Lucent Technologies
Bell Labs Innovations

Stinger®

ATM Configuration Guide

Part Number: 7820-0765-006
For software version 9.5-206
August 2003

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.

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

Ordering Information

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

Feedback

Lucent Technologies appreciates customer comments about this manual. Please send them to techcomm@lucent.com.

Lucent Technologies

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

Figures

Tables

About This Guide

To use the information in this guide, you must have already installed the Stinger unit and configured its physical interfaces. For information about configuring physical interfaces, see the individual module guides for the line interface modules (LIMs) or trunk modules supported in the system.

Instructions for installing and configuring the management functions of the system are found in the *Getting Started Guide* for your Stinger platform.

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 the "Safety-Related Physical, Environmental, and Electrical Information" appendix in the *Getting Started Guide* for your Stinger unit.

What is in this guide

This guide focuses on Asynchronous Transfer Mode (ATM) switching and permanent virtual circuits (PVCs). It also describes bandwidth and virtual connection provisioning in the system, flexible queuing of the controller ATM switch, and the Stinger implementation of standard ATM features such as quality of service (QoS) and connection admission control (CAC).

The Stinger platform has several models, each of which can support hardware modules and licensing options for transport or termination methods that are not covered in this guide. For example, you might need one of the following documents:

- *Stinger Private Network-to-Network Interface (PNNI) Supplement*, for information about soft PVC (SPVC) ATM circuits
- *Stinger IDSL 32-Port Line Interface Module (LIM) Guide*, for information about cross-connections between frame relay and FRF8 ATM
- *Stinger IP2000 Configuration Guide*, for information about IP termination and Gigabit Ethernet configuration

Stinger units with a trunk aggregation module (TRAM) are often used for subtending applications. For details about that module and how it expands system capacity, see the *Stinger Trunk Aggregation Module (TRAM) Guide.*

If you use Simple Network Management Protocol (SNMP) utilities to manage the system, see the *Stinger SNMP Management of the ATM Stack*.

Documentation conventions

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

Convention	Meaning
`Monospace text`	Represents text that appears on your computer's screen, or that could appear on your computer's screen.
`Boldface monospace text`	Represents characters that you enter exactly as shown (unless the characters are also in ***`italics`***—see *Italics*, below). If you could enter the characters but are not specifically instructed to, they do not appear in boldface.
Italics	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 Stinger platform. Shows how to install your Stinger chassis and hardware. This guide also shows you how to use the command-line interface to configure and verify IP access and basic access security on the unit, and how to configure Stinger controller redundancy on units that support it.
  - Module guides. For each Stinger line interface module (LIM), trunk module, or other type of module, 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 integrate the Stinger into the ATM and Digital Subscriber Line (DSL) access infrastructure. The guide explains how to configure 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 controller, this guide describes how to integrate the system into the IP infrastructure. Topics include IP-routed switch-through ATM PVCs and RFC 1483 PVCs that terminate on the IP2000, IEEE 802.1Q VLAN, and forwarding multicast video transmissions on DSL interfaces.
  - *Stinger Private Network-to-Network Interface (PNNI) Supplement*. For the optional PNNI software, this guide provides quick-start instructions for configuring PNNI and soft PVCs (SPVCs), and describes the related profiles and commands.
  - *Stinger SNMP Management of the ATM Stack Supplement.* Describes 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.
  - *Stinger T1000 Module Routing and Tunneling Supplement.* For the optional T1000 module, this guide describes how to configure the Layer 3 routing and virtual private network (VPN) capabilities.
- **RADIUS:** *TAOS RADIUS Guide and Reference*. Describes how to set up a unit to use the Remote Authentication Dial-In User Service (RADIUS) server and contains a complete reference to RADIUS attributes.
- **Administration and troubleshooting:** *Stinger Administration Guide*. Describes how to administer the Stinger unit and manage its operations. Each chapter

focuses on a particular aspect of Stinger administration and operations. The chapters describe tools for system management, network management, and Simple Network Management Protocol (SNMP) management.

- **Reference**:
  - *Stinger Reference*. An alphabetic reference to Stinger profiles, parameters, and commands.
  - *TAOS Glossary*. Defines terms used in documentation for Stinger units.

Stinger ATM Overview

1

Stinger units support ATM switching for user data sessions. Unless the system has an IP2000 controller or an optional T1000 module, it does not support IP routing for user data sessions. For information about using IP routing for user data sessions, see the *Stinger IP2000 Configuration Guide* or *Stinger T1000 Routing and Tunneling Supplement*.

ATM switching operations

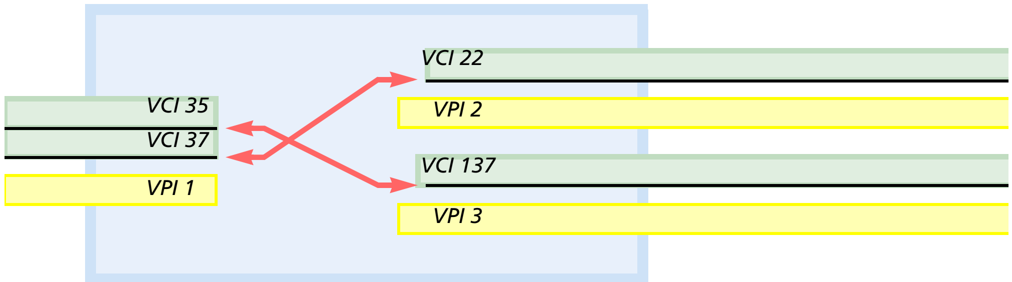
An ATM virtual circuit is a point-to-point connection between an end system (such as a CPE device) and an end point in the ATM network (the point at which the cell stream leaves the ATM layer). The cells of a virtual circuit are identified in the ATM cell headers by a virtual path identifier (VPI) and a virtual channel identifier (VCI). Because the headers specify two identifiers, an ATM switch can support two types of virtual connection and switching operations:

- A virtual channel connection (VCC) is identified by VPI-VCI pair. Switching on the basis of VPI-VCI pairs is called virtual channel (VC) switching.
- A virtual path connection (VPC) is identified by the VPI only. A VPC is a bundle of VCCs, all of which use the same VPI. Switching based solely on the VPI number is called virtual path (VP) switching.

VC switching

In VC switching, a Stinger unit examines both the VPI and VCI fields of ATM cell headers and relays the cell stream to its egress interface on the basis of both values. An example of how VC switching works is shown in Figure 1-1. During the switching operation, both the VPI and VCI values are examined and possibly changed in each cell header.

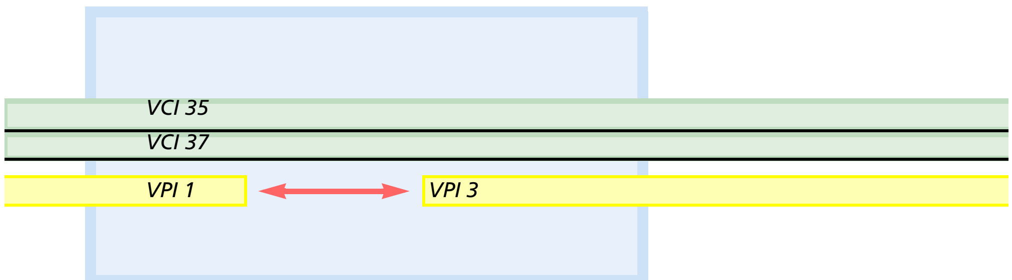
Figure 1-1. VC switching



VP switching

In VP switching, a Stinger unit examines only the VPI field, and relays the cell stream to its egress interface on the basis of that value alone. An example of how VP switching works is shown in Figure 1-2.

