i>Not currently supported.</i>

## Configuring GE-OLIM trunk ports 9 and 10

The GE-OLIM trunk ports can be used to access an upstream video server for multicast or unicast transmissions on IP routed or routed VLAN interfaces. Like the GE-OLIM CR ports, the GMAC physical interface for a trunk port must be explicitly enabled in the port's ethernet profile.

### Configuring an IP routed interface for a GE-OLIM trunk port

To configure GE-OLIM trunk port 10 in slot 12 to support IP traffic, follow these steps:

- 1 Enable the GMAC interface in the ethernet profile. For example:

```
HOST-IP2100> read ethernet { 1 12 10 }
HOST-IP2100> set enabled = yes
HOST-IP2100> write -f
```
- 2 Specify an IP address in the system-generated ip-interface profile for the port. For example:

```
HOST-IP2100> read ip-interface { { 1 12 10 } 0 }
HOST-IP2100> set ip-address = 1.1.1.1/24
HOST-IP2100> write -f
```

In this sample configuration, the GigE interface is connected to the 1.1.1 subnet. RIP is not supported on GOLIM trunk ports, so to enable the interface to communicate with routers on other local subnets; the system must have a static route configuration to another router in its own subnet. For details, see the *Stinger IP Control Module Configuration Guide*.

You can verify that the system can transfer IP packets across the interface by pinging another host on the same network segment, as shown in the following example:

```
HOST-IP2100> ping 1.1.1.19
PING 1.1.1.19: 56 Data bytes
64 bytes from 1.1.1.19: icmp_seq=0 ttl=255 time=0 ms
...
```

## Configuring a routed VLAN interface for a GE-OLIM trunk port

In a Stinger IP DSLAM system, a routed VLAN interface is always mapped to a virtual IP interface on a Gigabit Ethernet port. After you enable the GMAC interface and assign an IP interface address as described in the preceding section, you can configure a sample routed VLAN interface for the GE-OLIM trunk port 10 in slot 12 by following these steps:

- 1 Define the VLAN Ethernet interface, specifying a unique VLAN ID as the logical item number of the profile index. For example:

```
HOST-IP2100> new vlan-ethernet
HOST-IP2100> set interface-address physical-address shelf = shelf-1
HOST-IP2100> set interface-address physical-address slot = slot-12
HOST-IP2100> set interface-address physical-address item-number = 10
HOST-IP2100> set interface-address logical-item = 100
HOST-IP2100> set enabled = yes
HOST-IP2100> write -f
```

- 2 Create a VLAN-enabled virtual IP interface, specifying the VLAN ID as the logical item number of the profile index. For example:

```
HOST-IP2100> new ip-interface
HOST-IP2100> set interface-address physical-address shelf = shelf-1
HOST-IP2100> set interface-address physical-address slot = slot-12
HOST-IP2100> set interface-address physical-address item-number = 10
HOST-IP2100> set interface-address logical-item = 100
HOST-IP2100> set ip-address = 192.1.1.1/24
HOST-IP2100> set netmask = 255.255.255.0
HOST-IP2100> set vlan-enabled = yes
HOST-IP2100> set vlan-id = 100
HOST-IP2100> write -f
```

For details about VLAN configuration, see the *Stinger IP Control Module Configuration Guide*.

## Enabling IP multicast on a GE-OLIM trunk port

To enable IP multicast on the routed VLAN interface created in the preceding section, follow these steps:

- 1 Enable multicast in the virtual IP interface used for the routed VLAN. For example:

```
HOST-IP2100> read ip-interface { { 1 12 10 } 100 }
HOST-IP2100> set multicast-allowed = yes
HOST-IP2100> write -f
```

- 2 Enable multicast forwarding and configure the virtual IP interface as an MBONE interface in the ip-global profile. For example:

```
HOST-IP2100> read ip-global
HOST-IP2100> set multicast-forwarding = yes
HOST-IP2100> set multiple-mbone mbone-lan 1 physical-address shelf = 1
HOST-IP2100> set multiple-mbone mbone-lan 1 physical-address slot = 12
HOST-IP2100> set multiple-mbone mbone-lan 1 physical-address item = 10
HOST-IP2100> set multiple-mbone mbone-lan 1 logical-item = 100
HOST-IP2100> write -f
```

For details about MBONE configuration, see the *Stinger IP Control Module Configuration Guide*.

## Configuring GE-OLIM trunk port link aggregation

You can configure the bandwidth of the external trunk ports (ports 9 and 10) of a GE-OLIM card to support 802.3ad Link Aggregation Control Protocol (LACP). When LACP is in use, the trunk ports function as a single link providing double the capacity of an individual link.

Currently, only ports 9 and 10 can be part of a Link Aggregation Group (LAG). In addition, the trunk ports can be configured only in a routed VLAN mode. Bridging is not supported on these ports.

### Benefits of link aggregation

Link aggregation provides the following benefits:

- Increased bandwidth  
The capacity of two GigE links is combined into one logical link. Both links must operate at the same data rate in full-duplex mode.
- Increased availability  
The failure or replacement of a single link within a Link Aggregation Group (LAG) does not affect service from a client perspective.
- Load sharing  
Traffic is distributed across both links.

## Configuration overview

To aggregate the GE-OLIM trunk ports, you must complete the following steps:

- 1 Create an ether-group profile for the LAG. The profile is indexed by a unique number. For example:  
ETHER-GROUP/1
- 2 Configure a virtual ethernet profile for the LAG. The index of this profile is a virtual physical address that includes the special slot designation slot-ether-group and the index number of the ether-group profile. For example, the index of a virtual ethernet profile for ether-group 1 is as follows:  
ETHERNET/{ shelf-1 slot-ether-group 1 }
- 3 Specify the ether-group index, and if necessary configure LACP options, in the ethernet port profiles.  
ETHERNET/{ shelf-1 slot-12 9 }  
ETHERNET/{ shelf-1 slot-12 10 }
- 4 If required, provide system-level LACP information in the following profile:  
LACP

## Settings in the Ether-Group profile

Following are the ether-group profile contents for link-aggregated ports, shown with default settings:

```
[in ETHER-GROUP/1]
index-item-number* = 1
enabled = yes
type = lacp
lacp-options = { 1 }
stp-options = { rstp 32768 20 2 15 }

[in ETHER-GROUP/1:lacp-options]
lag-id = 0
```

<b>Parameter</b>	<b>Setting</b>
index-item-number	The number of the group. You must assign a nonzero value to this field.
enabled	Enables or disables the profile. The profile is enabled by default. Setting this parameter to no disables link aggregation on the trunk ports.
type	The type of group. Currently, the lacp and stp types are supported. The lacp value is required when configuring 802.3ad LACP.

<b>Parameter</b>	<b>Setting</b>
LACP lag-id	<p>This is used in all LACP communication. The default value is 0 and the valid range is 0 - 12. You need to change the default value to a valid value (1-12) for LACP to function correctly.</p> <p>On any given slot, the LAG ID must be unique. The LACP stack uses the parameter lag-id. The ether-group value continues to be the external interface for ethernet profiles, [1 slot-ether-group ether-group-number] and ethernet-&gt;ether-group ] on the Stinger.</p> <p>When configuring LACP between the Stinger GE-OLIM and an external switch, the lag-id configured on the Stinger must match the lag-id used at the remote end.</p>

The ether-group number can have a range of 1-65535. Any of the Stinger slots can use the ether-group-number. An ether-group gets attached to a particular slot after ethernet >ether-group is configured. After an ether-group is attached to a particular slot, it cannot be attached to another slot.

### Virtual Ethernet profile settings

The virtual ethernet profile representing a LAG is an operator-created ethernet profile indexed by a special virtual physical address.

When the GigE ports are operating as a LAG, all port-specific settings are taken from the virtual ethernet profile rather than the ethernet profiles for the physical ports. This ensures that the two ports will have identical configurations, and that any changes to the configuration can be made in one place only.

When you create a virtual ethernet profile, some default values are not applicable for GigE ports. Following are the default settings in a new ethernet profile:

```
[in ETHERNET/{ any-shelf any-slot 0 }]
interface-address* = { any-shelf any-slot 0 }
link-state-enabled = no
enabled = yes
ether-group = 0
ether-if-type = utp
bridging-enabled = no
filter-name = ""
duplex-mode = full-duplex
pppoe-options = { no no "" }
bridging-options = { 0 no no transparent-bridging 0 0 "" 0 }
lACP-options = { 65535 active }
media-speed-mbit = 100mb
auto-negotiate = no
vlan-stack-tag-type = 91:00
```

<b>Parameter</b>	<b>Setting</b>
interface-address	For an ethernet profile representing a LAG, you must specify a virtual physical address ( <code>{ shelf slot item }</code> ) with the following settings: <code>shelf</code> The shelf number. <code>slot</code> slot-ether-group <code>item</code> The index of an ether-group profile. For example, the address of a LAG ethernet profile associated with ether-group 1 is: <code>{ shelf-1 slot-ether-group 1 }</code>
link-state-enabled	A setting (not required) for deleting routes to a link when the link state is down.
enabled	Enables or disables the profile.
ether-group	Not used in a virtual ethernet profile representing a LAG.
ether-if-type	Not used in a virtual ethernet profile representing a LAG.
bridging-enabled	Enables or disables layer 2 bridging for VLAN operations on the LAG. See the <i>Stinger IP Control Module Configuration Guide</i> .
filter-name	Name of a filter to apply to all non-VLAN traffic on the GigE interface. See the <i>Stinger IP Control Module Configuration Guide</i> .
duplex-mode	For a virtual ethernet profile representing a LAG, this value must be set to full-duplex.
pppoe-options	Not currently used.
bridging-options	Not currently used.
lacp-options	Not used in a virtual ethernet profile representing a LAG.
media-speed-mbit	For a virtual ethernet profile representing a LAG, this value must be set to 1000mb.
auto-negotiate	Enable or disable auto negotiation.
vlan-stack-tag-type	If the layer-2 core network is using a specific EtherType value for stacked VLAN frames, you must set the <code>vlan-stack-tag-type</code> parameter to that value. See the <i>Stinger IP Control Module Configuration Guide</i> .

## Settings in Ethernet profiles for the physical GigE ports

To attach two GigE ports to a LAG, the following settings are required in each port's system-generated ethernet profile. When link aggregation is in use, these parameters (shown with default settings) are the only settings taken from these profiles:

```
[in ETHERNET/{ shelf-1 slot-12 9 }]  
interface-address* = { shelf-1 slot-12 9 }
```

## Hosted System Configuration

### Configuring GE-OLIM trunk port link aggregation

---

```
enabled = yes
ether-group = 0
[in ETHERNET/{ shelf-1 slot-12 9 }:lacp-options]
priority = 65535
participation = active
```

Every other parameter from the port ethernet profile is ignored and the values found in the LAG ethernet profile are used instead.

Parameter	Setting				
enabled	Enables or disables the port. You can set this parameter to no to bring the port down without detaching it from the LAG.				
ether-group	<p>The index of an ether-group profile. When set to 0 (default), the port operates individually. If set to a nonzero value, the system searches for an ether-group profile indexed by this value. If it finds one, the port will be attached to that group provided that the following conditions are true:</p> <ul style="list-style-type: none"><li>■ The ether-group profile is enabled.</li><li>■ The ether-group profile specifies a type of lacp (the only type currently supported).</li><li>■ A valid ethernet profile has been created for the LAG.</li></ul> <p>If the port cannot be attached it will continue to operate as an individual port. You can use this setting in the port profile to detach the port from a LAG or attach it to a new one.</p>				
lacp-options	<p>A subprofile where port-level link aggregation parameters are configured. There are currently two LACP parameters:</p> <table><tbody><tr><td>priority</td><td>802.3ad port priority. The higher the number, the lower the priority. A configured port priority may be useful to the remote LACP peer for arbitration between aggregation candidates if the peer has a restriction on the number of ports in a LAG.</td></tr><tr><td>participation</td><td>802.3ad participation (active or passive). With the default active value, the port will initiate LACP negotiation. If set to passive, the port only responds to LACP negotiation.</td></tr></tbody></table>	priority	802.3ad port priority. The higher the number, the lower the priority. A configured port priority may be useful to the remote LACP peer for arbitration between aggregation candidates if the peer has a restriction on the number of ports in a LAG.	participation	802.3ad participation (active or passive). With the default active value, the port will initiate LACP negotiation. If set to passive, the port only responds to LACP negotiation.
priority	802.3ad port priority. The higher the number, the lower the priority. A configured port priority may be useful to the remote LACP peer for arbitration between aggregation candidates if the peer has a restriction on the number of ports in a LAG.				
participation	802.3ad participation (active or passive). With the default active value, the port will initiate LACP negotiation. If set to passive, the port only responds to LACP negotiation.				

## LACP profile settings

The system LACP profile has only one parameter, shown with its default value;

```
[in LACP]
system-priority = 65535
```

<b>Parameter</b>	<b>Setting</b>
system-priority	802.3ad system priority. The higher the number, the lower the priority. A configured system priority may be useful to the remote LACP peer for arbitration between aggregation candidates if the peer has a restriction on the number of ports in a LAG.

## Sample link aggregation configuration

The following sample configuration aggregates the trunk ports into a 2Gb LAG.

- 1 Create an ether-group profile. For example:

```
HOST-IP2100> new ether-group
HOST-IP2100> set index-item-number = 1
HOST-IP2100> set enabled = yes
HOST-IP2100> set type = lacp
HOST-IP2100> set type = lacp-options = { 1 }
HOST-IP2100> set type =stp-options = { rstp 32768 20 2 15 }
HOST-IP2100> set type = lag-id = 0
HOST-IP2100> write -f
```
- 2 Create a new virtual ethernet profile for the aggregated link. For example:

```
HOST-IP2100> new ethernet { 1 slot-ether-group 1 }
HOST-IP2100> set ether-group = 1
HOST-IP2100> set media-speed-mbit = 1000mb
HOST-IP2100> set auto-negotiate = yes
HOST-IP2100> write -f
```
- 3 Modify the system-generated ethernet profiles for the trunk ports. For example:

```
HOST-IP2100> read ethernet { 1 12 9 }
HOST-IP2100> set enabled = yes
HOST-IP2100> set ether-group = 1
HOST-IP2100> write -f
HOST-IP2100> read ethernet { 1 12 10 }
HOST-IP2100> set enabled = yes
HOST-IP2100> set ether-group = 1
HOST-IP2100> write -f
```

## Configuring a routed VLAN that uses the aggregated bandwidth

The following sample configuration creates a routed VLAN that uses the 2Gb LAG.

- 1 Create a `vlan-ethernet` profile. Specify the index of the virtual ethernet profile as the physical address. For example:

```
HOST-IP2100> new vlan-ethernet
HOST-IP2100> set interface-address physical shelf = shelf-1
HOST-IP2100> set interface-address physical slot = slot-ether-group
HOST-IP2100> set interface-address physical item-number = 1
HOST-IP2100> set interface-address logical-item = 555
HOST-IP2100> set enabled = yes
HOST-IP2100> set bridging-options bridge-type = no-bridging
HOST-IP2100> write -f
```

- 2 Create a virtual IP interface for the routed VLAN. Specify the index of the virtual ethernet profile as the physical address. For example:

```
HOST-IP2100> new ip-interface
HOST-IP2100> set interface-address physical shelf = shelf-1
HOST-IP2100> set interface-address physical slot = slot-ether-group
HOST-IP2100> set interface-address physical item-number = 1
HOST-IP2100> set interface-address logical-item = 555
HOST-IP2100> set ip-address = 185.1.1.10/24
HOST-IP2100> set multicast-allowed = yes
HOST-IP2100> set vlan-enabled = yes
HOST-IP2100> set vlan-id = 555
HOST-IP2100> write -f
```

For details about routed VLAN configuration, see the *Stinger IP Control Module Configuration Guide*.

## Configuring an MBONE interface on the aggregated trunk ports

The following commands configure an MBONE interface that uses the aggregated trunk bandwidth and the routed VLAN interface created in the preceding section:

```
HOST-IP2100> read ip-global
HOST-IP2100> set multicast-forwarding = yes
HOST-IP2100> set multiple-mbone mbone-lan 1 physical shelf = shelf-1
HOST-IP2100> set multiple-mbone mbone-lan 1 physical slot = slot-ether-group
HOST-IP2100> set multiple-mbone mbone-lan 1 physical item-number = 1
HOST-IP2100> set multiple-mbone mbone-lan 1 logical-item = 555
HOST-IP2100> write -f
```

For details about MBONE configuration, see the *Stinger IP Control Module Configuration Guide*.

## LACP implementation details

The information in this section relates to the IEEE 802.3ad specification, and provides details that may be useful in communicating with a remote LACP peer.

- Distribution and collection of frames

The Stinger LACP implementation has coupled control, which means that the system does not separate distributing and collecting functions.

- Configuration capabilities and restrictions

Currently, only the GE-OLIM trunk ports 9 and 10 can be part of a LAG. However, the LACP implementation does not enforce a limitation on the number of ports in a LAG. For example, some implementations might support LACP on ten ports but restrict the number of ports in a LAG to eight. Because the system does not enforce any such limitation, the arbitration mechanisms from 802.3 section 43.6 do not apply.

- Admin and Operational keys

The Stinger LACP implementation is static in the sense that GigE ports are not automatically and dynamically aggregated. LACP only runs on ports that have been configured to be part of a LAG.

Ports that are part of a LAG have the same Admin Key by construction, but they may not have the same Operational Key. For example, one of the ports might have a cable disconnect or a cabling error. In this case, only the first port to be aggregated will be part of the configured LAG, and the other port will be unusable until the operational error is corrected.

- Addressing

Because the Stinger LACP implementation is static, the LAG MAC address does not fluctuate as ports go up and down in the LAG. The LAG takes the MAC address of its lowest numbered port. You can view the MAC address assigned to the LAG in the LAG ETHER-INFO profile.

- Distribution algorithm

The Stinger LACP implementation uses the IP header checksum algorithm described in RFC 1071, *Computing the Internet Checksum*. Of course, the checksum is only relevant provided that both ports are distributing. If one of the two links is down, all traffic uses the other link.

- For bridged traffic, the checksum is calculated based on the MAC source address plus the MAC destination address.
- For routed traffic, the checksum is calculated based on the IP source address plus the IP destination address.

- Limitations

- Currently, the Link Aggregation Marker Protocol (LAMP) is not supported.
- Single-port LAG is not supported. (You cannot create a LAG that contains a single port.)
- LACP cannot be used in conjunction with L2TP.

## Enabling host communication to remote shelves

After the physical installation of a Compact Remote system is complete, the remote GE-COP automatically comes up in *slave mode*, ready to communicate with the master CM through the link to the GE-OLIM.

To enable the host system to identify and communicate with the remote shelves, you must complete the following steps:

- Configure the IP2100 CM to operate in master mode, then reset the host system.
- Create a `remote-shelf-config` profile for each remote shelf.

Optionally, you can also configure remote shelf validation. For details, see “Configuring remote shelf validation (optional)” on page 4-20.

## Configuring the host system to operate in master mode

To configure the IP2100 CM in the host Stinger to operate in master mode, 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. The upgrade instructions in the release note for the new software version will provide details.
- 2 Enable master mode in the system profile. Following are the required commands:

```
HOST-IP2100> read system
```

```
HOST-IP2100> set shelf-controller-type = master
```

```
HOST-IP2100> write -f
```

The master CM is always in 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.

## Configuring remote shelf settings

For each remote shelf you want to put into service, you must 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.

### Overview of profile settings

Following are the `remote-shelf-config` parameters, shown with default settings:

```
[in REMOTE-SHELF-CONFIG/any-shelf]
remote-shelf-id* = any-shelf
host-port = { { shelf-1 any-slot 0 } 0 }
host-port-2 = { { shelf-1 any-slot 0 } 0 }
enabled = no
name = ""
location = ""
nailed-group-bin = 0
```

```
remote-shelf-type = stngr-cr-3  
validation-config = { system-defined 0 }
```

<b>Parameter</b>	<b>Setting</b>
remote-shelf-id	Remote shelf ID. The setting must be <i>shelf-N</i> , where <i>N</i> is from 2 to 166. A maximum of 48 remote IP DSLAM shelves can be supported by a single host.
host-port	Physical address of the GE-OLIM port connected to the port labeled GIGE-1 in the remote GE-COP. The address consists of a shelf ID, which is always 1 for the host, followed by the slot and port number of the GE-OLIM.
host-port-2	Physical address of the GE-OLIM port connected to the port labeled GIGE-2 in the remote GE-COP, if applicable. The second port must be on the same GE-OLIM as the first one. See “Enabling GE-OLIM CR port link aggregation” on page 4-17 for details.
enabled	Enables or disables the remote shelf and the control channel between the host and remote shelf.
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 (CLLI™) 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.
nailed-group-bin	A number from 2 to 84 that identifies how many nailed-group values are allocated to the remote shelf. The default value is equal to <code>remote-shelf-id</code> . If <code>remote-shelf-id</code> is greater than 84, you must specify a unique <code>nailed-group-bin</code> value within the range of 2 to 84 to be able to write the profile. <ul style="list-style-type: none"><li>■ With a value of 1 (the host), 4000 nailed-group values are allocated to the shelf.</li><li>■ With a value from 2 through 7, 2000 nailed-group values are allocated to the remote shelf.</li><li>■ With a value from 8 through 84, 600 nailed-group values are allocated to the remote shelf</li></ul>
remote-shelf-type	Displays the type of remote shelf. This field is currently read-only. It must always display <code>stngr-cr-3</code> for Compact Remote shelves.
validation-config	Used for shelf validation. See “Configuring remote shelf validation (optional)” on page 4-20.

**Sample remote-shelf-config configuration**

To enable communications with a remote shelf connected to a GE-OLIM port 1 in slot 2 of the host system, follow these steps.

- 1 Create a remote-shelf-config profile and assign a unique shelf number. For example:

```
HOST-IP2100> new remote-shelf-config
```

```
HOST-IP2100> set remote-shelf-id = shelf-7
```

- 2 Specify the GE-OLIM port to which the remote shelf is connected. For example:

```
HOST-IP2100> set host-port physical-address slot = slot-2
```

```
HOST-IP2100> set host-port physical-address item-number = 1
```

- 3 If required, assign a name or CLI code to identify the remote shelf, and specify the shelf's physical location to simplify maintenance procedures. For example:

```
HOST-IP2100> set name = ZOWISAAASCR
```

```
HOST-IP2100> set location = ZoowieIsland-Saskatchewan
```

- 4 Enable the control channel to the remote shelf, and write the profile.

```
HOST-IP2100> set enabled = yes
```

```
HOST-IP2100> write -f
```

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

When the control channel becomes active, the show command output should include the remote shelf.

For example:

```
HOST-IP2100> show
```

```
Shelf 1 ( master ):
```

```
Controller { first-control-module } ( PRIMARY ):
```

	Reqd	Oper	Slot	Type
{ shelf-1 slot-1 0 }	UP	UP		stngr-golim-card
{ shelf-1 slot-2 0 }	UP	UP		stngr-golim-card
{ shelf-2 slot-1 0 }	UP	UP		geb-gs-ads12plus-card
{ shelf-2 slot-2 0 }	UP	UP		geb-gs-ads12plus-card
{ shelf-2 slot-3 0 }	UP	UP		geb-gs-ads12plus-card
{ shelf-2 first-control-m+	UP	UP		gecrt-cm
{ shelf-7 slot-1 0 }	UP	LOAD		geb-gs-ads12plus-card
{ shelf-7 slot-2 0 }	UP	LOAD		geb-gs-ads12plus-card
{ shelf-7 slot-3 0 }	UP	LOAD		geb-gs-ads12plus-card
{ shelf-7 first-control-m+	UP	UP		gecrt-cm

First the remote shelf COP (gecrt-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 (geb-gs-ads12plus-card) will also be in the UP state.

## Enabling GE-OLIM CR port link aggregation

Link aggregation between GE-OLIM CR ports and a remote GE-COP is enabled automatically when you configure both the `host-port` and `host-port-2` addresses in the `remote-shelf-config` profile.

When link aggregation is enabled, the aggregate allowed guaranteed upstream bandwidth of the RLIMs in the remote shelf increases from 1Gbps to approximately 2Gbps. Traffic distribution occurs over the two aggregated links according to the frame distribution algorithm implemented in hardware.

The increase to 2Gbps bandwidth is used in CAC checks on the GE-OLIM ports (if LIM port CAC is enabled for the GE-OLIM) and on the RLIMs in the remote shelf. If LIM port CAC is not enabled for the GE-OLIM, no CAC bandwidth checks are performed on the GE-OLIM slot.

When link aggregation is enabled, if either GE-OLIM port goes down and the other port is still up, CAC bandwidth does not change and all connections stay established.

The `gecacstat` command displays GE-OLIM CAC bandwidth information. For an example of its use, see “Sample configuration enabling link aggregation” on page 4-18.

## CAC bandwidth checks for guaranteed connections

The system allocates an upstream payload bandwidth pool for guaranteed connections. Guaranteed connections have a constant bit rate (CBR), realtime variable bit rate (rtVBR) or non-realtime VBR (nrtVBR) QoS contract. CAC checks are performed only for guaranteed connections. No CAC checks are performed for the GE-OLIM slot bandwidth.

The `cac-preference` setting in the system profile specifies whether all CAC checks systemwide are performed at the time a connection is being established (the default) or at the time a connection is provisioned.

For RLIMs, CAC checks are performed at the LIM slot level by default, at the time a connection is being established.

For the GE-OLIM ports, CAC bandwidth checks are performed only when LIM port CAC is enabled in the GE-OLIM `slot-static-config` profile. No CAC checks are performed on the GE-OLIM slot.

You enable LIM port CAC in the GE-OLIM's `slot-static-config` profile. For example, the following commands enable port-level CAC checks for the GE-OLIM in slot 5:

```
HOST-IP2100> read slot-static-config { 1 5 0 }
HOST-IP2100> set port-cac-enable = yes
HOST-IP2100> write -f
```

For details about CAC and how to configure it, see the Bandwidth Management chapter of the *Stinger ATM Configuration Guide*.

