

Lucent Technologies
Bell Labs Innovations



Stinger® MS+

Getting Started Guide

Part Number: 363-217-002R9.7
For software version 9.7.0
August 2004

Copyright © 2004 Lucent Technologies Inc. All rights reserved.

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

Notice

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

European Community (EC) RTTE compliance

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

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

Safety, compliance, and warranty Information

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

Security statement

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

Trademarks

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

Ordering Information

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

Feedback

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

Customer Service

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

Finding information and software

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

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

Obtaining technical assistance

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

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

Obtaining assistance through email or the Internet

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

Calling the technical assistance center (TAC)

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

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

Contents



Customer Service	iii
About This Guide	xiii
What is in this guide	xiii
What you should know	xiii
Documentation conventions	xiii
Stinger documentation set	xiv
Chapter 1 Preparing for the Installation.....	1-1
Stinger MS+ overview.....	1-1
The Stinger MS+ chassis	1-1
Modular plug-in components	1-3
Selecting an installation site	1-3
Required tools and equipment	1-4
Preventing static discharge damage.....	1-4
Use a wrist strap.....	1-4
Remove plastics from your work area	1-6
Store components properly	1-6
Unpacking the Stinger.....	1-6
Verifying the hardware configuration.....	1-6
Checking the front of the chassis.....	1-7
Verifying the control module model	1-7
Control module support	1-8
Control module interfaces.....	1-8
Checking the LIMs	1-9
Checking the of the chassis.....	1-10
Verifying the trunk module	1-10
Checking the LPMs	1-12
Chapter 2 Installing a Stinger MS+	2-1
Before you begin	2-1
Mounting the unit.....	2-1
Connecting cables to a Stinger unit.....	2-3
Connecting to the LPMs	2-3
Securing the connectors.....	2-3
Connecting the subscriber lines	2-4
Connecting the trunk modules.....	2-5
Optical trunk module connections	2-5
DS3-ATM or E3-ATM trunk module connections	2-5

Control module connections	2-6
System clocking.....	2-7
Alarm monitoring	2-7
Connecting to monitor Stinger unit alarm status	2-7
Connecting a Stinger unit to monitor the alarm status of other devices.....	2-8
Connections from the control module	2-8
What's next	2-9
Chapter 3 Determining the Operating Status	3-1
Before you begin	3-1
Connecting power to a Stinger unit	3-1
Turning on power to a Stinger unit	3-2
Status lights	3-3
Control module status lights.....	3-3
LIM status lights.....	3-5
Trunk module status lights	3-5
Fan status light.....	3-5
What's next	3-6
Chapter 4 Stinger Operational Overview.....	4-1
Stinger MS+ operation as a DSL access multiplexer	4-1
Stinger ATM switching overview.....	4-2
Stinger configuration overview.....	4-2
Control module configuration	4-2
Line interface module (LIM) configuration	4-2
Trunk module configuration	4-3
System clocking modes.....	4-3
Stinger management features	4-3
Using the command-line interface	4-3
Onboard flash memory and software updates.....	4-4
SNMP support.....	4-4
RADIUS support	4-4
Tracking system activity.....	4-4
Verifying software and control module versions	4-5
Status windows	4-5
What's next	4-5
Chapter 5 Configuring the Control Module and System Timing	5-1
Control module configuration overview.....	5-1
Administrative connections.....	5-1
Serial connection to a console	5-2
Network connection to a workstation console	5-2
Connecting a dial-in backup management connection	5-3
Backup management with an external modem.....	5-3
Modem country codes.....	5-4
Backup management with an internal modem	5-5
Logging into the control module.....	5-6
Restricting administrative access.....	5-7
Changing defaults for serial-port logins.....	5-7
Changing the default admin password	5-8

Setting a Telnet password	5-9
Providing a basic system IP configuration	5-9
IP address syntax	5-10
Netmasks.....	5-10
Subnets.....	5-10
Assigning the Ethernet IP addresses	5-12
Defining the soft IP interface	5-12
Configuring a default route	5-13
Verifying a LAN connection for administrators	5-14
Configuring system clocking	5-14
Using the default (controller) clock source.....	5-14
Using the BITS clock source.....	5-15
Loss of BITS signal indications and fall-back.....	5-15
Changing the BITS clock source.....	5-16
Using a LIM or trunk module clock source	5-16
Configuring trunk ports as eligible clock sources.....	5-17
Typical trunk port clock source configurations	5-17

Chapter 6 Installing and Removing Modules6-1

Installation and replacement considerations.....	6-1
Replacing and installing control modules	6-2
Removing a control module	6-2
Installing a control module.....	6-3
Slot numbering and module placement.....	6-5
Installing and replacing LIMs	6-5
Installing a LIM.....	6-5
Replacing a LIM	6-5
Installing and replacing LPMs	6-6
Installing an LPM.....	6-6
Replacing an LPM.....	6-7
Installing and replacing PCMCIA cards.....	6-8
Replacing the cooling module.....	6-8
Replacing a power filter	6-9
Replacing the alarm module	6-10

Appendix A Stinger Intended Use A-1

User line interfaces	A-1
Network interfaces	A-1
Control module interfaces.....	A-2

Appendix B Cables and Connectors B-1

Diagnostic port and cable pinouts	B-1
Alarm input port pinouts	B-2
Ethernet interface specifications	B-2
10BaseT cables	B-3
100BaseT cables	B-3
LPM cable specifications.....	B-3
LPM two-wire cable specifications.....	B-3
LPM four-wire cable specifications	B-7

Appendix C Safety-Related Electrical, Physical, and Environmental Information C-1

- Electrical and electronic information C-1
 - Electronic and electrical specifications..... C-1
 - USOC jack and code information C-2
 - EMI class C-3
 - Minimum ground wire size C-3
- Physical specifications C-3
- Site specifications C-4
 - Operating environment C-4
 - Space requirements C-5
- Special requirements and recommendations for installation and maintenance C-5
 - Lifting requirements C-5

Index Index-1

Figures

Figure 1-1	The Stinger MS+ (front view)	1-2
Figure 1-2	The Stinger MS+ (rear view).....	1-2
Figure 1-3	Wrist grounding strap	1-5
Figure 1-4	Wrist strap plugged into a grounding jack	1-5
Figure 1-5	The Stinger MS+ (front view)	1-7
Figure 1-6	Model B control module interfaces.....	1-9
Figure 1-7	The Stinger MS+ (rear view).....	1-10
Figure 1-8	OC3-ATM trunk module fiber optic connection points	1-11
Figure 1-9	OC12-ATM trunk module fiber optic connection points	1-11
Figure 1-10	DS3-ATM or E3-ATM trunk module connection points.....	1-11
Figure 1-11	TRAM module connection points	1-12
Figure 1-12	Fast Ethernet trunk module connection points	1-12
Figure 2-1	Stinger MS+ chassis models for rack mounting	2-2
Figure 2-2	LPM 50-pin connector	2-4
Figure 2-3	Connecting to LPMs in a Stinger MS+ unit	2-4
Figure 2-4	Connecting an OC3-ATM trunk module	2-5
Figure 2-5	Connecting a DS3-ATM or E3-ATM trunk module	2-6
Figure 2-6	Stinger MS+ alarm module	2-7
Figure 2-7	Connecting to the alarm input port	2-9
Figure 3-1	Connecting the power filters.....	3-2
Figure 3-2	Control module status lights	3-3
Figure 4-1	Example of DSLAM operations	4-1
Figure 5-1	Serial management connection to a Stinger MS+.....	5-2
Figure 5-2	Ethernet connection.....	5-3
Figure 5-3	Backup administrative connection with a modem to the Stinger MS+ unit.....	5-4
Figure 5-4	Connection for internal modem.....	5-6
Figure 5-5	Default netmask for class C IP address	5-10
Figure 5-6	Local backbone router to be used as default route.....	5-13
Figure 6-1	Removing a control module.....	6-3
Figure 6-2	Installing a control module	6-4
Figure 6-3	Removing an LPM.....	6-7
Figure 6-4	Replacing the cooling module	6-9
Figure 6-5	Replacing a power filter	6-10
Figure 6-6	Replacing an alarm module	6-11
Figure B-1	USOC RJ-21X 50-pin connector	B-3

Tables

Table 1-1	Control module model designations and product codes	1-7
Table 1-2	Control module models and features	1-8
Table 3-1	Status lights on the control module	3-4
Table 3-2	Fan status light	3-5
Table 4-1	Location of configuration information	4-5
Table 5-1	IP address classes and number of network bits	5-10
Table 5-2	Decimal subnet masks and prefix lengths	5-11
Table B-1	Diagnostic port and cable pinouts	B-1
Table B-2	Alarm input pinouts	B-2
Table B-3	Single or lower connector pin assignments for two-wire connections	B-4
Table B-4	Upper connector pin assignments for two-wire connections	B-5
Table B-5	Middle connector pin assignments for two-wire connections (72-port LIM only)	B-6
Table B-6	Lower connector pin assignments for four-wire connections	B-7
Table B-7	Upper connector pin assignments for four-wire connections	B-8
Table C-1	Stinger electronic and electrical specifications	C-1
Table C-2	Stinger T1 module USOC jacks and codes	C-2
Table C-3	Stinger FS minimum ground wire sizes	C-3
Table C-4	Stinger MS+ physical specifications	C-3
Table C-5	Stinger MS+ site specifications	C-4

About This Guide

What is in this guide

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

- Physical installation of the Stinger chassis
- Connection of an administrative terminal to the control module
- Configuration of the control module for basic network connectivity

This guide also provides Stinger technical specifications and an operational overview of the Stinger. When you finish performing the instructions in this guide, the Stinger will be installed and you will be able to access it via a Telnet connection for further configuration.



Note You may also use this guide to configure the basic control module functions of the Stinger IP2000 control module. For detailed configuration information for the gigabit Ethernet interface, ATM configuration and aggregation, IGMP multicast, and other IP2000 capabilities, see the *Stinger IP2000 Configuration Guide*.

What you should know



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 C, “Safety-Related Electrical, Physical, and Environmental Information.”

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

Documentation conventions

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

Convention	Meaning
Monospace text	Represents text that appears on your computer’s screen, or that could appear on your computer’s screen.

Convention	Meaning
Boldface monospace text	Represents characters that you enter exactly as shown (unless the characters are also in <i>italics</i> —see <i>Italics</i> , below). If you could enter the characters but are not specifically instructed to, they do not appear in boldface.
<i>Italics</i>	Represent variable information. Do not enter the words themselves in the command. Enter the information they represent. In ordinary text, italics are used for titles of publications, for some terms that would otherwise be in quotation marks, and to show emphasis.
[]	Square brackets indicate an optional argument you might add to a command. To include such an argument, type only the information inside the brackets. Do not type the brackets unless they appear in boldface.
	Separates command choices that are mutually exclusive.
>	Points to the next level in the path to a parameter or menu item. The item that follows the angle bracket is one of the options that appear when you select the item that precedes the angle bracket.
Key1+Key2	Represents a combination keystroke. To enter a combination keystroke, press the first key and hold it down while you press one or more other keys. Release all the keys at the same time. (For example, Ctrl+H means hold down the Ctrl key and press the H key.)
Press Enter	Means press the Enter or Return key or its equivalent on your computer.
 Note	Introduces important additional information.
 Caution	Warns that a failure to follow the recommended procedure could result in loss of data or damage to equipment.
 Warning	Warns that a failure to take appropriate safety precautions could result in physical injury.
 Warning	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 IP2000 Configuration Guide*. For Stinger systems with the IP2000 control module, this guide describes how to integrate the system into the IP infrastructure. Topics include IP-routed switch-through ATM PVCs and RFC 2684 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

About This Guide

Stinger documentation set

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.

Preparing for the Installation



1

Stinger MS+ overview	1-1
Selecting an installation site	1-3
Required tools and equipment	1-4
Preventing static discharge damage	1-4
Unpacking the Stinger	1-6
Verifying the hardware configuration	1-6

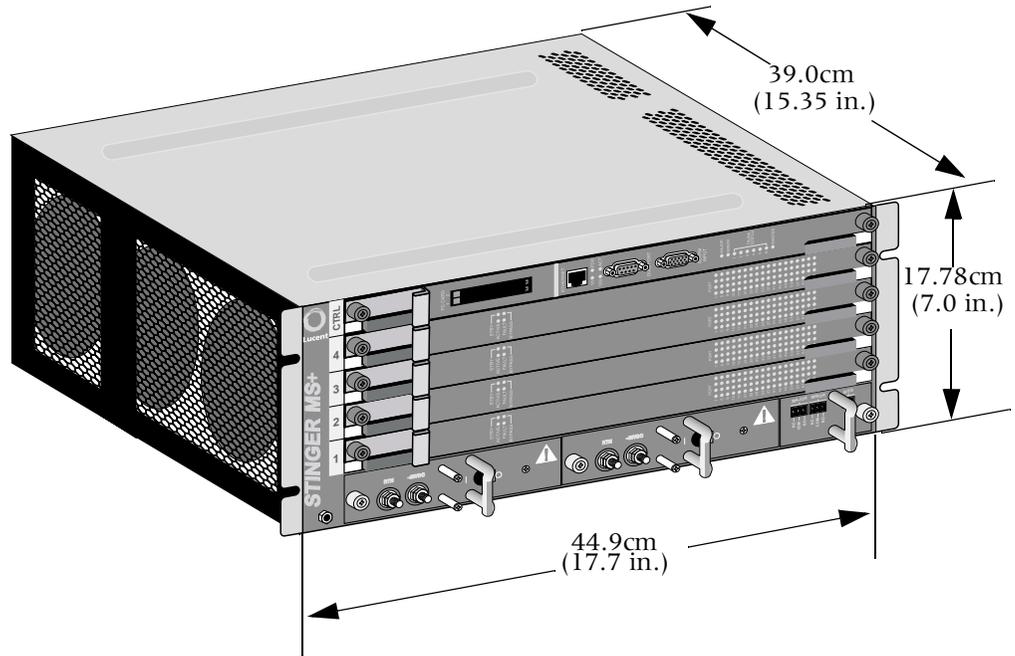
Stinger MS+ overview

The Stinger MS+ chassis is designed for use in a central office environment where rack space is limited, or the local user population does not require a larger Stinger FS+ or Stinger LS unit. The Stinger MS+ uses a mid-plane design, similar to the larger Stinger FS+, and can be equipped with the control modules, trunk modules, LIMs, and LPMs that are used in the Stinger FS+. (For more environmental information, see “Site specifications” on page C-4.)

The Stinger MS+ chassis

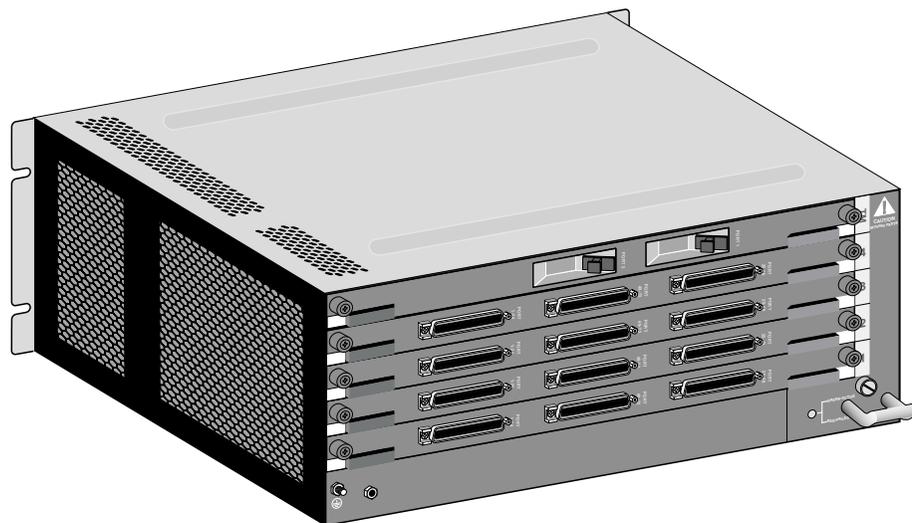
The Stinger MS+ chassis, shown in Figure 1-1, has horizontal slots in the front and rear that engage the midplane bus. The front of the Stinger MS+ chassis has five horizontal slots for modular plug-in components and two lower bays for redundant power filters. The horizontal slots accept up to four line interface modules (LIMs) and one control module in a designated slot. Unless LIMs with integrated line protection are used, each LIM must be matched by a line protection module in a corresponding slot in the rear of the chassis. A single trunk module can also be installed a designated slot in the rear of the chassis.

Figure 1-1. The Stinger MS+ (front view)



The rear of the Stinger MS+ has five horizontal slots for designated modular plug-in components. The horizontal slots accept up to four line protection modules (LPMs) and one trunk module. Access to the cooling module is also provided in the rear of the chassis.

Figure 1-2. The Stinger MS+ (rear view)



Modular plug-in components

The Stinger MS+ chassis supports the following modular plug-in components:

- The control module—A single control module is installed in the front of the chassis provides a TAOS management interface for configuration and management of the unit. The control module manages the operation of the Stinger MS+ unit and the traffic through the unit. It also maintains information about the configuration of the unit.
- LIMs—Up to four line interface modules (LIMs) are installed in the front of the chassis to provide the internal interfaces that are configured to provide service for individual DSL subscriber lines.
- Line protection modules (LPMs)—Up to four line protection modules (LPMs) are installed in the rear of the chassis to provide physical connection points for the DSL subscriber lines associated with the LIMs in the front of the chassis. The LPMs also provide protection for the unit from transient conditions on the subscriber lines.
- The trunk module—A single trunk module or trunk aggregation module (TRAM) is installed in the top slot in the back of the chassis. This can be any of the trunk modules that can be installed in the Stinger FS+. Including:
 - OC3-ATM trunk module
 - DS3-ATM trunk module
 - E3-ATM trunk module
 - OC3 TRAM module
 - OC12-ATM trunk module
 - Fast Ethernet trunk module
- Power filters—Two power filters, installed in the front of the chassis, provide redundant inputs for power to the Stinger MS+.
- The alarm module—A small module provides external connections for monitoring the major and minor alarm status of the unit. It also provides connections for an external BITS signal.
- The cooling module—A replaceable module contains fans that circulate air through the unit, and the electronics to control and monitor their operation.

Selecting an installation site

Before you choose a location for the Stinger unit, read and follow the site and electrical requirements defined in the *Edge Access and Broadband Access Safety and Compliance Guide*.

Select the setup location carefully. Keep in mind that the unit requires sufficient clearance for cabling, module replacement, and proper ventilation (see “Space requirements” on page C-5). You can rack-mount the Stinger MS+ in a standard equipment cabinet that is 19 inches or 23 inches (48.26cm or 58.42cm) wide (see “Mounting the unit” on page 2-1).

Required tools and equipment

To install and configure the Stinger hardware, you need the following tools and equipment:

- Console terminal connection to the control module's serial port to configure the unit
- ASCII or VT100 console terminal (Internal Lucent number: ITE 6938) or equivalent with the following setup:
 - 9600 bps
 - Direct connection
 - 8 data bits
 - No parity
 - 1 stop bit
 - No flow control
- RS-232 straight-through modem cable for connecting the console terminal or equivalent to the unit (Internal Lucent number: ITE-6801 List 22)
- Antistatic wrist strap (Internal Lucent number: R-4987C)
- Number 2 Phillips screwdriver
- 1/8-inch and 3/16-inch flathead screwdrivers
- 3/8-inch wrench or socket
- *(Optional)* Ethernet LAN connection for connecting the unit to the Ethernet (Internal Lucent number for the 7-foot (2.13m) cable: ITE-7131; for the 12-foot (3.67m) cable: ITE-7180)
- An SC fiber optic connector cleaner (Cletop, Optipop, or equivalent), if an OC3-ATM or OC12-ATM trunk module is being installed

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.