Figure 1-2. VP switching



In VP switching, the VCI is not changed. Each virtual channel in the virtual path has the same VCI number on the egress interface as on the ingress interface.

VP switching is not supported between line interface module (LIM) interfaces, and it cannot be configured in RADIUS profiles. For details about limitations on VP switching on LIMs, see "VPI-VCI configuration for trunk interfaces" on page 3-2.

Types of permanent virtual circuits (PVCs)

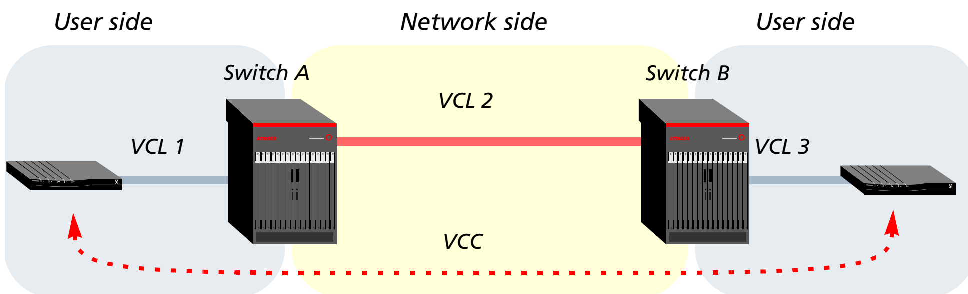
ATM permanent virtual circuits (PVCs) are manually configured connections. A PVC can be a virtual link that terminates in the Stinger unit or a virtual link that is switched to another virtual link on a different interface (a cross-connect). In the Stinger command-line interface, a cross-connect is called an *ATM circuit*.

When Private Network-to-Network Interface (PNNI) is enabled, Stinger units also support soft PVCs (SPVCs). For details about SPVCs, see the *Stinger Private Network-to-Network Interface (PNNI) Supplement*.

Overview of ATM virtual connections

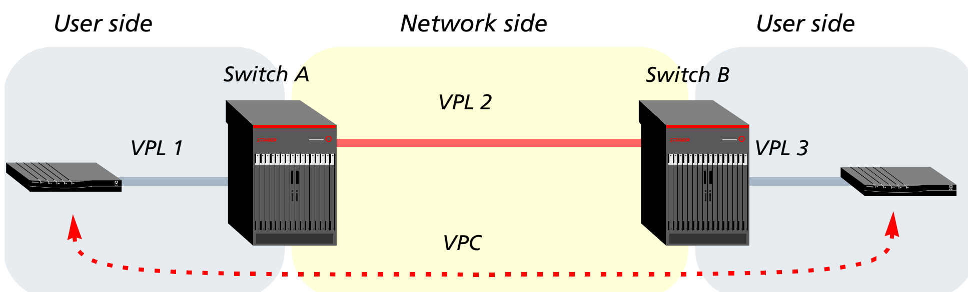
An ATM connection between one device and another is a *virtual link*. Multiple virtual links can be concatenated across several ATM switches to form *virtual connections* between two end points. When virtual links are switched using VC switching, they are virtual channel links (VCLs). When concatenated across multiple switches, VCLs form a virtual channel connection (VCC), as shown in Figure 1-3.

Figure 1-3. Virtual channel links forming a VCC



Each switch along the path receives the cell stream on one interface and transmits it on another, a function called a *cross-connect.* When virtual links are switched using VP switching, they are virtual path links (VPLs). Figure 1-4 shows multiple VPLs concatenated to form a virtual path connection (VPC).

Figure 1-4. Virtual path links forming a VPC



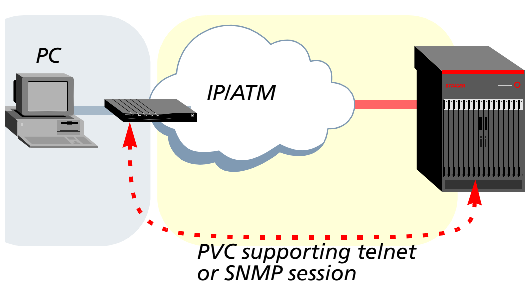
The individual virtual links inherit traffic characteristics (such as service category) from the VCC or VPC of which the link is a part.

Terminating PVCs for management connections

A terminating PVC uses a single interface in the Stinger unit. Typically, terminating connections are used for logging into the Stinger interface for management purposes. For ATM adaptation layer 5 (AAL5) connections, the cell stream terminates in the Stinger unit, where it is reassembled into packets and processed as a data stream.

A terminating PVC can consist of a single virtual link, or can be concatenated across multiple switches in the ATM network to terminate in the Stinger unit. Figure 1-5 shows a terminating PVC on an AAL5 interface.

Figure 1-5. Terminating PVCs on AAL5 interfaces

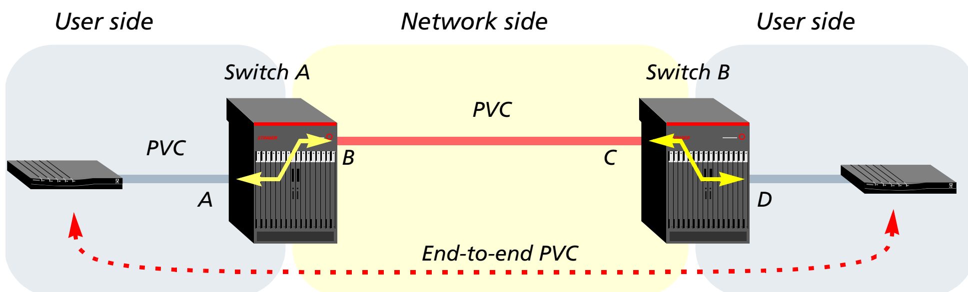


Cross-connect PVCs or ATM circuits

In the Stinger command-line interface, you configure a PVC cross-connect by creating an *ATM circuit* configuration in a `connection` profile. For PVCs, you must manually specify both sides of the circuit.

For example, Figure 1-6 shows a PVC connection between two end points across two switches. Switch A has an ATM circuit configuration between two PVCs on its interfaces labeled A and B. Switch B has a similar ATM circuit configuration on its interfaces labeled C and D.

Figure 1-6. PVC with cross-connects in each switch



Maximum number of PVCs with the current software version

In an environment that supports only PVCs, the Stinger unit supports up to 3200 active PVCs. For information about virtual circuit guidelines in a mixed environment that supports both PVCs and SPVCs, see the *Stinger Private Network-to-Network Interface (PNNI) Supplement*.

Introduction to ATM-related profiles and commands

Table 1-1 lists the profiles you use to configure ATM interfaces and connections when PNNI has not been enabled, and shows where to find information about using the profiles. For details about specific types of physical interfaces (LIMs, trunks, or TRAMs), see the relevant module guide.