## Sample configuration enabling link aggregation

To enable link aggregation and increase the allowed upstream bandwidth for one of the remote shelf's RLIMs, follow these steps:

- 1 Enable link aggregation to a remote shelf. For example:

```
HOST-IP2100> read remote-shelf-config 11
HOST-IP2100> list
[in REMOTE-SHELF-CONFIG/shelf-11]
remote-shelf-id* = shelf-11
host-port = { { shelf-1 slot-5 2 } 0 }
host-port-2 = { { shelf-1 any-slot 0 } 0 }
enabled = yes
name = REMOTE-CR-11
location = ""
nailed-group-bin = 11
remote-shelf-type = stngr-cr-3
validation-config = { system-defined 0 }
HOST-IP2100> set host-port-2 = { { 1 5 3 } 0 }
HOST-IP2100> write -f
```

- 2 Verify that link aggregation is enabled. For example:

```
HOST-IP2100> remoteshelf -s 11
Shelf:          11
Shelf Name:     REMOTE-CR-11
Shelf Location:
Shelf Type:     3 slot Compact Remote
Host Port:     {{ 1 5 2 } 0 }
Host Port 2:   {{ 1 5 3 } 0 }
Link Aggr:     Enabled
Admin State:   Enabled
Oper State:    OPER_UP
Up Count:      3
Last Up Time:  Mon Jul 18 0:37:03 2005
Last down Time: Mon Jul 18 0:36:55 2005
Nail Group Bin: 11
```

- 3 Use the `gecacstat` command to verify that the CAC bandwidth for the GE-OLIM port configured as `host-port` is doubled, as shown for port `{ 1 5 2 }` in the following command output:

```
HOST-IP2100> gecacstat 1 5
GE LIM port Cac Data for shelf : 1 slot : 5
PORT {1 5 1} (stngr-golim-card) (ACTIVE)
Stream Total BW      Gtd BW  Gtd Allocated  Gtd Available
UP      1000000        1000000 0              1000000
DN      1000000        1000000 0              1000000
PORT {1 5 2} (stngr-golim-card) (ACTIVE)
Stream Total BW      Gtd BW  Gtd Allocated  Gtd Available
UP      2000000        2000000 0              2000000
DN      2000000        2000000 0              2000000
PORT {1 5 3} (stngr-golim-card) (ACTIVE)
Stream Total BW      Gtd BW  Gtd Allocated  Gtd Available
```

```

UP      1000000      1000000 0      1000000
DN      1000000      1000000 0      1000000
PORT {1 5 4} (stngr-golim-card) (ACTIVE)
Stream Total BW      Gtd BW Gtd Allocated  Gtd Available
UP      1000000      1000000 0      1000000
DN      1000000      1000000 0      1000000
PORT {1 5 5} (stngr-golim-card) (ACTIVE)
Stream Total BW      Gtd BW Gtd Allocated  Gtd Available
UP      1000000      1000000 0      1000000
DN      1000000      1000000 0      1000000
PORT {1 5 6} (stngr-golim-card) (ACTIVE)
Stream Total BW      Gtd BW Gtd Allocated  Gtd Available
UP      1000000      1000000 0      1000000
DN      1000000      1000000 0      1000000
PORT {1 5 7} (stngr-golim-card) (INACTIVE)
Stream Total BW      Gtd BW Gtd Allocated  Gtd Available
UP      1000000      1000000 0      1000000
DN      1000000      1000000 0      1000000
PORT {1 5 8} (stngr-golim-card) (INACTIVE)
Stream Total BW      Gtd BW Gtd Allocated  Gtd Available
UP      1000000      1000000 0      1000000
DN      1000000      1000000 0      1000000
PORT {1 5 9} (stngr-golim-card) (INACTIVE)
Stream Total BW      Gtd BW Gtd Allocated  Gtd Available
UP      1000000      1000000 0      1000000
DN      1000000      1000000 0      1000000
PORT {1 5 10} (stngr-golim-card) (INACTIVE)
Stream Total BW      Gtd BW Gtd Allocated  Gtd Available
UP      1000000      1000000 0      1000000
DN      1000000      1000000 0      1000000

```

- 4 Increase upstream bandwidth for an RLIM #1 on the remote shelf. Optionally, you can also configure oversubscription. For example:

```

HOST-IP2100> read slot-static-config { 11 1 }
HOST-IP2100> set allow-max-up-stream-bandwidth = 1000000
HOST-IP2100> set allow-guaranteed-up-stream-bandwidth = 1000000
HOST-IP2100> set slot-over-subscription = 20
HOST-IP2100> write -f

```

- 5 Use the `atmcacstat -b debug-level` command to see the allocated and available upstream and downstream bandwidth on the RLIM. To use this command, you must log into the system as `super`, or another user profile that has debug permissions enabled. For example:

```

HOST-IP2100> atmcacstat -b 11 1
Cac Data for shelf : 11 slot : 1
UP STREAM
    Total B/W Kbits/sec      : 1000000
    Guaranteed B/W Kbits/sec : 2000000
    Allocated Guaranteed B/W : 1931774
    Available Guaranteed B/W  : 68226
DN STREAM
    Total B/W Kbits/sec      : 1000000

```

## Hosted System Configuration

*Configuring remote shelf validation (optional)*

---

Guaranteed B/W Kbits/sec : 2000000  
Allocated Guaranteed B/W : 1931774  
Available Guaranteed B/W : 68226

## Configuring remote shelf validation (optional)

Remote shelf validation provides a layer of error checking for indicating if a remote shelf is disconnected from one GE-OLIM port and accidentally reconnected to the wrong GE-OLIM port. This level of error checking is important especially when an GE-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.

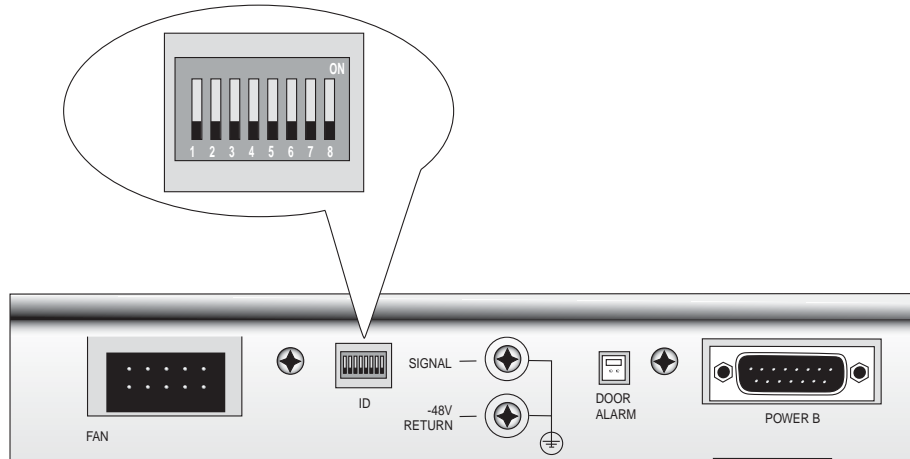
If the validation ID in `remote-shelf-config` is set to a nonzero value, validation is performed if validation has been enabled for the shelf.

## Setting the chassis ID on a remote shelf

To avoid connecting a remote shelf to the wrong GE-OLIM port on the host, each Stinger Compact Remote 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 system. This comparison verifies that a specific Stinger Compact Remote chassis has been connected to a specific optical port of a GE-OLIM on the host. Detection of the chassis ID can be enabled or disabled on the host.

The chassis ID DIP switches are located behind the cooling unit in the top rear area of the Stinger Compact Remote chassis, as shown in Figure 4-2.

Figure 4-2. 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 4-3. 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

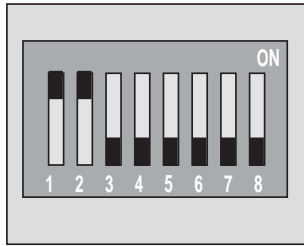
The decimal value of validation ID is the total of all decimal values for DIP switches that are set to ON. For example, the binary 8-bit ID number created by setting only DIP switches 1 and 2 ON is 11000000. The decimal value of the validation ID produced by this setting is 192. This setting is shown in Figure 4-3.

## Hosted System Configuration

Configuring remote shelf validation (optional)

---

Figure 4-3. 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 Compact Remote chassis.
- 2 Remove the 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 cooling module as described in “Replacing the chassis cooling module” on page 3-13.

## Configuring remote shelf validation on the host system

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						
validation-enable	<p>Enables/disables validation. For the system to perform ID comparison, validation must be enabled and validation-id must also have a nonzero value.</p> <p>In the system profile, valid values are yes and no.</p> <p>In the remote-shelf-config profile, following are valid values:</p> <table><tbody><tr><td>system-defined</td><td>Use the setting in the system profile to determine if validation is enabled for this shelf.</td></tr><tr><td>yes</td><td>Enable validation for this shelf. The system profile setting is not used.</td></tr><tr><td>no</td><td>Disable validation for this shelf. The system profile setting is not used.</td></tr></tbody></table>	system-defined	Use the setting in the system profile to determine if validation is enabled for this shelf.	yes	Enable validation for this shelf. The system profile setting is not used.	no	Disable validation for this shelf. The system profile setting is not used.
system-defined	Use the setting in the system profile to determine if validation is enabled for this shelf.						
yes	Enable validation for this shelf. The system profile setting is not used.						
no	Disable validation for this shelf. The system profile setting is not used.						

Parameter	Setting
validation-id	<p>A validation ID, from 1 to 255, to compare against the DIP-switch setting of the remote shelf.</p> <p>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.</p> <p>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.</p>

The following commands configure the host to validate the remote shelf with the number 192, which was set on the remote shelf DIP switch as shown in Figure 4-3 (page 4-22).

```
HOST-IP2100> read remote-shelf-config shelf-3
HOST-IP2100> set validation-config validation-id = 192
HOST-IP2100> write -f
```

For validation to take effect, you must reset the remote shelf. Validation takes effect when the control link between the host and the remote shelf has been reestablished. For example, the following command resets remote-shelf 3.

```
HOST-IP2100> reset -s 3
```



**Note** All traffic on the remote shelf is interrupted during the reset.

## Configuring subscriber connections

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

Table 4-4 lists currently supported types of subscriber connections:

Table 4-4. Subscriber connection types

Traffic path	Connection type
RLIM ↔ IP2100 Gigabit Ethernet port	VLAN bridging (1:1)
	VLAN stacking
	GigE port routed VLAN
	RLIM PPPoE routed connections terminated on the system

Table 4-4. *Subscriber connection types (Continued)*

<b>Traffic path</b>	<b>Connection type</b>
RLIM ↔ GE-OLIM trunk port	GigE port routed VLAN RLIM PPPoE routed connections terminated on the system RLIM BIR connections for multicast traffic only
RLIM ↔ host ATM trunk port	ATM circuit between an RLIM port and a host trunk port

## Enabling remote shelf RLIM interfaces

For subscriber connections to become active, the RLIM interfaces must be explicitly enabled. This section shows how to enable RLIM interfaces. For details about configuring the ADSL2+ interfaces to interoperate with specific CPE, see the *Stinger ADSL Annex A Line Interface Module (LIM) Guide for LIMs with ADSL2+ Capability*.

- 1 Enable the RLIM interfaces.

The following commands enable the first two RLIM interfaces on remote shelf 7:

```
HOST-IP2100> read al-dmt { 7 1 1 }
HOST-IP2100> set enabled = yes
HOST-IP2100> write -f
HOST-IP2100> read al-dmt { 7 2 1 }
HOST-IP2100> set enabled = yes
HOST-IP2100> write -f
```

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

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

```
HOST-IP2100> dmtal -u
```

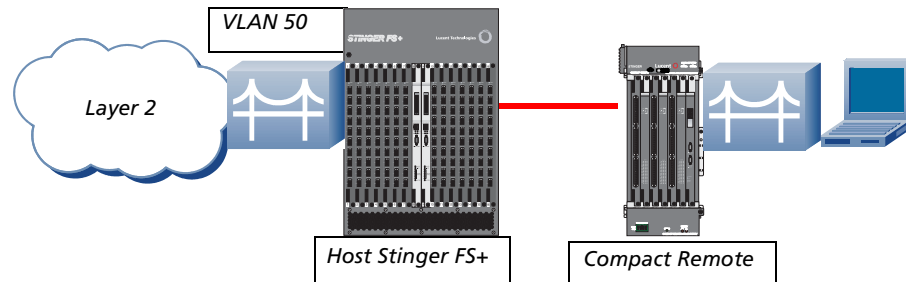
In-Use DMT ADSL lines:

	(dvOp	dvUpSt	dvRq	sAdm	naIlg)
Line { 7 1 1 }	(Up	Assign	UP	UP	14001)
Line { 7 2 1 }	(Up	Assign	UP	UP	14101)

## VLAN bridging (1:1) connection with CM egress

The following example shows how to provision a VLAN bridging connection, which maps one user PVC to one unique VLAN ID as shown in Figure 4-4.

Figure 4-4. Bridging one PVC to one VLAN on IP2100 Gigabit Ethernet ports



For details about VLAN configuration, see the *Stinger IP Control Module Configuration Guide*. To configure this sample VLAN circuit, follow these steps:

- 1 Enable bridging on the IP2100 Gigabit Ethernet interface to be used. For example:

```
HOST-IP2100> read ethernet { 1 8 2 }
HOST-IP2100> set bridging-enabled = yes
HOST-IP2100> write -f
```
- 2 Create a vlan-ethernet profile and specify the VLAN ID in the index:

```
HOST-IP2100> new vlan-ethernet { { 1 8 2 } 50 }
HOST-IP2100> set enabled = yes
HOST-IP2100> set bridging-options bridging-group = 222
HOST-IP2100> write -f
```
- 3 Determine the nailed group assignment for the RLIM interface to be used. For example:

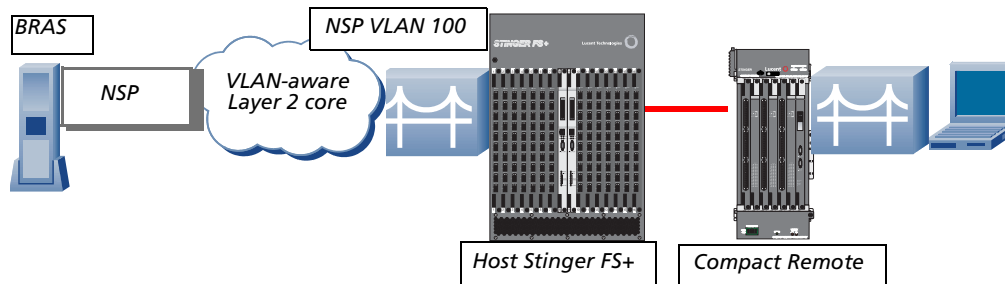
```
HOST-IP2100> which -n { 7 2 1 }
Nailed group corresponding to port { shelf-7 slot-2 1 } is 14101
```
- 4 Create a connection profile for the PVC side of the VLAN circuit. The bridging-group number must match that of the VLAN interface.

```
HOST-IP2100> new connection dslcpe
HOST-IP2100> set active = yes
HOST-IP2100> set encapsulation-protocol = atm
HOST-IP2100> set ip-options ip-routing-enabled = no
HOST-IP2100> set bridging-options bridging-group = 222
HOST-IP2100> set bridging-options bridge = yes
HOST-IP2100> set atm-options vpi = 8
HOST-IP2100> set atm-options vci = 100
HOST-IP2100> set atm-options nailed-group = 14101
HOST-IP2100> write -f
```

## VLAN stacking connection with CM egress

The following example shows how to provision a stacked VLAN connection, which maps a user PVC to a remote NSP VLAN, as shown in Figure 4-5.

Figure 4-5. Bridging a PVC to an NSP VLAN (stacked VLANs)



For details about stacked VLAN configuration, see the *Stinger IP Control Module Configuration Guide*. To configure this sample connection, follow these steps:

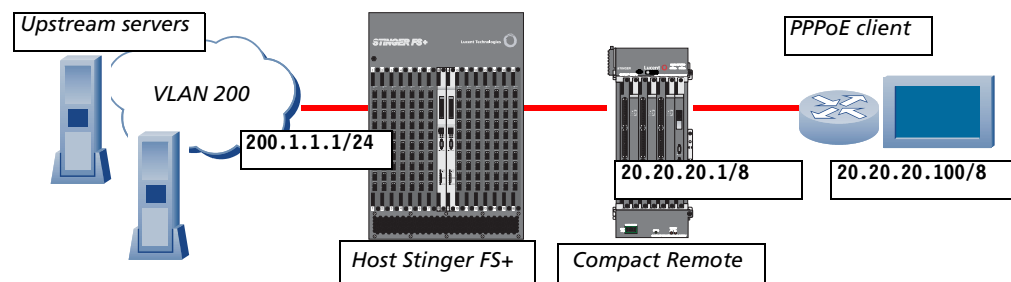
- 1 Configure the ethernet profile of the egress interface in the host.  
The ethernet profile must enable bridging. In addition, because there is not yet a standard for NSP VLAN ID headers, you must configure `vlan-stack-tag-type` to inform the next hop switch that the packet is a stacked VLAN packet.  
For example, this set of commands sets `vlan-stack-tag-type` to 81:00:  
HOST-IP2100> **read ethernet { 1 first-control-module 2 }**  
HOST-IP2100> **set bridging-enabled = yes**  
HOST-IP2100> **set media-speed-mbit = 1000mb**  
HOST-IP2100> **set auto-negotiate = yes**  
HOST-IP2100> **set vlan-stack-tag-type = 81:00**  
HOST-IP2100> **write -f**
- 2 Configure the stacked VLAN interface to the NSP. For example:  
HOST-IP2100> **new vlan-ethernet { 1 first-control-module 2 } 100}**  
HOST-IP2100> **set enabled = yes**  
HOST-IP2100> **set bridging-options bridging-group = 100**  
HOST-IP2100> **set bridging-options bridge = yes**  
HOST-IP2100> **set bridging-options bridge-type = stacked-vlan**  
HOST-IP2100> **write -f**
- 3 Create a connection profile to the DSL end-user. For example:  
HOST-IP2100> **new connection vlan-stack**  
HOST-IP2100> **set active = yes**  
HOST-IP2100> **set encapsulation-protocol = atm**  
HOST-IP2100> **set ip-options ip-routing-enabled = no**  
HOST-IP2100> **set bridging-options bridging-group = 100**  
HOST-IP2100> **set bridging-options bridge = yes**  
HOST-IP2100> **set bridging-options bridge-type = stacked-vlan**

```
HOST-IP2100> set bridging-options vlan-stack-user-vlan-id = 10
HOST-IP2100> set atm-options vpi = 8
HOST-IP2100> set atm-options nailed-group = 4002
HOST-IP2100> write -f
```

## Routed VLAN on a GE-OLIM trunk port with a PPPoE routed connection

In this example, a PPPoE subscriber connection can receive both unicast routed video (Video on Demand or VoD) and multicast video (such as IPTV) across the same routed VLAN interface on a GE-OLIM trunk port.

Figure 4-6. A routed PPPoE connection with an upstream routed VLAN interface



This example uses a GE-OLIM trunk port, but routed VLANs are also supported on the master CM GigE ports. For background information, see the *Stinger IP Control Module Configuration Guide*. To configure this sample connection, follow these steps:

- 1 Configure a routed VLAN interface on a GE-OLIM trunk port. For example, the following commands create VLAN 200 on the GE-OLIM trunk port 10 in slot 3:

```
HOST-IP2100> new vlan-ethernet
HOST-IP2100> set interface-address physical-address shelf = shelf-1
HOST-IP2100> set interface-address physical-address slot = slot-3
HOST-IP2100> set interface-address physical-address item-number = 10
HOST-IP2100> set interface-address logical-item = 200
HOST-IP2100> set enabled = yes
HOST-IP2100> write -f
HOST-IP2100> new ip-interface
HOST-IP2100> set interface-address physical-address shelf = shelf-1
HOST-IP2100> set interface-address physical-address slot = slot-3
HOST-IP2100> set interface-address physical-address item-number = 10
HOST-IP2100> set interface-address logical-item = 200
HOST-IP2100> set ip-address = 200.1.1.1/24
HOST-IP2100> set multicast-allowed = yes
HOST-IP2100> set vlan-enabled = yes
HOST-IP2100> set vlan-id = 200
HOST-IP2100> write -f
```

- 2 Enable multicast forwarding in the ip-global profile, and specify the routed VLAN as an MBONE interface. For example:

```
HOST-IP2100> read ip-global
HOST-IP2100> set multicast-forwarding = yes
HOST-IP2100> set multiple-mbone mbone-lan 1 physical shelf = shelf-1
HOST-IP2100> set multiple-mbone mbone-lan 1 physical slot = slot-3
HOST-IP2100> set multiple-mbone mbone-lan 1 physical item = 10
HOST-IP2100> set multiple-mbone mbone-lan 1 logical-item = 200
HOST-IP2100> write -f
```
- 3 Enable PPP authentication in the answer-defaults profile. For example:

```
HOST-IP2100> read answer-defaults
HOST-IP2100> set ppp-answer receive-auth-mode = any-ppp-auth
HOST-IP2100> set ppp-answer bi-directional-auth = allowed
HOST-IP2100> write -f
```
- 4 Enable the RLIM port. For example:

```
HOST-IP2100> read al-dmt { 2 1 7 }
HOST-IP2100> set enabled = yes
HOST-IP2100> write -f
```
- 5 Create the ATM circuit connection profile that provides the interface over which ATM frames are received from the CPE. This profile terminates traffic on the RLIM internal interface (one port number higher than the highest physical port number). For example:

```
HOST-IP2100> new connection
HOST-IP2100> set station = pppoe-circuit
HOST-IP2100> set active = yes
HOST-IP2100> set ip-options ip-routing-enabled = no
HOST-IP2100> set mp-options enabled = no
HOST-IP2100> set atm-options vpi = 8
HOST-IP2100> set atm-options nailed-group = 4007
HOST-IP2100> set atm-connect-options vpi = 8
HOST-IP2100> set atm-connect-options nailed-group = 4049
HOST-IP2100> write -f
```
- 6 Configure the PPPoE terminating connection. For example:

```
HOST-IP2100> new connection
HOST-IP2100> set station = pppoe-client
HOST-IP2100> set active = yes
HOST-IP2100> set encapsulation-protocol = ppp
HOST-IP2100> set ip-options remote-address = 20.20.20.100/8
HOST-IP2100> set ip-options local-address = 20.20.20.1/8
HOST-IP2100> set ip-options multicast-allowed = yes
```

```
HOST-IP2100> set ip-options multicast-max-groups = 16
HOST-IP2100> set ip-options fast-leave = yes
HOST-IP2100> set ppp-options recv-password = ascend
HOST-IP2100> set mp-options enabled = no
HOST-IP2100> set pppoe-options pppoe = yes
HOST-IP2100> write -f
```

Following is a comparable RADIUS user profile:

```
pppoe-client Password = "ascend"
  User-Service = Framed-User,
  Framed-Protocol = PPP,
  Ascend-PPPoE-Enable = PPPoE-Yes,
  Ascend-Call-Type = Switched,
  Framed-Address = 20.20.20.100,
  Framed-Netmask = 255.0.0.0,
  Ascend-PPP-Address= 20.20.20.1,
  Ascend-IF-Netmask = 255.0.0.0,
  Ascend-Route-IP = Route-IP-Yes,
  Ascend-Multicast-Client = Multicast-Yes,
  Ascend-Multicast-Fast-Leave = Ascend-Multicast-Fast-Leave-Yes,
  Ascend-Multicast-Max-Groups = 16
```

## Bridged IP routing (BIR) connections on RLIMs for multicast traffic only

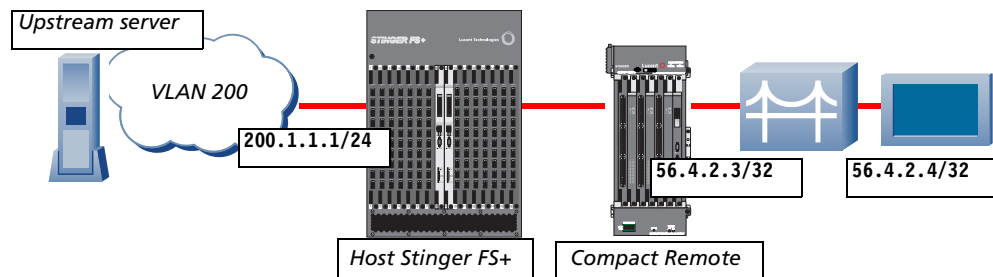
You can terminate a bridged IP routing (BIR) connection on an RLIM for the purpose of forwarding multicast traffic. The system brings up the BIR connection, accepts IGMP Join messages from the client, and forwards traffic based on multicast group membership. Currently, the system forwards only IGMP packets on the BIR connection. All other types of traffic are discarded.

The following functionality is currently not supported on BIR connections that terminate on an RLIM in a hosted Compact Remote IP DSLAM:

- Routing and unicast traffic forwarding (upstream as well as downstream)
- DHCP support for IP address allocation
- Filters
- RIP

For example, in Figure 4-7, a subscriber set-top box (STB) receives IPTV transmissions.

Figure 4-7. BIR connection for multicast video traffic



A GE-OLIM trunk port is used for sourcing the multicast video stream. To configure this sample connection, follow these steps:

- 1 Configure a routed VLAN interface on a GE-OLIM trunk port. For example, the following commands create VLAN 200 on the GE-OLIM trunk port 10 in slot 3:

```
HOST-IP2100> new vlan-ethernet
HOST-IP2100> set interface-address physical-address shelf = shelf-1
HOST-IP2100> set interface-address physical-address slot = slot-3
HOST-IP2100> set interface-address physical-address item-number = 10
HOST-IP2100> set interface-address logical-item = 200
HOST-IP2100> set enabled = yes
HOST-IP2100> write -f
HOST-IP2100> new ip-interface
HOST-IP2100> set interface-address physical-address shelf = shelf-1
HOST-IP2100> set interface-address physical-address slot = slot-3
HOST-IP2100> set interface-address physical-address item-number = 10
HOST-IP2100> set interface-address logical-item = 200
HOST-IP2100> set ip-address = 200.1.1.1/24
HOST-IP2100> set multicast-allowed = yes
HOST-IP2100> set vlan-enabled = yes
HOST-IP2100> set vlan-id = 200
HOST-IP2100> write -f
```

- 2 Enable multicast forwarding in the ip-global profile, and specify the routed VLAN as an MBONE interface. For example:

```
HOST-IP2100> read ip-global
HOST-IP2100> set multicast-forwarding = yes
HOST-IP2100> set multiple-mbone mbone-lan 1 physical shelf = shelf-1
HOST-IP2100> set multiple-mbone mbone-lan 1 physical slot = slot-3
HOST-IP2100> set multiple-mbone mbone-lan 1 physical item = 10
HOST-IP2100> set multiple-mbone mbone-lan 1 logical-item = 200
HOST-IP2100> write -f
```

- 3 Enable the RLIM port. For example:

```
HOST-IP2100> read al-dmt { 7 2 1 }
HOST-IP2100> set enabled = yes
HOST-IP2100> write -f
```

- 4 Determine the nailed group assignment for the RLIM interface to be used. For example:

```
HOST-IP2100> which -n { 7 2 1 }
Nailed group corresponding to port { shelf-7 slot-2 1 } is 14101
```

- 5 Configure the BIR terminating connection. For example:

```
HOST-IP2100> new connection
```

```
HOST-IP2100> set station = video-client-1
HOST-IP2100> set active = yes
HOST-IP2100> set encapsulation-protocol = atm
HOST-IP2100> set ip-options remote-address = 56.4.2.4/32
HOST-IP2100> set ip-options local-address = 56.4.2.3/32
HOST-IP2100> set ip-options multicast-allowed = yes
HOST-IP2100> set atm-options nailed-group = 14101
HOST-IP2100> set bir-options enable = yes
HOST-IP2100> write -f
```

With this configuration, the system brings up the BIR connection and assigns the IP addresses assigned in the profile. When the BIR connection has been established, the system accepts IGMP Join messages from the client and forwards multicast traffic to the client on the basis of group membership.

## ATM circuit between an RLIM port and a host trunk port

This section shows how to configure an ATM circuit between an RLIM port and an ATM trunk port on the host shelf. For details about configuring ATM circuits, see the *Stinger ATM Configuration Guide*.

Currently, ATM circuits between an RLIM and host trunk do not support the following features:

- AAL0 (only AAL5 frames are currently supported)
- OAM
- Virtual path connections

The following command shows the system inventory of a host with both ATM trunks and a remote shelf:

```
HOST-IP2100> show
Shelf 1 ( master ):
Controller { first-control-module } ( PRIMARY ):
      Reqd Oper  Slot Type
{ shelf-1 slot-1 0 }      UP  UP  stngr-golim-card
{ shelf-1 slot-3 0 }      UP  UP  sds1-atm-v2-card
{ shelf-1 trunk-module-1 0 } UP  UP  oc3-atm-trunk-daughter-card
{ shelf-1 trunk-module-2 0 } UP  UP  oc3-atm-trunk-daughter-card
{ shelf-2 slot-1 0 }      UP  UP  geb-gs-ads12plus-card
{ shelf-2 first-control-mod+ UP  UP  gecrt-cm
```

The following commands configure an ATM circuit between an RLIM on the remote shelf and an ATM trunk port:

```
HOST-IP2100> new connection rlim-circuit-1
HOST-IP2100> set active = yes
HOST-IP2100> set encapsulation-protocol = atm-circuit
HOST-IP2100> set ip-options ip-routing-enabled = no
HOST-IP2100> set atm-options vpi = 8
HOST-IP2100> set atm-options nailed-group = 4001
```

## Hosted System Configuration

*Configuring subscriber connections*

---

```
HOST-IP2100> set atm-connect-options vpi = 10
HOST-IP2100> set atm-connect-options nailed-group = 851
HOST-IP2100> write -f
```

---

# Hosted System Management



# 5

Hosted system distributed multicast mechanism . . . . .	5-1
Slot-based address assignment for PPPoE connections . . . . .	5-7
IP filters for RLIM data connections. . . . .	5-11
Administrative tools for hosted environments. . . . .	5-13

This chapter describes management considerations specific to hosted Compact Remote IP DSLAM systems. For more general system management procedures, see the *Stinger Administration Guide*.

## Hosted system distributed multicast mechanism

A distributed multicast mechanism allows each of the following types of module to replicate multicast streams:

- Master CM (IP2100 control module)
- GE-OLIM
- GE-COP
- ADSL2+ IP LIMs

Each of these *multicast-capable modules* acts as a multicast replication point and operates as a standalone multicast router that manages its own multicast interfaces.

The distributed multicast model does not introduce changes to the existing IP multicast configuration process. You still configure IP multicast as described in the *Stinger IP Control Module Configuration Guide*. However, note that the IP2100 GigE interfaces cannot provide MBONE for remote clients in multicast groups.