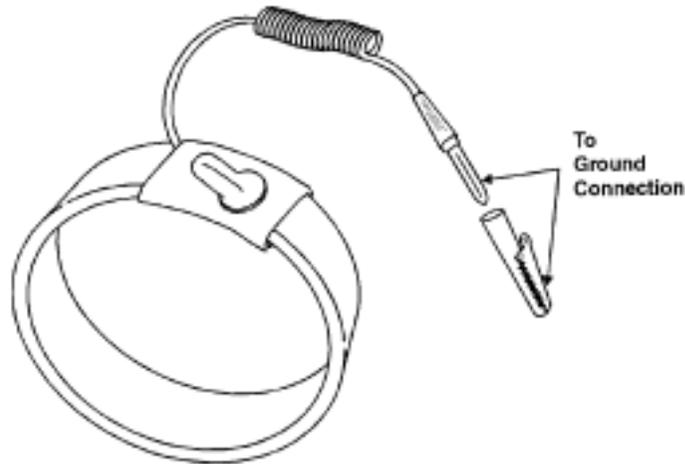
Use a wrist strap

To reduce the static potential on your body by proper grounding, wear an approved antistatic wrist strap (Figure 1-3) when installing, removing, or handling modules, or while handling any Lucent device containing semiconductor components.



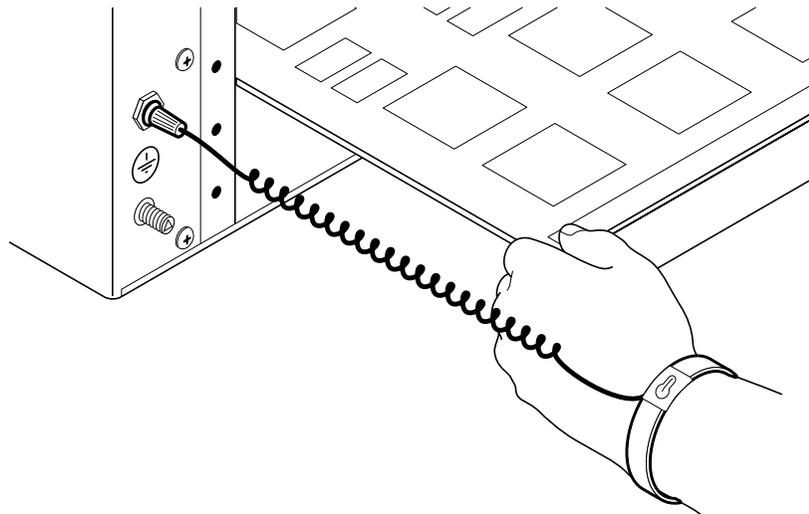
Caution Correct use of an approved antistatic wrist strap is the only reliable way to prevent damage to components by electrostatic discharge from your body

Figure 1-3. Wrist grounding strap



To minimize entanglement, right-handed people can wear the strap on the left hand. Plug the other end of the wrist strap into the grounding jack provided on most Lucent products, as shown in Figure 1-4.

Figure 1-4. 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

The Stinger unit is delivered in a protective shipping carton, in an electro-static protection bag, with all the ordered modules installed. Before you remove the Stinger unit from the shipping carton, check for damage. If you see any damage, follow the instructions described in your product warranty.

To avoid potential damage to the unit, Lucent Technologies recommends moving the unit to the installation site *before* unpacking it from the shipping carton.



Warning A Stinger MS+ with all components and modules installed weighs up to 66 pounds (30kg). To avoid potential injury, at least two people or a mechanical lift should be used for moving or rack-mounting a fully populated unit.

Verifying the hardware configuration

The Stinger MS+ has a midplane design that enables the control module and line interface modules in the front of a unit to connect to the line protection modules (LPMs) and trunk module in the back.

All units are equipped with a cooling module, power filters, and an alarm module. Other modules ordered with the unit are installed prior to shipment. Check the unit to verify that it is configured as ordered and to identify the connection points for power and data. The cable connectors for standard LPMs and the trunk module are located in the back of the chassis. Connections for the power filters, alarm monitoring, and BITS timing are located in the front of the chassis.

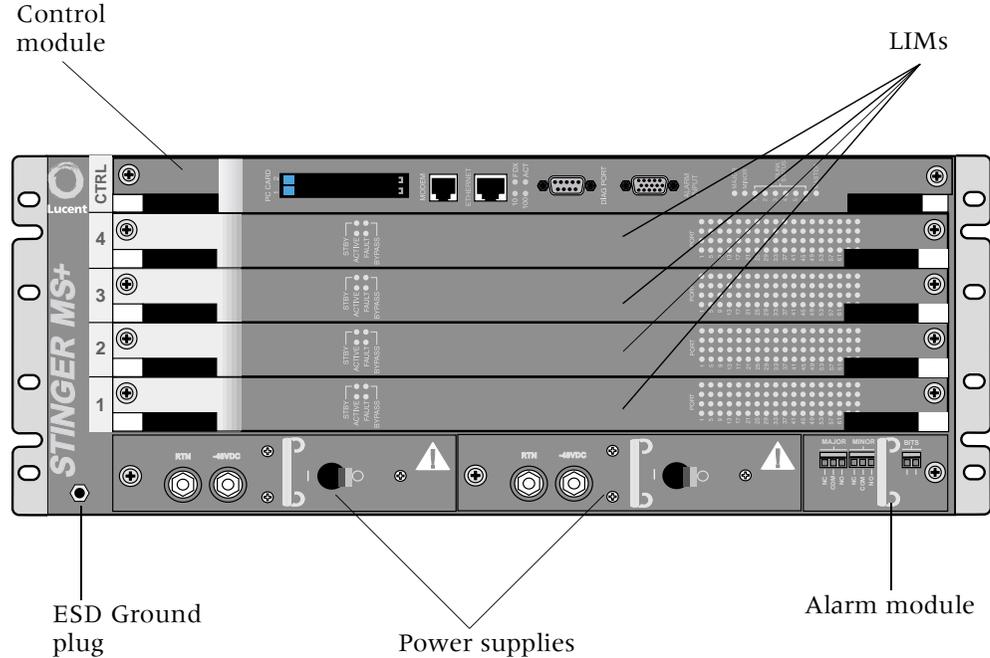


Caution Wear an antistatic wrist strap before handling any of the unit components. This can be connected to one of two electrostatic discharge (ESD) grounding jacks (banana jacks), located at the bottom left corner of the front of the unit (Figure 1-5) and in a similar location the rear of the unit (Figure 1-7).

Checking the front of the chassis

Figure 1-5 shows the front slots of a fully configured Stinger MS+.

Figure 1-5. The Stinger MS+ (front view)



The top slot in the front of the Stinger MS+, labeled CTRL, is reserved for the control module; it cannot be used for line interface modules (LIMs). To maintain the uniformity across the Stinger product line, this slot is logically referred to by the TAOS software as slot 8. Slots that are not occupied by modules must be masked with blank covers to ensure proper air flow through the unit.

Verifying the control module model

The Stinger MS+ unit supports three different revision 2 control modules, and a revision 2.1 control module.

The following table details the Stinger FS and Stinger FS+ control modules:

Table 1-1. Control module model designations and product codes

Model	Control module product code	Revision designation
A	STGR-CM-A	2.0
A-J	STGR-CM-A-J	2.0
B	STGR-CM-B	2.0
C	STGR-CM-C	2.0
E	STGR-CM-A2	2.1

Note Stinger units can also be equipped with the specialized IP2000 control module. Information specific to the IP2000 control module is found in the *Stinger IP2000 Configuration Guide*.

Table 1-2 shows the features provided by the revision 2 and 2.1 Stinger control modules.

Table 1-2. Control module models and features

STGR-CM-A	STGR-CM-A2	STGR-CM-B	STGR-CM-C	Features
Yes	Yes	Yes	Yes	Accepts seven alarm inputs from external devices to centralize alarm reporting.
Yes	Yes	Yes	Yes	Memory increased to 128Mb of internal synchronous dynamic RAM (SDRAM) and 32Mb of nonvolatile RAM on a PCMCIA card.
No	No	Yes	Yes	Contains an internal 56Kbps modem for dial-in remote administration.
No	No	No	Yes	Contains an internal Stratum 3 clock.

Note The `version` command displays information about the version and type of control module installed in a Stinger unit. For details, see “Verifying software and control module versions” on page 4-5.

Control module support

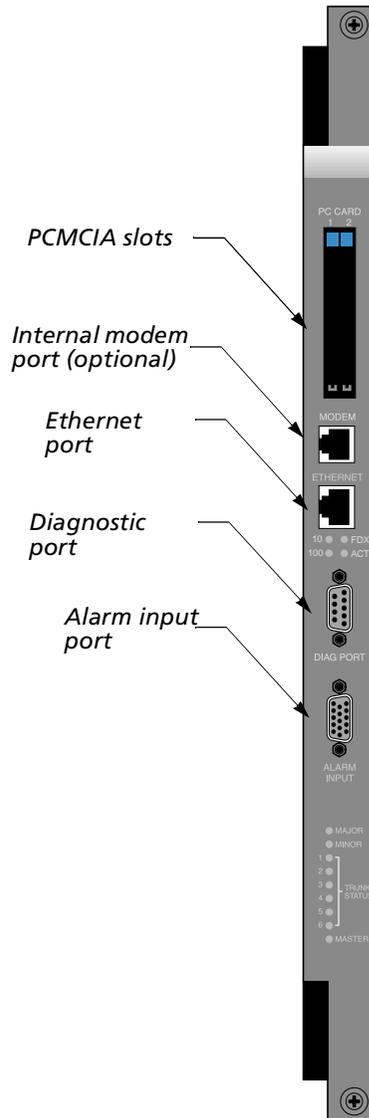
TAOS 9.4-185.2 introduced support for a Model E version of the control module (STGR-CM-A2). The Model E control module utilizes enhanced chip-sets and replaces the older Model A control module. The Model E control module is identified in TAOS as hardware revision 2.1. The Stinger Model A control module (STGR-CM-A), introduced with TAOS 9.1-142.1, is also supported by the current version of TAOS.

Control module interfaces

Figure 1-6 shows the location of the modem port, Ethernet port, serial diagnostic port, alarm input port, and Personal Computer Memory Card International Association (PCMCIA) slots on a model B control module.

Note See the *Stinger IP2000 Configuration Guide* for information about the specialized interfaces on the IP2000 control module.

Figure 1-6. Model B control module interfaces



The control module comes with onboard flash memory, and each PCMCIA card provides its own additional memory. The PCMCIA cards store the software and the configuration information for all modules. The system configuration is also stored in the onboard nonvolatile RAM (NVRAM).

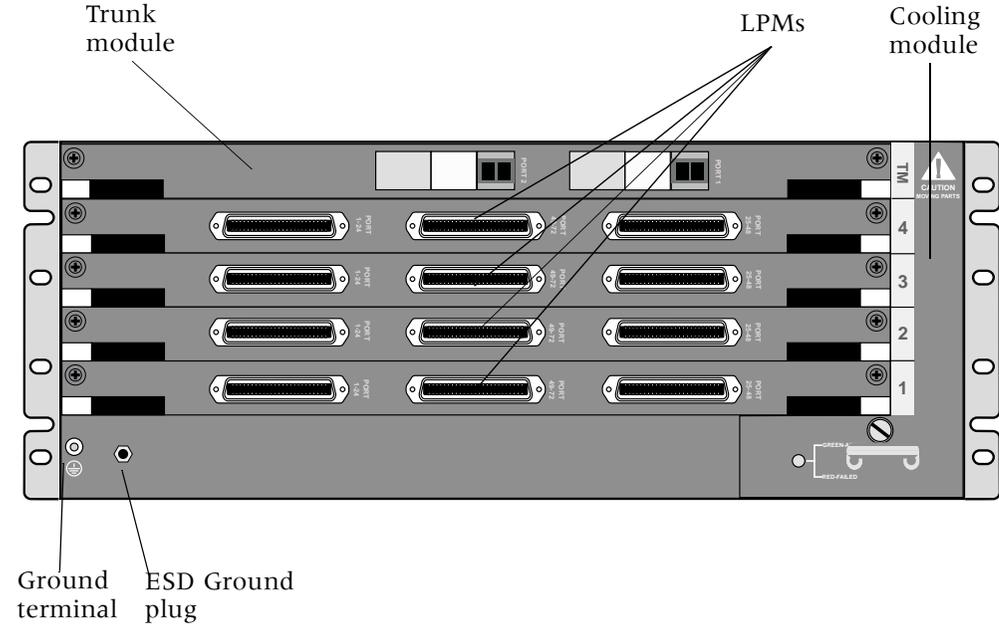
Checking the LIMs

Several line interface modules (LIMs) are available to provide different types of line service. Line interface modules are installed in slots 1 through 4 in the front of the chassis. All LIMs that do not contain integrated protection circuitry, connect to their respective line facilities through an associated line protection module (LPM) located in the slot behind the LIM. Verify that the correct number of LIMs are installed. Specific hardware and configuration details for each type of LIM are contained in the matching LIM guide for that module.

Checking the of the chassis

Figure 1-7 shows the back of the Stinger MS+ chassis.

Figure 1-7. The Stinger MS+ (rear view)



Unless LIMs with integrated protection circuitry are used, each LIM installed in the unit must have a corresponding LPM installed in the matching slot at the back of the unit. The top slot in the back of the Stinger MS+ is reserved for a trunk module; it cannot be used for an LPM. Slots that are not occupied by modules must be masked with blank covers to ensure proper air flow through the unit.

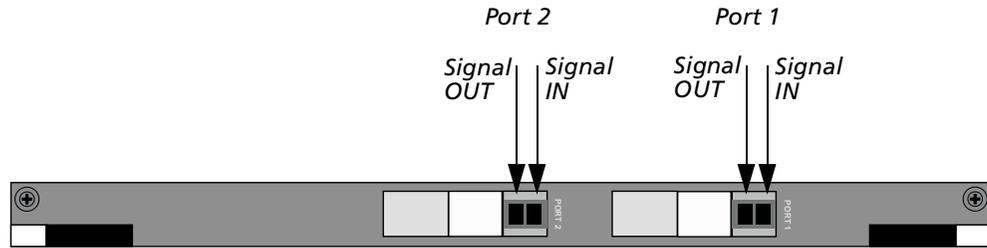
Verifying the trunk module

The top slot in the rear of the Stinger MS+ chassis can contain a trunk module. The trunk module supports connection to either optical or copper media, depending on the type of module supplied. This top rear slot is labeled, "TM." To maintain the uniformity across the Stinger product line, this slot is logically referred to by the TAOS software as slot 17.

OC3-ATM trunk modules

Figure 1-8 shows the location of the optical fiber connections on an OC3-ATM trunk module.

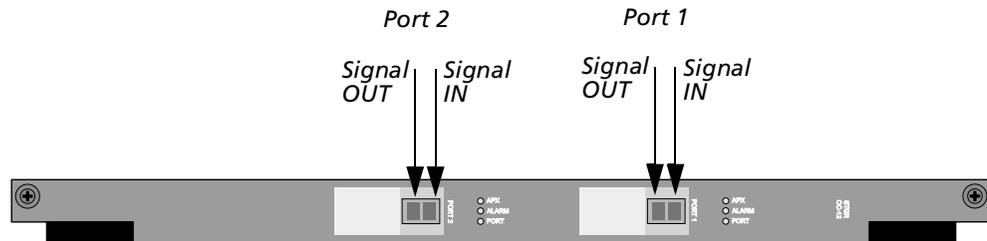
Figure 1-8. OC3-ATM trunk module fiber optic connection points



OC12-ATM trunk modules

Figure 1-9 shows the location of the optical fiber connections on an OC12-ATM trunk module.

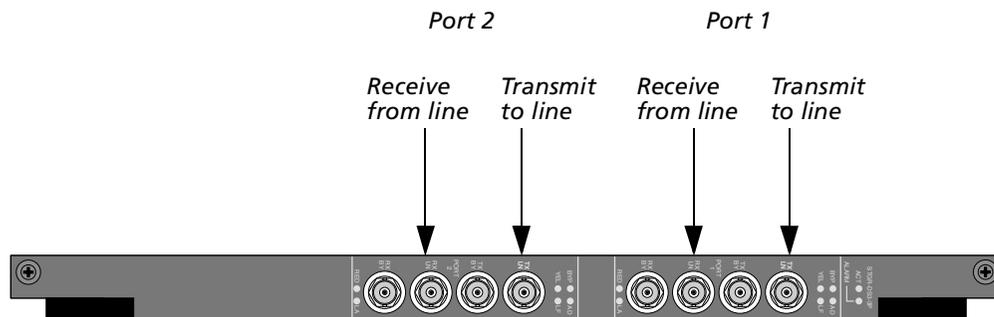
Figure 1-9. OC12-ATM trunk module fiber optic connection points



DS3-ATM and E3-ATM trunk modules

Figure 1-10 shows the location of the coaxial connections on a DS3-ATM or E3-ATM trunk module.

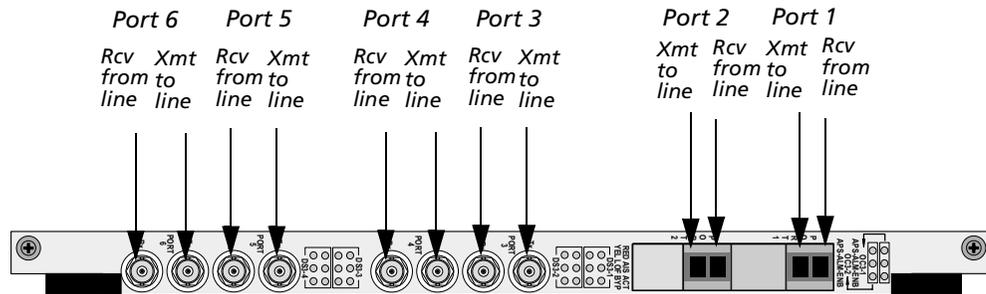
Figure 1-10. DS3-ATM or E3-ATM trunk module connection points



TRAM modules

Figure 1-11 shows the location of the DS3 or E3 coaxial connections and the OC3 optical fiber connections on a TRAM module. TRAM modules are also available that support only OC3 connections. See the *Stinger Trunk Aggregation Module (TRAM) Guide* for details.

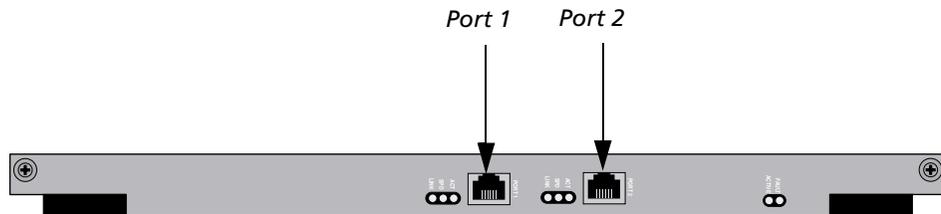
Figure 1-11. TRAM module connection points



Fast Ethernet Trunk module

Figure 1-12 shows the location of the two RJ-45 10Base-T/100Base-T Ethernet connectors. See the *Stinger Fast Ethernet Trunk Configuration Guide* for details.