Table 1-1. List of ATM configuration profiles described in this guide

Profile	Where to find related information
`atm-addr-alias`	*Stinger Private Network-to-Network Interface (PNNI) Supplement*
`atm-config`	Chapter 2, "Bandwidth Management," Chapter 3, "VPI-VCI Allocation on ATM Interfaces," and Chapter 7, "Terminating PVC Configuration."
`atm-if-config`	Chapter 3, "VPI-VCI Allocation on ATM Interfaces," and Chapter 8, "SNMP MIB Support."
`atm-if-sig-params`	*Stinger Private Network-to-Network Interface (PNNI) Supplement*
`atm-if-stat`	Chapter 3, "VPI-VCI Allocation on ATM Interfaces"
`atm-internal`	*Stinger T1000 Module Configuration Guide*
`atm-oam`	*Stinger Administration Guide*

Table 1-1. List of ATM configuration profiles described in this guide (Continued)

Profile	Where to find related information
atm-prefix	*Stinger Private Network-to-Network Interface (PNNI) Supplement*
atm-qos	Chapter 2, "Bandwidth Management," Chapter 4, "Configurable Quality of Service," Chapter 5, "Queues and VP Shaping," Chapter 6, "ATM Circuit Configuration," and Chapter 7, "Terminating PVC Configuration."
atm-spvc-addr-config	*Stinger Private Network-to-Network Interface (PNNI) Supplement*
atm-spvc-config	*Stinger Private Network-to-Network Interface (PNNI) Supplement*
atm-vcl-config	Chapter 8, "SNMP MIB Support"
atm-vpl-config	Chapter 8, "SNMP MIB Support"
atmpvc-stat	*Stinger Administration Guide*
atmvcc-stat	*Stinger Administration Guide*
bandwidth-stats	Chapter 2, "Bandwidth Management,"
connection	Chapter 6, "ATM Circuit Configuration," Chapter 2, "Bandwidth Management," and Appendix A, "CALEA Compliance."
high-speed-slot-static-config	Chapter 2, "Bandwidth Management" and Chapter 5, "Queues and VP Shaping"
slot-static-config	Chapter 2, "Bandwidth Management" and Chapter 5, "Queues and VP Shaping"
switch-config	Chapter 5, "Queues and VP Shaping"

The *Stinger Reference* also contains entries for each profile and parameter in the Stinger command-line interface. Additional profiles for configuring ATM interfaces are described in the *Stinger Private Network-to-Network Interface (PNNI) Supplement*. The *Stinger Adminstration Guide* describes monitoring the status of active interfaces.

To provide information about active virtual links, the software supports the following ATM-related commands:

```
admin> ? | grep atm
 atmConnectionFailures        ( system )
 atmInternalLines             ( system )
 atmqos                       ( system )
 atmsig                       ( system )
 atmtrunkmgr                  ( diagnostic )
 atmtrunkreset                ( diagnostic )
 atmvccstat                   ( system )
 atmvcl                       ( system )
 atmvcx                       ( system )
 atmvpl                       ( system )
 atmvpx                       ( system )
```

These ATM commands are described in the *Stinger Reference*. Examples of how to use the commands are provided in the *Stinger Adminstration Guide*. Some examples of command usage are also shown in Chapter 6, "ATM Circuit Configuration."

Bandwidth Management

2

The division of a Stinger unit's total bandwidth among its active connections is influenced by a number of important factors, including how the LIM bandwidth is distributed in the `atm-config` profile, connection admission control (CAC), quality of service (QoS) guarantees, and trunk-side virtual path shapers. This chapter describes CAC and LIM bandwidth allocation on all Stinger platforms except the Stinger MRT.

Note Stinger MRT units do not support configurable upstream bandwidth.

For information about configuring and applying QoS guarantees, see Chapter 4, "Configurable Quality of Service." For information about applying virtual path shapers to a trunk interface, see Chapter 5, "Queues and VP Shaping."

Configuring allowed guaranteed upstream bandwidth

The Stinger system supports a maximum upstream payload bandwidth of 599,040Kbps for guaranteed connections from all LIMs. Additional upstream payload bandwidth is allocated separately for internal management. Guaranteed connections are connections with constant bit rate (CBR), realtime variable bit rate (rtVBR) or non-realtime VBR (nrtVBR) QoS contracts.

Each LIM is configured with an allowed guaranteed upstream bandwidth (set by default to 42,500Kbps per LIM). The sum of allowed guaranteed upstream bandwidth over all LIMs cannot exceed 599,040Kbps. Connection admission control ensures that contracted upstream bandwidth for all guaranteed connections associated with a LIM does not exceed the configured allowed guaranteed bandwidth for each LIM, and thereby does not exceed the system limit for guaranteed upstream bandwidth of 599,040Kbps for all LIMs.

Note The Stinger MRT system determines the correct LIM bandwidth value automatically, so the `bandwidth-config` subprofile does not appear in the `atm-config` profile on those systems.

Notice about reconfiguring upstream bandwidth

When you reconfigure the allowed guaranteed upstream bandwidth of a LIM slot in the `atm-config` profile, the system checks that the new bandwidth value is not less than the bandwidth currently guaranteed for connections on that slot. Otherwise, some connections would fail due to CAC calculations.

For example, if 39,304Kbps bandwidth has been guaranteed for connections and you attempt to reduce the guaranteed bandwidth to 39,000Kbps, the system refuses to write the `atm-config` profile and displays a message such as the following:

```
ERROR: Slot 1 guaranteed up B/W (39000) is less than current B/W (39304)
```

To reduce the bandwidth below what has been assigned to active connections, you must first put those connections out of service administratively by setting `active` to `no` in the `connection` profiles.

Overview of LIM `bandwidth-config` settings

The system recognizes the total upstream payload bandwidth of 599,040Kbps, of which a default guaranteed upstream bandwidth of 42,500Kbps is allocated to each of the 14 LIM slots. These payload rates for each LIM are configurable in the following settings. Although you can adjust the upstream bandwidth of a particular LIM slot, the total LIM upstream bandwidth cannot exceed 599,040Kbps.

```
[in ATM-CONFIG:bandwidth-config]
bandwidth-config[1] = { 70000 42500 }
bandwidth-config[2] = { 70000 42500 }
bandwidth-config[3] = { 70000 42500 }
bandwidth-config[4] = { 70000 42500 }
bandwidth-config[5] = { 70000 42500 }
bandwidth-config[6] = { 70000 42500 }
bandwidth-config[7] = { 70000 42500 }
bandwidth-config[10] = { 70000 42500 }
bandwidth-config[11] = { 70000 42500 }
bandwidth-config[12] = { 70000 42500 }
bandwidth-config[13] = { 70000 42500 }
bandwidth-config[14] = { 70000 42500 }
bandwidth-config[15] = { 70000 42500 }
bandwidth-config[16] = { 70000 42500 }
```

```
[in ATM-CONFIG:bandwidth-config[n]]
allow-max-up-stream-bandwidth = 70000
allow-guaranteed-up-stream-bandwidth = 42500
```

Parameter	Setting
`allow-max-up-stream-bandwidth`	Maximum upstream bandwidth for the slot, expressed in kilobits per second. Valid values are from 0 to 148,598 (payload OC3 bandwidth). The default value is 70,000Kbps for a LIM.
`allow-guaranteed-up-stream-bandwidth`	Guaranteed upstream bandwidth for the slot, expressed in kilobits per second. Valid values are from 0 to 148,598 (payload OC3 bandwidth). The default value is 42,500Kbps for a LIM.

Guaranteed vs. maximum upstream bandwidth

Each LIM is configured with an allowed maximum upstream payload bandwidth, which is set by default to 70,000Kbps. You can increase this value up to a maximum of 148,598Kbps for any LIM by setting the `allow-max-up-stream-bandwidth` parameter. Upstream traffic is shaped by the LIM to the specified maximum bandwidth. The portion of bandwidth for guaranteed connections that exceeds the allowed guaranteed upstream bandwidth on a LIM is not guaranteed, although the system makes its best effort to deliver it.

The slot must be able to send upstream traffic at up to the specified `allow-guaranteed-up-stream-bandwidth` value even when the system is heavily loaded or the network is congested. The total guaranteed upstream bandwidth of all slots cannot exceed the maximum upstream payload capacity of the system. Typically, guaranteed connections are provided for applications that have stringent delay and cell loss requirements, such as voice or video applications.