### Required setting on the master CM

The `multicast-forwarding` parameter must be set to `yes` in the host system's `ip-global` profile. For example:

```
HOST-IP2100> read ip-global
HOST-IP2100> set multicast-forwarding = yes
HOST-IP2100> write -f
```

## Distributed multicast domains

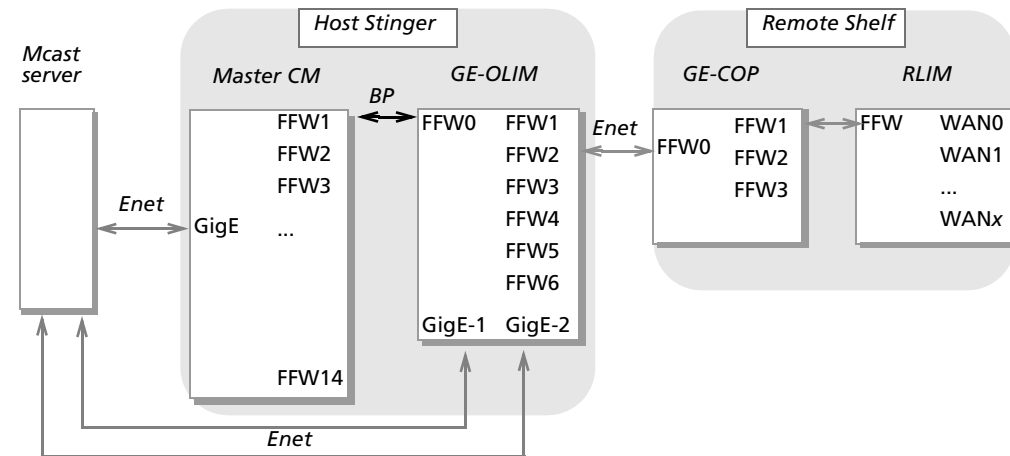
Currently, when a multicast server is sourced through a master CM GigE port, only LIMs in the host chassis can receive multicast streams through the CM ports.

When a multicast server is sourced through a GE-OLIM trunk port, only the RLIM interfaces on remote shelves connected to that GE-OLIM can receive multicast streams from that server. That is, when the GE-OLIM trunk ports are used to access a video server, the service is limited to the GE-OLIM domain.

## Internal fast-forwarding interfaces

Each module acting as a multicast router is interconnected to the next module acting as a multicast router through special interfaces called Fast Forwarding (FFW) interfaces. The FFW interfaces are not user configurable, and are unnumbered (they do not have an IP address). Figure 5-1 shows the interfaces for each multicast-capable module.

Figure 5-1. FFW interfaces on multicast-capable modules



From a multicast point of view, the master CM does not manage all interfaces in the system. For example:

- The CM manages its GigE port and its own FFW interfaces.
- The GE-OLIM manages its two trunk video ports and its FFW interfaces.
- The GE-COP manages its own FFW interfaces.
- The RLIM manages its own WAN interfaces and its FFW interfaces.

## MBONE and multicast client interactions on FFW interfaces

Table 5-1 shows the MBONE and multicast client behavior of the FFW interfaces on each multicast-capable module.

Table 5-1. FFW interfaces registered as multicast backbone or multicast client

<b>Module</b>	<b>FFW interfaces</b>	<b>FFW multicast type</b>
Master CM	One FFW interface to each slot in the system. The internal port is the physical port linked to the module.	multicast-client

Table 5-1. FFW interfaces registered as multicast backbone or multicast client (Continued)

Module	FFW interfaces	FFW multicast type
GE-OLIM	One FFW interface to the master CM	multicast-mbone
	One FFW interface to each connected GE-COP	multicast-client
GE-COP	One FFW interface to the GE-OLIM	multicast-mbone
	One FFW interface to each RLIM	multicast-client
RLIM	One FFW interface to the GE-COP	multicast-mbone

### What happens when a CPE joins a multicast group

In this example, the master CM is not represented. The CPE devices access a video server through the GE-OLIM trunk ports.

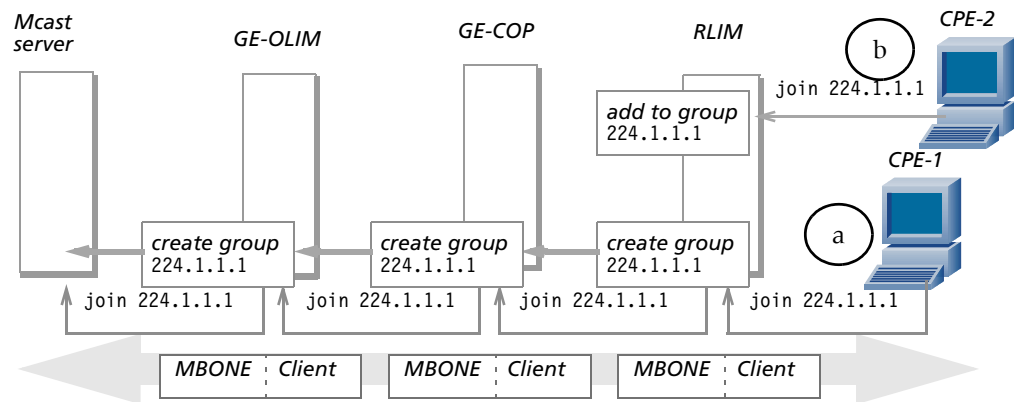
For each multicast router in the hosted system, the receipt of an IGMP Join message on a `multicast-client` interface causes the following behavior:

- 1 If the multicast group does not exist on the module, create it. Otherwise, skip to step 4.
- 2 Register the MBONE interfaces to this group.
- 3 Proxy the IGMP Join on the MBONE interfaces.
- 4 Connect the client to the multicast group.

For example, in Figure 5-2, two CPEs join multicast group 224.1.1.1.

When the system first receives an IGMP Join message from CPE-1, the RLIM and each subsequent multicast router in the distributed system performs all four steps listed above. Once the group has been created, additional Join messages cause the system to simply connect the client to the multicast group at the RLIM.

Figure 5-2. Two IGMP Join requests for the same multicast group



If one of the CPEs in Figure 5-2 issues another IGMP Join message for a different multicast group, such as 224.2.2.2, the process labeled “a” is repeated for the new group.

## What happens when a CPE leaves a multicast group

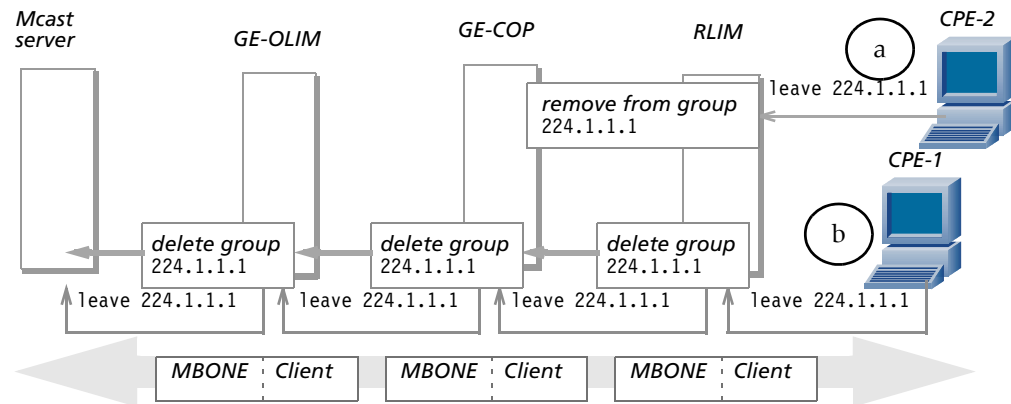
In this example, the master CM is not represented. The CPE devices access a video server through the GE-OLIM trunk ports.

For each multicast router in the hosted system, the receipt of an IGMP Leave message on a `multicast-client` interface causes the following behavior:

- 1 Unregister the client from the multicast group.
- 2 If this is the last active client in the group, proceed to step 3. Otherwise, no further management action is taken.
- 3 Unregister the MBONE interfaces from this group.
- 4 Proxy the IGMP Leave on the MBONE interfaces.

For example, in Figure 5-2, the two CPEs leave multicast group 224.1.1.1. When the system first receives an IGMP Leave message from CPE-2, the system simply removes the client from the multicast group at the RLIM. When the last client in a group sends a Leave message, the RLIM and each subsequent multicast router in the distributed system performs all four steps listed above.

*Figure 5-3. Two IGMP Join requests for the same multicast group*



## Displaying multicast information

The `igmp` commands display multicast information in the context of a specific multicast-capable module. These commands work on all multicast-capable modules.

For example, an `igmp` command on a GE-OLIM module does not display the WAN interface of a multicast client, it displays the FFW interface local to the GE-OLIM module instead. The following example shows multicast information on a GE-OLIM in slot 11 of the host chassis.

- 1 Open a session to the GE-OLIM module.  
**HOST-IP2100> open 1 11**
- 2 Use the `ifmgr -d` command to obtain interface numbers. For example, this output shows that interfaces 1 and 11 are FFW interfaces:

```
slot-1/11> ifmgr -d
if slot:if u p ifname      mac addr      local-addr
-----
000 0:00:000 * pb0        000000000000  0.0.0.0/32
```

```
001 1:11:001 * ffw-2-8    020000010b01    0.0.0.0/32
009 1:08:028 * ie1-11-9    00c07b08e859    1.1.1.1/32
010 1:08:029 * ie1-11-10   00c07b08e85a    1.2.1.1/32
011 1:11:011 * ffw-1-8    020000010b01    0.0.0.0/32
<end>
```

- 3 Use the `igmp mbone` command to display the proxy MBONE interfaces registered on the GE-OLIM:

```
slot-1/11> igmp mbone
Current Igmp Proxy MBONES:
Slot 1:11 ifNum = 9
Slot 1:11 ifNum = 11
```

- 4 Use the `igmp clients` command to display the multicast client interfaces on the GE-OLIM:

```
slot-1/11> igmp clients
IGMP Clients
      Client      Version  RecvCount   CLU   ALU
      9(Mbone)    2         0         0     0
      11(Mbone)   2         0         0     0
      1           2         0         0     0
```

- 5 Use the `igmp groups` command to display multicast groups on the GE-OLIM:

```
slot-1/11> igmp groups
IGMP Group address Routing Table
Up Time: 0d 17:02:14
Group Address  MemberIf  Expire time  Counts
224.1.1.1     1         00:03:44    0::0 S2
              *         (Mbone)     0::0 S2
              *         (Mbone)     0::0 S2
```

## Displaying FFW interface information

You can display FFW interfaces using Stinger diagnostic commands.



**Note** The `ifmgr` and `info` commands are available only in the debug environment. For information about enabling the debug environment and using these commands, see the Diagnostics appendix of the *Stinger IP Control Module Configuration Guide*.

For example, the following command output shows that the FFW interface connected to the GE-OLIM port in slot 1-6 is assigned the interface ID 20.

```
HOST-IP2100> ifmgr -d
bif slot sif u m p ifname      host-name  remote-addr      local-addr
-----
000 1:08 000 *    ie0       -           0.0.0.0/32      134.112.28.82/32
001 1:08 001 *    ie1       -           0.0.0.0/32      192.168.7.82/32
006 1:08 006 *    lo0       -           0.0.0.0/32      127.0.0.1/32
007 0:00 000 *    rj0       -           0.0.0.0/32      127.0.0.2/32
008 0:00 000 *    bh0       -           0.0.0.0/32      127.0.0.3/32
009 1:08 000 *    wanabe    -           0.0.0.0/32      127.0.0.3/32
010 0:00 000 *    local    -           0.0.0.0/32      127.0.0.1/32
011 0:00 000 *    mcast    -           0.0.0.0/32      224.0.0.0/32
012 0:00 000 -    tunne10  -           0.0.0.0/32      127.0.0.5/32
013 0:00 000 *    vr0_main  -           0.0.0.0/32      127.0.0.4/32
```

## Hosted System Management

Hosted system distributed multicast mechanism

---

```
014 0:00 000 - sip0 - 0.0.0.0/32 0.0.0.0/32
015 1:06 002 * p wan15 atm 1.1.1.2/32 1.1.1.1/32
016 1:08 000 - p wan16 atm-ckt-10 0.0.0.0/32 0.0.0.0/32
017 1:08 000 - p wan17 bir 20.20.20.20/32 20.20.20.82/32
018 1:08 000 - p wan18 ppp-2 4.4.4.4/32 4.4.4.1/32
019 1:08 000 - p wan19 ppp-3 0.0.0.0/32 0.0.0.0/32
020 1:08 020 * ffw-1-6 - 0.0.0.0/32 0.0.0.0/32
```

You can also use the `ifmgr -d` command in an open session with any multicast-capable module. For example, following is command output on an RLIM:

```
HOST-IP2100> open 2 1
```

```
geb-gs-dmt-48-2/1> ifmgr -d
```

```
bif slot sif u m p ifname host-name remote-addr local-addr
```

```
-----
000 0:00 000 * pb0 - 0.0.0.0/32 0.0.0.0/32
001 2:01 001 * ffw-2-8 - 0.0.0.0/32 0.0.0.0/32
003 1:08 024 * wan3 ipoa-2-1-2 2.2.2.2/32 2.2.2.1/32
```

```
<end>
```

The `info` command also displays information about FFW interfaces. For example, the following command output shows active connections on a LIM interface, a GigE interface, and a FFW interface:

```
HOST-IP2100> info np conn
```

```
Connection Handles
```

```
if sh/sl act cPort dPort type uctl udata qos dct1 ddata qos
15 1/6 Y 000005 000005 LIM 0/124 0/123 default 0/124 0/123 default
1 1/8 Y 000000 000000 GE 0/868 0/868 default 0/868 0/868 default
20 1/8 Y 000000 000005 FFW 0/17 0/12 0/17 0/12 default
```

```
Total 3 Connections <end>
```

To display greater detail about the FFW interface, include the shelf, slot, and interface number on the command line. For example:

```
HOST-IP2100> info np conn 1 8 20
```

```
Connection Handles
```

```
Connection Handles
```

```
if sh/sl act cPort dPort type uctl udata qos dct1 ddata qos
20 1/8 Y 000000 000005 FFW 0/17 0/12 0/17 0/12 default
```

```
Encaps: AAL5-VC - MTU=1800 (50)
```

```
Control & Data Service Queues:
```

```
-----
```

```
ControlQID          262    Lport          0008
Scheduler           CBR    CosQueue       1
```

```
DataQID            264    Lport          0005
Scheduler           UBR    CosQueue       3
```

```
PDU Ids:
```

```
-----
```

```
PduID    port    vpi/vci    Tree
065665   0x0008   0/17       3072
```

000130    0x0205    0/12    3072

VLAN Configuration            : Vlan is not enabled

Packet Flow configuration: No Packet Flow is attached

Multicast Configuration    : Multicast Client

Bridge Configuration        : Bridging is not enabled

Filter Configuration        : No Filters applied

**DID List:**

Did	Type	QId	cosId
2002	CNTL_EX	263	1
2005	DATA_EX	265	1
15375	MULTICAST	266	2
55155	UNICAST	267	3

## Slot-based address assignment for PPPoE connections

Stinger IP DSLAMs support address pools for centralized definition of pools of contiguous IP addresses for assignment to incoming connections. Typically, a user's connection profile specifies an address-pool index, or the zero index to indicate that it will accept the next available address from any pool.

For increased control over the user address space, you can map an address-pool index to a specific LIM slot. When you use slot-based address assignment, all connections established on the specified slot obtain an address from the same pool. If the slot contains a GE-OLIM, all connections on RLIMs connected to that GE-OLIM obtain an address from the same pool.



**Note** Slot-based address assignment causes the system to select an address-pool index for an incoming connection from a configured `slot-vr-config` profile rather than from the user's connection profile. Once the system has selected the address-pool index, however, the rest of the system behavior for address pool capabilities, including pool chaining and so forth, still operate in the same way. For details about address pool capabilities, see the *Stinger IP Control Module Configuration Guide*.

For address assignment to occur, the Stinger system must have an address available for assignment, the `answer-defaults` profile must enable dynamic assignment, the client profile must specify dynamic assignment, and the client's PPP software must be configured to acquire its IP address dynamically.

### Overview of profile settings

Following are the profile settings, shown with default values, for slot-based address assignment:

```
[in IP-GLOBAL]
pool-selection = connection-based
[in SLOT-VR-CONFIG/{ { any-shelf any-slot 0 } "" }]
index* = { { any-shelf any-slot 0 } "" }
address-pool = 0
```

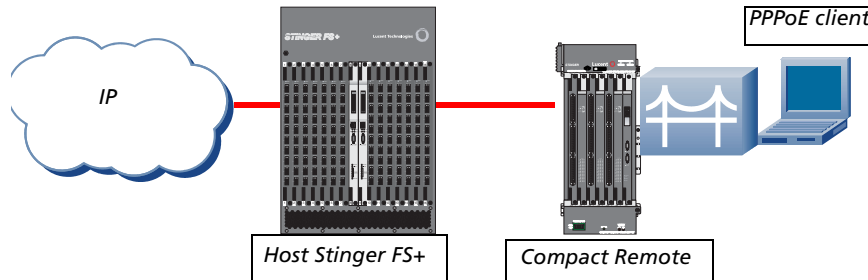
<b>Parameter</b>	<b>Setting</b>
pool-selection	<p>Specifies the method by which to determine the address-pool index to use in selecting a pool.</p> <p>connection-based    Select a pool on the basis of the address-pool setting of the subscriber's connection profile. This is the default setting, and is consistent with previous software versions.</p> <p>slot-based            Select a pool on the basis of the address-pool setting of the slot-vr-config profile for the slot on which the connection is being established. If the slot-vr-config profile is not present, address allocation fails and the connection is not established.</p>
index	<p>Specifies the physical address of a LIM or GE-OLIM slot<sup>1</sup>. Slot-based address assignment is not enabled for IMA LIMs.</p> <p>The system uses the slot-vr-config index to select an address pool for incoming connections. The index consists of the following fields:</p> <p>physical-address    The physical-address field contains three subfields:</p> <p style="padding-left: 2em;"><i>shelf slot item-number</i></p> <p style="padding-left: 2em;">The shelf must be set to 1 (the master shelf).</p> <p style="padding-left: 2em;">The slot must be set to a valid LIM slot number (from 1 to 7 and from 10 to 16).</p> <p style="padding-left: 2em;">The item-number must be set to zero.</p> <p>vrouter                The default null string represents the global router. This is the only supported value for this software version.</p>
address-pool	<p>Specifies the index of an address pool (a number from 0 to 150) to be used for connections established on the slot identified in the index parameter. Multiple slots can share an address pool by configuring multiple slot-vr-config profiles with different index values and the same address-pool.</p>

1.        The system also creates slot-vr-config profiles for OLIMs in a hosted Compact Remote ATM DSLAM. However, PPP connections are not currently supported on ATM-based OLIMs.

## Sample slot-based address configuration using the global router

Figure 5-4 shows a Stinger Compact Remote IP DSLAM. The CPE is configured as a bridge to send PPPoE packets. The WAN interface of the CPE connects to the RLIM which in turn connects to the GE-OLIM on slot-11 of the host Stinger.

Figure 5-4. Example of a PPPoE session on a DSL interface



The CPE has a configured profile used to bridge IP packets between Ethernet and WAN interfaces, in which dynamic address assignment is enabled.

On the host Stinger, the following devices are installed:

```
HOST-IP2100> show
Shelf 1 ( master ):
Controller { first-control-module } ( PRIMARY ):
      Reqd Oper Slot Type
{ shelf-1 slot-11 0 }      UP   UP   stngr-golim-card
{ shelf-2 slot-1 0 }      UP   UP   geb-gs-ads12plus-card
{ shelf-2 first-control-mod+ UP   UP   gecrt-cm
```

To configure address pools and a CPE connection that uses slot-based dynamic address assignment, follow these steps:

- 1 Configure address pools on the host. For example:

```
HOST-IP2100> read ip-global
HOST-IP2100> set pool-summary = yes
HOST-IP2100> set pool-selection = slot-based
HOST-IP2100> set pool-base-address 11 = 194.194.1.1
HOST-IP2100> set pool-base-address 12 = 194.194.2.1
HOST-IP2100> set pool-base-address 13 = 194.194.3.1
HOST-IP2100> set assign-count 11 = 254
HOST-IP2100> set assign-count 12 = 254
HOST-IP2100> set assign-count 13 = 254
HOST-IP2100> write -f
```
- 2 Configure the system-generated slot-vr-config profile for the GE-OLIM slot. Specify one of the configured address pools for use by this slot. For example:

```
HOST-IP2100> read slot-vr-config { { 1 11 0 } }
HOST-IP2100> set address-pool = 12
HOST-IP2100> write -f
```

- 3 Enable PPP authentication and dynamic address assignment in the answer-defaults profile.

```
HOST-IP2100> read answer-defaults
HOST-IP2100> set ppp-answer receive-auth-mode = any-ppp-auth
HOST-IP2100> set ppp-answer bi-directional-auth = allowed
HOST-IP2100> set ip-answer assign-address = yes
HOST-IP2100> write -f
```

- 4 Create the ATM circuit connection profile that provides the interface over which ATM frames are received from the CPE. This profile terminates on the RLIM internal port.

To determine the nailed group of a RLIM's WAN and internal ATM interfaces, use the `which` command. For example:

```
HOST-IP2100> which -n { 2 1 3 }
Nailed group corresponding to port { shelf-2 slot-1 3 } is 4003
HOST-IP2100> which -n { 2 1 49 }
Nailed group corresponding to port { shelf-2 slot-1 49 } is 4049
```

The following commands enable an ADSL interface in shelf 2, slot 1, and configure an ATM circuit from the DSL interface to the RLIM's ATM internal interface:

```
HOST-IP2100> read al-dmt { 2 1 3 }
HOST-IP2100> set enabled = yes
HOST-IP2100> write -f
HOST-IP2100> new connection
HOST-IP2100> set station = atmckt26
HOST-IP2100> set active = yes
HOST-IP2100> set mp-options enabled = no
HOST-IP2100> set atm-options vci = 37
HOST-IP2100> set atm-options nailed-group = 4003
HOST-IP2100> set atm-connect-options vci = 37
HOST-IP2100> set atm-connect-options nailed-group = 4049
HOST-IP2100> write -f
```

- 5 Configure the PPPoE connection profile used to establish PPP connectivity. For example:

```
HOST-IP2100> new connection
HOST-IP2100> set station = pppoe2
HOST-IP2100> set active = yes
HOST-IP2100> set encapsulation-protocol = ppp
HOST-IP2100> set ip-options source-if = sip0
HOST-IP2100> set telco-options call-type = off
HOST-IP2100> set ppp-options send-auth-mode = pap-ppp-auth
```

```
HOST-IP2100> set ppp-options rcv-password = ascend
HOST-IP2100> set pppoe-options pppoe = yes
HOST-IP2100> write -f
```

When the PPPoE connection is established, the following command shows that the address assigned to the remote device is in the address space assigned to address pool 12:

```
HOST-IP2100> ifmgr -d | grep pppoe2
bif slot sif u m p ifname      host-name  remote-addr      local-addr
-----
044 2:01 003 *      wan44      pppoe2          194.194.2.1/32   220.220.220.112/32
```

## IP filters for RLIM data connections

IP filters are supported in the upstream direction for PPPoE connections established on RLIMs. Except for the limitations described in the next section, IP filters are defined and applied to connections as described in the *Stinger IP Control Module Configuration Guide*.

### Current limitations on filtering RLIM connections

Currently, the following limitations apply to packet filtering on RLIM data connections:

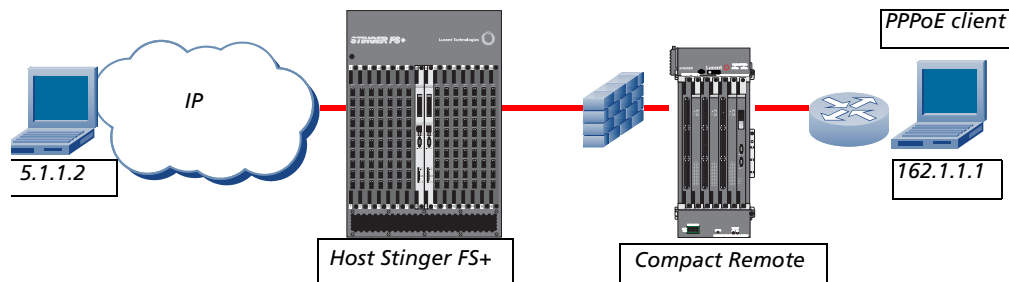
- Only input filters are supported on RLIM connections.
- Only IP filters are supported on RLIM.
- An RLIM can support a maximum of 1728 filter rules. This number is obtained by multiplying the number of connections supported on an RLIM (144) times 12.
- An RLIM connection can support a maximum of 30 filter rules.
- IP filters on RLIMs do not support the `tcp-estab` and `icmp-type` fields.
- The `protocol` field in IP filters on RLIMs supports only the following protocol types:
  - ICMP (1)
  - TCP (6)
  - UDP (17)
  - OSPF (89)
  - IGMP (2)
  - IGRP (88)
  - IGP (9)
  - GRP (7)
  - GRE (47)
  - IP (4)

Attempts to configure other protocol numbers result in a log message stating that the protocol number is not supported.

## Sample input IP filtering on an RLIM connection

Figure 5-4 shows a Stinger Compact Remote IP DSLAM with a PPPoE client with the remote address 162.1.1.1. With the configured IP filter, if the PPPoE client initiates a UDP-based session to the remote PC at 5.1.1.2, the upstream traffic on the connection is dropped.

Figure 5-5. PPPoE client with a filtered upstream traffic stream



To configure a filter and apply it to the PPPoE connection, follow these steps:

- 1 Create an IP filter. For example, the following filter specifies that a UDP traffic stream (protocol 17) from the client to the remote address 5.1.1.2 should not be forwarded. The default rule at the end of the filter definition specifies that all other IP traffic should pass:

```
HOST-IP2100> new filter
HOST-IP2100> set filter-name = ran-ip
HOST-IP2100> set input-filters 1 valid-entry = yes
HOST-IP2100> set input-filters 1 forward = no
HOST-IP2100> set input-filters 1 Type = ip-filter
HOST-IP2100> set input-filters 1 ip-filter protocol = 17
HOST-IP2100> set input-filters 1 ip-filter source-address = 162.1.1.1
HOST-IP2100> set input-filters 1 ip-filter dest-address = 5.1.1.2
HOST-IP2100> set input-filters 2 valid-entry = yes
HOST-IP2100> set input-filters 2 forward = yes
HOST-IP2100> set input-filters 2 Type = ip-filter
HOST-IP2100> write -f
```

- 2 Create the PPPoE client profile and apply the filter to it. For example:

```
HOST-IP2100> new connection
HOST-IP2100> set station = pppoe-client
HOST-IP2100> set active = yes
HOST-IP2100> set encapsulation-protocol = ppp
HOST-IP2100> set ppp-options rcv-password = !test
HOST-IP2100> set pppoe-options pppoe = yes
HOST-IP2100> set ip-options remote-address = 162.1.1.1/8
HOST-IP2100> set session-options data-filter = ran-ip
```

```
HOST-IP2100> set atm-options vci = 36
HOST-IP2100> set atm-options nailed-group = 4127
HOST-IP2100> set mp-options enabled = no
HOST-IP2100> write -f
```

## Administrative tools for hosted environments

Many of the Stinger administrative tools are described in the *Stinger Administration Guide*, and apply in a similar way to hosted and standalone environments. For example, to monitor remote shelf status on an ongoing basis, you can set alarms and traps to notify an SNMP management station when certain conditions occur on a remote shelf. See the *Stinger Administration Guide* for details about setting alarms and traps for remote shelf and GE-OLIM status.

You can use the `stats` command on an RLIM, GE-OLIM, or GE-COP to obtain statistics about traffic on the module. For details about the command, see the *Stinger Reference*. For examples of its use in a hosted environment, see “Displaying traffic statistics” on page 5-16.

In addition, the system provides the following tools specific to monitoring remote shelf status:

- `remote-shelf-stat` profiles—a read-only profile that maintains dynamic state information regarding a remote shelf. This profile is accessible by SNMP managers.
- The `remoteself` command displays information about enabled remote shelves in the hosted system.

### Viewing the `remote-shelf-stat` profile

The host system creates a `remote-shelf-stat` profile for each enabled remote shelf. 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-2 1 } 0 }
host-port-2 = { { shelf-1 any-slot 0 } 0 }
remote-shelf-oper-state = remote-shelf-link-failed
name = ""
location = ""
nailed-group-bin = 3
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 = { disabled 0 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
```

## Hosted System Management

Administrative tools for hosted environments

---

```
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.
host-port	Address of the GE-OLIM port to which the remote shelf COP GIGE-1 port is linked.
host-port-2	If the remote shelf supports two links to the host, this parameter displays the address of the second GE-OLIM port to which the remote shelf COP GIGE-2 port is linked.
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.  remote-shelf-oper-state-up      The remote shelf is operating normally.  remote-shelf-link-failed      Link failure was detected on the OC3 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.  remote-shelf-one-link-up      The remote shelf is configured to have two link to the host, but only one link has come up.  remote-shelf-host-port-mismatch      The GE-OLIM port(s) designated as host-port and host-port-2 in the remote-shelf-config profile are not designated for cr usage in the olim-port-usage profile.
name	Name of the remote shelf as configured in the remote-shelf-config profile.