Figure 1-12. Fast Ethernet trunk module connection points



Checking the LPMs

Several line protection modules (LPMs) are available to provide the correct number or connections for their associated LIMs. Line protection modules are installed in slots 1 through 4 in the back of the chassis. All LIMs connect to their respective line facilities through an associated line protection module. Verify that the correct number of LPMs are installed. Specific hardware details for each type of LPM are contained in the *Stinger Line Protection Module (LPM) Guide*.

Installing a Stinger MS+



2

Before you begin	2-1
Mounting the unit	2-1
Connecting cables to a Stinger unit	2-3
Control module connections	2-6
System clocking	2-7
Alarm monitoring	2-7

Before you begin

Verify that you have completed the following tasks:

- Selected the installation site
- Unpacked the Stinger unit
- Gathered the tools and equipment needed for installation
- Checked the module configuration in the unit



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

Mounting the unit

Stinger MS+ units are delivered with mounting brackets installed on the chassis. Three Models can be ordered with brackets for different rack-mounting requirements.

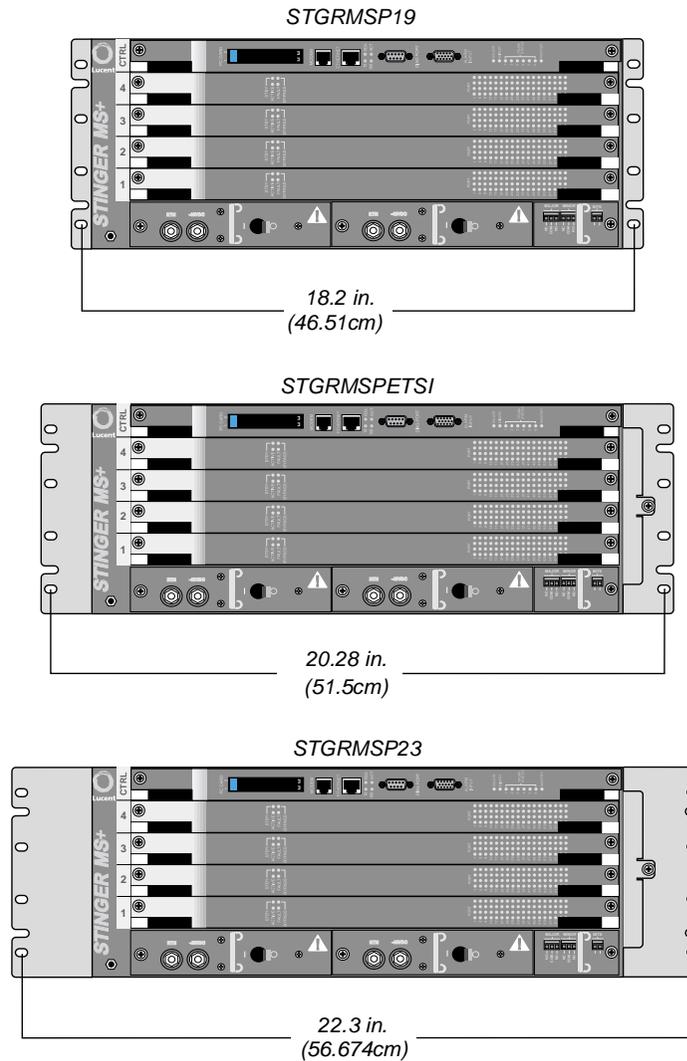
- STGRMSP19—for mounting in a 19-inch (48.26cm) equipment rack
- STGRMSPETSI—for mounting in a a 51.5cm (20.28-inch) European Telecommunications Standards Institute (ETSI) equipment rack
- STGRMSP23— for mounting in a a 23-inch (58.42cm) equipment rack



Note The rack-mount spacing meets IEC 297-2 and ANSI/EIA-RS-310-C standards.

Figure 2-1 displays the available Stinger MS+ models with their mounting brackets.

Figure 2-1. Stinger MS+ chassis models for rack mounting



The procedure for installing the unit into a cabinet requires that you supply a minimum of four cross-head screws of the appropriate size to support the unit in the cabinet.



Warning Installing a rack-mounting a unit with all components installed requires more than one installer. A fully populated Stinger MS+ weighs up to 30kg (66 pounds).

To rack-mount a Stinger unit into an equipment cabinet:

- 1** Carefully raise the unit to the appropriate installation height.
- 2** Align the screw holes on the mounting bracket with the screw holes on the equipment cabinet.
- 3** Using a number 2 Phillips screwdriver, install cross-head screws of the appropriate size through the mount bracket on the unit into the mounting bracket on the equipment cabinet.

Connecting cables to a Stinger unit

Once the Stinger unit is set up in the desired location, connect the unit to the local facilities or to its frame access points by attaching the appropriate cables to the LPMs. Connect the Stinger unit to the ATM network by attaching the copper or fiber connections to the trunk modules.

Connecting to the LPMs

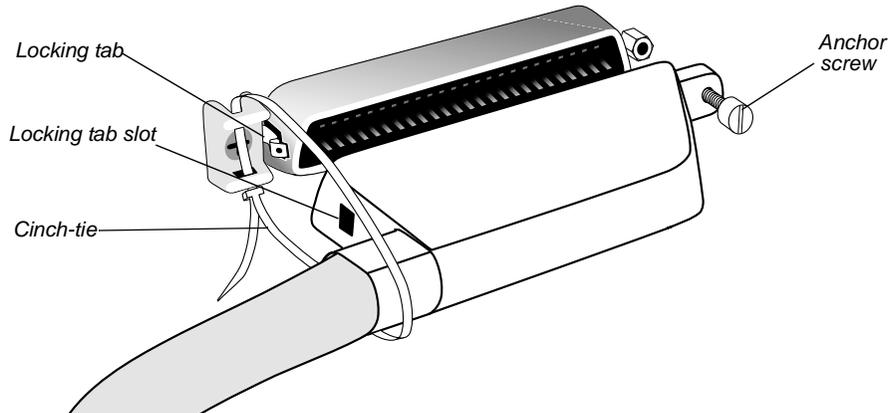
LPMs provide physical connections for the DSL lines supported by their associated LIMs. LPMs are available with 50-pin connectors that support 24, 48, or 72 port LIMs. An LPM is also available with 64-pin connectors that contains internal splitters to support up to 48 ports of ADSL-over-POTS service. For specific information about the connectors, pinouts, and cables associated with your LPMs, see the *Stinger Line Protection Module (LPM) Guide*.

Securing the connectors

Connections to 50-pin connectors can be secured by three mechanisms shown in Figure 2-2. It is recommended that you use these mechanisms to make the connections as secure as possible.

- An anchor screw on the far end of the connector can be screwed into a fitting on the LPM. Some connectors can use anchor screws at both ends of the connector.
- A locking tab under the cable side of the connector automatically secures the connector upon installation.
- A nylon cinch-tie can be used secure the cable end of the connector to a tie-down fitting on the LPM. If the connectors you are using have a slot to accept the connector locking tab, use of a nylon cinch-tie is optional.

Figure 2-2. LPM 50-pin connector



Note Connections for 64-pin connectors are secured by anchor screws on the top and bottom of each connector.

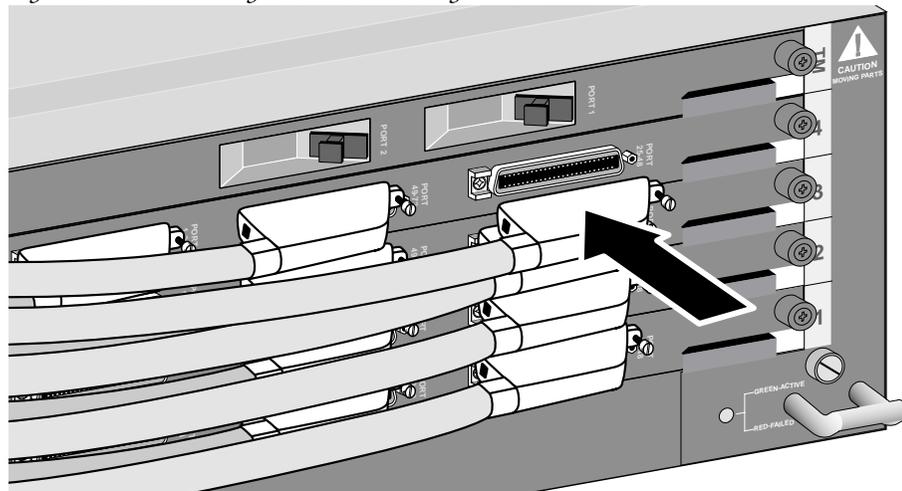
Connecting the subscriber lines

In the rear of the chassis, cables are routed toward the left, as shown in Figure 2-3, to allow for removal and replacement of the cooling module.

Use the following procedure to connect the cables to the line ports of an LPM with 50-pin RJ-21 connectors, installed in the Stinger MS+ unit:

- 1 Carefully insert the on the line connections of the LPMs in the Stinger MS+ unit, as shown in Figure 2-3.

Figure 2-3. Connecting to LPMs in a Stinger MS+ unit



Note See Figure 2-2 for details of the connector locking tab, anchor screw, and cable cinch-tie.

- 2 Push the cable connectors onto the chassis connectors until each locking tab is engaged.
- 3 Tighten the anchor screw on each cable connector.

- 4 Secure the cable connectors to the chassis with a cable cinch-tie around the connectors and through the security fixtures on the left side of the line connectors on the chassis. (Optional, if your cable connectors have a slot to engage the locking tab.)

Connecting the trunk modules

The trunk module cables are either coaxial (for DS3 or E3) or fiber optic (for OC-3/STM-1 optical or OC-12/STM-4 optical).

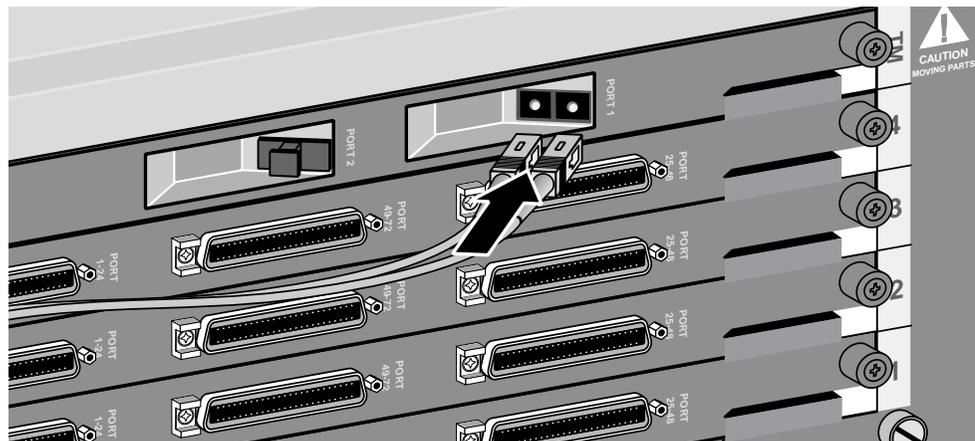
Optical trunk module connections

The OC3-ATM and OC12-ATM trunk modules require duplex SC fiber optic cable. Bind excess cable lengths in a figure-eight pattern. Do not wind excess cable into circular coils.

Note Clean any fiber optic cables prior to connecting them.

To connect the cables to an OC3-ATM or OC12-ATM trunk module, carefully insert the head of each cable into a connector on the trunk module. An example of this connection on an OC3-ATM trunk module is shown in Figure 2-4.

Figure 2-4. Connecting an OC3-ATM trunk module



DS3-ATM or E3-ATM trunk module connections

Connect the DS3 or E3 line to the RX LN and TX LN connectors on a DS3-ATM or E3-ATM trunk module, using two 75-ohm coaxial cables (RG 59/U).

To configure a redundant DS3 or E3 connection, connect the BY connectors on the primary trunk module to the LN connectors on the backup trunk module as shown in Figure 2-5. If the primary port fails, the traffic is switched over to the secondary module's port.

Figure 2-5. Connecting a DS3-ATM or E3-ATM trunk module



Inform your service provider that the equipment is connected, so they can activate the line.

Control module connections

The control module provides the following ports and connections:

needed to connect the Stinger unit to a workstation or a console. See Appendix B, “Cables and Connectors,” for console cable pinouts.

Each control module supports three types of network management connections for communication with the Stinger unit:

- A female DB-9 serial port, labeled DIAG PORT. This connector is used with an RS-232 shielded straight-through cable (ITE6801), to a terminal for basic configuration. See “Serial connection to a console” on page 5-2, for details about this connection.

It can also be connected to an external modem for dial-in administrative access. See “Backup management with an external modem” on page 5-3, for details of this connection.

- A female DB-15 connector labeled ALARM INPUT. This connector provides access for connecting of up to 7 pairs of wires that monitor the alarm condition of up to 7 external devices. See “Connecting a Stinger unit to monitor the alarm status of other devices” on page 2-8, for details of this connection.
- An RJ-11 jack that provides a connection for an external analog telephone line to an optional internal modem. See “Backup management with an internal modem” on page 5-5, for details of this connection.



Note The optional internal modem is only available on Revision 2 control module models B and C.

- An RJ-45 connector that provides a 10BaseT or 100BaseT Ethernet network connection through unshielded twisted pair (UTP) cable. This connection can provide access to an administrative network, and is not designed for end-user data. See “Network connection to a workstation console” on page 5-2, for details of this connection.

System clocking

The control module has four possible timing sources:

- External. The Stinger unit can accept timing from a T1 line, or a building interoffice timing source (BITS) clock, connected to the alarm module BITS connectors. (See Figure 2-6.)
- Trunk. The Stinger unit can accept timing from an OC3, DS3, or E3 line clock.
- LIMs. The Stinger unit can accept timing from an ADSL or SDSL line clock.
- Internal clock source. If the selected clock sources fail, the system is automatically reconfigured so that it is synchronized with the control module's internal clock.

The T1 or BITS timing inputs work with DS1 timing references that comply with the ANSI T1.102 standard. The system timing is configured through the TAOS command-line interface. For detailed information about the profile and options that configure system clocking, see "Configuring system clocking" on page 5-14.

Alarm monitoring

There are two groups of alarm connections on the Stinger MS+. One group, on the chassis alarm module, communicates the major or minor alarm status of the Stinger MS+ unit to an external system or status indicator. The Stinger MS+ can use another group of connections on a revision 2 or revision 2.1 control module to monitor and report the alarm status of up to seven other external systems.

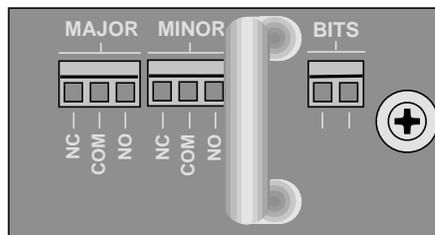
Connecting to monitor Stinger unit alarm status

The alarm module on the front of the unit, in the lower right corner, contains three sets of connectors for connecting the following:

- Major alarms
- Minor alarms
- External BITS clock

The alarm module along with its BITS and alarm connections is shown in Figure 2-6.

Figure 2-6. Stinger MS+ alarm module



The alarm module contains alarm terminals for monitoring the status of the Stinger MS+ unit. The Stinger MS+ can monitor itself for major and minor alarm conditions and illuminate appropriate status lights on the control module. In addition, you can connect audio and visual alarms to the normally open or normally closed alarm relay contracts of the alarm terminals to remotely monitor the unit for these conditions.

The alarm-relay contacts operate during loss of power, during hardware failure, or whenever the Stinger unit is being reset, such as during its power-on self test (POST). A normally closed (NC) or normally opened (NO) contact is used in combination with the common (COM) contact to monitor the normally opened or normally closed operation of the major or minor alarm relays. (See Figure 2-6.)

The gauge of the wire you use to connect to the Stinger alarm relay must be based on the current flow of the circuit that the relay is attached to and the capacity of the alarm relay. Because the Stinger alarm relay can carry a maximum of 2 amps, 18 AWG to 20 AWG (0.8mm² to 0.5mm²) wire is adequate.

To connect a remote alarm:

- 1** Locate the appropriate terminal for the alarm connection you want to make.
- 2** Using a 1/8-inch flathead screwdriver, loosen the screws on the Major and Minor normally opened (NO) or normally closed (NC) and common (COM) terminals.
- 3** Using 18AWG to 20AWG (0.8mm² to 0.5mm²) solid or stranded wire, strip the ends of the wire approximately 1/4 inch (6.35 mm).
- 4** Insert the wire leads into the appropriate positive terminal connector and its return.
- 5** Using a 1/8-inch flathead screwdriver, tighten the screws on the positive and return terminals to secure the leads.

Connecting a Stinger unit to monitor the alarm status of other devices

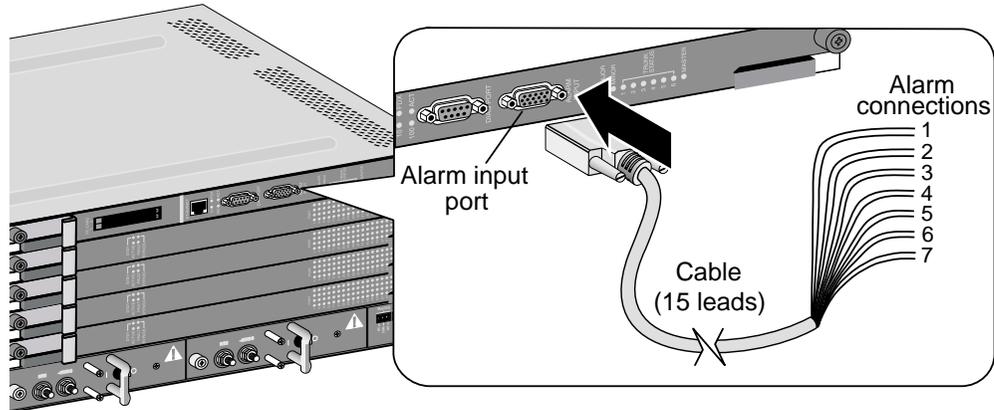
Revision 2 and revision 2.1 control modules have a DB-15 connector that can accept connections to monitor the alarm status of up to seven external devices. The connection for each external device consists of a pair of 24-gauge to 28-gauge connectors. One connector supplies ground, and the other senses 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 pinout arrangement of these connectors on the DB-15 connector, see “Alarm input port pinouts” on page B-2.

Connections from the control module

To connect to a remote device:

- 1** Using a male DB-15 connector, connect a 15-lead cable to the ALARM INPUT connector of the control module. One lead is unused.
- 2** Run one pair of leads to the alarm connectors of each remote device to be monitored by the Stinger unit, as shown in Figure 2-7.

Figure 2-7. Connecting to the alarm input port



The alarm relays of external devices can be either normally opened or normally closed. The Stinger unit can be configured to sense an alarm condition for the opening of a normally closed relay, or the closing of a normally open relay. For information on the configuration of these parameters, see the information about SNMP alarm support for input relay alarms in the *Stinger Administration Guide*.

What's next

When you finish physically installing the Stinger unit you can proceed to Chapter 3, "Determining the Operating Status."

Determining the Operating Status

3

Before you begin	3-1
Connecting power to a Stinger unit	3-1
Turning on power to a Stinger unit	3-2
Status lights	3-3

Before you begin

Before you begin, verify that the following tasks are complete:

- Set up the Stinger hardware (as either a free-standing or rack-mounted unit)
- Connected cables and console terminal to the Stinger unit
- Set up the workstation to configure the Stinger unit
- Connected the workstation to the Stinger unit
- (Optional) Connected the system clock source
- (Optional) Connected the remote alarms

Connecting power to a Stinger unit



Caution Before connecting power, see the *Edge Access and Broadband Access Safety and Compliance Guide* for safety instructions and circuit regulatory information.