Guidelines for high-bandwidth LIMs

For some high-bandwidth LIMs, the default `allow-max-up-stream-bandwidth` setting of 70,000Kbps is too low, a condition that can cause a fully loaded LIM to drop upstream data cells. For example, the 48-port SDSL LIM (STGR-LIM-SQ-48), which provides high-speed symmetric data transfer up to 2.3Mbps per interface, requires a maximum upstream bandwidth setting of 112,000Kbps to accommodate all of its ports (48 × 2.32 = 112). For this LIM and any other LIM that supports greater than 70Mbps upstream bandwidth, you must configure the `allow-max-up-stream-bandwidth` setting to prevent the module from dropping data cells when it is fully loaded.

For example, the following commands increase the maximum allowed upstream bandwidth for a 48-port SDSL LIM in slot 1:

```
admin> read atm-config
ATM-CONFIG read

admin> set bandwidth-config 1 allow-max = 112000

admin> write -f
ATM-CONFIG written
```

Sample configuration that redistributes upstream bandwidth

The following commands reallocate the upstream bandwidth capacity of the system by increasing guaranteed bandwidth to the LIMs in slots 4 and 5, and decreasing guaranteed bandwidth for slots 11 through 16:

```
admin> read atm-config
ATM-CONFIG read

admin> set bandwidth-config 4 allow-max = 148598

admin> set bandwidth-config 4 allow-guaranteed = 70000

admin> set bandwidth-config 5 allow-max = 148598

admin> set bandwidth-config 5 allow-guaranteed = 70000

admin> set bandwidth-config 11 allow-guaranteed = 41400

admin> set bandwidth-config 12 allow-guaranteed = 41400

admin> set bandwidth-config 13 allow-guaranteed = 41400
```

```
admin> set bandwidth-config 14 allow-guaranteed = 41400
admin> set bandwidth-config 15 allow-guaranteed = 41400
admin> set bandwidth-config 16 allow-guaranteed = 41400
admin> write -f
ATM-CONFIG written
```

The LIMs in slots 4 and 5 each have a guaranteed upstream bandwidth of 70,000Kbps rather than the default 42,500Kbps. This is a combined increase of 55,000Kbps bandwidth, for which a compensating decrease must be configured on some of the remaining LIMs. In the sample commands, the LIMs in slots 11 through 16 each have a guaranteed upstream bandwidth of 41,400Kbps. The bandwidth of each of those slots has been reduced by 11,000Kbps, for a combined decrease of 55,000Kbps.

Displaying `bandwidth-stats` information

The `bandwidth-stats` profile is a static, read-only profile that reports current bandwidth statistics of the system. Its settings show the maximum upstream bandwidth the system can handle and how much of the trunk bandwidth is in use on active ports. Following are the relevant parameters, shown with default values:

```
[in BANDWIDTH-STATS]
max-upstream-bandwidth = 599040
active-upstream-bandwidth-on-trunks = 0
standby-upstream-bandwidth-on-trunks = 0
```

Parameter	Indicates
`max-upstream-bandwidth`	Maximum upstream bandwidth of all configured LIMs, in kilobits per second.
`active-upstream-bandwidth-on-trunks`	Active trunk-side bandwidth, in kilobits per second.
`standby-upstream-bandwidth-on-trunks`	*Not currently used.* Total bandwidth of standby trunks. A standby trunk becomes active and takes over traffic handling only when an active trunk becomes unavailable.

Connection admission control

Connection admission control (CAC) calculations provide verification that a port's bandwidth capacity can support an `atm-qos` profile (a QoS contract) assigned to a connection on the port. CAC also provides for oversubscription of a port's payload bandwidth.

For CBR contracts, a port must be able to support the `atm-qos` profile's peak rate. For rtVBR and nrtVBR contracts, a port must be able to support the `atm-qos` profile's sustainable rate. No CAC is performed on unspecified bit rate (UBR) connections.

For a connection, the system can perform CAC calculations at three interface points:

- Trunk interface (for upstream and downstream bandwidth)
- LIM slot (for upstream bandwidth)
- LIM interface (for upstream and downstream bandwidth)

Notice about modifying the `atm-qos` profile for existing connections

When you modify the QoS definitions in an `atm-qos` profile, all `connection` profiles (both active and inactive) that specify the use of that profile are affected. The system deallocates the bandwidth assigned to those connections and then reallocates it according to the new definitions in the `atm-qos` profile. If it does not have sufficient bandwidth for all connections, the system allocates the guaranteed bandwidth for as many connections as possible. The remaining connections (if any) that use the modified `atm-qos` profile are allocated no bandwidth.

Note If a modified `atm-qos` profile causes additional bandwidth requirements, and the system does not have sufficient bandwidth available for all connections that use the modified `atm-qos` profile, some connections are allocated no bandwidth and therefore do not come up.

Specifying when CAC calculations are performed (`cac-preference`)

By default, the system performs CAC calculations when it is establishing connections. If insufficient bandwidth is available, the system fails to establish the connection. However, you can configure the system to perform CAC calculations when you provision a connection, and to disallow provisioning of connections beyond a port's bandwidth capacity. Following is the relevant parameter, shown with its default setting:

```
[in ATM-CONFIG]
cac-preference = connection-time
```

Note After changing the value of this parameter, a system reset is required for the new setting to take effect.

Parameter	Setting
`cac-preference`	Time when the system reserves bandwidth for a connection: when the connection is being established (`connection-time`, the default) or when the connection is provisioned (`provisioning-time`). When the system reserves bandwidth at connection setup time, it is possible for the operator to provision more connections than the system can support with guaranteed bandwidth. When the system allocates bandwidth at connection provisioning time, you can configure a new connection or modify an existing one only if sufficient bandwidth can be reserved for it. CAC is performed on LIM ports only when `cac-preference` is set to `provisioning-time`.

For example, the following commands cause the system to reserve bandwidth when a connection is provisioned:

```
admin> read atm-config
ATM-CONFIG read

admin> set cac-preference = provisioning-time
```

```
admin> write -f
New Cac preference only takes effect after system reset
ATM-CONFIG written
```

```
admin> reset
```

When the system has been configured to reserve bandwidth at connection provisioning time, the following CAC conditions apply:

- CAC is performed on both active and inactive circuits, on all trunk ports (including T1/E1 and IMA), all LIM slots, and ADSL, SDSL, SHDSL, and HDSL2 LIM ports.
- For PVC switch-through and terminating connections, CAC is performed at provisioning time.
- For SPVC initiator connections, upstream CAC (for ingress traffic) is performed at provisioning time, and downstream CAC (for egress traffic) is performed at connection time.

If CAC fails during the creation of a new `connection` profile, the system refuses to write the profile and displays an error message such as the following:

```
Failed bandwidth allocation for circuit adsl-cac-2 slot 17 port 1
```

If CAC fails when you have modified the `nailed-group` assignment or `atm-qos` profile assignment of an existing `connection` profile, the system refuses to write the changes and displays an error message such as the following:

```
Failed new bandwidth provisioning for circuit spvc-1-1-1-1.1, retaining old
parameters
```

When the system refuses to modify an existing configuration due to lack of sufficient available bandwidth, the existing CAC bandwidth is maintained for the connection.

Trunk-side CAC

CAC calculations occur at the trunk interface for terminating PVCs, SPVC initiator connections, and egress traffic of a LIM-to-trunk cross-connection. If the upstream and downstream trunk-side CAC tests are successful, bandwidth is allocated for the connection. If these tests fail and `cac-preference` is set to `provisioning-time`, the system refuses to write the `connection` profile and displays a log message such as the following:

```
Failed bandwidth allocation for circuit adsl-cac-2 slot 17 port 1
```

If the tests fail and `cac-preference` is set to `connection-time`, the system rejects the connection.