<b>Parameter</b>	<b>Setting</b>
location	Location of the remote shelf as configured in the remote-shelf-config profile.
nailed-group-bin	A number from 2 to 84 that identifies how many nailed-group values are allocated to the remote shelf. The default value is equal to remote-shelf-id. For details, see “Configuring remote shelf settings” on page 4-14.
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 validation-id setting in the remote-shelf-config profile matches the validation ID specified by the remote shelf’s DIP-switch 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.
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 remoteshelf command

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

```
HOST-IP2100> help remoteshelf
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-IP2100> remoteshelf -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 Jul 19 10:08:51 2005
Last down Time:       Tue Jul 19 10:08:45 2005
```

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-IP2100> remoteshelf -s 5
Remote shelf 5 does NOT exist!
```

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

```
HOST-IP2100> remoteshelf -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-IP2100> remoteshelf
Shelf Name      AdminState OperState  host-port      up-count
  2  ZOWISAAASCR  Enabled   OPER_Down  {{ 0 0 0 } 0 }  0
```

## Displaying traffic statistics

This section describes how to use the command for statistics related to PPPoE, IPoA, and terminating AAL5 connections.

Following is the syntax of the stats command for gathering these statistics:

```
stats cmd type [port|conn-id|all]
```

The *cmd* argument specifies one of the following actions to be performed for the specified *type* on the specified port and/or connection ID:

- **enable** (Begin gathering statistics.)
- **disable** (Stop gathering statistics.)
- **traffic** (Display traffic statistics.)
- **rate** (Display traffic statistics each second. Entering the same command again causes the frequent updates to stop.)
- **error** (Display error statistics.)
- **clear** (Clear statistics.)

The *type* argument specifies the type of statistics to report, which may be combined with a specific port and/or connection ID, as shown in the following list:

- **aal5 all** (Use the *all* argument to get a list of valid connection IDs.)
- **aal5 conn-id** (Statistics for the specified AAL5 connection.)
- **atm all** (Use the *all* argument to get a list of valid UTOPIA port IDs.)
- **atm port-id** (Statistics for ATM traffic on the specified UTOPIA port.)
- **bridge slot-id port-id** (Traffic statistics for bridged connections terminating on the module. Only the *traffic* command is currently supported with this argument.)
- **mcast group-ip-addr** (Statistics for multicast traffic in the specified group. Only the *traffic* command is currently supported with this argument.)

### Opening a session to the RLIM, GE-OLIM, or GE-COP

To use the *stats* command, you must first open a session to a module. For example the following commands open and then close a session with an RLIM in shelf 9:

```
HOST-IP2100> open 9 2
geb-gs-dmt-48-9/2> quit
```

The following commands open and then close a session with the GE-COP in shelf 9:

```
HOST-IP2100> open 9 8
shelf-router-9/8> quit
```

The following commands open and then close a session with a GE-OLIM in slot 3 of the host:

```
HOST-IP2100> open 1 3
golim-1/3> quit
```

### Displaying statistics for terminating AAL5 connections

To view statistics for AAL5 traffic originating from CPE, coming into the system from DSL connections and terminating on the IP DSLAM, you first initiate statistics collection by using the *stats enable aal5* command, and then display it by using either the *stats traffic aal5* command (for traffic statistics), or the *stats error aal5* (for error statistics).

The following command enables statistics collection and obtains valid connection IDs:

```
geb-gs-dmt-48-9/2> stats enable aal5 all
Statistics collection enabled : connection 0
Statistics collection enabled : connection 16
Statistics collection enabled : connection 19
Statistics collection enabled : connection 22
```

The following command displays traffic statistics for AAL5 connection 22:

```
geb-gs-dmt-48-9/2> stats traffic aal5 22
Rx frames           : 0           Tx frames           : 125270
Aborted frames      : 0
CLP frames          : 0
```

## Hosted System Management

Administrative tools for hosted environments

---

```
L3 Iw Frames          : 125265
Rx CLP0 Cells         : 250530
Rx CLP1 Cells         : 0
```

The next command displays error statistics for the connection:

```
geb-gs-dmt-48-9/2> stats error aa15 22
ConnIDCRC      SIZE-ERR  UNDERFLOW  MAXSDU      IWUNDRUN    IW MAXMRU
22    0          0           0           0           0           0
```

The next commands display traffic statistics as they are updated each second, and then disable the continuous display:

```
geb-gs-dmt-48-9/2> stats rate aa15 22

ConId Rx Frames Tx Frames Aborts   CLP Frms  Iw Frames Rx CLP0  Rx CLP1
22    0         55         0         0         55       110       0
22    0         89         0         0         89       178       0
22    0         90         0         0         90       180       0
22    0         90         0         0         90       180       0
22    0         89         0         0         89       178       0
22    0         90         0         0         90       180       0
22    0         90         0         0         90       180       0
22    0         89         0         0         89       178       0
22    0         90         0         0         90       180       0
```

```
ConId Rx Frames Tx Frames Aborts   CLP Frms  Iw Frames Rx CLP0  Rx CLP1
22    0         90         0         0         90       180       0
22    0         89         0         0         89       178       0
```

```
geb-gs-dmt-48-9/2> stats rate aa15 22
```

The following commands display the traffic statistics before and after clearing them:

```
geb-gs-dmt-48-9/2> stats traffic aa15 22
Rx frames          : 0           Tx frames          : 180840
Aborted frames     : 0
CLP frames         : 0
L3 Iw Frames       : 180833
Rx CLP0 Cells      : 361666
Rx CLP1 Cells      : 0
```

```
geb-gs-dmt-48-9/2> stats clear aa15 22
```

statistics cleared for connection :22

```
geb-gs-dmt-48-9/2> stats traffic aa15 22
Rx frames          : 0           Tx frames          : 1652
Aborted frames     : 0
CLP frames         : 0
L3 Iw Frames       : 1652
Rx CLP0 Cells      : 3304
Rx CLP1 Cells      : 0
```

The following command disables statistics collection on connection 22:

```
geb-gs-dmt-48-9/2> stats disable aa15 22
Statistics collection disabled : connection 22
```

## Displaying statistics for ATM traffic

Statistics are always being collected on the ATM UTOPIA port (port 0), so you do not need to enable collection, and you cannot disable it. ATM traffic includes AAL5 traffic. To display statistics for ATM traffic terminating on the module via the GE-COP's ATM ASIC, use the `stats traffic atm` command (for traffic statistics), or the `stats error atm` (for error statistics). For example,

```
geb-gs-dmt-48-9/2> stats traffic atm 0
Utopia port           : 0
Rx cells              : 222451      Tx Cells              : 222450
Rx CLP1 Cells        : 0           Tx CLP1 Cells        : 0
Rx EFCI Cells        : 0           Tx EFCI Cells        : 0
Rx OAM Cells         : 0           Tx OAM Cells         : 0
Rx Rm Cells          : 0           Tx Rm Cells          : 0
Rx GFC Cells         : 0
Rx Last Unknownaddr  : 2098
```

```
geb-gs-dmt-48-9/2> stats error atm
Port Rx Err Len Rx Addr Miss
0    0      28372
```

The next commands display traffic statistics as they are updated each second, and then disable the continuous display:

```
geb-gs-dmt-48-9/2> stats rate atm 0

P# Rx Cells TxCells Rx CLP1 Tx C1P1 Rx OAM Tx OAM Rx GFC
0  180     180     0       0       0       0       0
0  178     178     0       0       0       0       0
0  180     180     0       0       0       0       0
0  179     180     0       0       0       0       0
0  179     178     0       0       0       0       0
0  180     180     0       0       0       0       0
0  178     180     0       0       0       0       0
0  180     178     0       0       0       0       0

P# Rx Cells TxCells Rx CLP1 Tx C1P1 Rx OAM Tx OAM Rx GFC
0  180     180     0       0       0       0       0
0  178     180     0       0       0       0       0
```

```
geb-gs-dmt-48-9/2> stats rate atm 0
```

The following commands display the traffic statistics before and after clearing them:

```
geb-gs-dmt-48-9/2> stats traffic atm 0
Utopia port           : 0
Rx cells              : 260307      Tx Cells              : 260312
Rx CLP1 Cells        : 0           Tx CLP1 Cells        : 0
Rx EFCI Cells        : 0           Tx EFCI Cells        : 0
Rx OAM Cells         : 0           Tx OAM Cells         : 0
Rx Rm Cells          : 0           Tx Rm Cells          : 0
Rx GFC Cells         : 0
Rx Last Unknownaddr  : 2098

geb-gs-dmt-48-9/2> stats clear atm 0
Atm statistics cleared for utopia port 0
```

```
geb-gs-dmt-48-9/2> stats traffic atm 0
Utopia port                : 0
Rx cells                   : 486           Tx Cells                : 488
Rx CLP1 Cells              : 0           Tx CLP1 Cells           : 0
Rx EFCI Cells              : 0           Tx EFCI Cells           : 0
Rx OAM Cells               : 0           Tx OAM Cells            : 0
Rx Rm Cells                : 0           Tx Rm Cells             : 0
Rx GFC Cells               : 0
Rx Last Unknownaddr       : 2098
```

## Displaying statistics for bridged connections

Bridge port statistics show the traffic statistics for bridged connections terminating on the module. Only traffic statistics are currently supported. For example:

```
geb-gs-dmt-48-9/2> stats traffic bridge 17 2
Bridge port statistics :
Rx frames : 0
Rx broadcast frames : 0
Rx multicast frames : 0
Forwarded unicast frames : 0
Forwarded broadcast frames : 0
Forwarded multicast frames : 0
Discard - VLAN filter : 0
Discard - ingress filter : 0
Discard - bridge classifier : 0
Discard - unknown source : 0
Discard - deny source address: 0
Discard - deny dest address : 0
```

## Displaying statistics for distributed multicast traffic

Multicast statistics show traffic information for a specific multicast group. To display statistics on an RLIM, specify the IP address of the group on the command line. For example:

```
geb-gs-dmt-48-9/2> stats traffic mcast 224.1.1.1
Statistics of multicast group 224.1.1.1
Mcast group flow statistics
  Forwarded packets      : 0
  Forwarded bytes        : 0
  FBP drop packets       : 0
  MTU drop packets       : 0
  TTL drop packets       : 0
  TX queue drop packets  : 0
  Denied packets         : 0
  Group filtered packets : 0
  GTP bad header         : 0
Mcast member statistics
Member IFF #25
  Buffers used          :0
  Dropped frames        :0
  Forwarded frames      :0
```

To display statistics for distributed multicast traffic on a GE-OLIM, you must specify the MBONE interface number on the `stats` command line. For example:

```
golim-1/1> stats traffic mcast -i 15
NP Multicast traffic statistics
Mcast mbone interface 15
BCM physical port ge8:
Rx L2MC : 721760
Tx L2MC : 7787
IPMC bridged : 364581
IPMC Routed : 364581
Rx IPMC dropped : 349041
Tx IPMC dropped : 0
```

To display statistics for distributed multicast traffic on the GE-COP of a remote shelf, specify the FFW interface number. For example:

```
shelf-router-9/8> stats traffic mcast -i 2
NP Multicast traffic statistics
Mcast client interface 2
BCM physical port ge1:
Rx L2MC : 0
Tx L2MC : 379381
IPMC bridged : 0
IPMC Routed : 0
Rx IPMC dropped : 0
Tx IPMC dropped : 0
```

## LACP-related diagnostics

When executed on the GE-OLIM module, the following commands provide information about link aggregation on the trunk ports:

- The `lACP` command displays information about control traffic and traffic that terminates on or originates from the Stinger host. For details, see the *Stinger Reference*.
- The `stats` command supports a new `lACP` option for displaying basic LACP distribution statistics for upstream traffic, and for clearing LACP statistics counters. For details, see the *Stinger Reference*.



---

# Stinger CR Intended Use



User line interfaces . . . . .	A-1
GE-COP interfaces . . . . .	A-1

The Stinger Compact Remote IP DSLAM unit is remote Stinger unit that extends the DSLAM capability of a host Stinger unit. It provides IP DSL connections for individual users that are too far from the Stinger host to be directly connected to it.

Users connect to the Stinger Compact Remote IP DSLAM over DSL lines supported by line interface modules (LIMs) that are installed in the unit. The Stinger Compact Remote IPDSLAM unit contains a GE-COP module that controls the operation of the unit and provides one or two Gigabit Ethernet links to the host Stinger unit. The physical interfaces on the unit provide DSL connections to digital lines, and a serial connection for configuration and administration, two Gigabit Ethernet optical ports, and an interface for monitoring the alarm status of other devices.

## User line interfaces

The 48-port ADSL IP LIM designed for use with the Stinger Compact Remote IP DSLAM allows 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)
- G.992.3 Annex L (READSL2)

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

## GE-COP interfaces

The GE-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

## Stinger CR Intended Use

### *GE-COP interfaces*

---

- No parity
- 1 stop bit
- No flow control
- A DB-9 female connector for alarm monitoring connections.
- Two SFP modules providing duplex LC optical connectors for Gigabit Ethernet.
- An RJ-45 connector for a 10/100BaseT Ethernet connection (not used on the IP DSLAM).

---

# The Host Stinger GE-OLIM



# B

Introducing the Stinger GE-OLIM . . . . .	B-1
Installing a GE-OLIM . . . . .	B-2
Interpreting GE-OLIM status lights . . . . .	B-4
GE-OLIM specifications . . . . .	B-5
Configuring a Stinger GE-OLIM. . . . .	B-6

The Gigabit Ethernet optical line interface module (GE-OLIM) is installed in a host Stinger unit and provides ten Gigabit Ethernet interfaces. Up to six of these interfaces can be used for connections to Stinger Compact Remote IP DSLAM units. Two of the remaining interfaces can be used as trunk connections for video data. Two other connections are reserved for later use.

The six Gigabit Ethernet interfaces for connections to Stinger Compact Remote IP DSLAM units can be used individually or in pairs, for single or dual connections to these units.



**Note** Other types of LIMs are not supported in a Stinger FS+ unit that is equipped with GE-OLIMs.

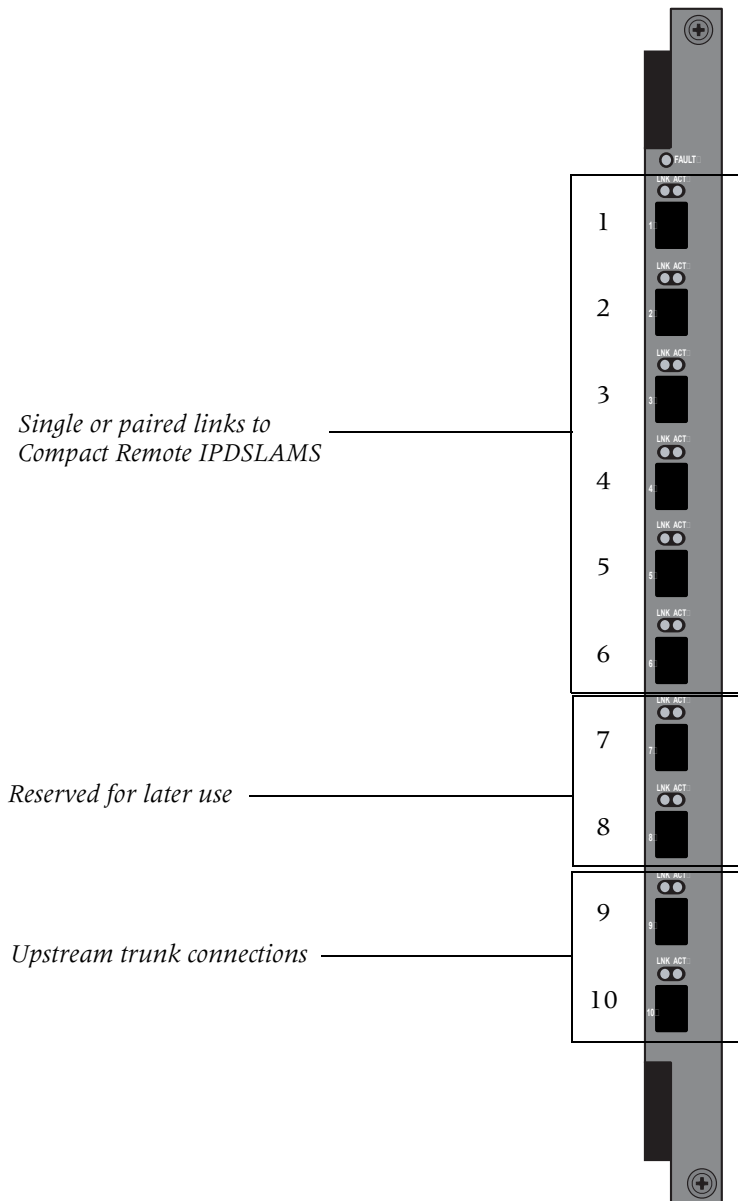
## Introducing the Stinger GE-OLIM

The interfaces on the Stinger GE-OLIM are numbered from 1 to 10. These interfaces are designed to support two different types of connections.

Interfaces 1 through 6 are designated for links to hosted Stinger Compact Remote IP DSLAM units. They can carry user data traffic and control channel data that integrates the configuration and management of hosted Stinger Compact Remote IPDSLAM units into the TAOS interface of the host Stinger unit. These hosted units are configured in the TAOS interface of the host Stinger as remote shelves. Interfaces 7 and 8 are reserved for later use. Interfaces 9 and 10 can be used to create trunk connections to upstream networks.

These interfaces and their applications are illustrated in Figure B-1.

*Figure B-1. GE-OLIM interface applications*



## Installing a GE-OLIM

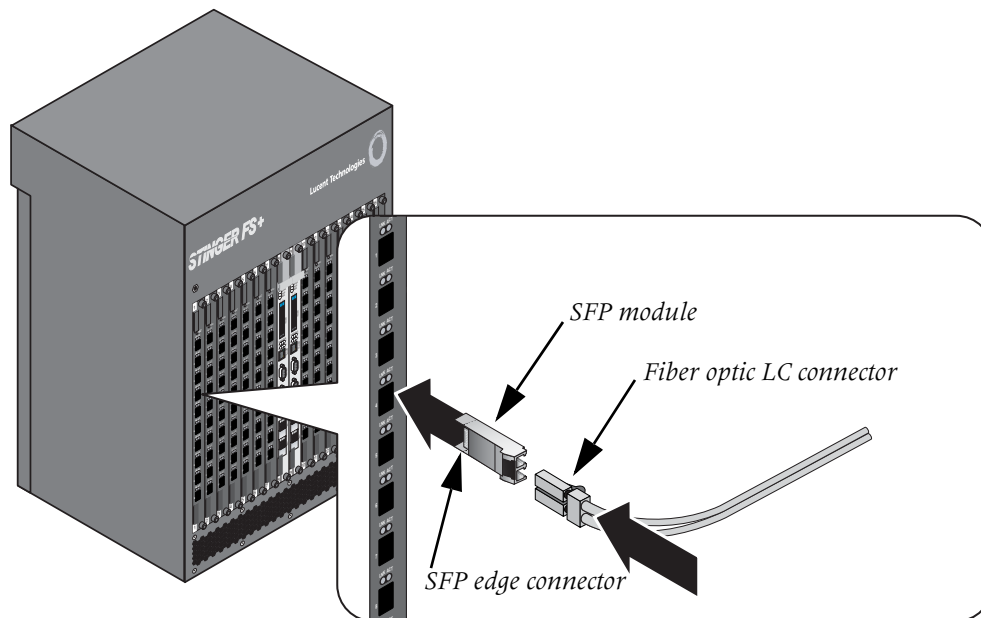
A fully populated host Stinger FS+ can support up to 42 hosted Stinger CR IP DSLAM units. The FS+ unit must be fully populated with 14 GE-OLIMs if all hosted units have dual Gigabit Ethernet links. Fewer GE-OLIMs are required if some hosted units use single Gigabit Ethernet links.

The procedure for installing a GE-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.

## Making connections to a GE-OLIM

All 10 interfaces of the GE-OLIM accept SFP modules to provide the optical connections for duplex small form factor (LC) fiber optic cables. After installing the GE-OLIM, install the SFP modules in all interfaces that are being placed into service. Then connect the fiber optic connections to the appropriate ports. This installation and connection is shown in Figure B-2.

Figure B-2. Optical connection to a GE-OLIM



Use the following procedure to install and connect the SFP module in a GE-OLIM port.

- 1 Align the SFP modules so the edge connector is visible on the left side. (See Figure B-2.)
- 2 Slide the module into the port.
- 3 Press firmly to seat the SFP module.
- 4 Align the LC connector on optical cable so the locking connector is on the right (not visible in Figure B-2).
- 5 Slide the optical connector into the SFP module until the locking connector engages with a slight click.

Long reach SFP modules can be used on all ports of the GE-OLIM. Optionally, short reach SFP modules can be used in ports 7 through 10. For additional details, see “SFP modules” on page C-21.

After installing the GE-OLIMs, SFPs, and making all necessary optical connections, check the status lights to verify the status of the card and its connections.

## Interpreting GE-OLIM status lights

The GE-OLIM has status lights that indicate the overall status of the card and each of its ten interfaces. Figure B-3 shows the Stinger OLIM.

Figure B-3. GE-OLIM status lights

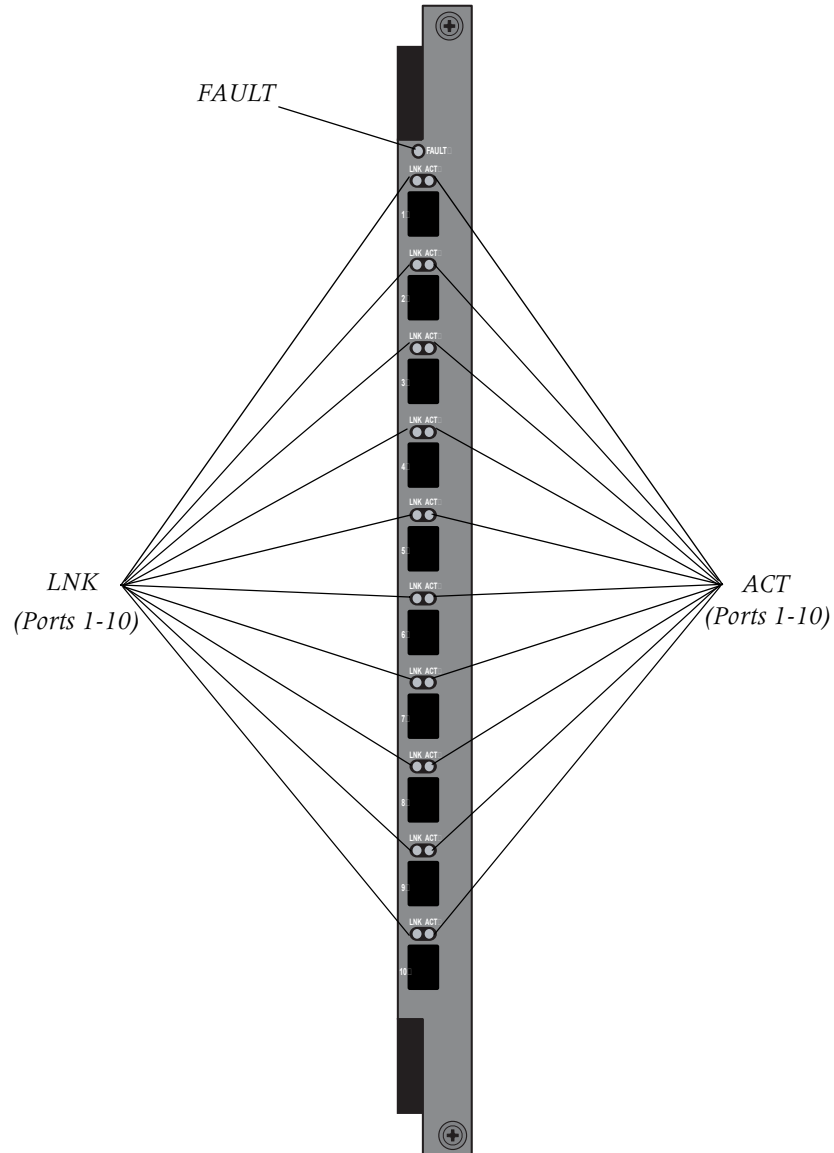


Table B-1 lists the GE-OLIM status light indications.

Table B-1. GE-OLIM status lights

Light	Color	Indication
Fault	Red	At startup—the card is performing its POST test. During operation—the card has failed.
LNK 1 through LNK 10	Green	An operational link is connected to the interface
ACT 1 through ACT 10	Green	Activity (data traffic) is present on the interface

## GE-OLIM specifications

The Stinger GE-OLIM provides up to ten Gigabit Ethernet interfaces for optical connections. Table B-2 lists Stinger GE-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 C-20.)
Physical interfaces	IEEE 802.3 optical GigaBit Ethernet <ul style="list-style-type: none"> <li>– Ports 1-6: long reach</li> <li>– Ports 7-10: long reach or short reach</li> </ul>
Maximum modules	14 GE-OLIMs supporting up to 42 active connections to Stinger Compact Remote hosted units.

Table B-2. OLIM specifications (Continued)

<b>Category</b>	<b>Specifications</b>
Minimum bend radius	3 inches (7.62 cm).

## Configuring a Stinger GE-OLIM

Each GE-OLIM supports six Gigabit Ethernet interfaces that can be used individually or in pairs to connect to Stinger Compact Remote units. For these ports, it is only necessary to identify the remote shelves that will be connected to them and the specific ports to which they will be connected. It is not necessary to configure specific IP parameters for the GE-interfaces that are connected to hosted Stinger Compact Remote IP DSLAM units. See Chapter 5 for detailed information about identifying remote shelves on the Stinger host and associating them with the optical interfaces on the OLIM.

Each GE-OLIM also supports two Gigabit Ethernet interfaces that can be used for trunk connections to a transport network. It is necessary to configure the IP-INTERFACE profiles for these interfaces. See Chapter 5, "Hosted System Management.", for details about how to configure these ports and associate them with Stinger Compact Remote IP DSLAM units.

---

# Cables and Connectors



# C

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
Power cables and connections . . . . .	C-17
Chassis door alarm connections . . . . .	C-20
Enclosure cable exit points . . . . .	C-20
Optical Gigabit Ethernet connectors . . . . .	C-21

## 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*

<b>DB-9 pin number</b>	<b>RS-232 signal name</b>	<b>Function</b>	<b>I/O</b>
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

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

DB-9 pin number	RS-232 signal name	Function	I/O
8	CTS	Clear to Send	O
9 <sup>1</sup>	RI	Ring Indicator	O

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

## Alarm input port pinouts

The ALARM port on the GE-COP 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 can be 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.

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 10	Pin 11
Alarm 3	Pin 3	Pin 4
Alarm 4	Pin 12	Pin 13
Alarm 5	Pin 5	Pin 6
Alarm 6	Pin 14	Pin 15
Alarm 7	Pin 7	Pin 8

## 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.

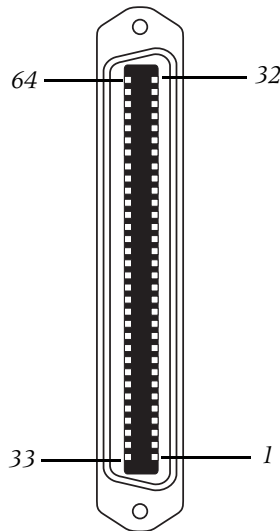
The following information details the association between the connections points of circuits on each LPM, and their location on the protection blocks. It also details the

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.

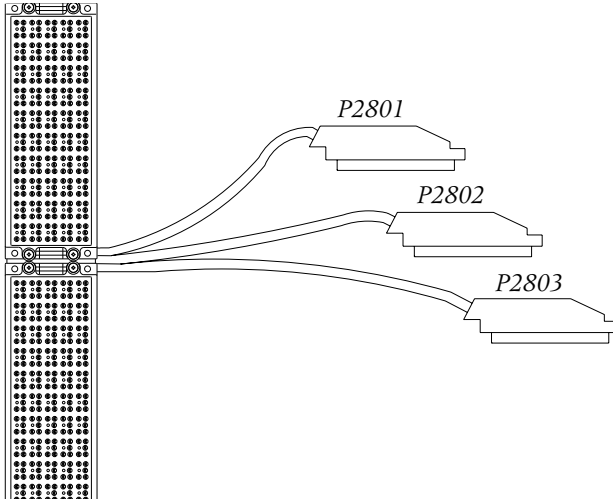
### LPM cables

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.

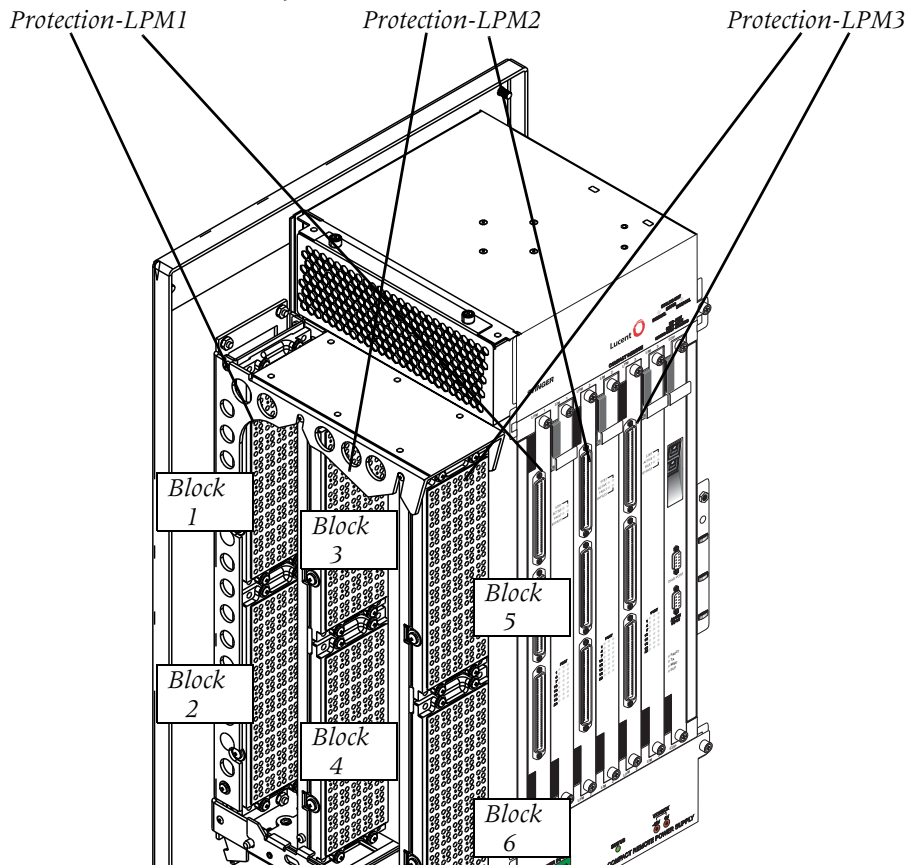
Figure C-2. Protection block cables



### 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-5.

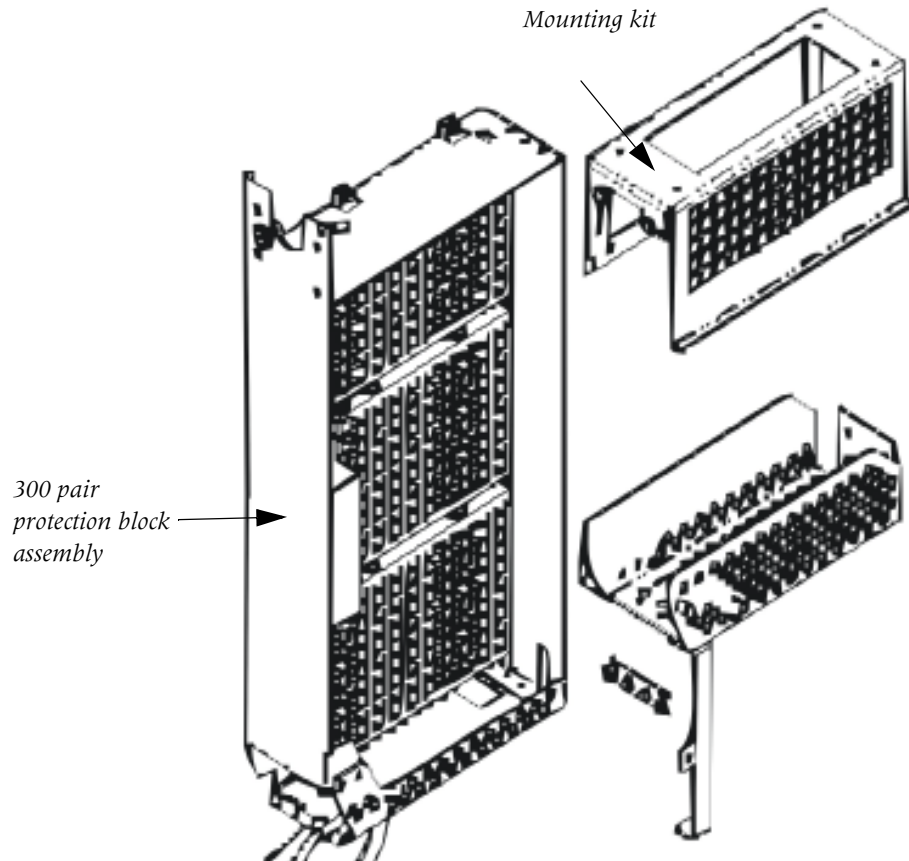
Figure C-3. LPMs and related protection blocks



**Note** The frames holding 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.

Figure C-4. Phase 2: Protection block assembly



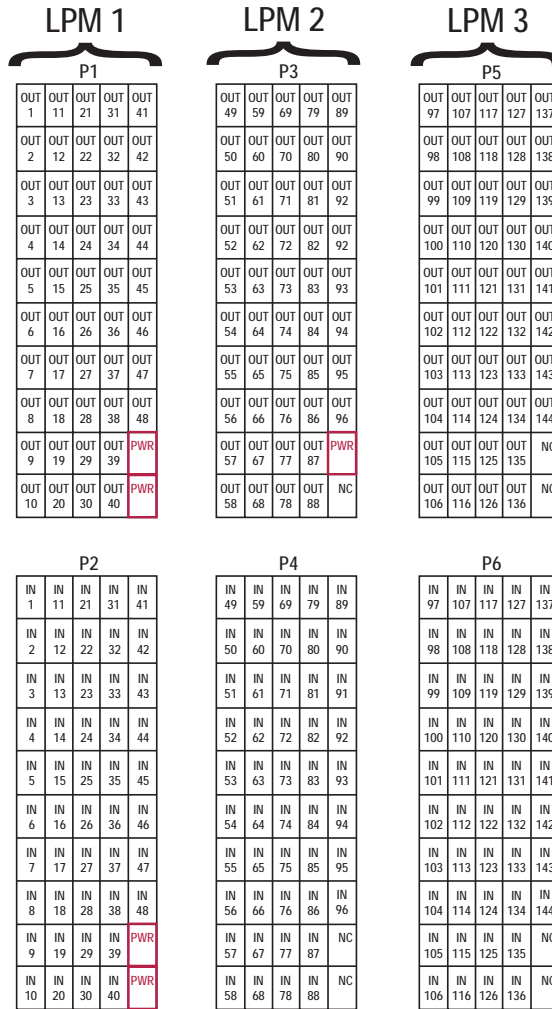
### Protection block Port numbering vs. TAOS port indexing

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-5 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-5. Protection block port assignments

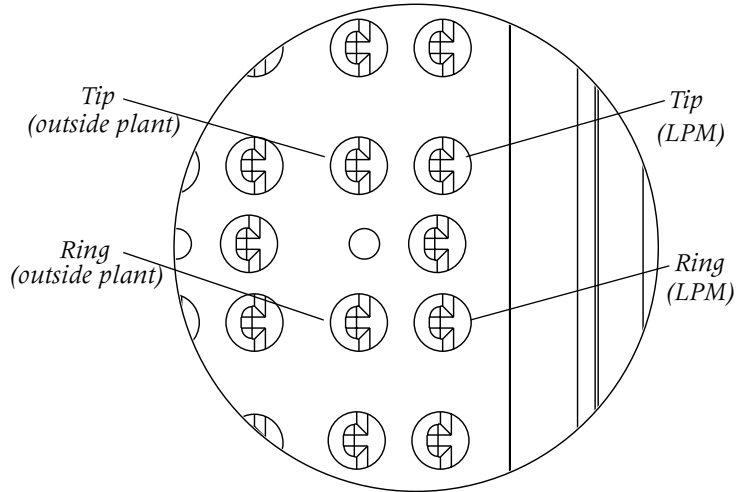


### Protector orientation details

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-6.

Figure C-6. Protection plug orientation example



For information about the type of protection elements that should be installed, see “Protection block elements” on page D-8.

### 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-5 on page C-6.

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

<b>P1 (LPM 1)</b>	<b>P3 (LPM 2)</b>	<b>P5 (LPM 3)</b>	<b>LPM connector</b>	<b>Pin No.</b>	<b>LPM 2-wire ports</b>
1T	49T	97T	P2801	33	1T(ADSL)
1R	49R	97R	P2801	1	1R(ADSL)
2T	50T	98T	P2801	34	2T(ADSL)
2R	50R	98R	P2801	2	2R(ADSL)
3T	51T	99T	P2801	35	3T(ADSL)
3R	51R	99R	P2801	3	3R(ADSL)
4T	52T	100T	P2801	36	4T(ADSL)
4R	52R	100R	P2801	4	4R(ADSL)

**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)*

<b>P1 (LPM 1)</b>	<b>P3 (LPM 2)</b>	<b>P5 (LPM 3)</b>	<b>LPM connector</b>	<b>Pin No.</b>	<b>LPM 2-wire ports</b>
5T	53T	101T	P2801	37	5T(ADSL)
5R	53R	101R	P2801	5	5R(ADSL)
6T	54T	102T	P2801	38	6T(ADSL)
6R	54R	102R	P2801	6	6R(ADSL)
7T	55T	103T	P2801	39	7T(ADSL)
7R	55R	103R	P2801	7	7R(ADSL)
8T	56T	104T	P2801	40	8T(ADSL)
8R	56R	104R	P2801	8	8R(ADSL)
9T	57T	105T	P2801	41	9T(ADSL)
9R	57R	105R	P2801	9	9R(ADSL)
10T	58T	106T	P2801	42	10T(ADSL)
10R	58R	106R	P2801	10	10R(ADSL)
11T	59T	107T	P2801	43	11T(ADSL)
11R	59R	107R	P2801	11	11R(ADSL)
12T	60T	108T	P2801	44	12T(ADSL)
12R	60R	108R	P2801	12	12R(ADSL)
13T	61T	109T	P2801	45	13T(ADSL)
13R	61R	109R	P2801	13	13R(ADSL)
14T	62T	110T	P2801	46	14T(ADSL)
14R	62R	110R	P2801	14	14R(ADSL)
15T	63T	111T	P2801	47	15T(ADSL)
15R	63R	111R	P2801	15	15R(ADSL)
16T	64T	112T	P2801	48	16T(ADSL)
16R	64R	112R	P2801	16	16R(ADSL)
17T	65T	113T	P2801	49	17T(ADSL)
17R	65R	113R	P2801	17	17R(ADSL)

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

<b>P1 (LPM 1)</b>	<b>P3 (LPM 2)</b>	<b>P5 (LPM 3)</b>	<b>LPM connector</b>	<b>Pin No.</b>	<b>LPM 2-wire ports</b>
18T	66T	114T	P2801	50	18T(ADSL)
18R	66R	114R	P2801	18	18R(ADSL)
19T	67T	115T	P2801	51	19T(ADSL)
19R	67R	115R	P2801	19	19R(ADSL)
20T	68T	116T	P2801	52	20T(ADSL)
20R	68R	116R	P2801	20	20R(ADSL)
21T	69T	117T	P2801	53	21T(ADSL)
21R	69R	117R	P2801	21	21R(ADSL)
22T	70T	118T	P2801	54	22T(ADSL)
22R	70R	118R	P2801	22	22R(ADSL)
23T	71T	119T	P2801	55	23T(ADSL)
23R	71R	119R	P2801	23	23R(ADSL)
24T	72T	120T	P2801	56	24T(ADSL)
24R	72R	120R	P2801	24	24R(ADSL)
25T	73T	121T	P2801	57	25T(ADSL)
25R	73R	121R	P2801	25	25R(ADSL)
26T	74T	122T	P2801	58	26T(ADSL)
26R	74R	122R	P2801	26	26R(ADSL)
27T	75T	123T	P2801	59	27T(ADSL)
27R	75R	123R	P2801	27	27R(ADSL)
28T	76T	124T	P2801	60	28T(ADSL)
28R	76R	124R	P2801	28	28R(ADSL)
29T	77T	125T	P2801	61	29T(ADSL)
29R	77R	125R	P2801	29	29R(ADSL)
30T	78T	126T	P2801	62	30T(ADSL)
30R	78R	126R	P2801	30	30R(ADSL)

**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)*

<b>P1 (LPM 1)</b>	<b>P3 (LPM 2)</b>	<b>P5 (LPM 3)</b>	<b>LPM connector</b>	<b>Pin No.</b>	<b>LPM 2-wire ports</b>
31T	79T	127T	P2801	63	31T(ADSL)
31R	79R	127R	P2801	31	31R(ADSL)
32T	80T	128T	P2801	64	32T(ADSL)
32R	80R	128R	P2801	32	32R(ADSL)
33T	81T	129T	P2802	33	33T(ADSL)
33R	81R	129R	P2802	1	33R(ADSL)
34T	82T	130T	P2802	34	34T(ADSL)
34R	82R	130R	P2802	2	34R(ADSL)
35T	83T	131T	P2802	35	35T(ADSL)
35R	83R	131R	P2802	3	35R(ADSL)
36T	84T	132T	P2802	36	36T(ADSL)
36R	84R	132R	P2802	4	36R(ADSL)
37T	85T	133T	P2802	37	37T(ADSL)
37R	85R	133R	P2802	5	37R(ADSL)
38T	86T	134T	P2802	38	38T(ADSL)
38R	86R	134R	P2802	6	38R(ADSL)
39T	87T	135T	P2802	39	39T(ADSL)
39R	87R	135R	P2802	7	39R(ADSL)
40T	88T	136T	P2802	40	40T(ADSL)
40R	88R	136R	P2802	8	40R(ADSL)
41T	89T	137T	P2802	41	41T(ADSL)
41R	89R	137R	P2802	9	41R(ADSL)
42T	90T	138T	P2802	42	42T(ADSL)
42R	90R	138R	P2802	10	42R(ADSL)
43T	91T	139T	P2802	43	43T(ADSL)
43R	91R	139R	P2802	11	43R(ADSL)

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

<b>P1 (LPM 1)</b>	<b>P3 (LPM 2)</b>	<b>P5 (LPM 3)</b>	<b>LPM connector</b>	<b>Pin No.</b>	<b>LPM 2-wire ports</b>
44T	92T	140T	P2802	44	44T(ADSL)
44R	92R	140R	P2802	12	44R(ADSL)
45T	93T	141T	P2802	45	45T(ADSL)
45R	93R	141R	P2802	13	45R(ADSL)
46T	94T	142T	P2802	46	46T(ADSL)
46R	94R	142R	P2802	14	46R(ADSL)
47T	95T	143T	P2802	47	47T(ADSL)
47R	95R	143R	P2802	15	47R(ADSL)
48T	96T	144T	P2802	48	48T(ADSL)
48R	96R	144R	P2802	16	48R(ADSL)
PWR	PWR	Modem T	NA	NA	
PWR	PWR	Modem R	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-5 on page C-6.

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

<b>P2 (LPM 1)</b>	<b>P4 (LPM 2)</b>	<b>P6 (LPM 3)</b>	<b>LPM connector</b>	<b>Pin No.</b>	<b>LPM connection</b>
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)
3T	51T	99T	P2803	35	3T(POTS)
3R	51R	99R	P2803	3	3R(POTS)
4T	52T	100T	P2803	36	4T(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)*

<b>P2 (LPM 1)</b>	<b>P4 (LPM 2)</b>	<b>P6 (LPM 3)</b>	<b>LPM connector</b>	<b>Pin No.</b>	<b>LPM connection</b>
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)
16T	64T	112T	P2803	48	16T(POTS)
16R	64R	112R	P2803	16	16R(POTS)
17T	65T	113T	P2803	49	17T(POTS)

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

<b>P2 (LPM 1)</b>	<b>P4 (LPM 2)</b>	<b>P6 (LPM 3)</b>	<b>LPM connector</b>	<b>Pin No.</b>	<b>LPM connection</b>
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)
29T	77T	125T	P2803	61	29T(POTS)
29R	77R	125R	P2803	29	29R(POTS)
30T	78T	126T	P2803	62	30T(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)

<b>P2 (LPM 1)</b>	<b>P4 (LPM 2)</b>	<b>P6 (LPM 3)</b>	<b>LPM connector</b>	<b>Pin No.</b>	<b>LPM connection</b>
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)
42T	90T	138T	P2802	58	42T(POTS)
42R	90R	138R	P2802	26	42R(POTS)
43T	91T	139T	P2802	59	43T(POTS)

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

<b>P2 (LPM 1)</b>	<b>P4 (LPM 2)</b>	<b>P6 (LPM 3)</b>	<b>LPM connector</b>	<b>Pin No.</b>	<b>LPM connection</b>
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	

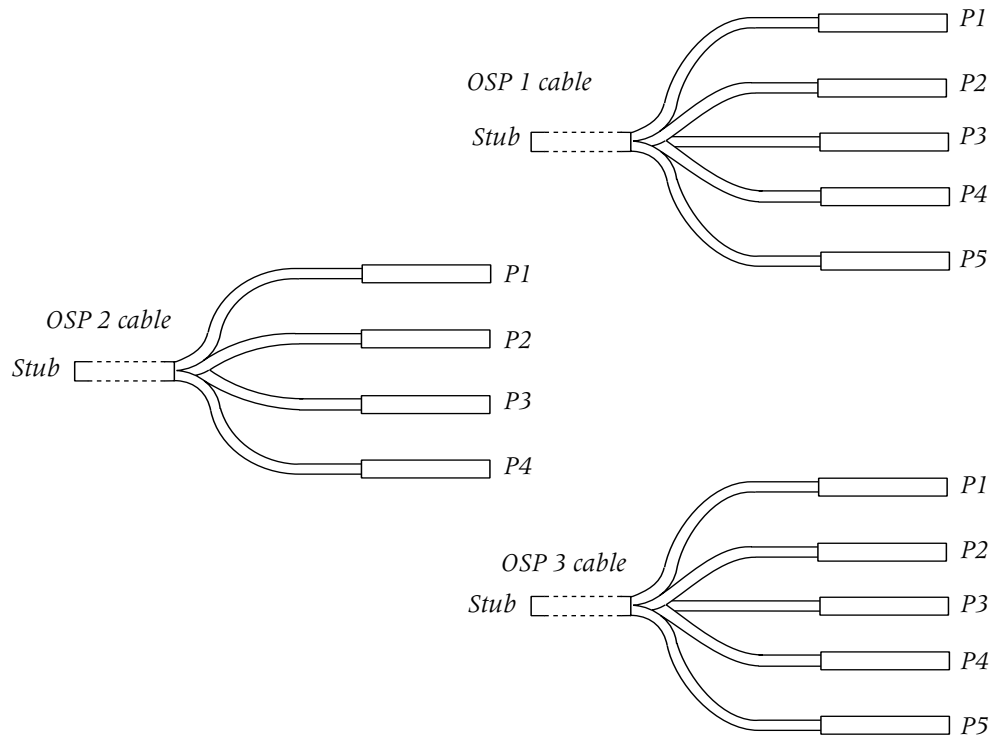
## Cable stub connections to protection blocks

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-7. 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 protections blocks.

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

<b>Cable</b>	<b>Binder</b>	<b>Pairs</b>	<b>Cable Connector</b>	<b>Protection block</b>	<b>Protection block Connector</b>	<b>LPM/ LIM No.</b>	<b>2-wire Circuits</b>
OSP 1	Blue	1-25	P1	2	OSP 3	1	POTS 1-25
OSP 1	Orange	1-23	P2	2	OSP 4	1	POTS 26-48
OSP 1	Orange	24-25	P3	4	OSP 3	2	POTS 1-2
OSP 1	Green	1-23	P3	4	OSP 3	2	POTS 3-25