Warning Verify that the power is off or disconnected at the source before beginning this procedure.

To connect the unit to dc power:

- 1 Verify that the correct power source is available for the Stinger unit.
- 2 Verify that the dc power cables comply with national standards and specifications as described in IEC 60950 and are terminated in number 10 ring lugs.
- 3 Figure 3-1 shows how to connect power to the Stinger unit. Be sure to attach a power cable to each set of power connectors as follows. Both power cables must be connected at all times when the unit is in operation.
 - Verify that the power switch on the power filters is set to the OFF position.
 - Locate the number 10 studs on the back of the unit.

Determining the Operating Status

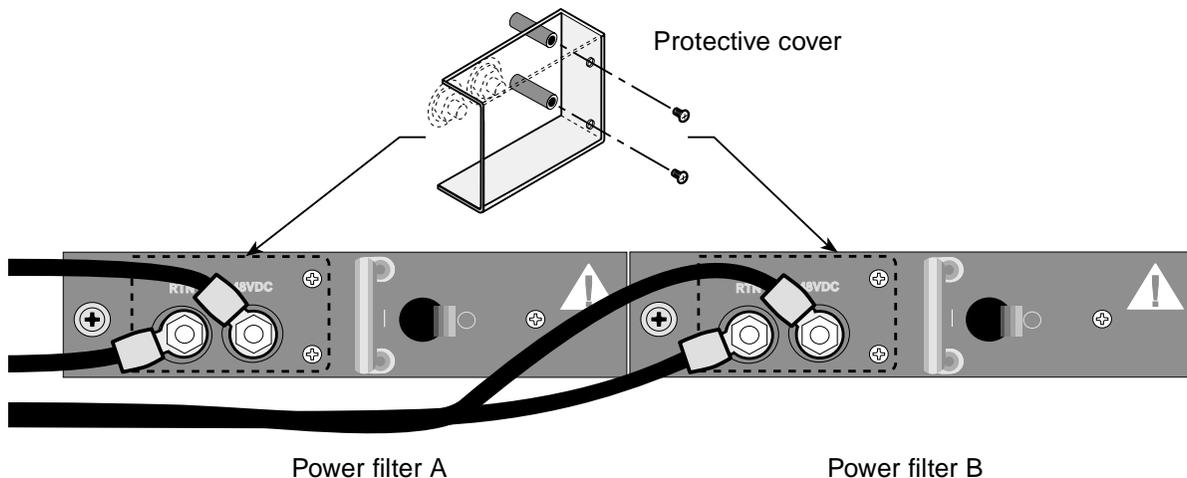
Turning on power to a Stinger unit

- Using a number 2 Phillips screwdriver, remove the two screws that secure the protective cover over the studs. Then remove the protective cover.
- Using a 3/8-inch wrench or socket, remove the top locking nut from each of the two studs (labeled -48V and RTN). Do not remove the bottom locking nut.
- Install the ring lugs onto the appropriate posts.

Note You can optionally ground the chassis to the enclosure by attaching dual mount ground lugs to the ground terminal on the back of the unit. Do not remove the ground lugs.

- Reinstall the locking nut onto each post, then use a 3/8-inch wrench or socket to tighten the nut.
- Reinstall the protective cover with the two screws.

Figure 3-1. Connecting the power filters



Turning on power to a Stinger unit



Caution Do not turn on power to a Stinger unit without a control module installed in the chassis. Starting up a unit with no control module installed can damage hardware components.

To turn on power to the unit, press the power switch on each power filter to the ON (|) position.

All Stinger status lights, except the MASTER light, momentarily turn ON just after startup.

On the control module, the MAJOR status light turns ON at startup. It then starts blinking slowly while the control module runs its POST in the boot loader. It continues to blink while the control module loads its operational code from the PCMCIA flash card. If the control module successfully loads its operational image from the PCMCIA flash card and again passes POST, the MAJOR status light turns OFF. If the MAJOR status light continues to blink, it indicates a failure.

After startup, all six TRUNK STATUS lights and the MINOR status light turn OFF. Then after the system comes up, each light monitors a particular status as described in the next section.

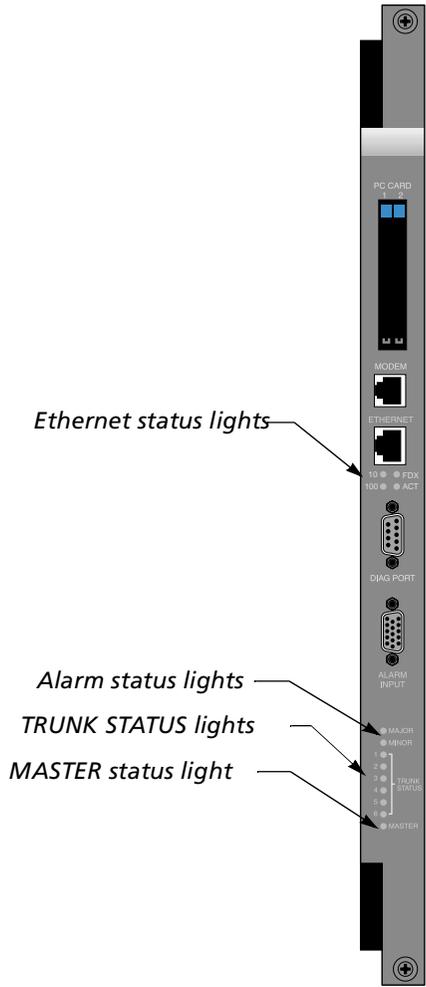
Status lights

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

Control module status lights

Figure 3-2 shows the locations of the control module status lights.

Figure 3-2. Control module status lights



All control module status lights except the MASTER light momentarily turn ON just after startup, and all six TRUNK STATUS lights turn OFF. After the system starts up, each light monitors a state as described in Table 3-1.

Determining the Operating Status

Status lights

The status lights in the upper portion of the control module indicate the status of the Ethernet interface. The status lights at the bottom of the control module indicate the status of the control module and the trunk modules.



Note The upper portion of the control module is on the left side, and the lower portion of the control module is on the right side, when the control module is installed in the MS+ chassis.

Table 3-1. Status lights on the control module

Status light	Color	Condition	Indicates
10	Green	ON	10BaseT Ethernet activity has been detected.
100	Green	ON	100BaseT Ethernet activity has been detected.
FDX	Green	ON	Full-duplex mode is active.
ACT	Green	ON	Activity detected on the Ethernet interface.
MAJOR	Amber	ON or blinking	<p>The control module has detected a major alarm. For information about configuring major alarms, see the <i>Stinger Administration Guide</i>.</p> <p>The MAJOR status light turns ON at startup. It then starts blinking slowly while the control module runs its POST in the boot loader. It continues to blink while the control module loads its operational code from the PCMCIA flash card. If the control module successfully loads its operational image from the PCMCIA flash card and again passes POST, the MAJOR status light turns OFF. If the MAJOR status light continues to blink, it indicates a failure.</p>
MINOR	Amber	ON or blinking	<p>The control module has detected a minor alarm. For information about configuring minor alarms, see the <i>Stinger Administration Guide</i>.</p> <p>The MINOR status light is ON at startup. It remains ON until the control module passes all POST tests. It then stays OFF until a minor alarm occurs.</p> <p>If the control module fails POST, the MINOR status light remains ON.</p>

Table 3-1. Status lights on the control module (continued)

Status light	Color	Condition	Indicates
TRUNK STATUS	Green	ON	The six TRUNK STATUS lights indicate the status of trunk module ports attached through the backplane to the control module. Only the first 3 lights are used on Stinger MS+ units to refer to ports 1, 2, and 3, if present, on the trunk module in the rear of the chassis. If a TRUNK STATUS light is ON, the port is fully operational.
TRUNK STATUS	Green	blinking	The port is installed but not operating.
TRUNK STATUS	Green	OFF	The trunk module port corresponding to the light is not present on the installed trunk module, or the trunk module is not installed.
MASTER	Green	ON	Indicates that the control module is the master (primary). On the single control module in the Stinger MS+ unit, this light is always lit.

LIM status lights

For detailed information about the status lights on each LIM and their expected behavior, see the module guide for the specific LIM in question.

Trunk module status lights

For detailed information about the status lights on each trunk module and their expected behavior, see the module guide for the specific trunk module in question.

Fan status light

In the rear of the chassis, on the fan unit, a status light indicates the operating status of the fans. The status indicated by this light is described in Table 3-2.

Table 3-2. Fan status light

Status light color	Indicates
Green	The fan has power and is operating normally.
Red	The fan is in a fault state.

What's next

Once the hardware installation is complete and the Stinger unit is powered up, you can begin basic configuration as described in the following chapters, or download a previous software configuration.

Stinger Operational Overview

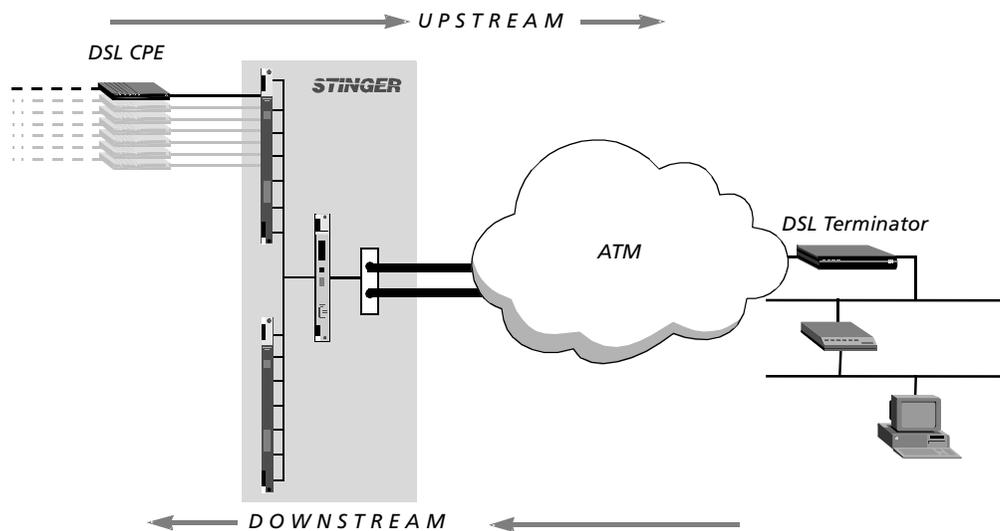
4

Stinger MS+ operation as a DSL access multiplexer	4-1
Stinger ATM switching overview	4-2
Stinger configuration overview	4-2
Stinger management features	4-3

Stinger MS+ operation as a DSL access multiplexer

A Stinger MS+ unit typically operates as an ATM switch-through digital subscriber line access multiplexer (DSLAM). It switches data from multiple xDSL subscribers onto a high-speed ATM backbone. Figure 4-1 shows this type of operation.

Figure 4-1. Example of DSLAM operations



Note A Stinger MS+ unit equipped with an IP2000 control module can also process IP traffic. With the IP2000, the unit typically routes IP traffic from subscribers to the IP infrastructure across a Gigabit Ethernet interface, and forwards IP multicast video transmissions to xDSL multicast clients. Configuration for this type of operation is described in the *Stinger IP2000 Configuration Guide*.

Stinger ATM switching overview

A Stinger unit receives ATM cells on a link that is identified by a pair of unique attributes. These attributes are known as the virtual path identifier (VPI) and the virtual channel identifier (VCI). The Stinger unit switches the cells from an incoming link to an outgoing link, based on the VPI and VCI attributes of each link. The connection between these links is usually a static configuration entered by an administrator, although a more dynamic method of forming link connections, known as a private network-to-network interface (PNNI), might be used.

This guide covers only basic installation information and configuration of the control module. More detailed information about configuring the unit to support ATM traffic can be found in the *Stinger ATM Configuration Guide* and the *Stinger Private Network-to-Network Interface (PNNI) Supplement*.

Stinger configuration overview

Before you configure a Stinger MS+ unit, create a diagram that illustrates how the unit will interoperate with your current network configuration. Creating a comprehensive network diagram helps prevent problems during installation and configuration, and can help in troubleshooting any problems later.

Stinger MS+ configuration tasks include the following:

- Configuring the control module
- Configuring the DSL line interface modules (LIMs)
- Configuring the trunk module
- Defining ATM traffic contracts
- Configuring connections, either locally or through RADIUS

Control module configuration

The control module has an RS-232 serial port (labeled DIAG PORT) and a 10/100BaseT Ethernet port. The serial port is for system management from a local workstation. It is also the standard port for error output, stack traces, and messages in the event of a system crash. Until you have configured an IP address on the Ethernet interface of the control module, you must use a local terminal or workstation connected to the serial port of the control module to configure the Stinger MS+ unit. There is no other way to log into the unit to perform the initial configuration.

The Ethernet port on the control module is intended for light data and management traffic. Once you have assigned an IP address, you can Telnet into the unit from a local host and download configuration files from a TFTP server to the Stinger system.

A Stinger unit has a range of options for configuring IP and for protecting the unit from unauthorized administrative access.

Line interface module (LIM) configuration

A Stinger unit supports any combination of ADSL, HDSL2, SHDSL, IDSL, or SDSL ATM modules. Each port on a LIM has a variety of configuration options, including line rates and bandwidth. The way you configure each line depends on your connectivity needs.

A T1 or E1 LIM is also available to provide up to 8 or 24 DS1 or E1 lines for traffic exiting the network (egress traffic), when the bandwidth of a DS3, E3, or OC3 trunk module is not needed.

For specific information about LIM configuration, see the module guide for the desired LIM.

Trunk module configuration

The Stinger MS+ unit supports a single trunk module or TRAM modules. Trunk modules with OC3-ATM, DS3-ATM, or E3-ATM interfaces are supported. OC3 TRAM modules with DS3, E3, or only OC3 interfaces are also supported. You can set up the unit to use the full trunk-side bandwidth actively, or you can designate one or two of the trunk ports as spares, to be used only if another trunk port fails.

The trunk module can connect the Stinger unit to another ATM switch. The line configuration includes settings that must match between the local and far-end switch interfaces.

For specific information about trunk module configuration, see the module guide for the desired trunk module.

System clocking modes

The Stinger unit requires a clock source for its timing subsystem. By default, it uses a built-in 8kHz clock on the control module as its timing source. You can configure the system to take its clock source from a trunk port or from an external building interoffice timing source (BITS) clock connected to the Stinger unit.

For detailed configuration information, see “Configuring system clocking” on page 5-14.

Stinger management features

To enable you to configure the system and monitor its activity, Stinger units support profiles, commands, and status windows in the command-line interface. Stinger units also support SNMP management, RADIUS profiles, and the ability to upload (back up) and download software and configuration files over TFTP or serial connections.

A Stinger system provides several permission levels to control the management and configuration functions that are accessible in the command-line interface. For information about User profiles and other management features, see the *Stinger Administration Guide*.

For an introduction to the command-line interface and its shortcuts, see the *The TAOS Command-Line Interface Guide*.

Using the command-line interface

The Stinger command-line interface provides access to commands, profiles, and status windows. You must use the command-line interface to provide the initial system and IP configuration for the unit, although you can choose to perform subsequent configuration tasks remotely through a Telnet session or SNMP, or by downloading configuration files using TFTP.

Onboard flash memory and software updates

You can perform software upgrades of the onboard flash memory in the field. You upgrade the Stinger unit by accessing it locally through its serial (DIAG) port and downloading software upgrades from a TFTP server. For details, see the *Stinger Administration Guide*.

SNMP support

In addition to managing a Stinger unit by means of the command-line interface, you can manage the unit by using an SNMP management station such as the NavisAccess™ product. A Stinger unit can generate SNMP traps (notifications) to indicate alarm conditions, and it relies on SNMP community strings to implement SNMP security.

For information about using SNMP with Stinger units, see the *Stinger Administration Guide* and the *Stinger SNMP Management of the ATM Stack Supplement*.

RADIUS support

You can use RADIUS to store user profiles for ATM circuits and terminating connections. The RADIUS server must be compliant with vendor-specific attributes (VSAs), as defined in RFC 2138. To use RADIUS, you must also configure the Stinger unit to communicate with the RADIUS server.

For information about configuring and using RADIUS, see the *TAOS RADIUS Guide and Reference*.

Tracking system activity

A Stinger unit supports many commands for monitoring system activity. To display the commands that are available with the permission settings in the current User profile, enter the `help` (or `?`) command. The following example shows the commands available for the `admin` login. The left column shows command names, and the right column shows the command *class*, which determines the permissions required to use the command.

```
admin> ?
?                               ( user )
arptable                         ( system )
auth                             ( user )
callroute                       ( diagnostic )
clear                            ( user )
clock-source                    ( diagnostic )
clr-history                     ( system )
connection                      ( system )
date                            ( update )
debug                           ( diagnostic )
delete                          ( update )
device                          ( diagnostic )
dir                             ( system )
dircode                         ( system )
ether-display                   ( diagnostic )
fatal-history                   ( system )
format                          ( code )
fsck                            ( code )
```

```

get                ( system )
hdlc               ( system )
[More? <ret>=next entry, <sp>=next page, <^C>=abort]

```

For details about each command, see the *Stinger Reference*. For more information about command help, see the *The TAOS Command-Line Interface Guide*.

Verifying software and control module versions

The `version` command displays the version of TAOS that is currently running in the Stinger unit and also displays the version and type of control module installed.

For example a model E revision 2.1 control module provides the following response to the `version` command:

```

admin> version

software version 9.7.0
* * * 9_7_0/stngrcm2 <tststngr> Jun 30 2004 04:09 * * *
Hardware revision: 2.1 Model E

```

Status windows

The command-line interface supports several status windows that focus on different aspects of system activity (such as connection status and log messages). The windows provide a great deal of read-only information about what is currently happening in the unit. To display a status window, enter the `Status` command:

```
admin> status
```

The system prompt moves to just below the status window. To close the status window, enter the command again:

```
admin> status
```

If the system prompt is not visible below the status window, press Escape to display it.

Note Stinger configuration settings are stored in onboard flash memory, and must be backed up to a TFTP host whenever changes are made. For details about backing up and restoring the Stinger configuration, see the *Stinger Administration Guide*.

What's next

When you have planned your network, you are ready to configure the Stinger unit. You can perform configuration tasks in any order you want. Table 4-1 shows where to look for the information you need.

Table 4-1. Location of configuration information

Configuration task	Location
Establish a serial connection	"Serial connection to a console" on page 5-2
Set up basic access security	"Restricting administrative access" on page 5-7
Configure IP	"Providing a basic system IP configuration" on page 5-9 and the <i>Stinger IP2000 Configuration Guide</i>
Configure the unit to use RADIUS	TAOS RADIUS Guide and Reference

Table 4-1. Location of configuration information (continued)

Configuration task	Location
Configure the unit's LIMs	LIM guide for the desired module
Checking LIM port status	LIM guide for the desired module
Configure the unit's trunk lines	Trunk module guide for the desired module
Checking trunk status	Trunk module guide for the desired module
Define ATM traffic contracts	<i>Stinger ATM Configuration Guide</i> and the <i>Stinger Private Network-to-Network Interface (PNNI) Supplement</i>
Configure ATM circuits	<i>Stinger ATM Configuration Guide</i> , the <i>Stinger Private Network-to-Network Interface (PNNI) Supplement</i> , and the <i>Stinger IP2000 Configuration Guide</i>
Configure virtual path switching	<i>Stinger ATM Configuration Guide</i> and the <i>Stinger Private Network-to-Network Interface (PNNI) Supplement</i>
Check details about parameters and commands	<i>Stinger Reference Guide</i>
Use SNMP with the unit	<i>Stinger Administration Guide</i> and the <i>Stinger SNMP Management of the ATM Stack Supplement</i>
Configure IP2000 gigabit Ethernet interfaces	Stinger IP2000 Administration Guide
Configure login permissions	<i>Stinger Administration Guide</i>
Back up the system configuration	<i>Stinger Administration Guide</i>
Test lines and ports	<i>Stinger Administration Guide</i>

Configuring the Control Module and System Timing

Control module configuration overview	5-1
Administrative connections	5-1
Logging into the control module	5-6
Restricting administrative access	5-7
Providing a basic system IP configuration	5-9
Configuring system clocking	5-14
Configuring system clocking	5-14

Control module configuration overview

The control module controls the operations of the Stinger unit. It manages and boots the LIMs, maintains a central repository of the unit's configuration, performs call control and processing operations, and manages all centralized functions, such as SNMP access or communication with a RADIUS server.