How CAC verifies that a trunk port can support a QoS contract

When CAC is performed on a trunk interface, the system must verify that the bit rates specified in an `atm-qos` profile can be supported.

The CAC algorithm uses the payload bandwidth of a line to calculate bandwidth allocation for ATM circuits, as shown in Table 2-1.

Table 2-1. Physical line rate and usable bandwidth for trunk usage

Line Type	Line rate (Kbps)	Usable payload bandwidth (Kbps)	
OC3	155,520	148,598	
OC12 (OC3x4)	622,080	594,392	
DS3	44,223	40,644 (PLCP)	
		44,166 (HEC)	
E3	34,000	33,901	
DS1	1,536	1,535	
		DS1 IMA (depends on frame length)	
		Framelen=32	3508 cps/link
		Framelen=64	3564 cps/link
		Framelen=128	3593 cps/link
		Framelen=256	3607 cps/link
E1	1,920	1,920	
		E1 IMA (depends on frame length)	
		Framelen=32	4384 cps/link
		Framelen=64	4455 cps/link
		Framelen=128	4490 cps/link
		Framelen=256	4503 cps/link

Configuring the **high-speed-slot-static-config** profile

If you modify CAC settings after connections have been established on a trunk interface, the new settings affect only new connections. Existing connections on the trunk port are not affected. Following are the parameters for configuring trunk-side CAC, shown with default values for an OC3-ATM trunk interface in slot 17, port 1.

```
[in HIGH-SPEED-SLOT-STATIC-CONFIG/{ shelf-1 trunk-module-1 1 }:
trunk-cac-config[1]]
enable = yes
port-num = 1:17:1
line-rate = 148598
over-subscription = 10
```

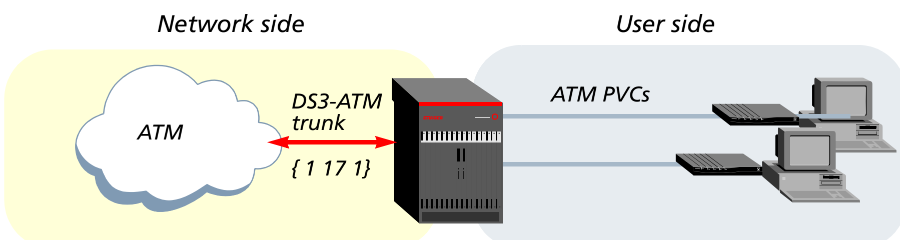
Parameter	Setting
`enable`	Enable/disable CAC on the port. CAC is enabled by default. If you change the parameter from `yes` to `no`, disabling CAC, the trunk module accepts all connection requests regardless of bandwidth. If you change it from `no` to `yes` on an active trunk, existing connections are not affected, but new connections that might cause the unit to exceed the port's bandwidth are rejected.
`port-num`	Read-only address of the trunk port within the unit.

Parameter	Setting
`line-rate`	Read-only value of the port's maximum payload capacity in kilobits per second. The trunk has real-time guaranteed bandwidth only up to this limit.
`over-subscription`	Factor (a number from 0 to 10,240) by which a trunk port allows oversubscription to its bandwidth. The allowed bandwidth is equal to the port's bandwidth (the `line-rate` value) multiplied by the over-subscription factor divided by 10 (*bandwidth* × *over-subscription*/10). The default value of 10 (which represents no over-subscription) prevents the port from accepting connections that would exceed its bandwidth. With a value of 50, the port can accept connections until the sum of bandwidths for all connections is five times the payload bandwidth. Values from 1 to 9 limit the port to less than payload capacity. With a value of 0 (zero), the port accepts connections without calculating whether its capacity has already been met or exceeded.

Sample setup showing use of an oversubscription factor

In the sample setup shown in Figure 2-1, the total trunk-side bandwidth required to handle the LIM-side connections is 200Mbps. The trunk module is DS3-ATM, with a maximum data rate on each interface of less than 45Mbps.

Figure 2-1. Sample setup for trunk-side connection admission control (CAC)



For the DS3-ATM interface to handle connections that expect up to 200,000Kbps of bandwidth (almost five times the payload bandwidth), you need to specify an oversubscription factor of 50. For example:

```
admin> read high-speed-slot-static-config { 1 17 1 }
HIGH-SPEED-SLOT-STATIC-CONFIG/{ shelf-1 trunk-module-1 1 } read

admin> set trunk-cac-config 1 over-subscription = 50

admin> write -f
HIGH-SPEED-SLOT-STATIC-CONFIG/{ shelf-1 trunk-module-1 1 } written

admin> list trunk-cac-config 1
[in HIGH-SPEED-SLOT-STATIC-CONFIG/{ shelf-1 trunk-module-1 1 }:trunk-cac-
config[1]]
enable = yes
port-num = 1:17:1
line-rate = 45000
over-subscription = 50
```

LIM-side CAC

Performing CAC at the LIM port interface occurs only when `cac-preference` has been set to `provisioning-time`. It is supported only for ADSL, SDSL, HDSL2, and SHDSL LIM interfaces. When the `cac-preference` parameter in the `atm-config` profile set to `provisioning-time`, CAC occurs in stages at three interface points:

1 LIM interface

2 LIM slot

3 Trunk interface

For cross-connections associated with DSL interfaces, CAC calculations are performed in three stages that verify bandwidth requirements at these three interface points. For details about the third stage of CAC (on a trunk interface) for a cross-connection, see "Trunk-side CAC" on page 2-6.

How CAC verifies that LIM port bit rates can support a QoS contract

The first stage of CAC calculations occurs at the LIM interface level. CAC verifies that the LIM port's provisioned bit rate is sufficient to support the upstream and downstream bandwidth requested in the QoS contracts applied in a `connection` profile. If the upstream and downstream tests are successful, CAC proceeds to the second stage calculations at the LIM slot level. If the first stage tests fail, the system refuses to write the `connection` profile and displays a log message such as the following:

```
Qos bandwidth higher than port bandwidth for adsl-cac slot 1 port 4
```

The bit rate parameters CAC uses are based on how the port is provisioned, as described in the following sections for ADSL, SDSL, HDSL2, and SHDSL interfaces.

ADSL bit rates used by CAC

The parameters that determine upstream and downstream ADSL port rates depend on the rate adaptation mode and latency settings in the `al-dmt` profile. For details about configuring ADSL, see the guide for your Stinger ADSL module.

Depending on the `rate-adapt-mode` and `line-latency` settings, one of the following sets of parameters determines the minimum upstream or minimum downstream port rates on the LIM:

Table 2-2. ADSL bit rates used by CAC

rate-adapt-mode	**line-latency**	**Rate used by upstream/downstream CAC**
automatic-at-startup	fast	fast-path-config min-bitrate-up
		fast-path-config min-bitrate-down
	interleave	interleave-path-config min-bitrate-up
		interleave-path-config min-bitrate-down
operator	fast	fast-path-config planned-bitrate-up
		fast-path-config planned-bitrate-down
	interleave	interleave-path-config planned-bitrate-up
		interleave-path-config planned-bitrate-down

In this example, the `atm-config` profile has the following setting:

```
[in ATM-CONFIG]
cac-preference = provisioning-time
```

And an ADSL port has been provisioned with the following settings:

```
[in AL-DMT/{ shelf-1 slot-13 7 }:line-config]
rate-adapt-mode-up = automatic-at-startup
line-latency = interleave
```

If a `connection` profile for an upstream connection specifies the nailed group for this ADSL port and applies a QoS contract that specifies, for example, a CBR service category with a peak rate of 256Kbps, CAC will use the value of the following parameter, shown with its default value, to determine if the ADSL port can support the connection:

```
[in AL-DMT/{ shelf-1 slot-13 7 }:interleave-path-config]
min-bitrate-up = 128
```

If the value of the `min-bitrate-up` parameter is 256 or greater, CAC at the LIM port will pass. With the default value shown, CAC at the ADSL port prevents writing of the `connection` profile and displays an error message.