OSP 1	Green	24-25	P4	4	OSP 3	2	POTS 26-27
OSP 1	Brown	1-21	P4	4	OSP 4	2	POTS 28-48

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

<b>Cable</b>	<b>Binder</b>	<b>Pairs</b>	<b>Cable Connector</b>	<b>Protection block</b>	<b>Protection block Connector</b>	<b>LPM/ LIM No.</b>	<b>2-wire Circuits</b>
OSP 1	Brown	22-25	P5	6	OSP 3 <sup>1</sup>	3	POTS 1-4
OSP 2	Blue	1-21	P1	6	OSP 3*	3	POTS 5-25
OSP 2	Blue	22-25	P2	6	OSP 4	3	POTS 26-29
OSP 2	Orange	1-19	P2	6	OSP 4	3	POTS 30-48
OSP 2	Green	1-21	P3	5	OSP 1*	3	ADSL 5-25
OSP 2	Green	22-25	P4	5	OSP 2*	3	ADSL 26-29
OSP 2	Brown	1-19	P4	5	OSP 2	3	ADSL 30-48
OSP 2	Brown	20	P4	5	OSP 2	NA	unused on IPDSLAM
OSP 3	Blue	1-25	P1	1	OSP 1	1	ADSL 1-25
OSP 3	Orange	1-23	P2	1	OSP 2	1	ADSL 26-48
OSP 3	Orange	24-25	P3	3	OSP 1	2	ADSL 1-2
OSP 3	Green	1-23	P3	3	OSP 1	2	ADSL 3-25
OSP 3	Green	24-25	P4	3	OSP 2	2	ADSL 26-27
OSP 3	Brown	1-21	P4	3	OSP 2	2	ADSL 28-48
OSP 3	Brown	22-25	P5	5	OSP 1*	3	ADSL 1-4

1. 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.

## Power cables and connections

Stinger Compact Remote IPDSLAM units are installed to utilize either  $\pm 190\text{Vdc}$  or  $-48\text{Vdc}$  power sources. Different stub ended power cables are provided to bring power into the enclosure, depending on the power source that is utilized.

### $\pm 190\text{Vdc}$ connections through the protection blocks

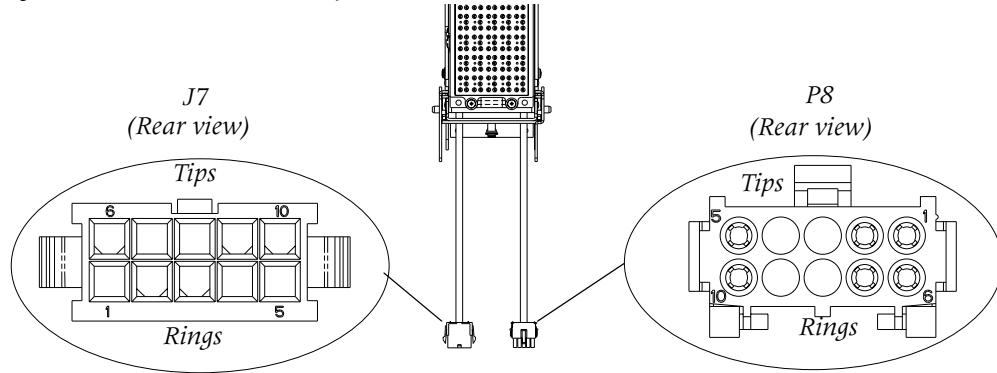
The  $\pm 190\text{Vdc}$  power is supplied from the central office over multiple pairs of telecommunications wires and connected to the stub end of the power cable. This cable is terminated inside the enclosure on a 10-pin Molex connector. Connector J7 connects to this cable, and brings the voltage 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

## Cables and Connectors

### Power cables and connections

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-8 shows the power connections through the protection blocks.

Figure C-8. Protection block power connectors



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

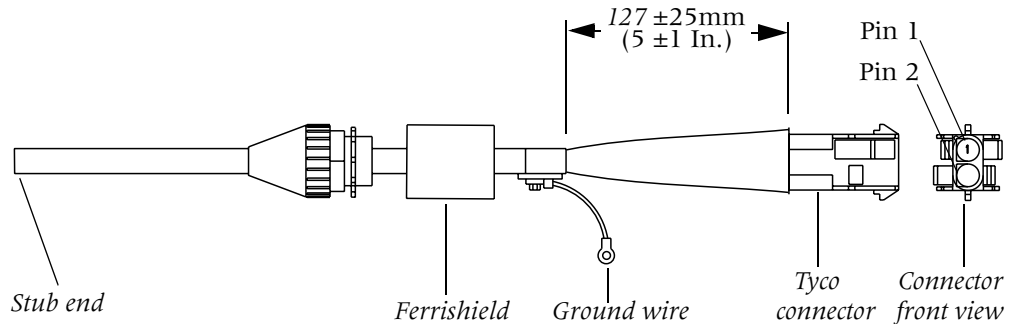
Table C-6. Wiring connection from the power stub

<b>P7 Color (power stub)</b>	<b>P7/J7 Pins</b>	<b>J7 Color</b>	<b>Protection Block</b>	<b>Protection Location</b>	<b>P8 Color</b>	<b>P8 Pins</b>
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

## -48Vdc Power connections

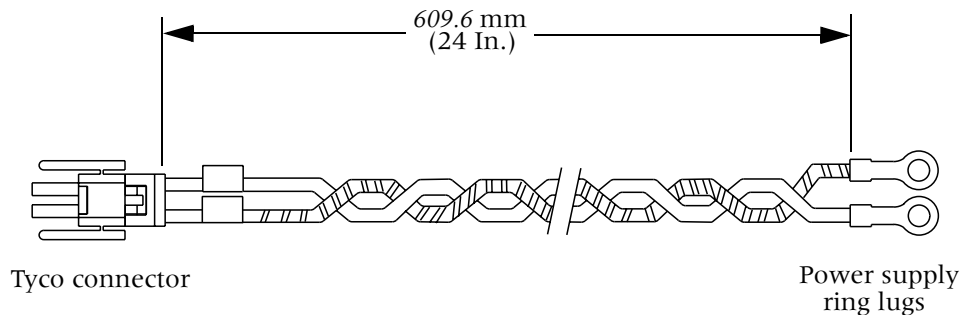
The -48Vdc power is supplied from a -48Vdc source and connected to a single pair of 19AWG wires on the stub end of the power cable. This cable is terminated inside the enclosure on a Tyco connector, as shown in Figure C-9.

Figure C-9. -48Vdc stub-ended power cable



The -48Vdc power does not pass through the protection blocks. A Tyco connector on a power supply cable connects directly to the stub-ended power cable within the enclosure and provides the ring connectors that connect directly to the -48Vdc power supply of the Stinger Compact Remote unit. The -48Vdc power supply cable is shown in Figure C-10.

Figure C-10. -48Vdc power supply cable



Connector J7 connects to this cable, and brings the voltage to the outside plant tips and rings of five connection points on the protection blocks.

Table C-7 describes the pin and wire assignments for -48Vdc power connections to the power supply.

Table C-7. Wire and pin assignments for -48Vdc cabling

Wire/Connector	0Vdc	-48Vdc
Stub-ended cable	White/Blue	Blue/White
Tyco connectors	Pin 2	Pin 1
Ring-lug wires	Black	Red

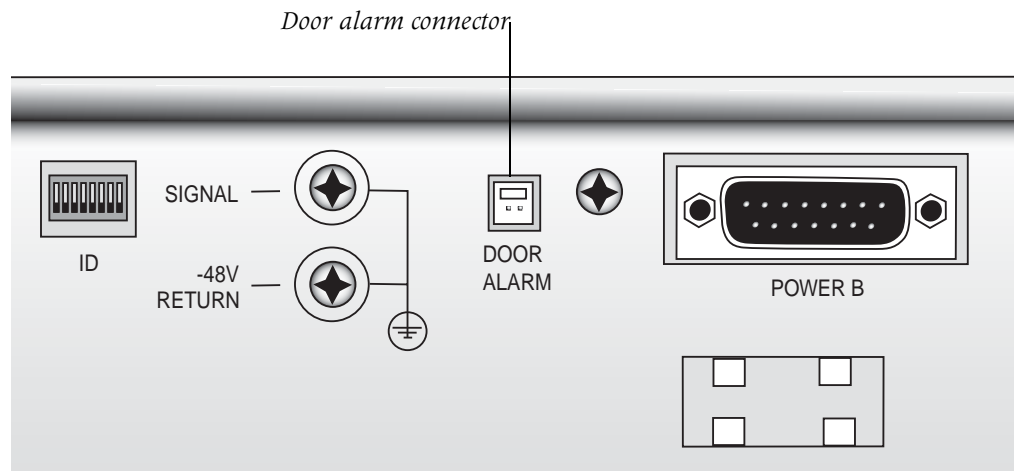
## Chassis door alarm connections

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

### Door alarm for hosted operation

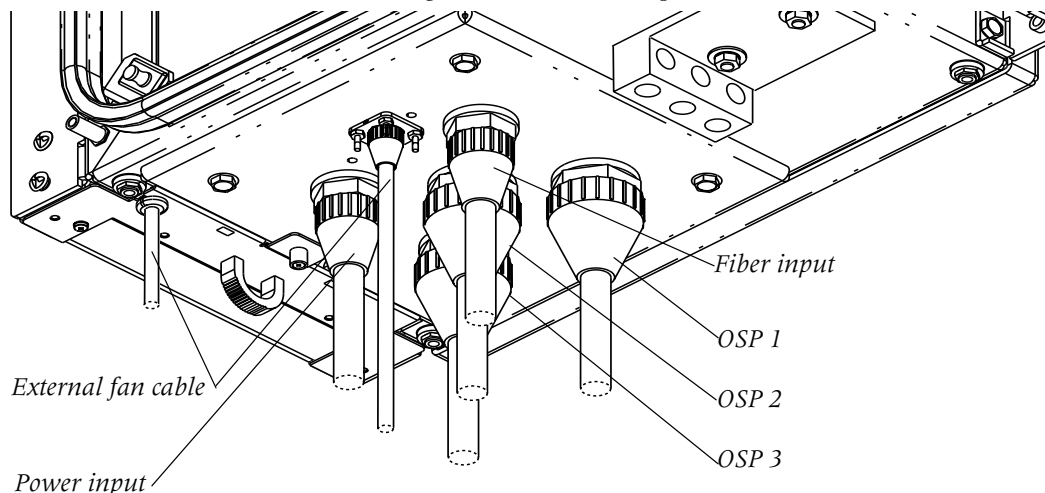
The door alarm switch is located in the lower left corner of the Stinger CR enclosure door opening. (See Figure 2-3 on page 2-5.) On Stinger Compact Remote IPDSLAM units, the black and white wires from this switch connect to a pair of pins on the Stinger Compact Remote chassis, behind the cooling unit. The location of this connector is shown Figure C-11 on page C-20

Figure C-11. Door alarm connectors on the Stinger CR chassis



## Enclosure cable exit points

All cables and fiber that connect to the Stinger CR enter the enclosure through the bottom of the unit. The following illustration identify each of these cables.



## Optical Gigabit Ethernet connectors

The Stinger Compact Remote unit and the host Stinger unit both use SFP modules for optical Gigabit Ethernet connections.

### SFP modules



**Caution** Follow all laser safety instructions in this manual when installing, connecting, or replacing SFP modules in Stinger units. (See “Laser safety” on page D-5.)

Several modules used in Stinger units use small form-factor pluggable (SFP) modules to provide Gigabit Ethernet interfaces. Table C-8 shows the application, reach, and product identification for these SFP modules.

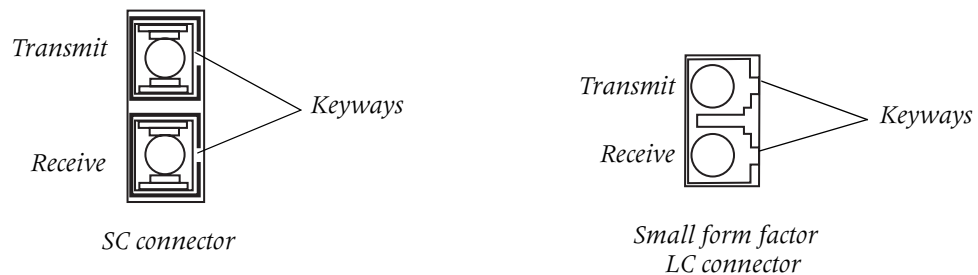
Table C-8. SFP module information

Product code	Lucent comcode	Reach (approx.)	Stinger modules supported
STGR-SFP-SX	300440252	550m	STGR-CM-IP2000-F STGR-OLIM-GE-10 (ports 7-10)
STGR-SFP-LX	300440237	10km	STGR-CM-IP2000-F STGR-OLIM-GE-10 (all ports) STGR-CR-COP-GE
STGR-SFP-ELX	408935229	>20km	STGR-CM-IP2000-F STGR-CM-IP2100-F

## Optical connectors

Most Stinger modules, including optical connectors for both types of COP modules in Compact Remote IPDSLAM units, both types of OLIMs, and all other optical modules in Stinger host units, except the OC3-ATM trunk module, use LC small form factor connectors. Stinger OC3-ATM trunk modules use SC optical connectors. The keyways and the transmit/receive orientation of these connectors are illustrated in Figure C-12.

Figure C-12. Optical Connectors





---

# Safety-Related Electrical, Physical, and Environmental Information



D

Safety Instructions . . . . .	D-1
Electrical and electronic information . . . . .	D-7
Protection block elements . . . . .	D-8
Laser safety . . . . .	D-9
Safety certifications . . . . .	D-12
Physical specifications . . . . .	D-12
Site specifications . . . . .	D-13
Weight and lifting requirements . . . . .	D-13

See the *Edge Access and Broadband Access Safety and Compliance Guide* for additional 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*.

## Safety Instructions

### Stinger CR, ±190 V dc Models Important Safety Instructions



### Stinger CR, ±190 V dc Models Important Safety Instructions



**Caution** Please read all operating and maintenance servicing instructions in the literature accompanying this product.

When installing this product, basic safety precautions should always be followed to reduce the risk of fire, electric shock, and injury to persons, including the following:

- 1 Follow all instructions provided with this unit.
- 2 Installation and maintenance procedures must be followed and performed only by trained personnel.

## Safety-Related Electrical, Physical, and Environmental Information

### Safety Instructions

---

- 3 Use caution when installing or modifying telecommunication lines.
- 4 This product should be serviced by qualified personnel, or taken to a qualified repair center for service or repair.
- 5 The product should only be installed by a qualified electrician and connected only to  $\pm 190$  Vdc Remote Feed Telecommunications (RFT-V) type power supply.
- 6 Never install this product, or telecommunication connections in wet locations.
- 7 Never install telecommunication wiring during a lightning storm.
- 8 Never touch un-insulated telecommunication wires or terminals unless the telecommunication line has been disconnected at the interface.



- 9 **Warning:** To avoid shock or injury, never touch un-insulated wiring or terminals carrying direct current or ringing current, or leave this wiring exposed.



- 10 **Warning:** To avoid shock and injury to service personnel, or electrical fire, protect and tape wires and terminals carrying direct current or ringing current.

- 11 To avoid overheating, never block the ventilation slots or openings in this unit.
- 12 To avoid electrical fires, all fuses used in this product must be replaced with fuses of the same type and rating.
- 13 The installation must have an independent frame ground drop.



- 14 **Caution:** This unit has up to five (5)  $\pm 190$  Vdc (RFT-V) input power feeders. To reduce the risk of injury, all power feeders must be disconnected to completely remove power from the system.



- 15 **Warning:** Install only equipment identified in the applicable Lucent Technologies Manual(s). Use of other equipment may result in improper connections of circuitry which could cause fire or injury.



- 16 **Warning:** Use this product only with telephone wiring protected by an AVAYA 3B or 3C Primary protector. See instruction manual.



- 17 **Warning:** Invisible laser radiation may be present when the enclosure is open and a fiber optic cable is disconnected. Avoid Direct Exposure to Beam.

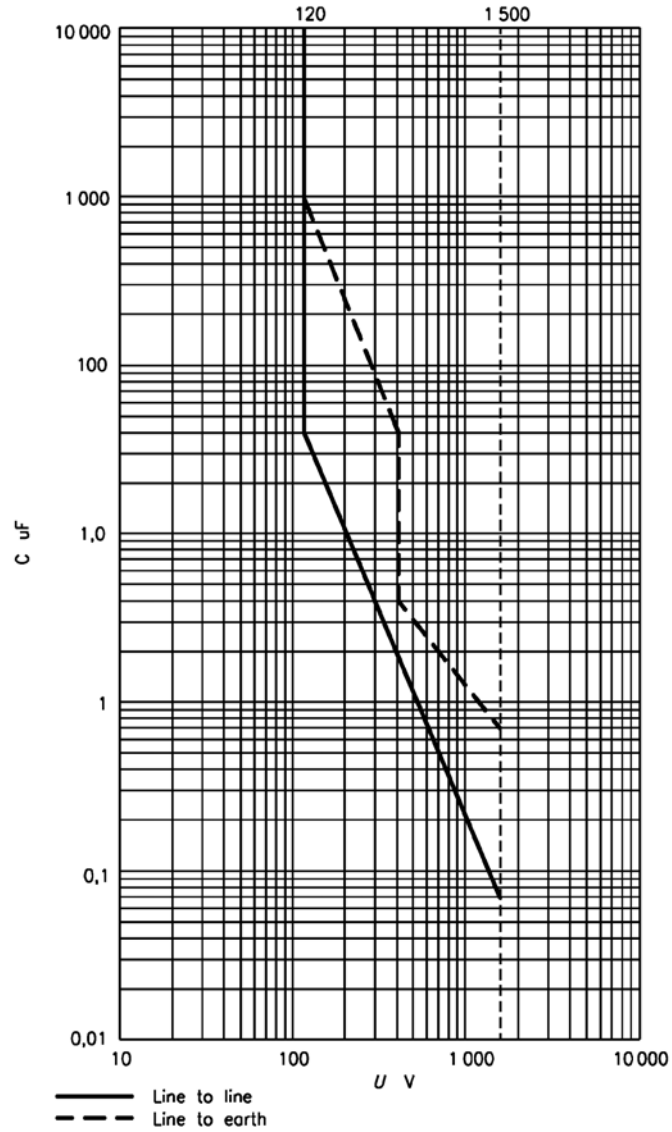


- 18 **Warning:** Un-terminated optical connections may emit laser radiation. Do Not View With Optical Instruments.

- 19 The effective capacitance of this product is 0.27  $\mu$ F between the connection points for the conductors of the telecommunication network and 3.9 nF between the connection point for one conductor of the telecommunication network and earth.
- 20 At the time of installation, you must check that all circuits being connected are RFT-V or RFT-C circuits.
- 21 At the time of installation the voltage rating of the wiring for the telecommunication Network must be checked to determine if it is adequate for the normal RFT-V circuit Voltage, together with superimposed transients.

- 22 At the time of installation a system assessment must be carried out to ensure that the effective capacitance of the total system, including the capacitance of the product does not exceed the values specified in UL60950-21, see Figure D-1.

Figure D-1. UL60950-21



## Stinger CR, -48 V dc Models Important Safety Instructions



**Caution** Please read all operating and maintenance servicing instructions in the literature accompanying this product.

When installing this product, basic safety precautions should always be followed to reduce the risk of fire, electric shock, and injury to persons, including the following:

- 1 Follow all instructions provided with this unit.
- 2 Installation and maintenance procedures must be followed and performed only by trained personnel.
- 3 Be cautious when installing or modifying telecommunication lines.
- 4 This product should be serviced by qualified personnel, or taken to a qualified repair center for service or repair.
- 5 Never install this product, or telecommunication connections in wet locations.
- 6 Never install telecommunication wiring during a lightning storm.
- 7 Never touch un-insulated telecommunication wires or terminals unless the telecommunication line has been disconnected at the interface.



- 8 **Warning:** To avoid shock or injury, never touch un-insulated wiring or terminals carrying direct current or ringing current, or leave this wiring exposed.



- 9 **Warning:** To avoid shock and injury to service personnel, or electrical fire, protect and tape wires and terminals carrying direct current or ringing current.
- 10 To avoid overheating, never block the ventilation slots or openings in this unit.
- 11 To avoid electrical fires, all fuses used in this product must be replaced with fuses of the same type and rating.
- 12 The installation must have an independent frame ground drop.



- 13 **Caution:** Install only equipment identified in the applicable Lucent Technologies Manual(s). Use of other equipment may result in improper connections of circuitry, which could cause fire or injury.



- 14 **Warning:** Use this product only with telephone wiring protected by an AVAYA 3B or 3C Primary protector. See instruction manual.



- 15 **Warning:** Invisible laser radiation may be present when the enclosure is open and a fiber optic cable is disconnected. Avoid Direct Exposure to Beam.



- 16 **Warning:** Un-terminated optical connections may emit laser radiation. Do Not View With Optical Instruments.

## Stinger CR, (Indoor Cabinet) -48 V dc Models Important Safety Instructions



**Caution** Please read all operating and maintenance servicing instructions in the literature accompanying this product.

When installing this product, basic safety precautions should always be followed to reduce the risk of fire, electric shock, and injury to persons, including the following:

- 1 **Warning:** This equipment is to be installed only in Restricted Access Areas.
- 2 Follow all instructions provided with this unit.
- 3 Installation and maintenance procedures must be followed and performed only by trained personnel.
- 4 Be cautious caution when installing or modifying telecommunication lines.
- 5 This product should be serviced by qualified personnel, or taken to a qualified repair center for service or repair.
- 6 Never install this product, or telecommunication connections in wet locations.
- 7 Never install telecommunication wiring during a lightning storm.
- 8 Never touch un-insulated telecommunication wires or terminals unless the telecommunication line has been disconnected at the interface.



- 9 **Warning:** To avoid shock or injury, never touch un-insulated wiring or terminals carrying direct current or ringing current, or leave this wiring exposed.



- 10 **Warning:** To avoid shock and injury to service personnel, or electrical fire, protect and tape wires and terminals carrying direct current or ringing current.
- 11 To avoid overheating, never block the ventilation slots or openings in this unit.
- 12 To avoid electrical fires, all fuses used in this product must be replaced with fuses of the same type and rating.
- 13 The installation must have an independent frame ground drop.



- 14 **Caution:** Install only equipment identified in the applicable Lucent Technologies Manual(s). Use of other equipment may result in improper connections of circuitry, which could cause fire or injury.



- 15 **Warning:** Use this product only with telephone wiring protected by an AVAYA 3B or 3C Primary protector. See instruction manual.



- 16 **Warning:** Invisible laser radiation may be present when the enclosure is open and a fiber optic cable is disconnected. Avoid Direct Exposure to Beam.



- 17 **Warning:** Un-terminated optical connections may emit laser radiation. Do Not View With Optical Instruments.



- 18 **Caution:** This unit has up to five (2) -48 V dc input power feeders. To reduce the risk of injury, all power feeders must be disconnected to completely remove power from the system.



- 19 Caution:** This equipment is designed to permit the connection of the earthed conductor of d.c. supply circuit to the earthing conductor at the equipment. If this connection is made, all of the following conditions must be met:
- The equipment shall be connected directly to the d.c. supply system earthing electrode conductor or to a bonding jumper from an earthing terminal bar or bus to which the d.c. supply system earthing electrode conductor is connected.
  - This equipment must be located in the same immediate area (such as, adjacent cabinets) as any other equipment that has a connection between the earthed conductor of the same d.c. supply circuit and the earthing conductor, and also the point of earthing of the d.c. system. The d.c. system should not be earthed elsewhere.
  - The d.c. supply source must be located within the same premises as this equipment.
  - Switching or disconnecting devices should not be in the earthed circuit conductor between the d.c. source and the point of connection of the earthing electrode conductor.

## 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*

<b>Application</b>	<b>Specification</b>
Input voltage	$\pm 190\text{Vdc}$ (must be from an Argus CSM36-BC power supply) or Native $-48\text{Vdc}$
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:

*Table D-2. Approved Plug-in 5-pin Protectors*

Item	5-Pin Position	Supplier	Supplier Part Number	Approval		
				Phase 1	Phase 1 (VDSL-2) retrofit	Phase 3 (VDSL-2)
1	Signal (Tip/Ring Pairs)	Commscope (formerly Avaya)	3C1S	APPROVED, see note C	NOT approved, see note D	
2		Corning	303M-09G1T0	NOT approved, see note F		APPROVED, see note C
3		Commscope (formerly Avaya)	3B1EW	APPROVED, see note C		
4	Power Feeds	Commscope (formerly Avaya)	3B1EW	APPROVED, see note C		
5		Corning	303M11A7T0	NOT approved, see note F		NOT approved, see note E