Control module configuration includes the following tasks:

- Connecting a console workstation to the serial port on the control module of the Stinger unit
- Logging into the Stinger unit
- Changing default security settings to protect the unit
- Configuring IP to make the system accessible by Telnet, SNMP, and Ping
- Configuring RADIUS access (if appropriate)

Stinger units equipped with the IP2000 control module can also be configured to support termination and aggregation of RFC 2684 Asynchronous Transfer Mode (ATM) PVCs, IGMP multicast v1/v2 and IEEE 802.1Q tagged virtual local area networks (VLANs). Information about these capabilities is contained in the *Stinger IP2000 Configuration Guide*. However, the following information will allow you to perform basic administrative configuration for IP2000 control modules.

Administrative connections

The serial port the control module in a Stinger MS+ unit is used for initial configuration from a console device. The port can also be configured to connect to a

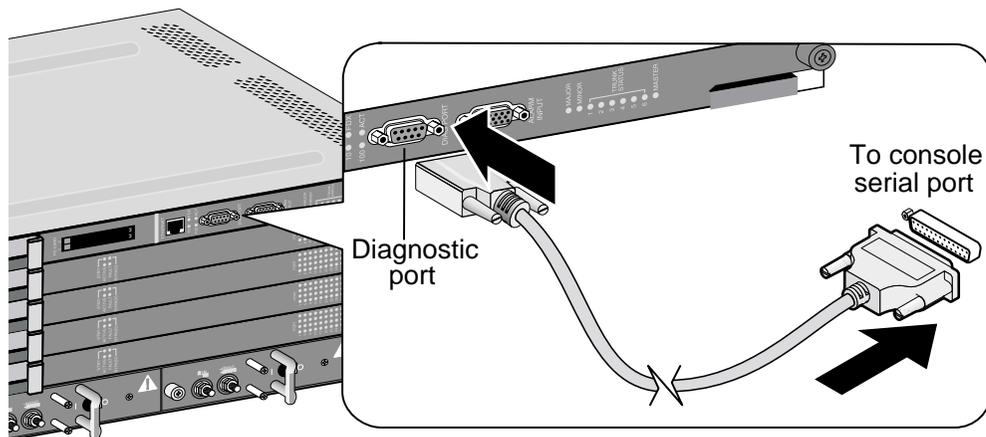
modem to provide dial-in administrative access to the unit. Revision 2 control module models B and C contain an internal modem, configured by default for autoanswer. On these models, you need only to connect the RJ-11 modem jack to the telephone line and then call in to the Stinger unit for an administrative connection.

Once the Stinger unit has been configured with an IP address, it can be reached on the IP network via a Telnet connection. The following information provides details of these connection methods.

Serial connection to a console

Figure 5-1 shows a cable connection from a Stinger MS+ to a console terminal.

Figure 5-1. Serial management connection to a Stinger MS+



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

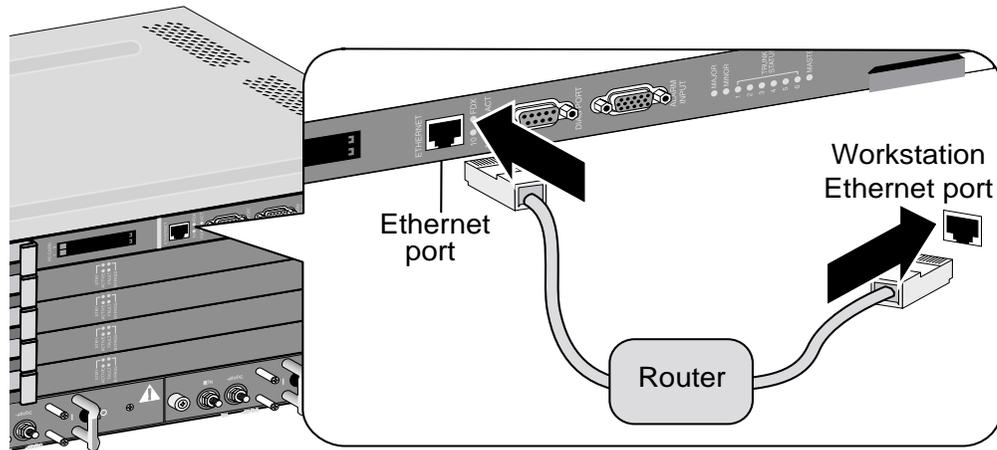
The diagnostic port on the control module consists of a female DB-9 connector. Examine the serial connector of your PC or dumb terminal to ensure that your shielded straight-through cable has the proper connectors. If needed, you can use DB-9-to-DB-25 converters or gender converters to complete this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

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

Network connection to a workstation console

After the IP address of the Stinger unit has been configured, and the unit has been connected to a network, an administrative Telnet connection can be established through the network. Figure 5-2 shows an Ethernet network connection from the Stinger unit to the management workstation.

Figure 5-2. Ethernet connection



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

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

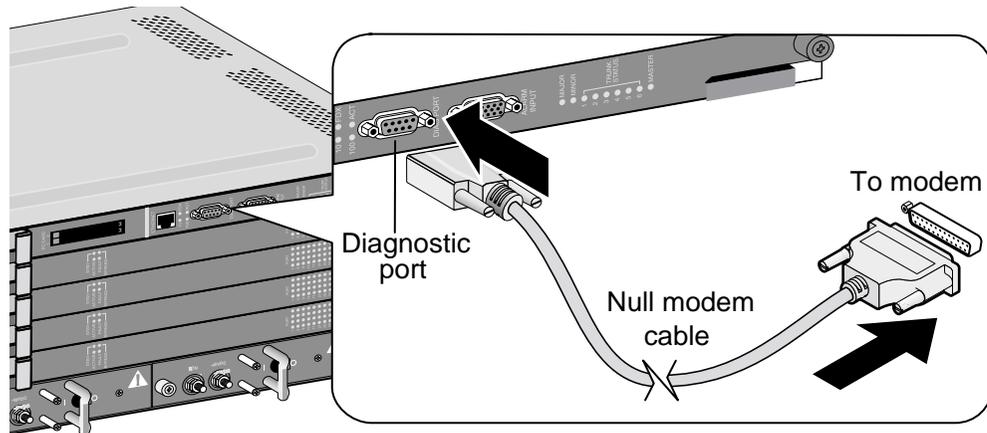
Connecting a dial-in backup management connection

Lucent Technologies recommends that you provision dial-up or some other access to each unit for backup administrative access. Dial-up access to a Stinger unit equipped with a revision 1 control module, a revision 2 model A control module, or a revision 2.1 model E control module, requires a properly configured *external* modem connected to the DIAG port on the control module. Revision 2 control module models B and C are equipped with an *internal* modem to support this type of backup management connection.

Backup management with an external modem

To configure a backup administrative connection with an external modem, connect the modem to the Stinger diagnostic port (DIAG PORT) with a null modem (crossover) cable. In addition, you might need a DB-25-to-DB-9 adapter. Figure 5-3 shows the backup administrative connection with a modem to the Stinger unit.

Figure 5-3. Backup administrative connection with a modem to the Stinger MS+ unit



The modem you use to connect to the Stinger unit must be configured as follows:

- Dumb mode. Dumb mode causes the modem to ignore data on the receive data (RD) lead.
- Ignore on-to-off transitions of the data-terminal ready (DTR) lead.
- Auto answer enabled.
- 8 bits, 1 stop bit, and no parity.

Configure the following AT commands on the modem:

at&d0	Ignore DTR state.
ats0=1	Answer automatically after one ring.
ate0	No echo (required).
at&c0	Assert the data carrier detect (DCD) signal.
atq1	Result codes are not sent.
at&w0	Store in nonvolatile RAM (NVRAM) as profile 0 (zero).
at&y0	Use stored configuration from profile 0 (zero) on startup.

Modem country codes

You can configure the internal modem in a revision 2 control module to support the national regulations of telephone companies in specific countries. If the modem supports the country that you have specified, the system programs the modem with the settings necessary for that country. The `country-code` parameter in the modem profile, shown here with its default value, is used for this setting.

```
[in MODEM/{ shelf-1 first-control-module 3 }]  
physical-address* = { shelf-1 first-control-module 3 }  
country-code = unitedstates
```

The `cmmodemShowCurrentCountry` debug command displays the country code that is currently configured in the modem.

The `cmmodemShowCountries` system-level command displays a list of countries that the modem installed in the revision 2 control module supports. The following is a sample output of this command:

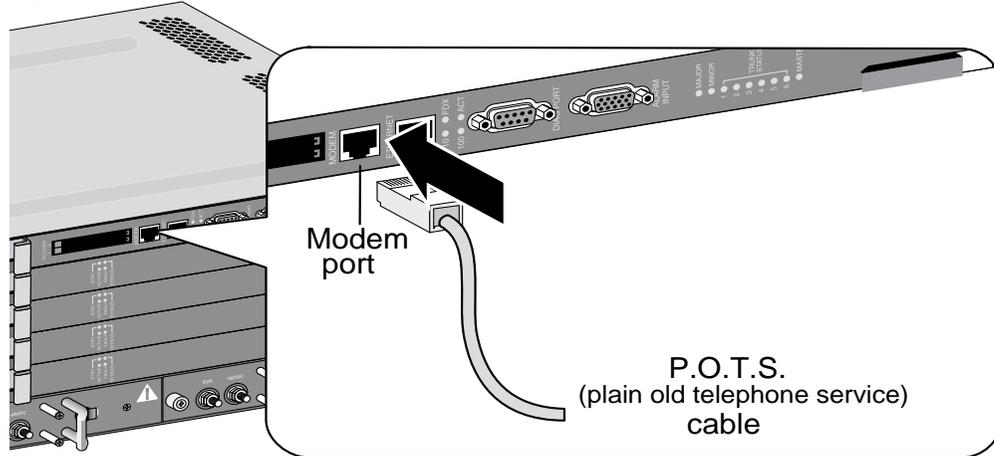
```
admin> cmmodemShowCountries
The country codes supported by this modem are:
0, Japan
9, Australia
a, Austria
f, Belgium
16, Brazil
26, China
31, Denmark
3c, Finland
3d, France
42, Germany
46, Greece
53, India
57, Ireland
59, Italy
61, Korea
6c, Malaysia
73, Mexico
7b, Netherlands
82, Norway
8a, Poland
8b, Portugal
9c, Singapore
9f, South Africa
a0, Spain
a5, Sweden
a6, Switzerland
b4, United Kingdom
b5, United States
fd, unknown
fe, Taiwan
```

For additional information about this parameter and these commands, see the *Stinger Reference*.

Backup management with an internal modem

Revision 2 control module models B and C are equipped with an internal modem. This modem is configured by default to automatically answer any incoming calls. For this reason, you need only connect the telephone line to the RJ-11 jack on the face of the control module. Figure 5-4 shows a connection for an internal modem.

Figure 5-4. Connection for internal modem



Use the Modem profile to set the autoanswer configuration of this modem. Following is a sample of this profile with its default setting:

```
[in MODEM/{ shelf-1 first-control-module 3 }]  
physical-address* = { shelf-1 first-control-module 3 }  
auto-answer = on
```

The auto-answer parameter has three valid settings:

Setting	Specifies
on	The internal modem automatically answers any incoming call and attempts to negotiate modem protocols with the caller.
off	The internal modem ignores incoming calls.
primary-only	Not used in the Stinger MS+ unit.

Note In Stinger units with redundant control modules, the internal modem automatically answers incoming calls only if the control module is the primary control module for the Stinger unit. When the control module is set as the secondary control module, the modem ignores incoming calls. This setting allows redundant controllers to share a single telephone line.

Logging into the control module

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

The default settings for the serial port profile allow anyone connecting to the diagnostics port to access the system as the administrative (admin) user, without logging in or being authenticated. When you connect to an unconfigured Stinger unit

to which power has been applied, you are presented with the prompt for the admin user:

```
admin>
```

After you have supplied basic IP information, as described in “Providing a basic system IP configuration” on page 5-9, you can access the Stinger command-line interface by using Telnet from an IP host. Or, you can log in by using an SNMP management station, such as NavisAccess™, from an IP host. These types of connections require that you authenticate a User profile and supply a password to acquire administrative permissions. During basic configuration, Lucent Technologies recommends that you also configure the serial port to require username and password authentication.

For details about User profiles, see the *Stinger Administration Guide*.

Restricting administrative access

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

Changing defaults for serial-port logins

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

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

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

A Stinger unit automatically creates a Serial profile for the control module. To list the Serial profiles, use the `Dir` command as follows:

```
admin> dir serial  
12 03/06/2003 02:57:48 { shelf-1 first-control-module 1 }
```

There is only one control module slot in Stinger MS+ units. The designation, `first-control-module`, refers to the slot labeled CTRL on the Stinger MS+ chassis. This slot is referred to as slot 8 or `first-control-module` in the TAOS interface to maintain the uniformity of the TAOS interface across the Stinger product line.

To make serial logins more secure, modify the Serial profile of the control module to specify a null User profile name, as shown in the following example. Anyone trying

to establish a connection through the serial port is then required to provide a username and password.

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

Changing the default admin password

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

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

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

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

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

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

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

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

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

Setting a Telnet password

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

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

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

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

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

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

```
% telnet 1.1.1.1
<stinger01> Enter Password: dpg01!

Trying 1.1.1.1...
Connected to 1.1.1.1
Escape character is '^]'.

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

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

Providing a basic system IP configuration

To enable Telnet and SNMP access to the unit, and to allow connectivity between the unit and local IP hosts, you must assign IP addresses to the Stinger Ethernet ports and configure basic IP routing. A basic configuration for remote inband management can be saved in a special file called `default.cfg`. If the basic configuration is saved in this way, the system can restart with the configured remote management capability,

even after nonvolatile memory has been cleared with the NVRAM command. For more information about retaining a configuration after clearing NVRAM, see the *Stinger Administration Guide*.

Note A Stinger unit *does not require* IP routing to operate as a DSLAM. IP routing is not used by the DSLAM activities. The system does not provide IP routing for DSLAM user data.

IP address syntax

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

Netmasks

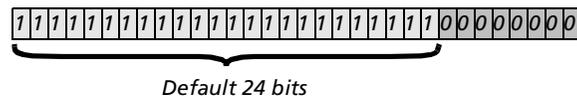
If no netmask is specified, the unit uses a default mask based on the class of the IP address that is supplied. Table 5-1 shows address classes and the number of network bits in the default mask for each class.

Table 5-1. IP address classes and number of network bits

Class	Address range	Default network bits
Class A	0.0.0.0 through 127.255.255.255	8
Class B	128.0.0.0 through 191.255.255.255	16
Class C	192.0.0.0 through 223.255.255.255	24

For example, a class C address, such as 198.5.248.40, has 24 network bits, leaving 8 bits for the host portion of the address. If no subnet mask is specified for a class C address, the Stinger unit uses the default mask of 24 bits, as shown in Figure 5-5.

Figure 5-5. Default netmask for class C IP address



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

Subnets

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

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

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

000 — Reserved for the network (base address)

001

010

100

110

101

011

111 — Reserved for the broadcast address of the subnet

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

Table 5-2 shows subnet masks and prefix lengths for a class C network.

Table 5-2. Decimal subnet masks and prefix lengths

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

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

198.5.248.120/29

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

198.5.248.120 – 198.5.248.127

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

198.5.248.40/32

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

Assigning the Ethernet IP addresses

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

```
admin> dir ip-interface
18 03/06/2003 16:36:32 { { any-shelf any-slot 0 } 0 }
29 03/06/2003 16:27:57 { { shelf-1 first-control-module 1 } 0 }
```

The IP interface profile identified as, `first-control-module 1`, refers to the IP interface of the first (and only) physical Ethernet port on the control module in the Stinger MS+ chassis. The IP-Interface profile with the zero index (the default `any-shelf any-slot` index) is reserved for the soft interface of the unit, which is described in “Defining the soft IP interface” on page 5-12.



Note The designation, `first-control-module`, refers to the slot position of the control module in Stinger units that support redundant control modules. There is only one control module slot in Stinger MS+ units. This slot is referred to as slot 8 or `first-control-module` in the TAOS interface to maintain the uniformity of the TAOS interface across the Stinger product line.

The following commands assign the address 1.1.1.56/24 to the ethernet interface on the control module:

```
admin> read ip-interface { { shelf-1 8 1 } 0 }
IP-INTERFACE/{ { shelf-1 first-control-module 1 } 0 } read
admin> set ip-address = 1.1.1.56/24
admin> write
IP-INTERFACE/{ { shelf-1 first-control-module 1 } 0 } written
```

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

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

Defining the soft IP interface

A Stinger unit supports a soft IP interface that can be assigned its own IP address. The address of the soft IP interface becomes a second (proxy) address for Ethernet port on the primary or only control module in the unit. In Stinger models that support redundant control modules, this soft address can be reached through the Ethernet interface of whichever control module is the primary control module. Therefore,

regardless of which control modules is functioning as the primary control module for the chassis, the unit can be accessed through the same soft interface address.

When power is applied to the system, the soft IP interface address is not initialized until a control module assumes the role of primary control for the Stinger unit. The Ethernet interface of the primary control module can then respond to ARP requests for the soft IP interface address in addition to requests for its own IP address, which was previously configured. If the secondary control module becomes primary, the system reinitializes the soft IP interface address to the Ethernet interface of the new primary control module.

The soft IP interface is configured in the IP-Interface profile with the zero index.

The following commands set the soft interface IP address to 1.1.1.128/24:

```
admin> read ip-interface {{ 0 0 0 }}
IP-INTERFACE/{ { any-shelf any-slot 0 } 0 } read

admin> set ip-addr = 1.1.1.128/24

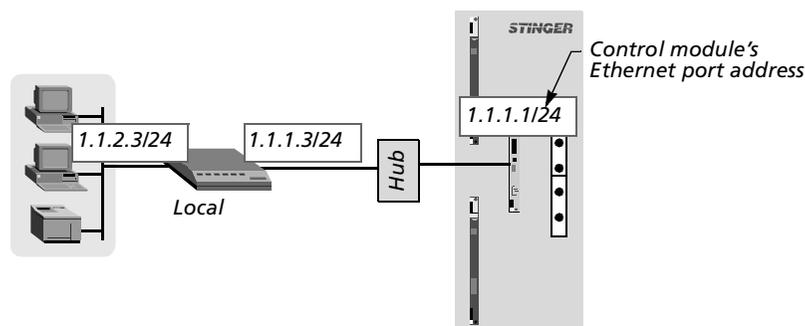
admin> write
IP-INTERFACE/{ { any-shelf any-slot 0 } 0 } written
```

Configuring a default route

A default route is a static route that specifies a destination for addresses that are not on the local network and to which a known route does not exist. The default route is generally the IP address of an external router that has more route information about how specific destinations can be reached. When the default route is configured, the Stinger unit routes all IP packets with unknown destinations to the specified external router. If no default route is defined, the unit drops IP packets for which it has no route.

Figure 5-6 shows the Stinger Ethernet interface on a subnet, connected to the same Ethernet segment as a local backbone router. In this network, the Stinger unit can use the local router as its default route.

Figure 5-6. Local backbone router to be used as default route



If a local router is the unit's default route, or gateway, the Stinger unit can pass all IP packets with an unrecognized address to that router, so its own routing table can remain small. The external router maintains larger routing tables and assumes the responsibility and overhead of routing most packets.

For example, the following commands define a default route to the LAN router in Figure 5-6:

Configuring the Control Module and System Timing

Configuring system clocking