SDSL bit rates used by CAC

The parameter that determines upstream and downstream SDSL port rates depends on the `data-rate-mode` setting in the `sdsl` profile. For details about configuring SDSL, see the guide for your Stinger SDSL module.

In `singlebaud` mode, CAC uses the `max-rate` value to determine if the port can support a QoS contract. For example, with the following settings, CAC allows any connection that does not exceed 784,000 bits per second of required bandwidth.

```
[in SDSL/{ any-shelf any-slot 0 }:line-config]
data-rate-mode = singlebaud
max-rate = 784000
```

In `autobaud` or `fastautobaud` mode, CAC uses the `auto-base-rate` value to determine if the port can support a QoS contract. For example, with one of the following sets of values, CAC allows any connection that does not exceed 272,000 bits per second of required bandwidth.

```
[in SDSL/{ any-shelf any-slot 0 }:line-config]
data-rate-mode = autobaud
auto-base-rate = 272000
```

```
[in SDSL/{ any-shelf any-slot 0 }:line-config]
data-rate-mode = fastautobaud
auto-base-rate = 272000
```

HDSL2 and SHDSL bit rates used by CAC

The parameter that determines upstream and downstream port rates for HDSL2 and SHDSL LIMs depends on the `rate-mode` setting in the `hdsl2` or `shdsl` profile. For details about configuring HDSL2 and SHDSL ports, see the guide for your Stinger SHDSL or SHDSL/HDSL2 module.

Note HDSL2 and SHDSL ports maintain an 8Kbps overhead link, so CAC calculates bandwidth based on the actual bit rate provisioned in the `hdsl2` or `shdsl` profile, minus 8000.

In `auto` mode, CAC uses the `min-rate` value minus 8000 to determine if the port can support a QoS contract. For example, with one the following sets of values, CAC allows any connection that does not exceed 64,000 bits per second of required bandwidth.

```
[in HDSL2/{ any-shelf any-slot 0 }:line-config]
rate-mode = auto
min-rate = 72000
```

```
[in SHDSL/{ any-shelf any-slot 0 }:line-config]
rate-mode = auto
min-rate = 72000
```

In `fixed` mode, CAC uses the `max-rate` value minus 8000 to determine if the port can support a QoS contract. For example, with one the following sets of values, CAC allows any connection that does not exceed 2,304,000 bits per second of required bandwidth.

```
[in HDSL2/{ any-shelf any-slot 0 }:line-config]
rate-mode = fixed
max-rate = 2312000
```

```
[in SHDSL/{ any-shelf any-slot 0 }:line-config]
rate-mode = fixed
max-rate = 2312000
```

How CAC verifies a LIM slot's available bandwidth capacity

The second stage of CAC calculations occurs at the LIM slot level. CAC verifies that the LIM slot's available guaranteed bandwidth is sufficient to support the upstream and downstream bandwidth requested in QoS contracts applied in the `connection` profile.

In the upstream direction for a LIM slot, the `allowed-guaranteed-up-stream-bandwidth` parameter in the `atm-config` profile is configurable up to a maximum rate of 148,598Kbps. Upstream CAC uses the value of that parameter to verify that there is sufficient available bandwidth remaining on the slot to support the connection.

In the downstream direction, allowed guaranteed bandwidth is always set to 148,598Kbps. Downstream CAC uses that hard-coded value to verify that there is sufficient available bandwidth remaining on the slot to support the connection.

For more details about these settings, see "Configuring allowed guaranteed upstream bandwidth" on page 2-1.

Note Use the `atmcacstat -b` debug-level command to see the allocated and available upstream and downstream bandwidth on a per-slot basis. To use this command, you must log into the system as `super`, or another `user` profile that has debug permissions enabled.

If these tests are successful, CAC proceeds to the third-stage calculations. If these tests fail, the system refuses to write the `connection` profile and displays a log message such as the following:

```
Failed bandwidth provisioning for circuit adsl-cac-2
```

Configuring the **atm-config lim-cac-config** subprofile

Following are the parameters for configuring LIM-side CAC, shown with their default values:

```
[in ATM-CONFIG:lim-cac-config]
lim-cac-config[1] = { yes 10 }
lim-cac-config[2] = { yes 10 }
lim-cac-config[3] = { yes 10 }
lim-cac-config[4] = { yes 10 }
lim-cac-config[5] = { yes 10 }
lim-cac-config[6] = { yes 10 }
lim-cac-config[7] = { yes 10 }
lim-cac-config[8] = { no 0 }
lim-cac-config[9] = { no 0 }
lim-cac-config[10] = { yes 10 }
lim-cac-config[11] = { yes 10 }
lim-cac-config[12] = { yes 10 }
lim-cac-config[13] = { yes 10 }
lim-cac-config[14] = { yes 10 }
lim-cac-config[15] = { yes 10 }
lim-cac-config[16] = { yes 10 }
```

```
[in ATM-CONFIG:lim-cac-config[N]]
enable = yes
over-subscription = 10
```

Parameter	Setting
`lim-cac-config[N]`	An array of indexed subprofiles, one for each LIM slot and each controller in the system. LIM-side CAC is not relevant to controllers. Note that CAC settings relate to the bandwidth and connections on individual ports of a LIM slot, but for the sake of simplicity, you configure LIM-side CAC once for all ports on a LIM.
`enable`	Enable/disable CAC on the LIM slot. CAC is enabled by default. If you change the parameter from `yes` to `no`, disabling CAC, the LIM accepts all connection requests regardless of bandwidth. If you change it from `no` to `yes` on an active LIM, existing connections are not affected, but new connections that might cause the system to exceed the allowed bandwidth on the line are rejected.

Parameter	Setting
`over-subscription`	Factor (a number from 0 to 10,240) by which a LIM port allows oversubscription to its bandwidth. The allowed bandwidth is equal to the port's bandwidth multiplied by the over-subscription factor divided by 10 (*bandwidth* × *over-subscription*/10). The default value of 10 (which represents no over-subscription) prevents the port from accepting connections that would exceed its provisioned bandwidth. With a value of 50, the port can accept connections until the sum of bandwidths for all connections is five times the provisioned bandwidth. However, no single connection can exceed the actual provisioned value of the port. For, example, if the port rate is 128,000 bits per second and `over-subscription` is set to 50, five connections at 128Kbps would be acceptable, but three connections at 128Kbps and one at 256Kbps would not be acceptable. Values from 1 to 9 limit the port to less than payload capacity. With a value of 0 (zero), the port accepts connections without calculating whether its capacity has already been met or exceeded.

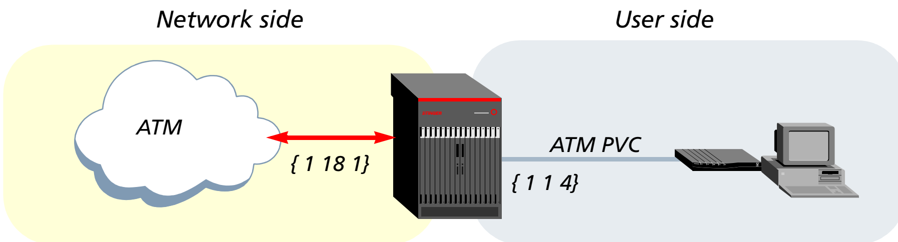
The next set of commands change `cac-preference` to `provisioning-time` (which requires a system reset to take effect) and configures an oversubscription factor of 50 for the ports of a LIM in slot 1:

```
admin> read atm-config
ATM-CONFIG read

admin> set cac-preference = provisioning-time

admin> set lim-cac-config 1 over-subscription = 50

admin> write -f
New Cac preference only takes effect after system reset
ATM-CONFIG written

admin> reset
```

Sample setup showing how LIM-side CAC works

The profiles configured in this example show both the system checks and consequent messages logged during CAC calculations.