6		Corning	303M-09G3T0	NOT approved, see note F		APPROVED, see note C

- A. 288 signal protectors are required per system.
- B. 5 power protectors are required per system.
- C. This protector is APPROVED for that particular application on the basis of Lucent testing.
- D. NOT approved for that particular application because it lowers reach of the VDSL-2.
- E. NOT approved for that particular application because it failed high temperature testing.
- F. NOT approved for that particular application because it is too tall.

## 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-3. 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)
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:

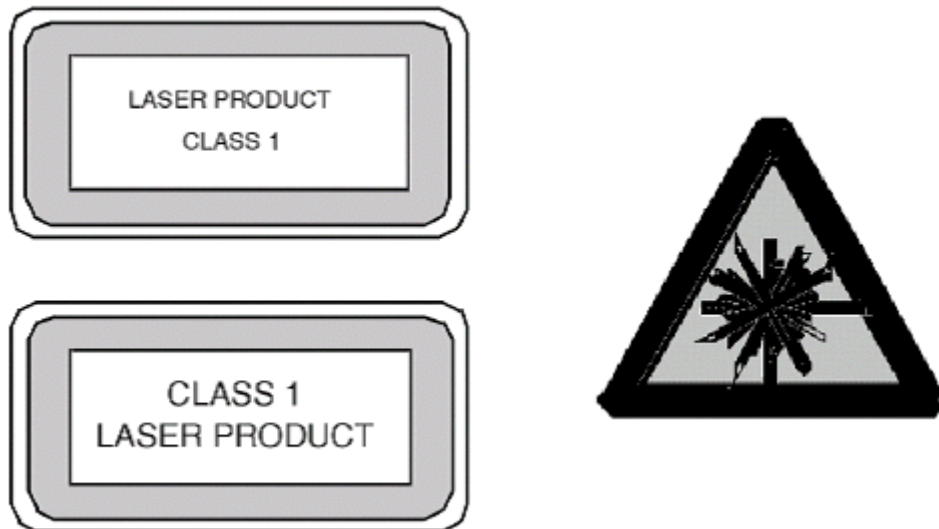
- Do not look into the end of an exposed fiber or an open connector when the optical source is on. (Even though viewing Class 1 lasers at distances greater than 250mm (10 inches) will normally not cause eye injury.)
- Only authorized technicians, who have satisfactorily completed an approved training 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-2. 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-4 describes the Stinger CR physical specifications.

*Table D-4. Stinger CR physical specifications*

<b>Specification</b>	<b>Description</b>
ATM standards	ATM Forum UNI (Version 3.0 and Version 3.1), ATM Forum Interim Interswitch Signaling Protocol (IISP)
WAN interfaces	Gigabit Ethernet
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 <sup>1</sup>	Height (enclosure only): 30.1 inches (76.5cm) Height (overall): 40.5 inches (102.9cm) Depth (enclosure only): hosted units—11.5 inches (29.2cm) stand-alone units—12 inches (30.5cm) Depth (overall): 12.6 inches (32cm) Width (enclosure only): 16.2 inches (41.2cm) Width (overall): 20.5 inches (52cm)
Unit weight	121 pounds (54.885kg) maximum (with fans, power supply, protection blocks, and cables)

1. 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-5 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-5. 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 215 pounds (97kg). For ease of installation the unit should be installed without its modular components in place.



---

# Replacing a Door Assembly on a Deployed Stinger CR



E

Replacing a compact remote door . . . . .	E-1
Before you begin . . . . .	E-1
Replacing the damaged door . . . . .	E-1

## Replacing a compact remote door

It is necessary to replace the Compact remote door if the door is damaged. This is done to prevent the excessive moisture that might enter the cabinet and damage the Stinger Compact Remote components.

You can also decide to replace the a door for non-functional reasons.

### Before you begin

Before proceeding to replace the damaged door, consider the following:

- You can replace the door when the Stinger Compact remote system is functional.
- Before replacing the damaged door, check the condition of gasket on the perimeter flange of enclosure for any damage. If you identify that the gasket is also affected, then you must replace it. Make sure that there is no other damage that can breach the environmental seal after replacing the gasket.

For details on replacing door gasket, refer *Inspecting and replacing the door gasket* section.

### Replacing the damaged door

Use the following procedure to replace the damaged door:

- 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 Unscrew knurled knob on fiber tray and pull the tray out. Now swing it down to gain access to the lower domed (“acorn”) nuts.
- 3 Loosen the domed nuts by using a metric standard “open-end” wrench on the 13 mm flats of the hexagonal portion of the domed nuts.

The domed nuts are located alongside the inner right wall of the enclosure (two at each of the two hinge locations). Refer Figure 1-1 “Replacing a door assembly on a deployed Stinger CR” on page E-2.

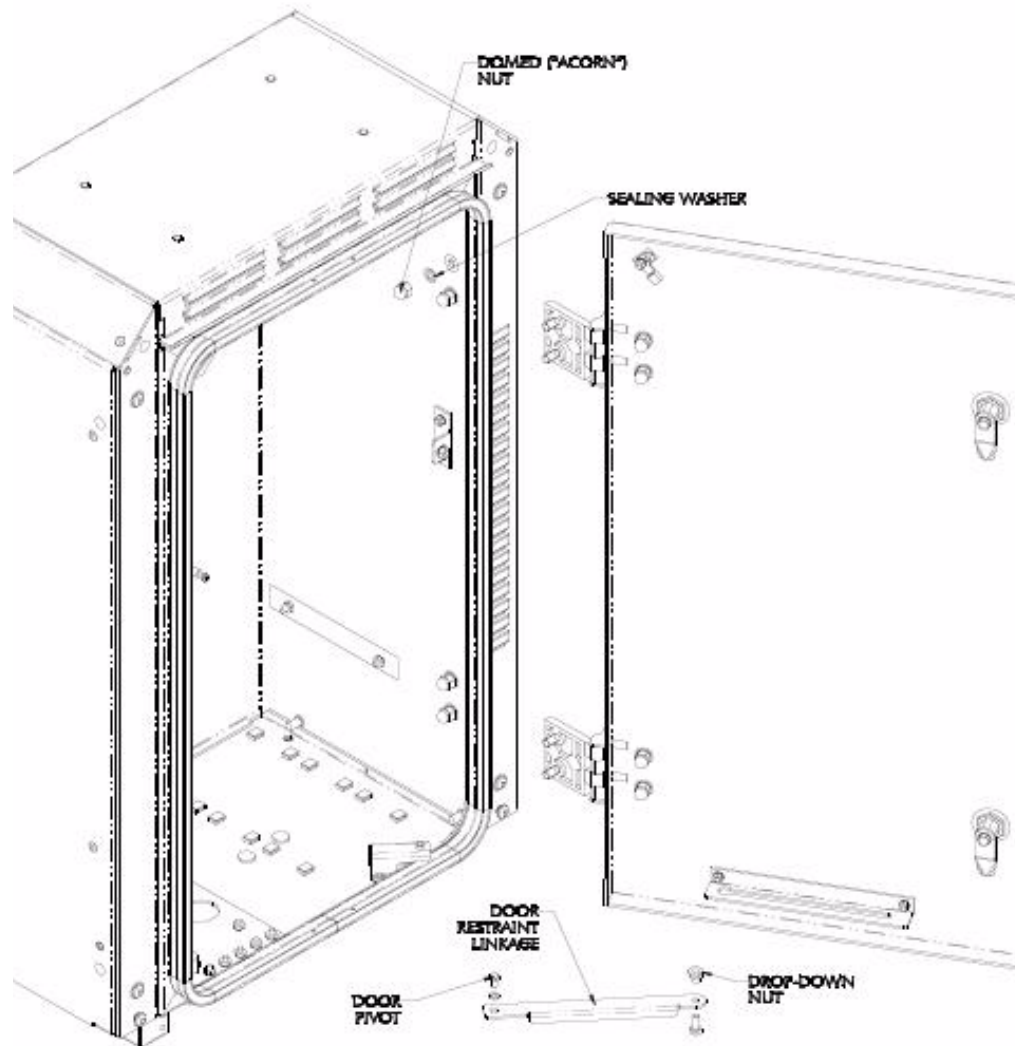
## Replacing a Door Assembly on a Deployed Stinger CR

Replacing a compact remote door

---



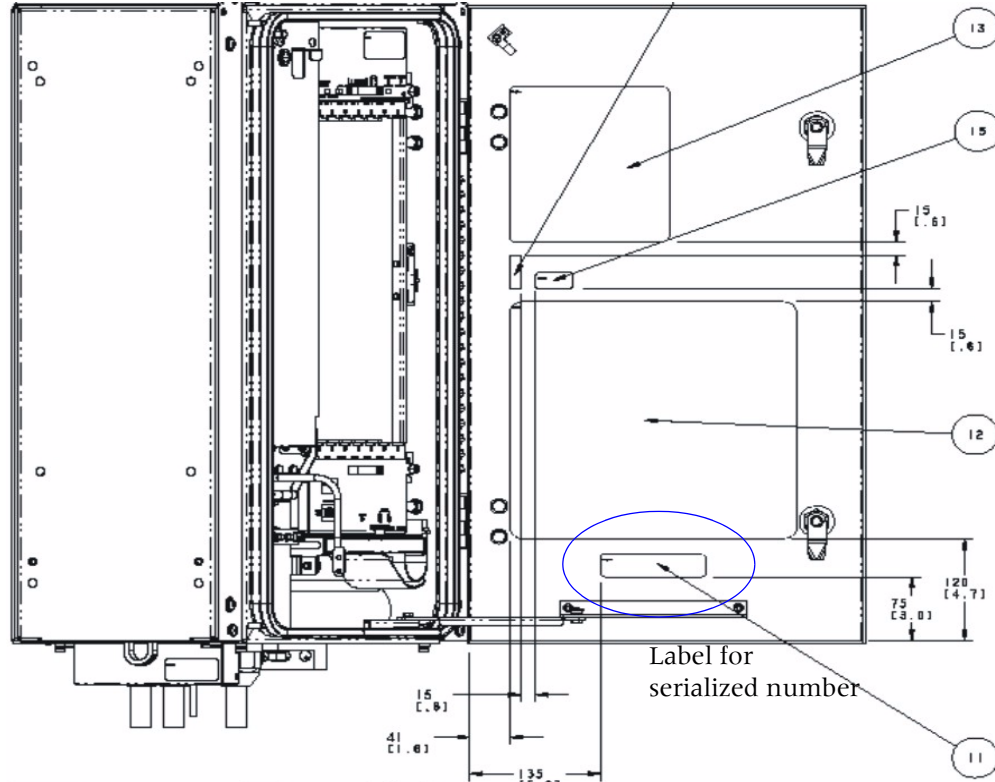
Figure E-1. Replacing a door assembly on a deployed Stinger CR



- 4 On the door restraint linkage, loosen the bolt by holding the "drop down" nut which is secured by that bolt. Retain both of these and associated pieces for the re-assembly phase.
- 5 Remove the ground cable connection at the upper left hand corner. There is a single nut (M5 thread) there.
- 6 Slowly remove the old door assembly.

- 7 Note the serialized label on the old door. This is the actual serial number for the entire system. This serialized label is located next to the corresponding printed barcode.

Figure E-2. Label for serialized number



- 8 Legibly write the serialized number on the corresponding blank portion of the label on the new door. This sustains the continued traceability of the system.

Figure E-3. Blank label portion on the new door



Use a fine point marker with indelible black ink such as the Sharpie industrial pen to write the serialized number. For details, refer to [www.sharpie.com](http://www.sharpie.com).

- 9 Align the new replacement door assembly carefully and connect the door restraint linkage by tightening the bolt holding the drop-down nut.
- 10 Reconnect the ground cable at the upper left hand corner.
- 11 Replace all the four sealing washers with the new ones in the original position and tighten all the four domed nuts alongside the inner right wall of the enclosure.



**Note** The domed nuts compress the special o-ring sealing washers (quantity 4) inside the enclosure. These sealing washers are also replaced with the new washers included in the door assembly kit. These sealing washers must be installed in order to prevent the damage on watertight seal.

## Replacing a Door Assembly on a Deployed Stinger CR

Replacing a compact remote door

---

### Torque requirement

In a factory setting, calibrated torque wrenches are used to install threaded fasteners as shown below:

Table E-1. Compact Remote Door Torque Requirements

Thread Size	Torque Requirement				Fastener Description
	SI Unit		US Customary Unit		
	(Nm)	(Nm)	(in X lbs)	(in Xlbs)	
M5 thread	4.0	+/- 0.6	35	+/- 5	Door pivot Ground cable stud
M6 thread	7	+/- 1	62	+/- 9	Drop down nut

**Note** In the absence of a calibrated torque wrench, you can use the “turn of the nut” method. For details, refer “Retrofit without torque wrenches” on page F-5.

12 Push the fiber tray back in to the position and tighten the knurled knob.

This completes the procedure to replace the damaged door.

---

# Upgrading Stinger Compact Remote



**F**

Retrofit Kit .....	F-1
Torque Requirement .....	F-4
Using Retrofit to Upgrade Compact Remote .....	F-5

## Retrofit Kit

Retrofit Kit lets you upgrade the Phase 1 version of Stinger Compact Remote (CR) system to support VDSL-2 Circuit Pack functionality.

The customer ordering code for Retrofit kit is 109603779.

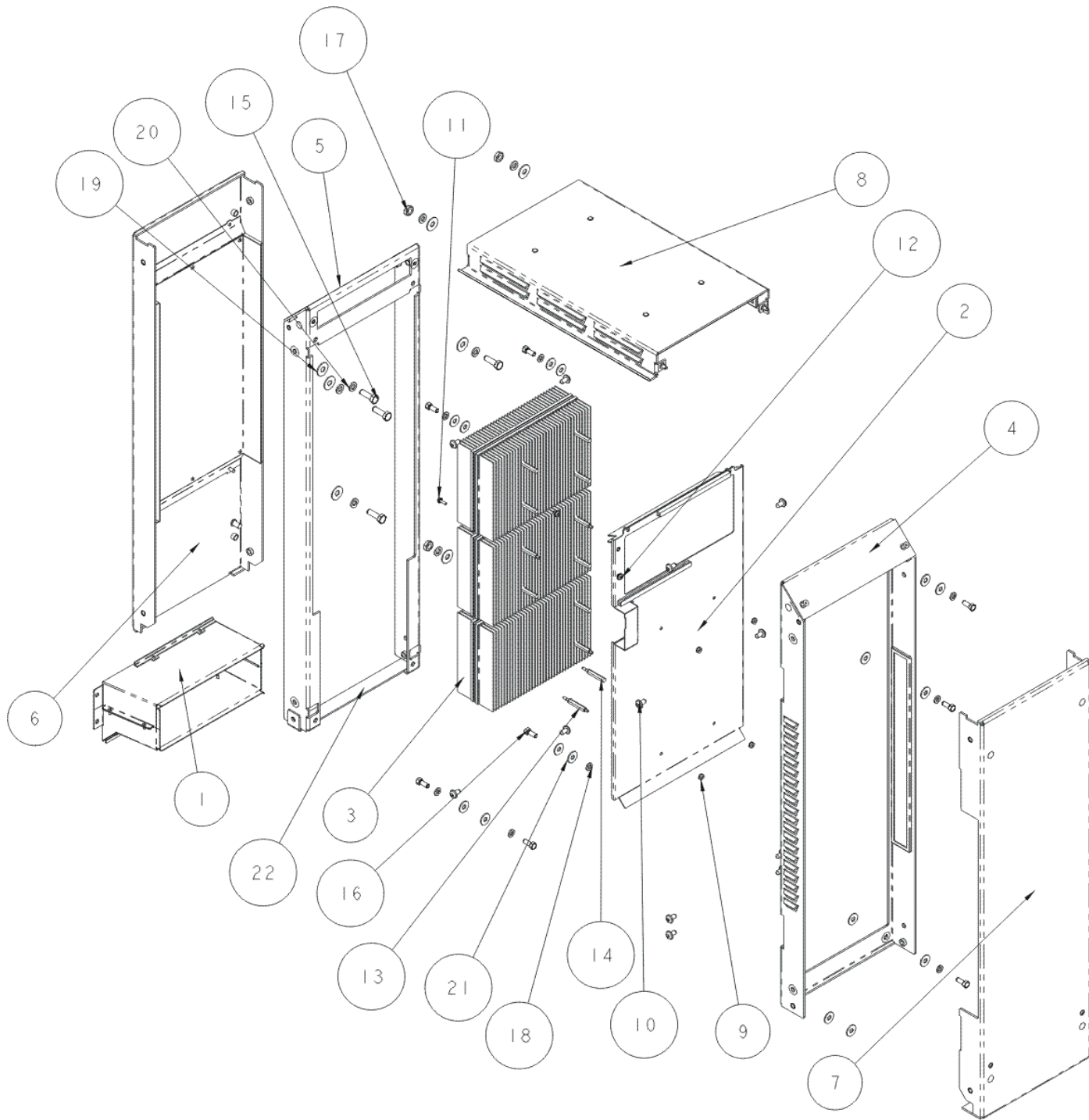
This Retrofit Kit for the Stinger Compact Remote consists of the following features:

- Heat sinks
- Internal air ducts
- Necessary fasteners.

**Upgrading Stinger Compact Remote  
Retrofit Kit**

The contents of single Retrofit kit are shown in following figure:

Figure F-1. Retrofit Kit Parts



The following table describes the contents of Retrofit kits  
*Table F-1. Contents of Retrofit kit:*

<b>Item</b>	<b>Quantity</b>	<b>COMCODE</b>	<b>Description</b>
1	1	1410-1715-001	Duct, Transition
2	1	1410-1717-001	Shroud, Heat Exchanger, Inner, Retrofit
3	6	1410-1718-002	Heat Sink Assembly With Thermal Interface Material
4	1	1410-1757-002	Bracket, enclosure mounting, right side
5	1	1410-1757-003	Bracket, enclosure mounting, left side
6	1	1410-1758-001	Mounting bracket / solar shield / air duct, left
7	1	1410-1758-002	Mounting bracket / solar shield / air duct, right
8	1	1410-1765-001	Roof, Solar Shield, Stinger Compact Remote
9	4	1810-0034-001	4 Nuts, hex, "k" lock type (kepnut), steel, #6-32 Four additional nuts are provided as spares.
10	12	408908853	Screw, security, trilobular recess, sst., 1/4-20 th., 0.50 in. len.
11	12	408984367	Screw, pan head, cross recess, cone washer sems, #6-32 x 0.5
12	2	408984383	Screw, pan head, cross recess, sems ext. tooth washer, m5 x 6
13	4	849033063	Standoff, "sems" type, male-male
14	8	849033089	Standoff, "sems" type, male-female
15	4	901349480	Bolt, hex_hd .3125-18x1.000
16	8	901350298	Nut hex, .3125-18
17	4	901352674	Nut hex, .3125-18
18	8	901352708	Wshr lk, hel_spg .250

Item	Quantity	COMCODE	Description
19	8	901353672	Wshr, flt reg .312
20	8	901375378	Wshr lk, hel_spg .312
21	16	901375378	Wshr, flt reg .250
22	1	NA	Bracket, shipping, temporary, disposable

**Note** Loose fasteners will be present in the marked bags.

## Torque Requirement

### Using torque wrenches for retrofit

In a factory setting, calibrated torque wrenches are used to install threaded fasteners. Using torque wrenches ensures the following:

- Fasteners are not over-tightened and prevent thread stripping.
- Fasteners are not under-tightened and prevent thread loosening.

Therefore, it is advised to use all threaded fasteners be torqued as described in the following table.

Table F-2. Torque Requirements.

Thread Size	Torque Requirement						Fastener Description
	SI Unit			US Customary Unit			
	Nominal	+/-	Tolerance	Nominal	+/-	Tolerance	
	(NM)	(Nm)	Nm)	(in X lbs)		(in X lbs)	
#6-32	1.5	+/-	0.2	14	+/-	2	Standoffs (Male-Male and Male-Female) and nuts
M5	4.0	+/-	0.6	35	+/-	5	Transition Duct
1/4-20	9.1	+/-	1.4	81	+/-	12	Security screws and side panel bolts
5/16-28	16.7		2.5	148	+/-	22	Nuts and bolts to secure CR for side mounting

## Retrofit without torque wrenches

However, it is recognized that all craft-persons may not be in possession of a torque wrench during the time of the retrofit. If the retrofit must be done without the torque wrenches, then complete the following method:

- 1 Engage the mating threads.
- 2 Turn by hand only
- 3 Stop when the fastener and mating part abut their respective surfaces.
- 4 Use an appropriate tool such as wrench, screwdriver, or a socket to rotate the fastener a minimum of one quarter turn (90°) but no more than a half turn (180°).

## Using Retrofit to Upgrade Compact Remote

Use the following instructions to upgrade Stinger Compact Remote (CR) system using Retrofit Kit

### Guidelines

- It is preferable to conduct this retrofit exercise within an indoor environment such as the warehouse, laboratory, or the service facility.
- However, it is recognized that there is a need to perform retrofits on installed, deployed systems. It is suggested that the retrofit occur during an interval of low wind velocity, minimal precipitation, moderate temperatures, and with proper illumination.



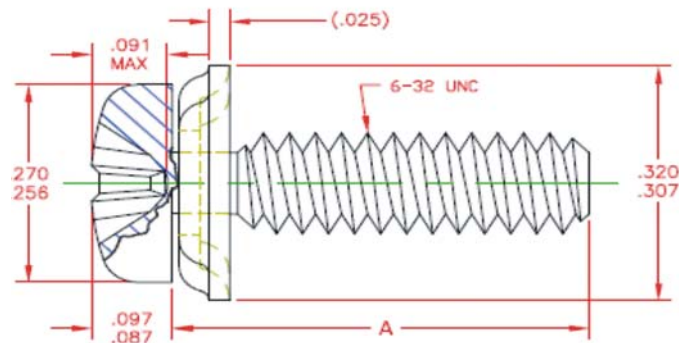
**Caution** The system might be powered and providing service. Therefore, take the required precautions and ensure no safety hazards occur.

### Installing retrofit kit

- 1 (Conditional) Close door of enclosure if open. Use the proper tool such as can wrench, 716 tool to engage both upper and lower quarter turn latches.  
This prevents damage to the door and especially the hinge while the unit is dismantled.
- 2 Dismount entire Compact Remote from its current mounting configuration.
  - Exercise utmost caution while dismantling because a fully populated system with additional mounting brackets weighs up to 97 kg [215 pounds].
  - Provide a maximum degree of freedom for the Outside Plant (OSP) cables to be coiled or uncoiled. You can remove cables ties to gain some freedom.
  - The Liquid Tight Strain Relief Fittings (watertight connectors) may need to be loosened to provide more slack in the cables
  - The exact method of dismantling is based on how the CR was deployed. The various mounting for Compact remote include side mount, rear mount, pedestal mount, pole mount, and rack mount.
  - Remove the security screws from the load bearing side, panel, or cover first, to facilitate the removal of that panel.

- Remove the Cable Cover (except for the rack mount where there is none and the pedestal mount where the mount is the cable cover).
  - The safest (lowest potential energy) temporary position for the CR is resting on its back.
  - To prevent scratching of paint or denting of sheet metal, arrange for a padded surface. This could be a board with carpet or rubber padding.
- 3 Remove the remainder of the five exterior, bolt-on panels.
- a Remove the security screws that hold the left and right outer panels. Use the appropriate tool for the style of security screw present (one-way versus trilobular recess).
  - b Remove the hex bolts that secure the left and right inner panels.
  - c Discard all of the loose fasteners. Discard or recycle the panels. They must not be used in this retrofit. The exception to this is the trilobular recess security screws. These screws can be used in the retrofit.
- 4 Install three heat sinks on the outside left enclosure wall.
- The heat sinks are the finned Aluminum heat sinks with a putty-like material (typically blue in color) that is the Thermal Interface Pad (T.I.P.). The T.I.P. comes shipped with a very thin protective plastic sheet as covering (typically white in color). Remove this sheet prior to installing the heat sinks.
  - d Use screws with captive washers. The following figure illustrates the screws with captive washers.

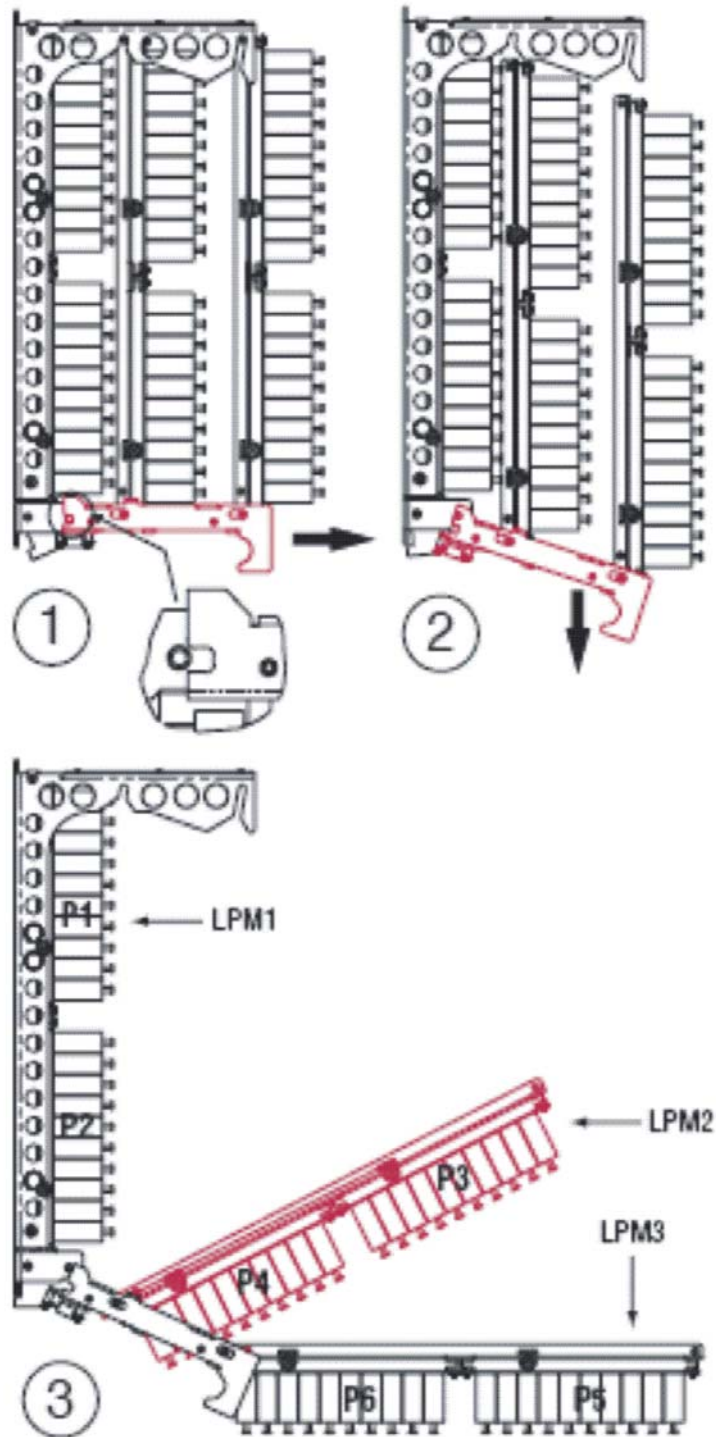
Figure F-2. Screws with captive washers



- 5 Install the five new exterior bolt-on panels
- a Observe the left and right versions of each.
  - b Use the new hex bolts and trilobular recess security screws provided.
  - c Remove the un-painted shipping bracket form the left hand side panel and discard. This is Item # 22 in parts list

- 6 Re-install the CR on the Cross-connect cabinet. Open door of enclosure and swing out the two layers of the Protection Block Assembly. Follow instructions provided on door decal.

Figure F-3. Protection block assembly



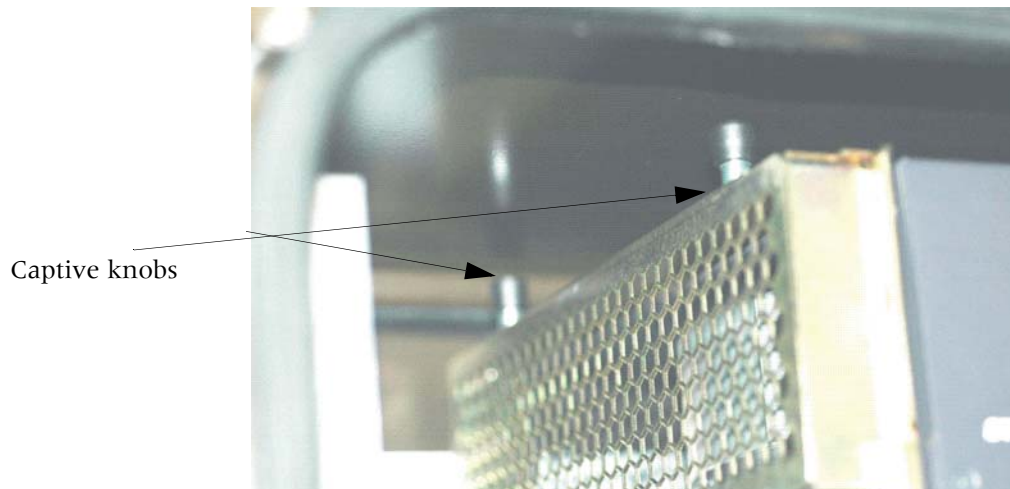
## Upgrading Stinger Compact Remote

Using Retrofit to Upgrade Compact Remote

---

- 7 Remove perforated guard at the top left of the card cage assembly.
  - Two captive knobs at top, with cross-recess drive heads.
  - Not enough room to use a right-angle screwdriver.
  - Small vise-grips recommended, but be careful not to crush the knobs.
  - Discard or store the par.

Figure F-4. Captive knobs



- 8 Install three heat sinks on the inside of the left enclosure wall.
  - Use standoffs observing specific locations for the eight male-female and four male-male versions (shown in red) of these standoffs.
  - A tool that greatly eases the standoff installation is this ratcheting box wrench shown below. It is available from [www.snapon.com](http://www.snapon.com). It is listed under Snap-On part number R810SC.

Figure F-5. Male-Male standoffs

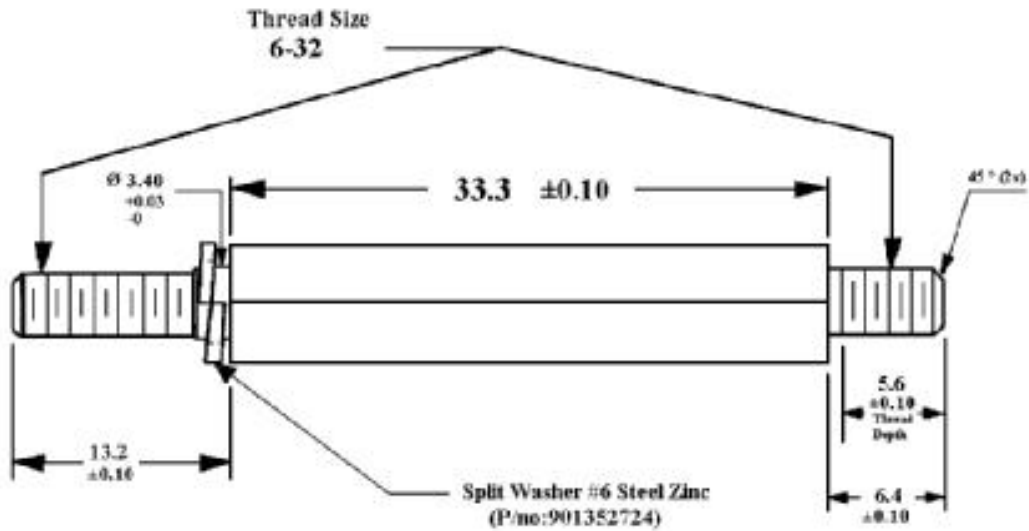
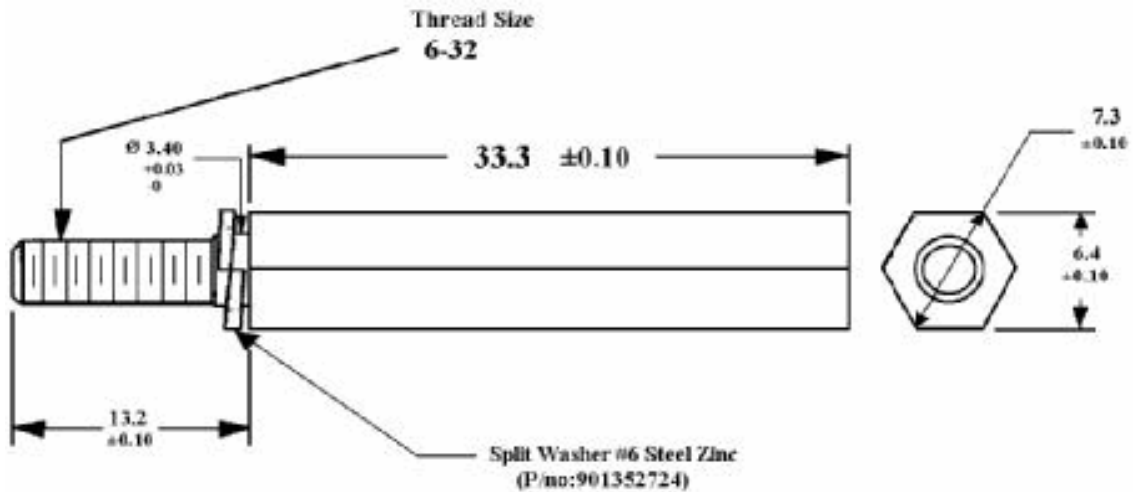
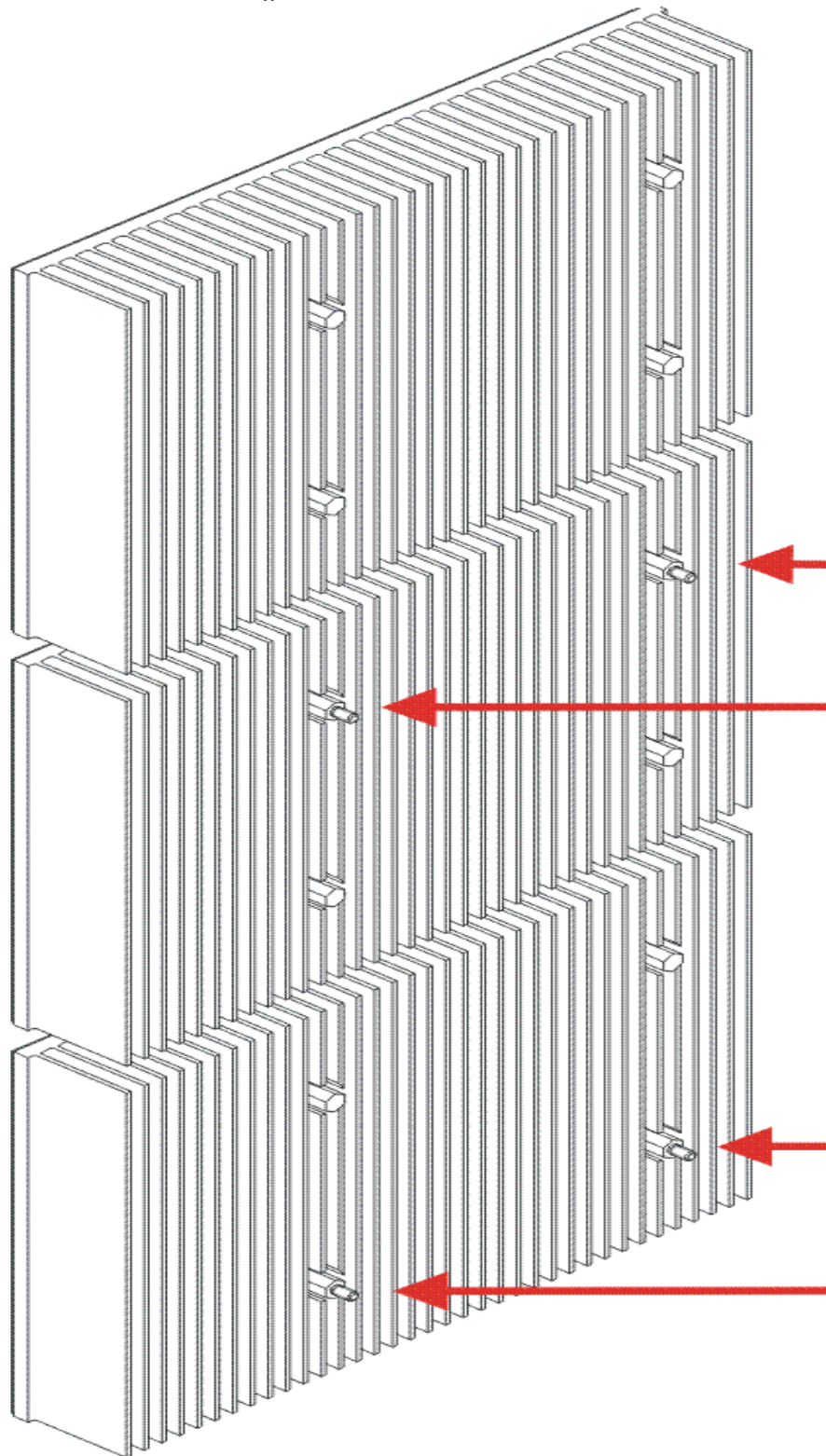


Figure F-6. Male-Female standoffs



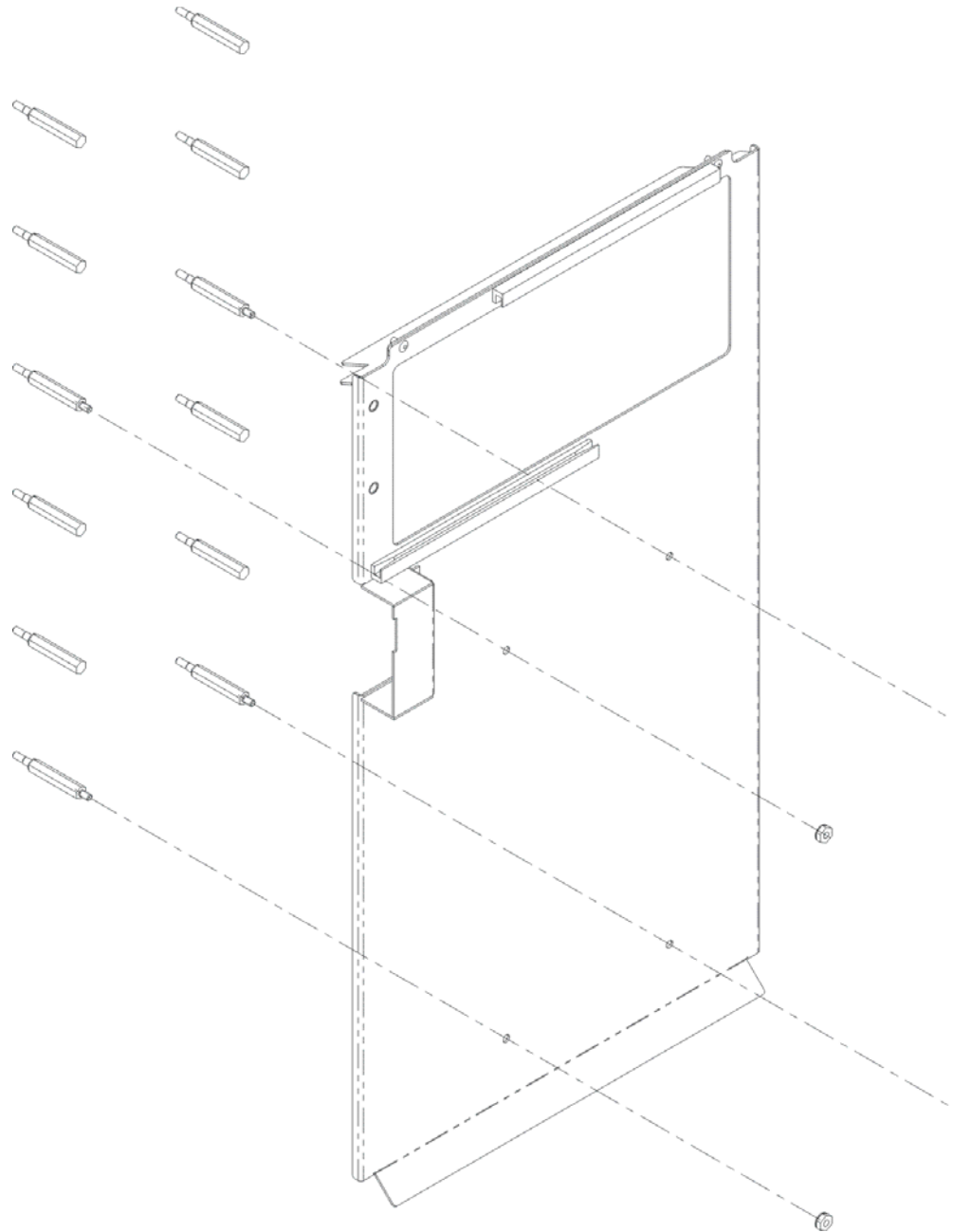
*Figure F-7. Male-Male standoffs*



**Note** The male-male standoffs are installed with the long threads first. This end also has a captive lock washer.

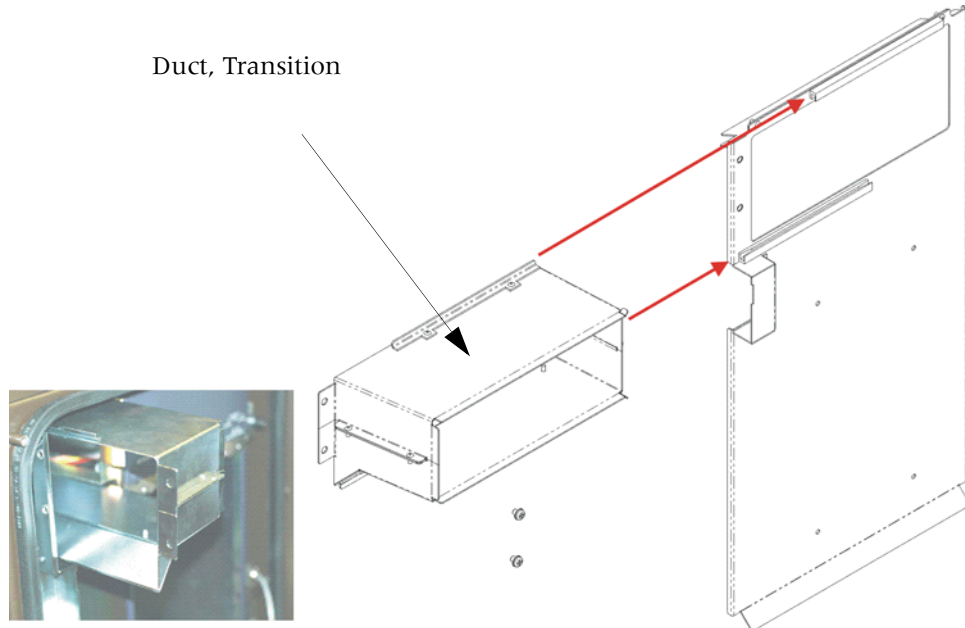
- 9 Install the “Shroud, Heat Exchanger, Inner, Retrofit”. Secure with nuts on the four male-male standoffs shown. Four additional nuts are provided as spares in case they are dropped. If any nuts fall down into the base of the cabinet, retrieve those nuts as a precaution.

*Figure F-8. Securing male-male standoffs*



- 10 Slide in the “Duct, Transition” into plastic grooves in shroud. Ensure that both of the metal rails of Transition Duct engage with the plastic card guides. Secure with the two M5 screws

Figure F-9. Sliding in the duct, transition



- 11 Swing layers of protection block assembly back into place. Follow instructions shown on door decal.
- 12 Observe LED's on circuit packs and the fan module to ensure that no impact to service was created as a result of the retrofit procedure.
  - The fan should have green lights shown for both Internal and External
  - The port activity lights on the circuit packs should remain roughly as they were.

Figure F-10. Fan lights



- 13 Shut enclosure door, latch, and padlock.
- 14 The purpose of the 12 black plastic plugs is to snap-in to the vacant holes on the side panels.

Revised CR



**Note** Larger (5/16 inch instead of the smaller 1/4 inch) diameter mounting bolts are used on the sides of the CR. This is to accommodate the increased mass of the CR resulting from the heat sinks and ducts.

---