```
admin> new ip-route default
IP-ROUTE/default read

admin> set gateway-address = 1.1.1.3

admin> set active-route = yes

admin> write
IP-ROUTE/default written
```

The system can support multiple default routes. The profile name does not have to be `default`. The only requirements are that the destination address must be zero, and Gateway-Address must specify a valid, accessible router.

For information about other settings in the IP-Route profile, see the *Stinger Reference Guide*.

Verifying a LAN connection for administrators

To enable administrators to log into the Stinger unit's interface from IP hosts, you must also make sure your local network can route to the unit. Your network router must have network connectivity through intermediate routers so that the administrative host can access the Stinger unit via its IP address. You can test this connectivity by pinging the unit from the local host. For example, the following command entered on a local host tests connectivity to the Stinger soft interface, identified previously:

```
% ping 1.1.1.128
PING 1.1.1.128 (1.1.1.128): 56 Data bytes
64 bytes from 1.1.1.128: icmp_seq=0 ttl=255 time=0 ms
64 bytes from 1.1.1.128: icmp_seq=7 ttl=255 time=0 ms
^C
--- 1.1.1.128 Ping statistics ---
8 packets transmitted, 8 packets received, 0% packet loss
round-trip min/avg/max = 0/0/0 ms
```

Configuring system clocking

The Stinger unit requires a clock source for its timing subsystem. By default, it uses a built-in 8kHz clock on the control module as its timing source. You can configure the system to take its clock source from a trunk port or from an external building interoffice timing source (BITS) clock connected to the Stinger MS+ unit.

Using the default (controller) clock source

The Stinger unit has an internal 8kHz clock on its control module. By default, the unit uses the clock on the control module as the source for its timing subsystem. To configure the unit to obtain its clock signal from another source, set the following parameter (shown with its default setting):

```
[in SYSTEM]
system-8k-clock = controller
```

Parameter	Setting
System-8K-Clock	<p>Source for the master system clock.</p> <p>With the default <code>controller</code> setting, the Stinger MS+ unit uses the built-in 8kHz clock on the control module.</p> <p>If set to <code>lim-or-trunk-module</code>, the unit obtains its clock signal from a trunk port that has been configured as an eligible clock source, using the ports in order of their priority. If no eligible trunk ports are available, it uses the control module clock.</p> <p>If set to <code>bits</code>, the unit sources its clock from the building interoffice timing source (BITS) T1 framer in its alarm unit.</p> <p>If set to <code>ami-8k</code>, a model A-J control module sources the 400Hz ISDN reference clock used in Japan, from the BITS input across the backplane for use by Annex C LIMs. (The model A-J control module is available only for the Stinger LS.)</p>

Using the BITS clock source

The following commands cause the system to first attempt to use a BITS clock as its clock source, and to use the built-in clock only if it does not find a valid BITS signal:

```
admin> read system
SYSTEM read

admin> set system-8k-clock = bits

admin> write
SYSTEM written
```

Loss of BITS signal indications and fall-back

If the `system-8K-clock` parameter in the `system` profile is set to `bits` and the system detects a loss of signal, it displays the following message:

```
LOG alert, Shelf 1, Controller-1, Time: 17:02:01--
BITS clock source has been lost - 8kHz clock is free running
```

If no other clock source is eligible, the system then displays the following message:

```
LOG notice, Shelf 1, Controller-1, Time: 17:02:01
Master clock source changed to local oscillator
```

When the Stinger unit recovers the BITS signal, it displays the following messages:

```
LOG alert, Shelf 1, Controller-1, Time: 17:02:03--
BITS clock source has been recovered - 8kHz clock is locked

LOG notice, Shelf 1, Controller-1, Time: 17:02:03--
Master clock source changed to T1 framer
```

If the Stinger unit detects a T1 signal in the BITS input, it prioritizes the clock source list as follows:

- If the `system-8k-clock` parameter of the `system` profile is set to `bits`, its priority is set to the highest (1) and the T1 framer is selected regardless of other available clock sources and priorities.
- If the `system-8k-clock` parameter of the `system` profile is set to a value other than `bits`, its priority is set as the lowest (3) and the T1 framer is selected as a clock source only if no other slot clock sources are available.

Changing the BITS clock source

The following examples show how to change the `system-8k-clock` parameter setting from `bits` to `lim-or-trunk-module` and use the `slot-clock-source` command to view the changes in clock source priority:

```
admin> set system-8k-clock = bits
admin> write
LOG notice, Shelf 1, Controller-1, Time: 17:55:34--
Master clock source changed to T1 framer
SYSTEM written
admin> slot-clock-source
Master line: T1 framer
Source List:
    Source: line 1 Available*      priority: 2
    Source: line 2 Available*      priority: 1
    Source: T1 framer Available*   priority: 1

admin> set system-8k-clock = lim-or-trunk-module
admin> write
LOG notice, Shelf 1, Controller-1, Time: 17:56:05--
Master clock source changed to slot-1/8 line 2
SYSTEM written
admin> slot-clock-source
Master line: 2
source List:
    Source: line 1 Available*      priority: 2
    Source: line 2 Available*      priority: 1
    Source: T1 framer Available*   priority: 3
```

Using a LIM or trunk module clock source

The following commands cause the system to first attempt to use a trunk port as its clock source, and to use the built-in clock only if it finds no ports that are eligible clock sources:

```
admin> read system
SYSTEM read
admin> set system-8k-clock = lim-or-trunk-module
```

```
admin> write
SYSTEM written
```

Configuring trunk ports as eligible clock sources

The DS3-ATM, OC3-ATM, and E3-ATM profiles support Clock-Source and Clock-Priority parameters for specifying whether the port can be used to source the ATM network clock and feed it to the primary control module as the master clock for the unit. Each of the two trunk ports can be configured as eligible or ineligible for this use, and can be assigned a high, middle, or low priority for being elected as the clock source. Following are the relevant parameters, shown with default settings:

```
[in DS3-ATM/{ any-shelf any-slot 0 }:line-config]
clock-source = not-eligible
clock-priority = middle-priority

[in OC3-ATM/{ any-shelf any-slot 0 }:line-config]
clock-source = not-eligible
clock-priority = middle-priority

[in E3-ATM/{ any-shelf any-slot 0 }:line-config]
clock-source = not-eligible
clock-priority = middle-priority
```

Parameter	Setting
Clock-Source	Enable/disable obtaining the system clock signal from the port. By default, ports are not eligible clock sources.
Clock-Priority	Priority of the interface as the system's clock source (high, middle, or low priority). Once the Stinger unit chooses a clock source, it uses that source until the interface becomes unavailable or a higher-priority source becomes available.

If more than one line is eligible to be the clock source, the system chooses the one with the highest priority, as specified by the Clock-Priority setting. If multiple sources of equal priority are present, the system selects the first valid clock source. (A clock source is valid if the Clock-Source parameter is set to `eligible` and the DS3, OC3, or E3 interface is synchronized.)

Once it has selected a clock source, the system uses that source until the source becomes unavailable or a higher-priority source becomes available. If no eligible external sources exist, the system uses an internal clock generated by the primary control module.

Typical trunk port clock source configurations

The following sample commands configure both ports of a DS3-ATM module as eligible clock sources, with the first port assigned a higher priority for this use:

```
admin> read ds3-atm { 1 trunk-module-1 1 }
DS3-ATM/{ shelf-1 trunk-module-1 1 } read
admin> set line-config clock-source = eligible
admin> set line-config clock-priority = high
admin> write
DS3-ATM/{ shelf-1 trunk-module-1 1 } written
```

Configuring the Control Module and System Timing

Configuring system clocking