Figure 2-2. Sample setup for illustrating LIM-side CAC operations



The following commands configure the ADSL interface to use a constant (operator) bit rate of 64Kbps upstream and 128Kbps downstream, using the fast channel in both directions:

```
admin> read al-dmt { 1 1 4 }
AL-DMT/{ shelf-1 slot-1 4 } read

admin> set enabled = yes

admin> set line-config line-latency-up = fast

admin> set line-config line-latency-down = fast

admin> set line-config rate-adapt-mode-up = operator

admin> set line-config rate-adapt-mode-down = operator

admin> set fast-path-config planned-bitrate-up = 64

admin> set fast-path-config planned-bitrate-down = 128

admin> write -f
AL-DMT/{ shelf-1 slot-1 4 } read
```

The next commands create two atm-qos profiles, one for upstream and one for downstream, that specify bandwidth consistent with that configured for the ADSL interface:

```
admin> new atm-qos adsl-qos-up
ATM-QOS/adsl-qos-up read

admin> set peak-rate = 64

admin> write -f
ATM-QOS/adsl-qos-up written

admin> new atm-qos adsl-qos-down
ATM-QOS/adsl-qos-down read

admin> set peak-rate = 128

admin> write -f
ATM-QOS/adsl-qos-down written
```

The following commands create a connection profile that switches through from the configured ADSL interface to a trunk interface, and apply the upstream and downstream traffic contracts:

```
admin> new connection adsl-cac
CONNECTION/adsl-cac read

admin> set atm-options vci = 38

admin> set atm-connect-options vci = 58

admin> set atm-options nailed = 4
```

```
admin> set atm-connect-options nailed = 851
admin> set atm-qos usr-up = adsl-qos-up
admin> set atm-qos usr-dn = adsl-qos-down
admin> set active = yes
admin> write -f
CONNECTION/adsl-cac written
```

If `cac-preference` is set to `provisioning-time`, when you enter the `write` command, CAC verifies that the LIM port can support the upstream and downstream bandwidth specified in the `atm-qos` profiles. In this example, it verifies that the connection does not require more bandwidth than specified in the `planned-bitrate-up` and `planned-bitrate-down` values in the `al-dmt` profile for the interface. If the connection cannot be supported, the system refuses to write the `connection` profile and displays an error message indicating that the QoS bandwidth is higher than port bandwidth.

If the QoS bandwidth can be supported by the provisioned port bit rate, CAC then tests whether the LIM slot has sufficient available guaranteed bandwidth. If the slot's guaranteed bandwidth is already fully allocated, the system refuses to write the `connection` profile and will display an error message indicating that bandwidth provisioning for the circuit failed.

LIM-side CAC-related log messages

If you have disabled LIM-side CAC in the `atm-config` profile and then subsequently enable it for a LIM slot, the system logs a warning that you must bounce the slot. The system logs the same warning if you change an oversubscription factor from zero to a nonzero value, if active connections are allocated on the slot.

```
Slot bounce is required for Slot#1, when slot CAC is re-enabled or over-
subscription is changed from 0 to a non-zero value
```

If active connections exist on a LIM port, and you modify the line rate or mode in a way that reduces the bandwidth, the system logs an error message and does not write the profile. ADSL port rates are determined for both upstream and downstream on the basis of mode settings in the `al-dmt` configuration profile. If you modify the `al-dmt` profile for an ADSL interface to reduce the upstream or downstream line rate or adaptation mode, the system logs a message such as one of the following:

```
ERROR: Port Up line rate/mode cannot be modified with CAC allocated
connections
```

```
ERROR: Port Down line rate/mode cannot be modified with CAC allocated
connections
```

On an SDSL, HDSL2, or SHDSL interface, the system logs the following message:

```
ERROR: Port line rate/mode cannot be modified with CAC allocated connections
```

If you attempt to reduce the oversubscription factor for a LIM slot in the `atm-config` profile, which might cause existing connections on the LIM port to fail, the system logs the following error message:

```
ERROR: Over-subscription not modified for slot 11, due to existing
connections
```

VPI-VCI Allocation on ATM Interfaces

3

The maximum virtual connection capacity of a Stinger unit that does not include a trunk aggregation module (TRAM) is a total of 32,768 (32K) bidirectional VCCs and VPCs. A TRAM provides its own ATM application-specific integrated circuit (ASIC) and up to six trunk ports, increasing the systemwide maximum capacity to 49,152 (48K) virtual connections. Under real operating conditions, performance and memory constraints in the Stinger unit limit the actual systemwide maximum of virtual connections to a lower number. However, it is the full ASIC capacity of the system that sets the maximum for trunk interface VPI-VCI assignments.

For LIM interfaces, the VPI-VCI range assignment occurs once for the entire module. All interfaces on a LIM must use the same range of VPI-VCI values for configured virtual connections.

Notice about reconfiguring VPI-VCI ranges

When you change the value of the `vc-switching-vpi` parameter for a trunk interface, or the `slot-vpi-vci-range` parameter for a LIM slot, the system disconnects and then rebuilds all connections on the interface.

If the new value removes a VPI or VCI value from the valid range, the system verifies that those values are not in use by active connections before allowing you to write the profile, because such a change would prevent the system from rebuilding those connections. If a deleted value is in use, the system refuses to write the change and displays a message such as the following:

```
ERROR: VPI <VPI#> cannot be deleted with existing connections
```

To delete a VPI or VCI that has been assigned to active connections, you must put those connections out of service administratively by setting `active` to `no` in the `connection` profiles.

VPI-VCI configuration for trunk interfaces

Table 3-1 shows VPI-VCI assignments for trunk interfaces, with default settings for a standard trunk module (not a TRAM) shown in boldface.

Table 3-1. Valid VPI and VCI assignments on trunk interfaces

VCCs		VPCs	
VPI	VCI	VPI	VCI
Up to 32 VPIs (**0**-255)	32-255	Up to 255 VPIs (1-255)	N/A
Up to 32 VPIs (**0**-255)	32-511	Up to 255 VPIs (1-255)	N/A
Up to 32 VPIs (**0**-255)	32-1023	Up to 255 VPIs (1-255)	N/A
Up to 32 VPIs (**0**-255)	32-2047	Up to 255 VPIs (1-255)	N/A
Up to 32 VPIs (**0**-255)	32-4095	Up to 255 VPIs (1-255)	N/A
Up to 32 VPIs (**0**-255)	**32-8191**	Up to 255 VPIs (1-255)	N/A
Up to 32 VPIs (**0**-255)	32-16393	Up to 255 VPIs (1-255)	N/A

The number of VCIs provisioned on a trunk interface (the VPI-VCI range) multiplied by the number of VPIs reserved for VCCs on the same trunk interface is the virtual connection capacity of the interface. The total configured capacity across all active trunk interfaces cannot exceed the full ASIC capacity of the system.

Configuring the VCC capacity of a trunk port

With the default settings, the system distributes the maximum number of virtual connections evenly across the available trunk or TRAM interfaces.

Note Changing the value of the `vc-switching-vpi` parameter on a trunk interface causes the system to disconnect and then rebuild all connections on the interface.