# Card Cage Rack Mount System (CCRMS)



G

CCRMS .....	G-1
CCRMS Installation .....	G-3
Site specifications .....	G-6
Additional brackets in CCRMS for stress prevention .....	G-8
Installing the additional brackets .....	G-9

**Warning** Before installing your Stinger unit, be sure to read the Appendix D, “Safety-Related Electrical, Physical, and Environmental Information”

## CCRMS



**Caution** The Stinger CR CCRMS is packed with the unit resting on its back. The CCRMS must not be moved until the unit is mounted to a rack. This is because the air intakes at the bottom are not intended to be structural members and, the system would be unstable if supported on the ducts.

This CCRMS for the Stinger Compact Remote consists of the following features:

- Power filters
- Fans
- Rack mount bracket assembly
- Card cages (with backplane assemblies)
- Air ducts
- Necessary fasteners



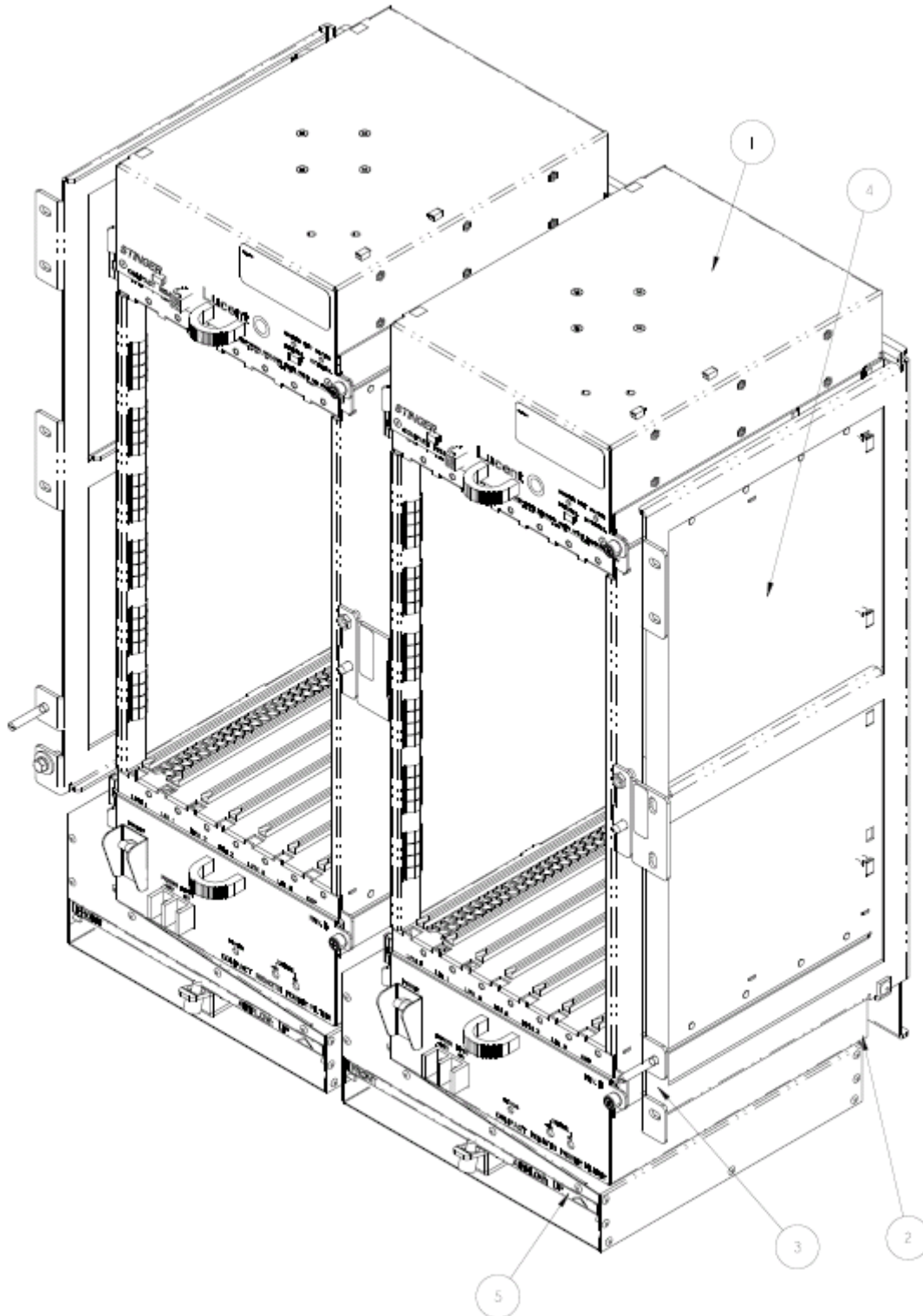
**Note** A Stinger CR CCRMS (dual card cages) will dissipate 570 Watts.

**Card Cage Rack Mount System (CCRMS)**  
CCRMS

---

The parts of a Rack Mount System for Stinger Compact Remote Card Cage are shown in “Card Cage Rack Mount System parts” on page G-2:

*Figure G-1. Card Cage Rack Mount System parts*



The following table describes the Card Cage Rack Mount System parts:

Table G-1. Card Cage Rack Mount System parts

Item	Quantity	Description
1	2	Fan Module, Stinger CR
2	2	Power Filter -48 V DC
3	1	Rack Mount Bracket Assembly, for Stinger Compact Remote Cage
4	2	Card Cage with Backplane Assembly, Stinger Compact Remote
5	2	Air Filter, Stinger Compact Remote Rack Mount Card Cage

## CCRMS Installation

- This is intended for “23 inch” (Legacy Bell System) style racks.
- Cutouts support the two major variants of vertical hole-to-hole spacings.
- Six screws with #12-24 UNC thread are included with the kit. These screws are to be installed such that one screw is at each of the four corners plus one screw at both the left and right vertical mid-span of the bracket.
- Utilize flat and lock washers to ensure a reliable, long-term fastened joint.
- The #12-24 screws must be torqued to  $5.4 \pm 0.8$  Nm [ $48 \pm 7$  in•lbs]. In absence of a calibrated torque wrench, these screws may be torqued with the “turn of the screw method” described in “Retrofit without torque wrenches” on page F-5.
- Two threaded alignment pins are provided as an installation aid. Install these two pins first, then the CCRMS, then the screws (with washers). Afterwards, the pins can be removed and screws put in their place.

To reduce the installation weight, it is advisable to remove all plug-in modules (two fans and two-power supplies) prior to mounting to the rack. See Table G-4 on page G-7 for CCRMS cumulative weight details.

## Replacing the air filter

To replace the filter, pull the spring-loaded plunger up on the rear (or the front) of the air intakes, and withdraw the air filter element. You can find the orientation of the airflow by the arrow showing upward airflow.

Lucent recommends replacing the air filter with a frequency according to the following table based on Total Suspended Particles (TSP) in the deployed environment:

TSP Count (Dust Loading)	Suggested filter maintenance (days) for differing ambient temperatures		
	25 C	35 C	45 C
micrograms/ cubic meter			
20	463	332	124
35	265	190	71
55	168	121	45
100	93	66	25
200	46	33	12

## Replacing the fan

When replacing a fan, the side blocking panel must be removed from the old fan and transferred to the new fan.



**Caution** Observe all other safety and operational recommendations for fan as shown in “Replacing the chassis cooling module” on page 3-28.

## Power filter

- Required feeds:  $-48 \pm 6 V_{dc}$ .
- Customer to supply power cable.
- 18 AWG or larger diameter conductor recommended.
- Two screws secure the power leads on the terminal block.
- Return clear plastic safety cover to position on terminal block after torquing down screws.
- Observe polarity for  $-48 V$  (black) and Return (red) wires.

There is a cable tie-off provision on the front face of the air intake. This is to secure the power cable.



**Caution** Observe all other safety and operational recommendations for power filter as shown in “Replacing the power supply” on page 3-31.

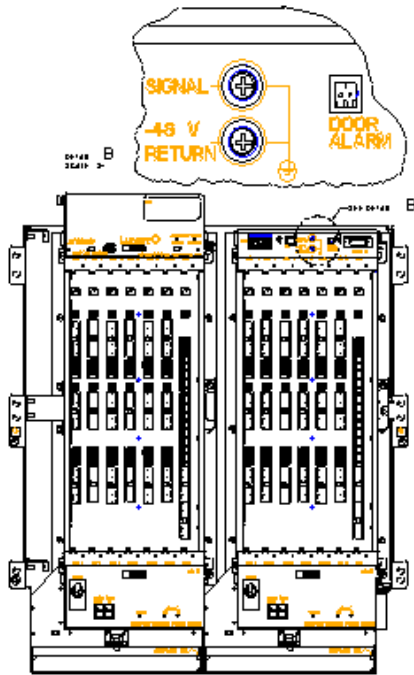
## Grounding

To facilitate grounding, #10 sized studs (and locking nuts) are on either side of the CCRMS. Use the appropriate gauge ground cable as defined in the “Minimum ground wire size” on page G-5.

The CCRMS will arrive from the factory with an “Isolated” grounding scheme for use with the –48 V power filter. When this system is powered by the ±190 V power supply, “Mesh” grounding is to be used. The following figure details about the grounding options.

Figure G-2. CCRMS grounding options

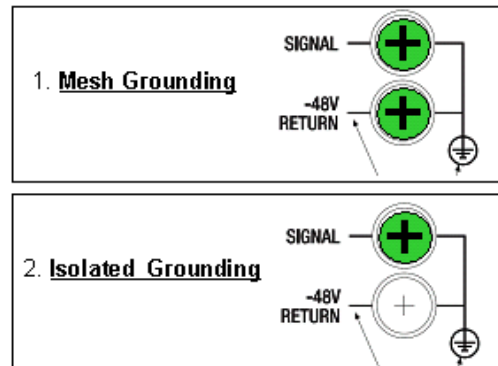
## Grounding Options



1. **Mesh Grounding** (for ±190 V Power Supply)
2. **Isolated Grounding** (for –48 V Power Filter)

Notes:

- a. Behind the fan, screw fasteners provide the connections to ground; the absence of those screws opens the circuits.
- b. The signal-to-ground connection is to be maintained for either Mesh or Isolated grounding.
- c. With Isolated Grounding, the alarm connector may not be used.



Lucent Technologies – Proprietary  
Use pursuant to company instruction

### Minimum ground wire size

The DSL lines connected to the Stinger can be subject to lightning surges. These surges must be discharged to ground through an adequate ground wire. An adequate ground wire must present a resistance of approximately 0.02 ohms to a surge of 500 amps.

## Card Cage Rack Mount System (CCRMS)

### Site specifications

---

The wire gauges shown in Table G-2 on page G-6 are appropriate for the wire lengths indicated.

Table G-2. Minimum ground wire sizes

Length	Wire gauge
0 to 10 feet (0m to 3.05m)	12 AWG (3.31mm <sup>2</sup> )
10 to 25 feet (3.05m to 7.62m)	9 AWG (6.63mm <sup>2</sup> )
25 to 50 feet (7.62m to 15.24m)	6 AWG (13.3mm <sup>2</sup> )
50 to 100 feet (15.24m to 30.48m)	3 AWG (26.7mm <sup>2</sup> )

Lucent Technologies does not recommend to use a ground wire longer than 100 feet (30.48m).

### ESD Jacks

An ESD jack is provided at the right of both card cages. Use this in conjunction with a customer supplied ESD wrist strap.

## Site specifications

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

### Operating environment

Table G-3 describes the environmental requirements for selecting an installation site for the [Product]hardware. The site requirements are based on Network Equipment Building System (NEBS) GR-63-CORE and GR-1089-CORE.

Table G-3. Site specifications

Parameter	Requirement
Ambient operating temperature	0°C to 55°C (32°F to 131°F)
Relative humidity	10% to 95% (non-condensing)
Operating altitude	To 13,123 feet (4000m)
Ambient storage temperature	-40°C to +85°C (-40°F to +185°F), 95% relative humidity
Storage altitude	-1,000 feet to +30,000 feet (-305m to 9150m)

## Space requirements

The [Product] CCRMS hardware requires the following minimum clearances for the chassis:

- 15 cm [6 inches] at the back panel for cable routing and airflow. If rear air filter removal is desired, then 30.5 cm [12 inches] of clearance.
- 54 cm [20 inches] at the front panel for module replacement and airflow

## Lifting requirements

Although a single person can lift an empty Stinger chassis, use a mechanical lift or at least two people to lift a full Stinger chassis for rack or wall mounting. For more information, see Chapter 3 Compact Remote Enclosure and Component Installation.

Table G-4 shows the cumulative weight as these plug-in modules are added.

*Table G-4. CCRMS Installation weight details*

<b>Description</b>	<b>Quantity</b>	<b>Cumulative Mass / Weight</b>
Rack Mount Card Cage Bracket Set	1	13 kg [28 lbs]
Air filter	2	13 kg [28 lbs]
Card cage	2	24 kg [53 lbs]
Power Filter module	2	29 kg [63 lbs]
Fan Modules, Internal	2	35 kg [76 lbs]
Cable set (18 Tip/Ring and 2 Power)	1	38 kg [83 lbs]
Line Interface modules, 48 port	6	46 kg [102 lbs]
Line Protection modules	6	55 kg [122 lbs]
Controller Optical packs	2	57 kg [126 lbs]

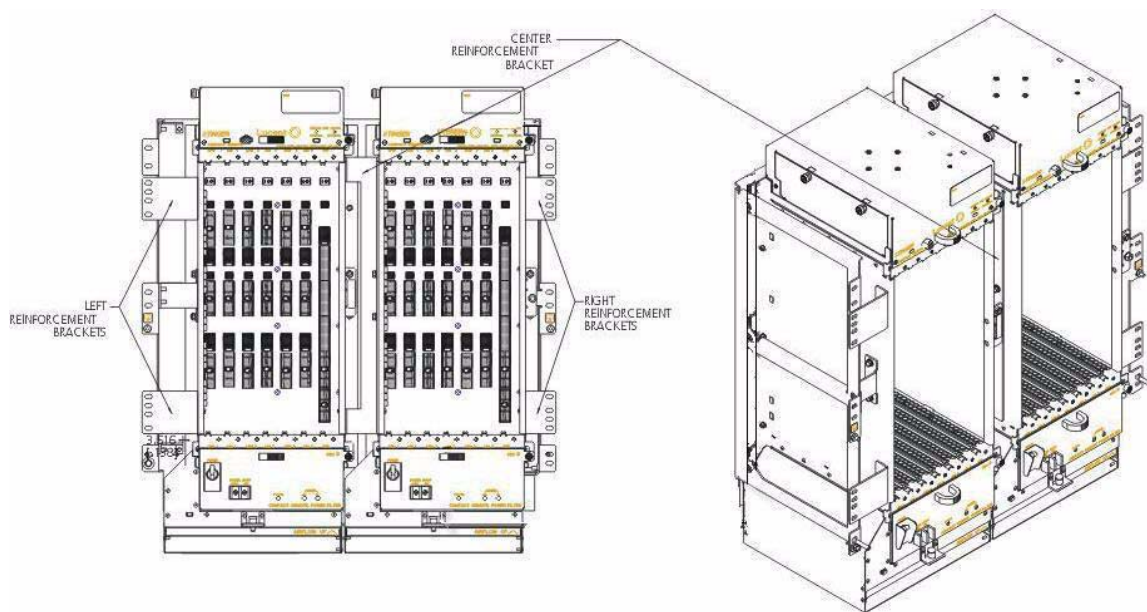
## Additional brackets in CCRMS for stress prevention

Additional brackets are installed in the CCRMS to reinforce the structure and to ensure that minor stress cracks will not develop during Zone 4 level seismic / earthquake activity.

This bracket set includes:

- 2 Right side brackets
- 2 Left side brackets
- 1 Center bracket
- Associated fasteners

*Figure G-3. Additional brackets in CCRMS for stress prevention*



## Installing the additional brackets

Follow the steps below to install the additional brackets for CCRMS (if this is shipped separately):

- 1 Install the main portion of the CCRMS on the rack.
- 2 Install the center bracket. This center bracket must be placed with two specific bolts, fastened to the left side of the right card cage.
- 3 Install the four side brackets (two left and two right); install two identical brackets on one side first and make sure to position them as close to the far corners as possible.



**Note** Ensure that the face of the smaller leg of the "L" is in contact with the card cage.

- 4 Repeat for the two brackets on the other side. These brackets have four slotted holes to accommodate the hole spacing on different racks, yet only two bolts will secure each bracket.
- 5 Ensure proper torque on these fasteners, 5.4 +/- 0.8 NM [4.0 +/- 0.6 ft lb].



---

# Index



## Numerics

- 12582
  - 2Head
    - Torque Requirement
    - Using torque wrenches for retrofit F-4
- 94960
  - 1Head
    - Retrofit Kit F-1, G-1

## A

- AAL5 statistics 5-17
- address pools. See slot-based address assignment
- address-pool 5-8
- administrative connections
  - alarms 3-35
  - diagnostic 3-35
- alarms
  - connector description C-2
  - input connector pinouts C-2
- altitude
  - operating D-13, G-6
  - storage D-13, G-6
- ATM traffic statistics 5-19
- ATM, standards D-12
- atmcaostat -b 4-19

## B

- bridged connection statistics 5-20
- bridging-enabled** 4-9

## C

- cables
  - diagnostic port C-1
  - power stub connections C-17

- serial port C-1
- Card Cage Rack Mount System G-1
- cascaded-port 4-4
- cautions about replacing modules 3-22
- chassis validation ID DIP switches 4-21
- cooling unit
  - checking 2-11
  - function 1-4
  - status lights 3-43, 3-44
- COP
  - installing and replacing 3-23
  - interfaces checking 2-8
  - status lights 3-40
- CR ports. See GE-OLIM CR ports

## D

- distributed multicast mechanism 5-1
  - CPE joins a multicast group 5-3
  - CPE leaves a multicast group 5-4
  - displaying multicast information 5-4
  - FFW interface multicast behavior 5-2
  - FFW interfaces 5-2, 5-5
  - traffic statistics 5-20
- door-open 5-15
- DSL subscriber connections
  - routed VLAN 4-27
  - types supported 4-23
  - VLAN bridging (1-to-1) connection with CM egress 4-25
  - VLAN stacking connection with CM egress 4-26

## E

- electrostatic discharge (ESD) jack 2-7
- enabled 4-15
- enclosure
  - illustrated 2-5
  - mounting 3-15

## Index

F

---

- size D-12
- environmental specifications D-13, G-6
- ESD, grounding jack 2-7
- ETHERNET profile 4-3
- Ethernet, must be enabled on GE-OLIM 4-3
- external-fan-unit-failed 5-15

## F

- fan status lights 3-43, 3-44
- FFW interfaces. See distributed multicast mechanism

## G

- gecacstat 4-18
- GE-COP
  - defined 4-2
  - FFW interfaces on 5-3
  - functions 1-4
  - GIGE-1 and GIGE-2 ports 4-15
  - links on GE-OLIM CR ports 4-17
  - opening a session to 5-17
- GE-OLIM
  - defined 4-2
  - description 4-2
  - enabling GMAC 4-3
  - FFW interfaces on 5-3
  - installation B-2
  - opening a session to 5-17
  - overview B-1
  - port function with current software 4-3
  - specifications B-5
  - status lights B-4
- GE-OLIM CR ports 4-4
  - CAC bandwidth checks 4-17
  - configuration 4-18
  - link aggregation 4-17
- GE-OLIM trunk ports
  - IP multicast configuration 4-6, 4-12
  - IP routing configuration 4-4
  - routed VLAN configuration 4-5
  - usage 4-4
- ground wire size G-5

## H

- hardware, verifying configuration 2-4
- host
  - defined 4-1

- description of functions 4-2
- enabling master mode 4-14
- hosted system architecture 4-1
  - enabling operations 4-14
- host-port 4-15, 5-14
  - physical-address 5-15
- host-port-2 4-15, 5-14
- humidity requirement D-13, G-6

## I

- index 5-8
- installation
  - cabinet mount 3-4, 3-14
  - cables and fibers 3-16
  - mounting hardware 3-2
  - pedestal mount 3-6
  - pole mount 3-8
  - pole-mount 3-3
  - prerequisites 3-1
  - rack mount 3-7
  - required tools 2-1
- Installing retrofit kit F-5
- intended use A-1
- internal-fan-unit-failed 5-15
- IP filters for PPPoE connections 5-11
  - current limitations 5-11
  - sample configuration 5-12
- IP multicast on GE-OLIM trunk ports 4-6
- IP multicast. See distributed multicast mechanism
- IP routing on GE-OLIM trunk ports 4-4
- IP2000
  - installing and replacing 3-23
- IP-GLOBAL profile 5-7

## L

- LEDs. See status lights
- LIM
  - checking 2-9
  - installing and replacing 3-24
- LIM port CAC 4-17, 4-18
- link aggregation for GE-OLIM CR ports 4-17
- link-state-enabled** 4-9
- location 4-15, 5-15
- LPM
  - 50-pin connector C-3
  - checking 2-11
  - connecting 3-36

function 1-4  
installing and replacing 3-26

## M

master mode 4-2  
  configuring on host CM 4-14  
modules, cautions about replacing 3-22  
monitor-control, pinouts C-1  
multicast-capable modules 5-1

## N

contact-closure 5-15  
nailed-group-bin 4-15, 5-15  
name 4-15, 5-14

## O

olim-port-config 4-3  
OLIM-PORT-USAGE profile 4-2  
over-temperature 5-15

## P

PCMCIA cards  
  described 2-9  
pinouts  
  alarm input C-2  
  alarm input connector C-2  
  monitor-control C-1  
plug-in components  
  cooling unit 1-4  
  GE-COP 1-4  
  LPM 1-4  
  power supply 1-4  
  RLIM 1-4  
pool-selection 5-8  
port-function 4-3  
power  
  cable connections to power unit C-17  
power supply  
  checking 2-12  
  function 1-4  
powering up, described 3-38  
PPPoE connections 5-7  
preventing static discharge damage 2-2

Protection block elements D-8  
protection blocks  
  tip/ring orientation C-7

## R

remote shelves  
  bringing up 4-16  
  configuration of 4-16  
  defined 4-1  
  description of functions 4-2  
  validation IDs 4-20  
  validation, setting 4-22  
remoteself -s 4-18, 5-16  
REMOTE-SHELF-CONFIG profile 4-14, 4-22  
remote-shelf-id 4-14, 5-14  
remote-shelf-oper-state 5-14  
REMOTE-SHELF-STAT profile 5-13  
remote-shelf-type 4-15  
Replacing a compact remote door E-1  
  Replacing the damaged door E-1  
Replacing a Door Assembly on a Deployed  
  Stinger CR E-1  
Retrofit Kit F-1, G-1  
Retrofit without torque wrenches F-5  
RLIM  
  defined 4-2  
  FFW interfaces on 5-3  
  function 1-4  
  opening a session to 5-17  
routed VLAN 4-27  
Routed VLAN on GE-OLIM trunk ports 4-5

## S

shelf-controller-type 4-14  
show command 4-16  
size of enclosure D-12  
slave mode 4-14  
slot numbering 3-22  
slot-based address assignment  
  how it works 5-7  
  sample configuration 5-9  
SLOT-STATIC-CONFIG profile 4-19  
SLOT-VR-CONFIG profile 5-7  
space requirements G-7  
specifications  
  cable pinouts C-1  
  electrical D-7

## Index

T

---

environmental D-13  
  physical D-12  
  space G-7  
startup sequence 3-38  
static discharge damage 2-2  
  preventing 2-2  
statistics  
  for ATM traffic 5-19  
  for bridged connections 5-20  
  for distributed multicast traffic 5-20  
  for terminating AAL5 connection 5-17  
stats command 5-16  
status lights  
  COP 3-40  
  fan and cooling unit 3-43, 3-44  
  GE-OLIM B-4  
SYSTEM profile 4-14, 4-22

## T

temperature  
  operating D-13, G-6  
  storage D-13, G-6  
tools and equipment required for installation 2-1  
Torque Requirement F-4  
traffic statistics 5-16  
trunk ports, configuration 4-4  
trunk-group 4-4

## U

Upgrading Stinger Compact Remote F-1  
Upgrading Stinger Compact Remote (CCRMS)  
  G-1  
  Additional brackets in CCRMS for stress  
  prevention  
  Installing the additional brackets G-9  
use of wrist strap 2-2  
Using Retrofit to Upgrade Compact Remote  
  Guidelines F-5  
Using torque wrenches for retrofit F-4

## V

validation-config 4-15  
validation-enable 4-22  
validation-id 4-23  
validation-status 5-15  
VLAN bridging (1-to-1) connection with CM

egress 4-25  
VLAN stacking connection with CM egress 4-26  
VLAN, routed 4-5, 4-27

## W

WAN interfaces supported D-12  
weight of unit D-12