```
admin> read ds3-atm { 1 trunk-module-1 2 }
DS3-ATM/{ shelf-1 trunk-module-1 2 } read
admin> set line-config clock-source = eligible
admin> set line-config clock-priority = low
admin> write
DS3-ATM/{ shelf-1 trunk-module-1 2 } written
```

Additional information about configuring OC3-ATM, DS3-ATM, and E3-ATM trunk modules can be found in the *Stinger OC3-ATM Trunk Module Guide*, the *Stinger DS3-ATM Trunk Module Guide*, and the *Stinger E3-ATM Trunk Module Guide*.

Installing and Removing Modules

Installation and replacement considerations	6-1
Replacing and installing control modules	6-2
Slot numbering and module placement	6-5
Installing and replacing LIMs	6-5
Installing and replacing LPMs	6-6
Installing and replacing PCMCIA cards	6-8
Replacing the cooling module	6-8
Replacing a power filter	6-9
Replacing the alarm module	6-10

Installation and replacement considerations

The Stinger unit design enables you to install, remove, and replace most 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 Do not attempt to replace the power filter on a Stinger FS or Stinger FS+ unit. Doing so, you risk contact with live, electrically charged components of the unit.



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 C, “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. 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.

Replacing and installing control modules



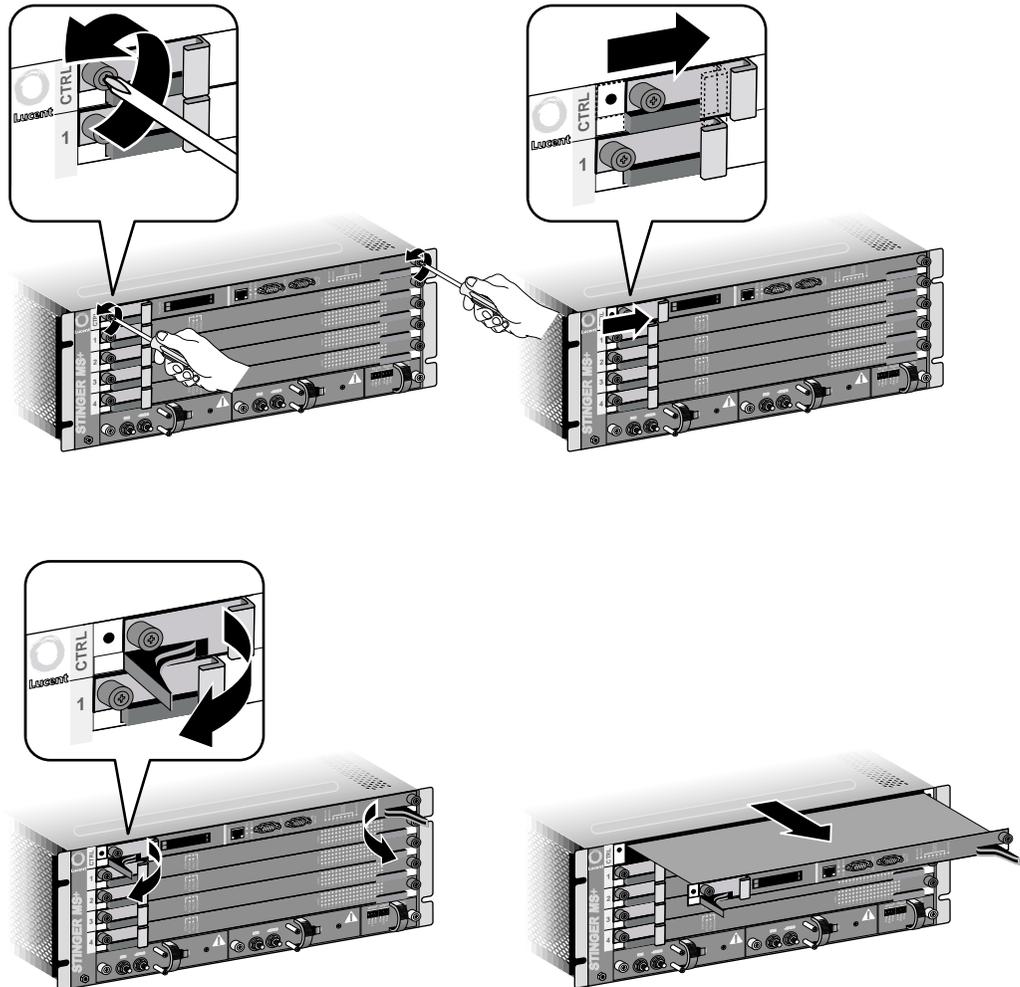
Caution The control module should not be replaced while the Stinger MS+ unit is in operation. Hot-swap replacement of an active control module causes a Stinger unit to crash.

Removing a control module

To remove a control module:

- 1** Put on the antistatic wrist strap, as recommended in “Preventing static discharge damage” on page 1-4, and plug it into the ESD grounding jack located on the front of the Stinger unit. (See Figure 1-5 on page 1-7.)
- 2** If the unit does not contain a redundant control module, or if both the primary control module and the secondary control module are being replaced simultaneously, notify all users that the unit is being shut down.
- 3** Turn off power to the unit.
- 4** Using a number 2 Phillips screwdriver, loosen the thumbscrews located on each side of the control module, as shown in Figure 6-1. Other screwdrivers might damage the screw heads.
- 5** Slide the ejector lock on the left side of the control module to the right to access the card ejector. This puts the module into a reset state.

Figure 6-1. Removing a control module



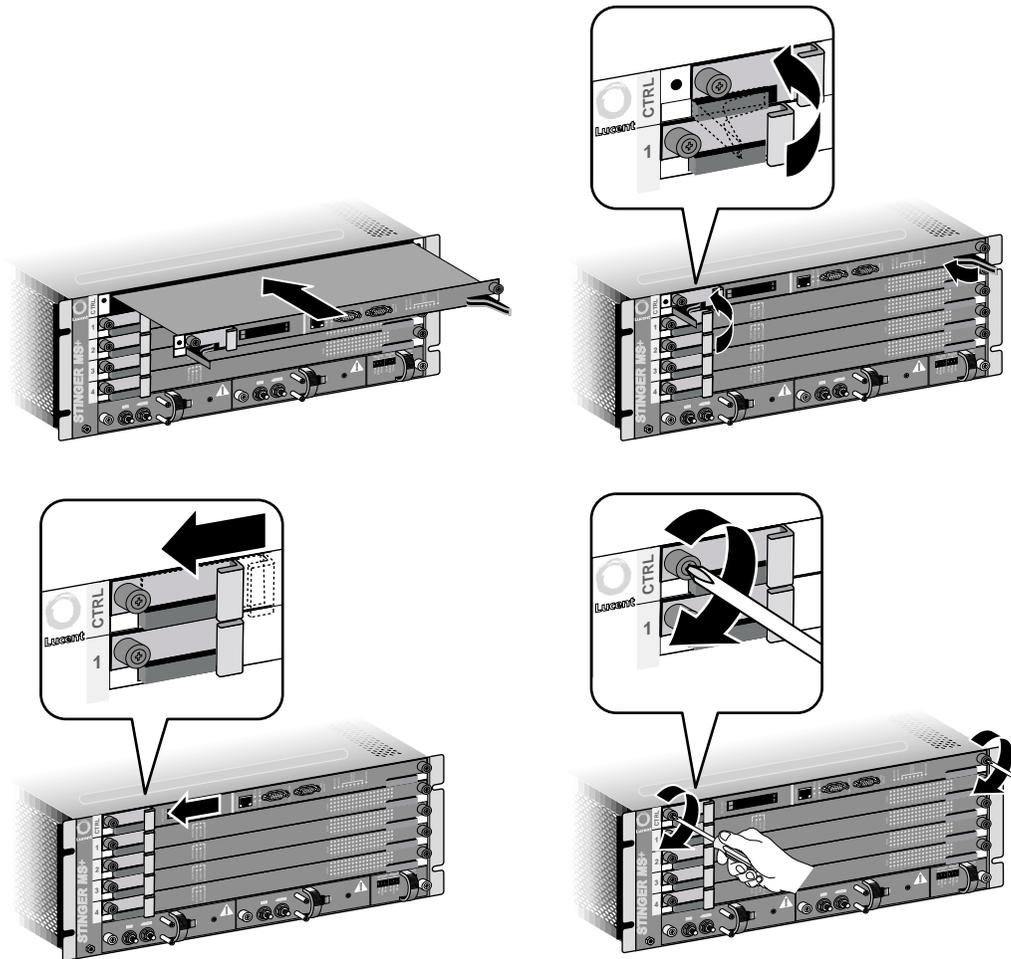
- 6 Lift the card ejectors on both sides of the card simultaneously to remove the module from the unit.
- 7 Carefully slide the control module out of the chassis, and place it into an antistatic container.

Installing a control module

To install a control module:

- 1 Put on the antistatic wrist strap, as recommended in “Preventing static discharge damage” on page 1-4, and plug it into the ESD grounding jack located on the front of the unit. (See Figure 1-5 on page 1-7.)
- 2 Align the replacement control module with the card guide and carefully slide the module into the unit, as shown in Figure 6-2.
- 3 Depress the card ejectors simultaneously to seat the module into the midplane.

Figure 6-2. Installing a control module



- 4 Slide the card ejector lock up.
- 5 Using a number 2 Phillips screwdriver, tighten the two thumbscrews.
- 6 If necessary, restore power to the unit.
- 7 Verify the following behavior of the status lights on the control module to verify its operational status:
 - The MAJOR alarm light on the newly installed control module turns ON (amber) when you turn on power to the unit, and then blinks while the TAOS software image is downloading. After several minutes of operation, the MAJOR alarm light turns OFF.
 - On a single or primary control module, the MASTER light at the bottom is ON (solid green) to indicate that the module is active.
 - On a redundant (secondary) control module, the MASTER light at the bottom is OFF to indicate that the module is in a standby mode.

Slot numbering and module placement

LIM are installed in the slots numbered from 1 to 4 in the front of the Stinger MS+ chassis. These slots are also logically referred to by the TAOS software as slots 1 through 4, corresponding with their physical location in the chassis.

The top slot in the front of the unit is labeled “CTRL”. This slot is reserved for the control module. To maintain the uniformity across the Stinger product line, this slot is logically referred to by the TAOS software as slot 8.

The top slot in the rear of the unit is labeled “TM”. This slot is reserved for a trunk or TRAM module. To maintain the uniformity across the Stinger product line, this slot is logically referred to by the TAOS software as slot 17.

Installing and replacing LIMs

Physical installation and replacement of a LIM are similar procedures to the installation and replacement of a control module. Refer to the illustration in Figure 6-2 on page 6-4, if necessary.

Installing a LIM

To install a LIM:

- 1 Put on the antistatic wrist strap, as recommended in “Preventing static discharge damage” on page 1-4, and plug it into the ESD grounding jack located on the front of the unit. (See Figure 1-5 on page 1-7.)
- 2 Remove the blank slot cover on the desired slot on the front of the unit. (See “Slot numbering and module placement” on page 6-5.)
- 3 Align the LIM with the card guides and carefully slide the module into the unit.
Note Keep the connector on the LIM being inserted away from components on adjacent LIMs. Do not force the card. Once the card has engaged its bus connector, press firmly to be sure it is fully seated.
- 4 Depress the ejectors simultaneously.
- 5 Slide the card ejector lock up.
- 6 Using a number 2 Phillips screwdriver, secure the LIM by tightening the thumbscrews.
- 7 If necessary, if all other installation tasks are complete, including the installation of an associated LPM, turn on power to the Stinger unit.
- 8 Wait several minutes and then verify the behavior of the status lights on the LIM to verify its operational status.

For status light information, see the module guide for the LIM you are installing.

Replacing a LIM



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

Refer to the illustration in Figure 6-1 on page 6-3, if necessary.

To replace a LIM:

- 1 Put on the antistatic wrist strap, as recommended in “Preventing static discharge damage” on page 1-4, and plug it into the ESD grounding jack located on the front of the unit. (See Figure 1-5 on page 1-7.)
- 2 Using a number 2 Phillips screwdriver, loosen the top and bottom thumbscrews attaching the module to the unit.
- 3 Slide the ejector lock located at the top of the LIM down to disconnect the module from the network.
- 4 Lift the top and bottom card ejectors simultaneously to remove the module from the unit. Lift both ejectors simultaneously to avoid damage to the module.
- 5 Carefully slide the LIM out of the unit and place it into an antistatic container.
- 6 Align the LIM with the card guides and carefully slide the module into the unit.
Note Keep the connector on the LIM being inserted away from components on adjacent LIMs. Do not force the card. Once the card has engaged its bus connector, press firmly to be sure it is fully seated.
- 7 Depress the ejectors simultaneously.
- 8 Slide the card ejector lock up.
- 9 Using a number 2 Phillips screwdriver, secure the module into the unit by tightening the thumbscrews on the LIM.
- 10 Wait several minutes and then verify the behavior of the status lights on the LIM to verify its operational status.

For status light information, see 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 line interface modules (LIMs), except that LPMs are installed in the rear of the chassis and their top ejector levers are not protected by ejector locks.

Openings for unused LPM slots are protected by blank covers. Unless LIMs with integrated protection are used, a companion LPM must be installed in the back of the unit 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 1-4, and plug it into the ESD grounding jack located on the back of the unit. (See Figure 1-7 on page 1-10.)
- 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 “Connecting to the LPMs” on page 2-3.

Replacing an LPM

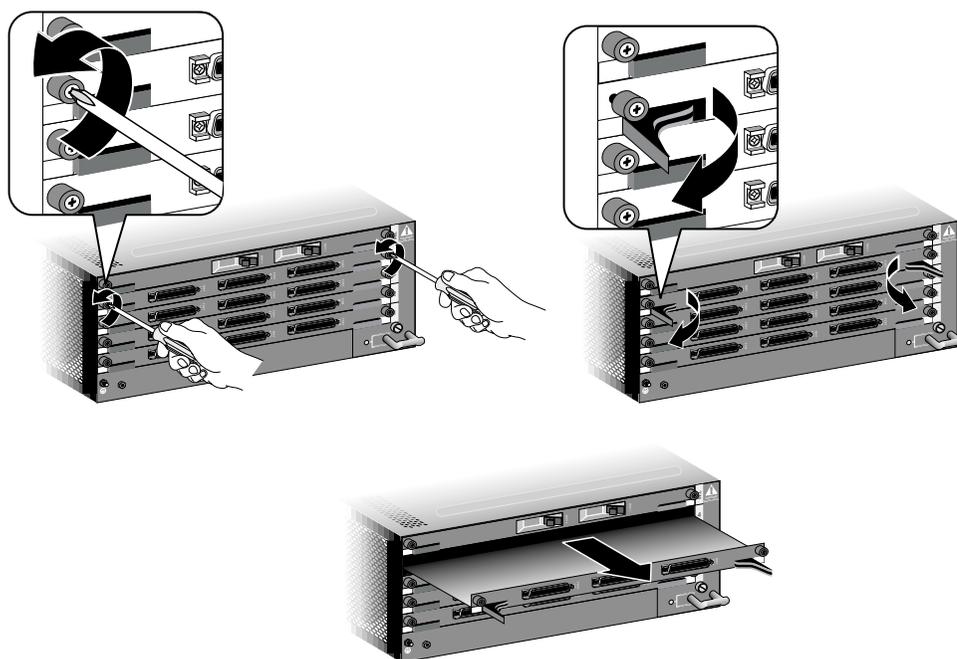


Caution Any circuits running through the LPM are interrupted when it is removed, which can result in data loss. Lucent Technologies recommends setting the associated LIM's administrative status to Down before removing the LPM from the unit. For instructions on changing a LIM's state to Down and then 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 1-4, and plug it into an ESD grounding jack located on the front or back of the unit. (See Figure 1-5 on page 1-7 and Figure 1-7 on page 1-10.)
- 2 Carefully unhook the cable ties securing the connectors and cables to the card and remove all connectors and cables.
- 3 Using a number 2 Phillips screwdriver, loosen the left and right thumbscrews attaching the module to the unit, as shown in Figure 6-3.

Figure 6-3. Removing an LPM



- 4 Lift the left and right card ejectors simultaneously to disengage the module from the midplane connectors. 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 “Connecting to the LPMs” on page 2-3.

Installing and replacing PCMCIA cards

To remove the PCMCIA cards from the control module, push the square, flat black buttons at the bottom of each PCMCIA card to eject the cards. After the cards are removed, make sure they remain guarded against static discharge.

To install the PCMCIA cards in the control module, line the card edge up with the guides, and push the card in until the black ejector button pops back up.

Replacing the cooling module

The cooling module contains fans for cooling the unit and the electronics that control and monitor their operation. The cooling module is installed in the rear of the chassis. It is not necessary to remove power from the unit while replacing the cooling module.



Caution To avoid overheating the unit, you must minimize the time that the cooling module is removed from the chassis. Have the new module unpacked and ready for installation before removing the old cooling module.

To replace an LPM:

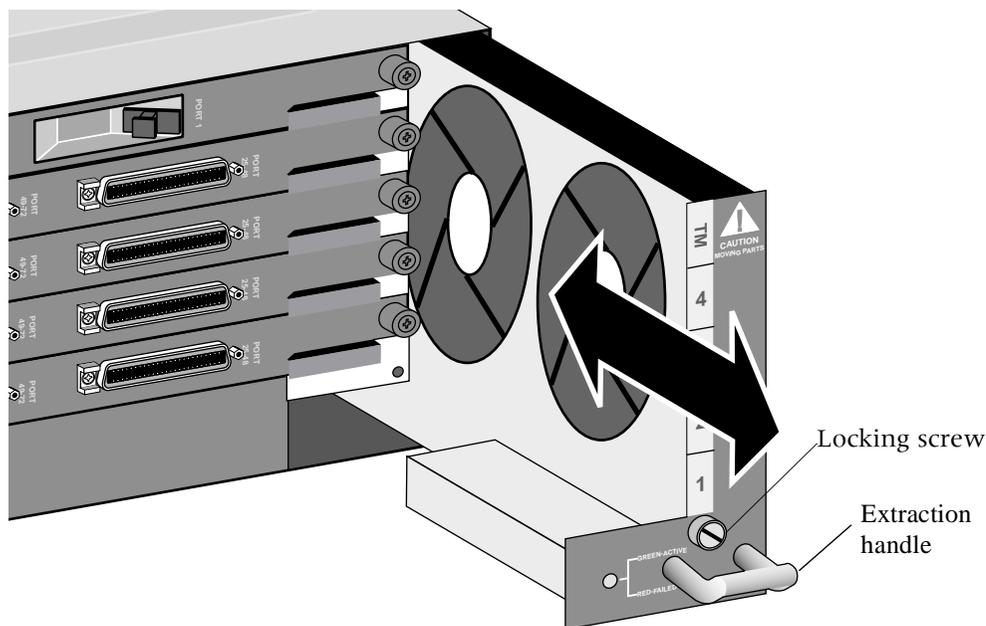
- 1 Put on the antistatic wrist strap, as recommended in “Preventing static discharge damage” on page 1-4, and plug it into an ESD grounding jack located on the front or back of the unit. (See Figure 1-5 on page 1-7 and Figure 1-7 on page 1-10.)
- 2 Using a number 2 Phillips screwdriver, fully loosen the cooling module locking screw, shown in Figure 6-4.



Warning Keep your fingers away from the fan blades in the cooling module. Fan blades may be moving with the cooling module is removed from the enclosure.

- 3 Grasp the extraction handle of the cooling module and pull the cooling module about 0.5in. (12.7mm) out of the enclosure. Wait until the fans stop moving (at least 20 to 30 seconds).
- 4 When the fan blades have stopped moving pull the cooling module straight out of the chassis, as shown in Figure 6-4.

Figure 6-4. Replacing the cooling module



- 5 Align the replacement module to slide straight into the opening in the back of the chassis.
- 6 Carefully slide the replacement cooling module into the chassis and press firmly to engage the power connector in the chassis.
- 7 Fully tighten the locking screw on the replacement cooling module.

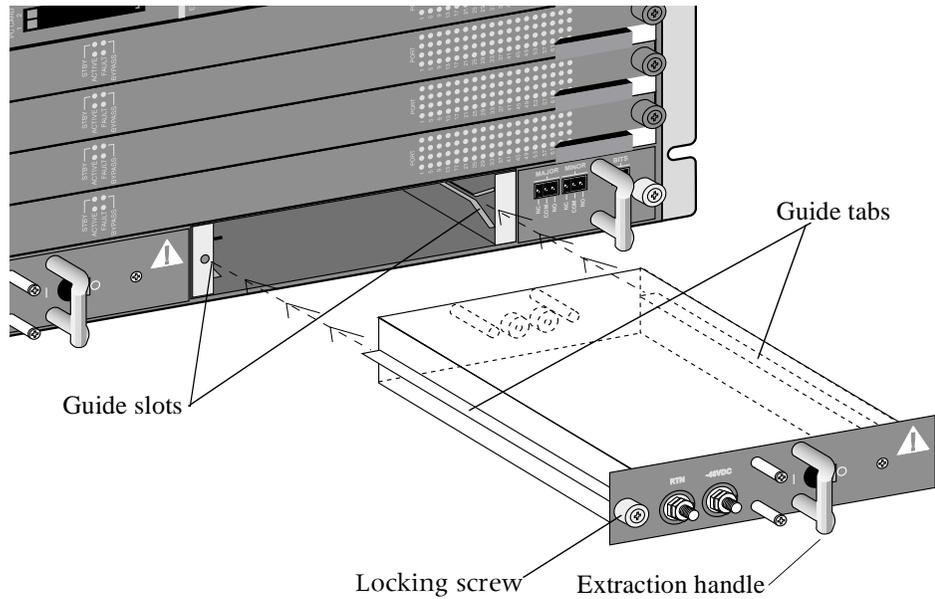
Replacing a power filter

The power filters are located in the front of the chassis. Before replacing a power filter, the Stinger unit must be removed from service and there must not be any supply voltage on the cables connected to the unit.

To replace a power filter:

- 1 Verify that power has been removed from the cables that connect to the power filter.
- 2 Remove the protective cover and power cables from the power filter, as illustrated in Figure 3-1 on page 3-2.
- 3 Using a number 2 Phillips screwdriver, fully loosen the power filter locking screw, shown in Figure 6-5.
- 4 Grasp the extraction handle of the power filter and pull it straight out of the chassis.

Figure 6-5. Replacing a power filter



- 5** Align the guide tabs on either side of the replacement power filter with the guide slots in the chassis.
- 6** Carefully slide the replacement power filter into the chassis and press firmly to engage the power connector.
- 7** Fully tighten the locking screw on the replacement power filter.

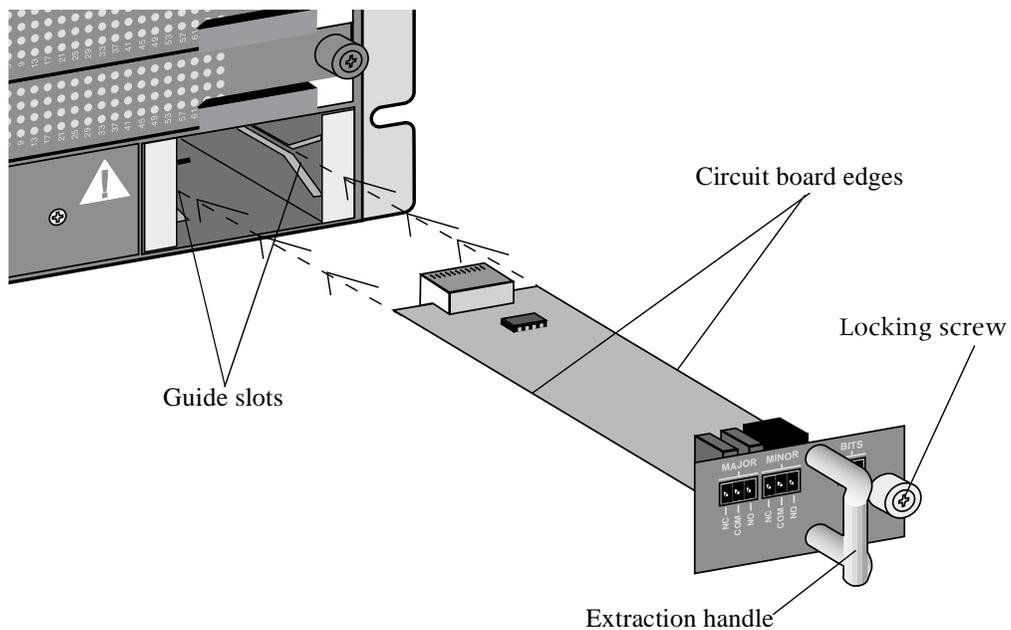
Replacing the alarm module

The alarm module is located in the front of the chassis.

To replace the alarm module:

- 1** Remove any connections to the alarm and BITS terminals. Note the way in which any wires are connected, so they can be returned to their connections after replacement of the module.
- 2** Using a number 2 Phillips screwdriver, fully loosen the alarm module locking screw, shown in Figure 6-6.
- 3** Grasp the extraction handle of the alarm module and pull it straight out of the chassis.

Figure 6-6. Replacing an alarm module



- 4 Align the edges of the replacement alarm module circuit board with the guide slots in the chassis.
- 5 Carefully slide the replacement alarm module into the chassis and press firmly to engage the connector.
- 6 Fully tighten the locking screw on the replacement alarm module.

Stinger Intended Use



User line interfaces	A-1
Network interfaces	A-1
Control module interfaces	A-2

The Stinger unit is a DSL ATM switch that provides DSL connections for individual users. Users connect to the unit over DSL lines supported by line interface modules (LIMs) that are installed in the Stinger unit. Every Stinger unit contains a special control module that controls the operation of the unit. Two control modules can be installed in a redundant arrangement, with one active and primary, and the other a spare. The physical interfaces on the unit provide DSL or ATM network connections to digital lines, and a serial or Ethernet LAN connection for configuration and administration. Units equipped with revision 2, or later, control modules also provide interfaces for monitoring the alarm status of other devices, and an optional internal modem.

User line interfaces

Depending on the LIMs that are installed, users can connect to the Stinger unit over DSL lines supporting several DSL protocols. LIMs are available to support the following DSL connections:

- ADSL Annex A, B, or C
- ADSL G.lite
- SHDSL

See the module guide of a specific LIM for an explanation of installation and configuration options.

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

Network interfaces

The Stinger unit extracts data from the digital subscriber line and switches it to remote ATM switches depending on the configuration of virtual circuit and path information. Stinger modules are available that support ATM connections to ATM network switches over the following types of digital lines:

- T1 (individual lines or aggregated bandwidth)
- E1 (individual lines or aggregated bandwidth)
- DS3
- E3
- OC3

For an explanation of installation and configuration options, see the guide for a specific module.

Control module interfaces

The control module is equipped with the following interfaces for configuration and administration. For an explanation of basic configuration options, see Chapter 5, “Configuring the Control Module and System Timing.”

- A DB-9 female connector for an RS-232 serial connection, with the following default settings:
 - 9600bps
 - Direct connection
 - 8 data bits
 - No parity
 - 1 stop bit
 - No flow control
- A DB-9 female connector for alarm monitoring connections (revision 2 control modules).
- An RJ-45 connector for a 10/100BaseT Ethernet connection.
- An RJ-11 connector for the optional internal modem.
- A PCMCIA interface, designed to accept PCMCIA flash-memory cards. Other PCMCIA devices are not supported.
- An RJ-45 connector for copper gigabit Ethernet connections, if equipped with an appropriate IP2000 control module.
- A duplex LC connector for optical gigabit Ethernet connections, if equipped with an appropriate IP2000 control module.

Cables and Connectors



B

Diagnostic port and cable pinouts	B-1
Alarm input port pinouts	B-2
Ethernet interface specifications	B-2
LPM cable specifications	B-3

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 B-1 applies to all [Product] models that use the RS-232 pinouts.

Note .

Table B-1. Diagnostic port and cable pinouts

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

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

Alarm input port pinouts

The alarm input port, found on revision 2 control modules, consists of a DB-15 female connector. 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 these alarm relays is sensed by the TAOS software, based on continuity or lack of continuity between the pair of pins to which it is connected.

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

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

Table B-2. Alarm input pinouts

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

Ethernet interface specifications

The base Stinger unit has an Ethernet interface that supports the physical specifications of IEEE 802.3 and IEEE 802.14 with Ethernet 2 (Ethernet/DIX) framing. The unit provides a single Ethernet interface that automatically senses the Ethernet type to which it is connected. It supports the following types of Ethernet interfaces:

- 10BaseT (unshielded twisted pair): Twisted-pair Ethernet and IEEE 802.3 (10BaseT) with an RJ-45 connector, labeled LAN UTP
- 100BaseT: 100Mbps baseband modulation on twisted pair

The Ethernet address used to identify the Ethernet interface resides in the [Product] unit's motherboard.

To install the Ethernet interface, you must have the cables described in either of the following two sections.

10BaseT cables

To install a 10BaseT interface, you need a twisted-pair Ethernet cable and a dual twisted-pair cable terminated with RJ-45 modular jacks.

Use an EIA/TIA 568 or IEEE 802.3 10BaseT cable.

100BaseT cables

To install a 100BaseT interface, you need a twisted-pair Ethernet cable and a dual twisted-pair cable terminated with RJ-45 modular jacks.

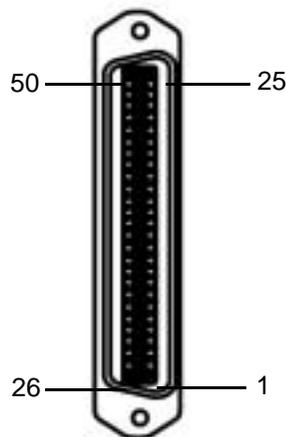
Use one of the following cables: 100BaseT2, 100BaseT4 (not very popular), 100BaseTX, or 100BaseFX.

LPM cable specifications

Depending on the type of DSL service being provided by the associated LIM, LPMs support two-wire or four-wire connections to the DSL end user.

The LPMs use USOC RJ-21X 50-pin telephone company connectors, as shown in Figure B-1.

Figure B-1. USOC RJ-21X 50-pin connector



LPM two-wire cable specifications

Depending on the number of ports provided by the associated LIM, an LPM can have one, two, or three connectors:

- Table B-3 shows the cable pinouts for the single 50-pin connector for two-wire connections on an LPM that supports LIMs with 24 ports
- Table B-4 shows the cable pinouts for the upper 50-pin connector for two-wire connections on an LPM that supports LIMs with more than 48 ports.
- Table B-5 shows the cable pinouts for the middle 50-pin connector for two-wire connections on an LPM that supports LIMs with 72 ports.

Table B-3. Single or lower connector pin assignments for two-wire connections

Pin	Signal	Color code	Pin	Signal	Color code
1	1R (line 1 ring)	Blue/white	26	1T (line 1 tip)	White/blue
2	2R	Orange/white	27	2T	White/orange
3	3R	Green/white	28	3T	White/green
4	4R	Brown/white	29	4T	White/brown
5	5R	Slate/white	30	5T	White/slate
6	6R	Blue/red	31	6T	Red/blue
7	7R	Orange/red	32	7T	Red/orange
8	8R	Green/red	33	8T	Red/green
9	9R	Brown/red	34	9T	Red/brown
10	10R	Slate/red	35	10T	Red/slate
11	11R	Blue/black	36	11T	Black/blue
12	12R	Orange/black	37	12T	Black/orange
13	13R	Green/black	38	13T	Black/green
14	14R	Brown/black	39	14T	Black/brown
15	15R	Slate/black	40	15T	Black/slate
16	16R	Blue/yellow	41	16T	Yellow/blue
17	17R	Orange/yellow	42	17T	Yellow/orange
18	18R	Green/yellow	43	18T	Yellow/green
19	19R	Brown/yellow	44	19T	Yellow/brown
20	20R	Slate/yellow	45	20T	Yellow/slate
21	21R	Blue/violet	46	21T	Violet/blue
22	22R	Orange/violet	47	22T	Violet/orange
23	23R	Green/violet	48	23T	Violet/green
24	24R	Brown/violet	49	24T	Violet/brown
25	Not used	N/A	50	Not used	N/A

Modules supporting more than 24 lines use the connections indicated in Table B-4 for the upper 50-pin connector.

Table B-4. Upper connector pin assignments for two-wire connections

Pin	Signal	Color code	Pin	Signal	Color code
1	25R (channel 1 ring)	Blue/white	26	25T (channel 1 tip)	White/blue
2	26R	Orange/white	27	26T	White/orange
3	27R	Green/white	28	27T	White/green
4	28R	Brown/white	29	28T	White/brown
5	29R	Slate/white	30	29T	White/slate
6	30R	Blue/red	31	30T	Red/blue
7	31R	Orange/red	32	31T	Red/orange
8	32R	Green/red	33	32T	Red/green
9	33R	Brown/red	34	33T	Red/brown
10	34R	Slate/red	35	34T	Red/slate
11	35R	Blue/black	36	35T	Black/blue
12	36R	Orange/black	37	36T	Black/orange
13	37R	Green/black	38	37T	Black/green
14	38R	Brown/black	39	38T	Black/brown
15	39R	Slate/black	40	39T	Black/slate
16	40R	Blue/yellow	41	40T	Yellow/blue
17	41R	Orange/yellow	42	41T	Yellow/orange
18	42R	Green/yellow	43	42T	Yellow/green
19	43R	Brown/yellow	44	43T	Yellow/brown
20	33R	Slate/yellow	45	33T	Yellow/slate
21	45R	Blue/violet	46	45T	Violet/blue
22	46R	Orange/violet	47	46T	Violet/orange
23	47R	Green/violet	48	47T	Violet/green
24	48R	Brown/violet	49	48T	Violet/brown
25	Not used	N/A	50	Not used	N/A

Modules supporting 72 lines have a third 50-pin connector that uses connections indicated in Table B-5.

Table B-5. Middle connector pin assignments for two-wire connections (72-port LIM only)

Pin	Signal	Color code	Pin	Signal	Color code
1	49R (channel 1 ring)	Blue/white	26	49T (channel 1 tip)	White/blue
2	50R	Orange/white	27	50T	White/orange
3	51R	Green/white	28	51T	White/green
4	52R	Brown/white	29	52T	White/brown
5	53R	Slate/white	30	53T	White/slate
6	54R	Blue/red	31	54T	Red/blue
7	55R	Orange/red	32	55T	Red/orange
8	56R	Green/red	33	56T	Red/green
9	57R	Brown/red	34	57T	Red/brown
10	58R	Slate/red	35	58T	Red/slate
11	59R	Blue/black	36	59T	Black/blue
12	60R	Orange/black	37	60T	Black/orange
13	61R	Green/black	38	61T	Black/green
14	62R	Brown/black	39	62T	Black/brown
15	63R	Slate/black	40	63T	Black/slate
16	64R	Blue/yellow	41	64T	Yellow/blue
17	65R	Orange/yellow	42	65T	Yellow/orange
18	66R	Green/yellow	43	66T	Yellow/green
19	67R	Brown/yellow	44	67T	Yellow/brown
20	68R	Slate/yellow	45	68T	Yellow/slate
21	69R	Blue/violet	46	69T	Violet/blue
22	70R	Orange/violet	47	70T	Violet/orange
23	71R	Green/violet	48	71T	Violet/green

Table B-5. Middle connector pin assignments for two-wire connections
(72-port LIM only) (Continued)

Pin	Signal	Color code	Pin	Signal	Color code
24	72R	Brown/violet	49	72T	Violet/brown
25	Not used	N/A	50	Not used	N/A

LPM four-wire cable specifications

A LIM that supports 24 four-wire connections, such as a T1 or E1 module, must use a 48-port LPM. Optionally, a 24-port LPM can be used for any LIM supporting 12 or fewer four-wire ports. Table B-6 shows the USOC RJ-21X cable pinouts for the lower 50-pin connector for four-wire connection. Table B-7 shows the cable pinouts for the upper 50-pin connector.

Table B-6. Lower connector pin assignments for four-wire connections

Four-wire interface	Transmit tip	Transmit ring	Receive tip	Receive ring
1	Pin 26	Pin 1	Pin 27	Pin 2
2	Pin 28	Pin 3	Pin 29	Pin 4
3	Pin 30	Pin 5	Pin 31	Pin 6
4	Pin 32	Pin 7	Pin 33	Pin 8
5	Pin 34	Pin 9	Pin 35	Pin 10
6	Pin 36	Pin 11	Pin 37	Pin 12
7	Pin 38	Pin 13	Pin 39	Pin 14
8	Pin 40	Pin 15	Pin 41	Pin 16
9	Pin 42	Pin 17	Pin 43	Pin 18
10	Pin 44	Pin 19	Pin 45	Pin 20
11	Pin 46	Pin 21	Pin 47	Pin 22
12	Pin 48	Pin 23	Pin 49	Pin 24

Table B-7. Upper connector pin assignments for four-wire connections

Four-wire interface	Transmit tip	Transmit ring	Receive tip	Receive ring
13	Pin 26	Pin 1	Pin 27	Pin 2
14	Pin 28	Pin 3	Pin 29	Pin 4
15	Pin 30	Pin 5	Pin 31	Pin 6
16	Pin 32	Pin 7	Pin 33	Pin 8
17	Pin 34	Pin 9	Pin 35	Pin 10
18	Pin 36	Pin 11	Pin 37	Pin 12
19	Pin 38	Pin 13	Pin 39	Pin 14
20	Pin 40	Pin 15	Pin 41	Pin 16
21	Pin 42	Pin 17	Pin 43	Pin 18
22	Pin 44	Pin 19	Pin 45	Pin 20
23	Pin 46	Pin 21	Pin 47	Pin 22
24	Pin 48	Pin 23	Pin 49	Pin 24

Safety-Related Electrical, Physical, and Environmental Information



Electrical and electronic information	C-1
Physical specifications	C-3
Site specifications	C-4
Special requirements and recommendations for installation and maintenance .	C-5

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



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

Electrical and electronic information

Electrical and electronic information for Stinger units includes specifications, universal service order code (USOC) information, ground wire size, and electromagnetic interference (EMI) class.

Electronic and electrical specifications

The Stinger unit is nominally powered from a -48Vdc source. This source is wired to the power filters on the left side at the front of the chassis. Table C-1 describes Stinger MS+ electronic and electrical specifications.

Table C-1. *Stinger electronic and electrical specifications*

Application	Specification
-48Vdc	17 amps, 770 watts (W) maximum
Input voltage	-40Vdc to -72Vdc
Inrush current	Minimal because all modules have inrush-limiting circuits
Power cable	In accordance with national standards and specifications as described in EN/IEC 60950 (CE)

Table C-1. *Stinger electronic and electrical specifications (Continued)*

Application	Specification
Connectors	Number 10 terminal lugs
Circuit breaker	50A
Standards	Bellcore GR-1089-CORE, classified A2

USOC jack and code information

Stinger equipment complies with Part 68 of the U.S. Federal Communications Commission (FCC) Rules and uses the universal service order code (USOC) jack type and code shown in Table C-2. For information about FCC Part 68, see the *Edge Access and Broadband Access Safety and Compliance Guide*.

Table C-2. *Stinger T1 module USOC jacks and codes*

Model name	Facility interface code	Service order code	Jack type
STGR-LIM-T1-8	04DU9-BN	6.0N	RJ-48C
STGR-LIM-T1-8	04DU9-DN	6.0N	RJ-48C
STGR-LIM-T1-8	04DU9-1KN	6.0N	RJ-48C
STGR-LIM-T1-8	04DU9-1SN	6.0N	RJ-48C
STGR-LIM-T1-8	04DU9-1ZN	6.0N	RJ-48C
STGR-LIM-T1-24	04DU9-BN	6.0N	RJ-48C
STGR-LIM-T1-24	04DU9-DN	6.0N	RJ-48C
STGR-LIM-T1-24	04DU9-1KN	6.0N	RJ-48C
STGR-LIM-T1-24	04DU9-1SN	6.0N	RJ-48C
STGR-LIM-E1-24	04DU9-1ZN	6.0N	RJ-48C
STGR-LIM-E1-8	04DU9-BN	6.0N	RJ-48C
STGR-LIM-E1-8	04DU9-DN	6.0N	RJ-48C
STGR-LIM-E1-8	04DU9-1KN	6.0N	RJ-48C
STGR-LIM-E1-8	04DU9-1SN	6.0N	RJ-48C
STGR-LIM-E1-8	04DU9-1ZN	6.0N	RJ-48C
STGR-LIM-E1-24	04DU9-BN	6.0N	RJ-48C
STGR-LIM-E1-24	04DU9-DN	6.0N	RJ-48C

Table C-2. Stinger T1 module USOC jacks and codes (Continued)

Model name	Facility interface code	Service order code	Jack type
STGR-LIM-E1-24	04DU9-1KN	6.0N	RJ-48C
STGR-LIM-E1-24	04DU9-1SN	6.0N	RJ-48C
STGR-LIM-E1-24	04DU9-1ZN	6.0N	RJ-48C

EMI class

The Stinger product belongs to EMI class A.

Minimum ground wire size

The DSL lines connected to the Stinger FS and Stinger FS+ 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. The wire gauges shown in Table C-3 are appropriate for the wire lengths indicated.

Table C-3. Stinger FS minimum ground wire sizes

Length	Wire gauge
0 to 10 feet (0m to 3.05m)	12 AWG (3.31mm ²)
10 to 25 feet (3.05m to 7.62m)	9 AWG (6.63mm ²)
25 to 50 feet (7.62m to 15.24m)	6 AWG (13.3mm ²)
50 to 100 feet (15.24m to 30.48m)	3 AWG (26.7mm ²)

Lucent Technologies does not recommend use of a ground wire longer than 100 feet (30.48m).

Physical specifications

Table C-4 describes the Stinger MS+ physical specifications.

Table C-4. Stinger MS+ physical specifications

Specification	Description
ATM standards	ATM Forum UNI (Version 3.0 and Version 3.1), ATM Forum Interim Interswitch Signaling Protocol (IISP)

Table C-4. Stinger MS+ physical specifications (Continued)

Specification	Description
WAN interfaces	DS3 and E3 (cell-based), OC3c/STM-1 (optical and electrical), T1, E1, and Ethernet
Management interfaces	Ethernet and RS-232
Physical characteristics	Basic unit includes two dc power filters, one control module, one trunk module, and up to four pairs of LIMs and LPMs
Overall chassis size ^a	Height: 7 inches (17.78cm) Depth: 15.35 inches (39cm) Width: 17.7 inches (44.9cm)
Unit weight	66 pounds (30kg) maximum (fully configured)

a. The depth measurement does not include calculations for cable spacing.

Site specifications

Stinger units require a particular operating environment and minimum clearance for proper operation (see “Space requirements”).

Operating environment

Table C-5 describes the environmental requirements for selecting an installation site for the Stinger MS+ hardware. The site requirements are based on Network Equipment Building System (NEBS) GR-63-CORE and GR-1089-CORE.

Table C-5. Stinger MS+ site specifications

Parameter	Requirement
Ambient operating temperature	0°C to 55°C (32°F to 131°F)
Relative humidity	10% to 95% (noncondensing)
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 Stinger MS+ hardware requires the following minimum clearances for the chassis:

- 20 inches (54cm) at the front panel for module replacement and cable routing
- 16 inches (40.6cm) at the back panel for module replacement and cable routing
- 3 in. (75mm) on either side of the chassis for airflow recommended (2 in. [50mm] min.)

Special requirements and recommendations for installation and maintenance

Follow these requirements and recommendations for Stinger installation and maintenance.

Lifting requirements

Use a mechanical lift or at least two people to lift a fully loaded Stinger MS+ chassis for rack mounting. For more information, see “Mounting the unit” on page 2-1.

Index



A

- activity, system 4-4
- addresses, IP
 - assigning for Ethernet 5-12
 - syntax 5-10
- admin login, recommended password change 5-8
- administrative access, restricting 5-7
- administrative connections 5-1
- alarm input
 - description B-2
 - pinouts B-2
- alarm monitoring
 - alarm module 2-7
 - Stinger monitoring other devices 2-8
- alarm relays, connecting
 - to monitor other devices 2-8
 - to monitor the Stinger 2-7
- altitude
 - operating C-4
 - storage C-4
- ATM, standards C-3

B

- backup management via external modem 5-3
- backups 4-5
- BITS clock source
 - changing 5-16
 - loss of 5-15
 - using 5-15

C

- cables
 - 100Base-T B-3
 - 10Base-T B-3
 - connecting 2-3
 - diagnostic port B-1
 - LPM four-wire B-7

- LPM two-wire B-3
- serial port B-1
- changing default logins 5-7
- chassis
 - size C-4
- clock source
 - BITS 5-15
 - connecting inputs and outputs 2-7
 - LIM 5-16
 - modes 4-3
 - trunk ports 5-17
- command help 4-5
- command-line interface, introduced 4-3
- commands
 - Dir 5-7
 - listing 4-4
 - Ping 5-14
 - Read and Write 5-12
 - Set 5-12
 - STATUS 4-5
- configuration
 - basic IP 5-9
 - initial serial port login 5-6
 - overview 4-2
- connecting
 - clock inputs and outputs 2-7
 - power cord to -48 Vdc power supply 3-1
- console terminal, connecting and setting up 5-2
- control module
 - functions 1-3
 - interfaces checking 1-8
- control modules
 - cautions about replacing 6-1
 - configuration overview 5-1
 - installing and replacing 6-2
 - interface-independent address 5-13
 - primary, logging into 5-6
 - status lights 3-3
- cooling module status lights 3-5

D

- default route, IP 5-13

Index

E

DIAG PORT. *See* serial port
DS3-ATM trunk modules
 checking 1-11
 clock source 5-14
 clock source settings 5-17
 connecting 2-5
DSLAM, diagram of operations 4-1

E

E3-ATM trunk modules
 checking 1-11
 clock-source 5-17
 connecting 2-5
electronic specifications C-1
electrostatic discharge (ESD) jack 1-6
EMI class C-3
environmental specifications C-4
ESD, grounding jack 1-6
Ethernet
 interface specifications B-2
 required equipment B-2, B-3
Ethernet ports
 IP addresses 5-12
 on control modules 4-2

F

fault tolerance
 controller IP address 5-12
flash memory
 backups 4-5
 upgrades 4-4

G

ground wire size C-3

H

hardware, verifying configuration 1-6
humidity requirement C-4

I

installation
 completing 3-1
 considerations 6-1

modules 6-1
mounting the unit 2-1
preparing the site 1-3
prerequisites 2-1
required tools 1-4
selecting a site 1-3
intended use A-1
IP
 address syntax 5-10
 addresses for control module Ethernet ports 5-12
 default route 5-13
 host routes 5-12
 minimal configuration 5-9
 soft interface address 5-13
 subnet notation 5-11
IP2000 control module xiii, 1-8
IP-Global profile 5-9
IP-Interface profile 5-12
IP-Route profiles 5-13

L

LAN connection 5-14
LAN UTP port interface B-2
LEDs. *See* status lights
lifting requirements C-5
LIM
 configuration overview 4-2
 function 1-3
 installing and replacing 6-5
logging into the Stinger 5-6
LPM
 connecting 2-3
 four-wire pinouts B-7
 function 1-3
 installing and replacing 6-6
 two-wire pinouts B-3

M

management
 backup connection via external modem 5-3
 backup connection via internal modem 5-5
 features 4-3
 types of connections supported 2-6, C-4
modems
 country codes 5-4
 dial-in management through 5-3
modules
 installation and replacement considerations

6-1

N

netmask 5-11

O

OC3-ATM trunk modules

checking 1-10, 1-11

clock source 5-14

clock-source settings 5-17

connecting 2-5

online help, commands 4-5

P

passwords

changing defaults 5-8

Telnet 5-9

PCMCIA cards

described 1-9

installing and replacing 6-8

permission levels 4-3

pinouts

alarm input B-2

LPM four-wire B-7

LPM two-wire B-3

plug-in components

control module 1-3

LIM 1-3

LPM 1-3

power filter 1-3

power filter

function 1-3

power supplies

-48 Vdc, connecting power to 3-1

powering up, described 3-2

preventing static discharge damage 1-4

primary control module. *See* control modules

profiles

IP-Global 5-9

IP-Interface 5-12

IP-Route 5-13

modem 5-6

Serial 5-7

User 5-8

R

rack-mounting the unit 2-3

S

security

changing admin password 5-8

changing default logins 5-7

Telnet password 5-9

serial port

initial login to unit 5-6

restricting access 5-7

Serial profile 5-7

size of chassis C-4

slot numbering 6-5

SNMP support 4-4

soft interface address 5-13

space requirements C-5

specifications

cable pinouts B-1

electrical C-1

EMI class C-3

environmental C-4

Ethernet interface B-2

physical C-3

space C-5

special requirements and recommendations
C-5

USOC jack and code C-2

startup sequence 3-2

static discharge damage 1-4

preventing 1-4

status lights

control module 3-3

cooling module 3-5

status windows, displaying 4-5

subnet mask 5-11

subnet notation 5-11

subscriber lines

connecting 2-4

system activity, tracking 4-4

T

Telnet password 5-9

temperature

operating C-4

storage C-4

terminal emulation settings, required 1-4, 5-6

Index

U

TFTP, downloading files 4-3
timing subsystem 4-3
tools and equipment required for installation 1-4
TRAM module
 checking 1-11
trunk modules
 clock source 5-17
 configuration overview 4-3
 overview 4-3
 See also DS3-ATM trunk modules
 See also E3-ATM trunk modules
 See also OC3-ATM trunk modules

U

unpacking the unit 1-6
use of wrist strap 1-4
user interface, terminal configuration for 1-4
User profile 5-8
USOC jack and code information C-2

V

vendor-specific attribute (VSA) requirements,
 RADIUS 4-4

W

WAN interfaces supported C-4
weight of unit C-4
workstation, connecting 5-2