Overview of VCC settings in trunk profiles

The following parameters are relevant to setting the number of configurable VC switching connections on a trunk port. The parameters are shown with default settings for an OC3-ATM TRAM port.

```
[in OC3-ATM/{ shelf-1 trunk-module-1 1 }:line-config]
vpi-vci-range = vpi-0-255-vci-32-4095
vc-switching-vpi = [ 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0+
```

```
[in OC3-ATM/{ shelf-1 trunk-module-1 1 }:line-config:vc-switching-vpi]
vc-switching-vpi[1] = 0
vc-switching-vpi[2] = 0
vc-switching-vpi[3] = 0
vc-switching-vpi[4] = 0
vc-switching-vpi[5] = 0
vc-switching-vpi[6] = 0
vc-switching-vpi[7] = 0
vc-switching-vpi[8] = 0
vc-switching-vpi[9] = 0
```

```
vc-switching-vpi[10] = 0
vc-switching-vpi[11] = 0
vc-switching-vpi[12] = 0
vc-switching-vpi[13] = 0
vc-switching-vpi[14] = 0
vc-switching-vpi[15] = 0
vc-switching-vpi[16] = 0
vc-switching-vpi[17] = 0
vc-switching-vpi[18] = 0
vc-switching-vpi[19] = 0
vc-switching-vpi[20] = 0
vc-switching-vpi[21] = 0
vc-switching-vpi[22] = 0
vc-switching-vpi[23] = 0
vc-switching-vpi[24] = 0
vc-switching-vpi[25] = 0
vc-switching-vpi[26] = 0
vc-switching-vpi[27] = 0
vc-switching-vpi[28] = 0
vc-switching-vpi[29] = 0
vc-switching-vpi[30] = 0
vc-switching-vpi[31] = 0
vc-switching-vpi[32] = 0
```

Parameter	Setting
vc-switching-vpi[*n*]	Indexed parameters from 1 to 32, representing up to 32 VPI numbers to be provisioned for VC switching on the interface. Each VPI number can be from 0 to 255. The default vc-switching-vpi value of 0 is always reserved for VC switching. If all 32 of these parameters specify the default value, the remaining VPIs (from 1 to 255) are available for VPCs on the interface. When you add another VC-switching VPI number to a port, you double the virtual connection capacity of the port, because the entire valid VCI range for the port can be combined with another VPI to form VPI-VCI pairs for VCCs. To increase the number of VC-switching VPIs on a port without increasing the port's virtual connection capacity, you must also reduce the valid VCI range for the port by setting the vpi-vci-range parameter. Because the total virtual connection capacity of all trunk interfaces cannot exceed the total systemwide ASIC limitation, if you increase the virtual connection capacity of one interface, you must decrease the capacity of another interface proportionally to stay within the system limitation.

Parameter	Setting
`vpi-vci-range`	Valid range of VCIs for VCCs on the interface. Following are the allowed settings: `vpi-0-255-vci-32-255` VCIs 32 to 255 are valid. `vpi-0-255-vci-32-511` VCIs 32 to 511 are valid. `vpi-0-255-vci-32-1023` VCIs 32 to 1023 are valid. `vpi-0-255-vci-32-2047` VCIs 32 to 2047 are valid. `vpi-0-255-vci-32-4095` VCIs 32 to 4095 are valid. `vpi-0-255-vci-32-8191` VCIs 32 to 8191 are valid. `vpi-0-255-vci-32-16383` VCIs 32 to 16383 are valid. By default, the system allocates one VPI (VPI 0) for VC switching and assigns a VCI range of 32 to 8191 for a trunk port, or a range of 32 to 4095 for a TRAM port. This distributes the systemwide maximum number of virtual connections evenly across the available interfaces.

Adding a VC-switching VPI number without increasing port capacity

The following commands configure two VC-switching VPIs on a TRAM port: VPI 0 (the default) and VPI 13. To keep the virtual connection capacity of the interface unchanged, the commands also reduce the default range of valid VCIs from 4K (the default `32-4095` range) to 2K (a range of `32-2047`):

```
admin> read oc3-atm { 1 17 1 }
OC3-ATM/{ shelf-1 trunk-module-1 1 } read
admin> set line-config vc-switching-vpi 1 = 13
admin> set line-config vpi-vci-range = vpi-0-255-vci-32-2047
admin> write -f
OC3-ATM/{ shelf-1 trunk-module-1 1 } written
```

With this configuration, the system allows up to 2K virtual connections to be configured for each VPI used for VC switching on the OC3-ATM interface, so the connection capacity of the port remains at 4K.

VPIs required for use by OAM

With the current Stinger segmentation assembly/reassembly (SAR) device and software architecture, the operations, administration, and maintenance (OAM) network management functions have a maximum total of 29 VPIs for internal use.

OAM functions must set up a virtual path from a trunk port to the SAR for every 2K VCI range on the trunk port.

- For a trunk module, with two ports and a default VCI range of 8K on each port, that requirement translates into 2 (two ports) times 4 (four 2K VCI ranges per port), or 8 SAR VPIs per module.

- For a TRAM, with two OC3 ports, four DS3/E3 ports, and a default VCI range of 4K on each port, the requirement translates into 6 (six ports) times 2 (two 2K VCI ranges per port), or 12 SAR VPIs per module.
- For a Stinger MRT system, two cascaded OC3-ATM trunk ports each have a default 8K VCI range, and eight DS1/E1 ports support a default 2K VCI range. So, the requirement translates into 2 (two ports) times 4 (four 2K VCI ranges per port) plus 8 (eight ports) times 1 (one 2K VCI range per port), or 16 SAR VPIs systemwide.

For every additional `vc-switching-vpi` value that you configure for a trunk port, the effective VCI range on the port doubles, which also doubles the number of SAR VPIs required. If OAM has insufficient VPIs available, OAM might not work on some of the VPIs.

A log message such as the following is displayed when the system brings up a connection but has used all 29 of the SAR VPIs for OAM purposes:

```
LOG notice, Shelf 1, Controller-1, Time: 15:25:28--
   OAM: Couldn't open OAM channel for slot=18 port=1 vpi=0 vci=1900
```

On Stinger MRT systems, the message has the following format:

```
LOG notice, Shelf 1, Controller, Time: 14:57:46--
   OAM: Couldn't open OAM channel for slot(18), port(2), vpi(214), vci(35)
```

When the system displays these messages, you can try freeing up SAR VPIs already in use by reducing the number of 2K VCI ranges on a port. You accomplish this by setting the `vpi-vci-range` parameter for a port to a smaller VCI range.

However, under some conditions, such as when you have configured a large number of `vc-switching-vpi` VPIs, you might not be able to free up enough SAR VPIs to fulfill OAM requirements. In those situations, you can allow the system to operate without OAM on some connections, and simply ignore the OAM-related log messages. If you then observe a real problem in some connection and must use OAM to troubleshoot it, you would need to test with a simple configuration that uses a smaller number of `vc-switching-vpi` VPIs. However, loading a simple configuration for testing purposes might cause the system to drop existing connections.

How VPCs affect a trunk port's virtual connection capacity

All VPIs that have not been reserved for VC switching (VPI 1 through 255 by default) are available for VPCs. Because the VCIs carried on a VPC are not examined by the unit, the channels are not counted as virtual connections—including some reserved VCIs used for management connections, each VPC uses approximately four of the total 32,768 connections.

How a TRAM affects the system's virtual connection capacity

A TRAM provides its own ATM ASIC. ATM traffic from one port of a TRAM to another port of the same TRAM is handled by the ASIC within the TRAM. This type of traffic does not require any backplane or controller resources from the Stinger unit.

ATM traffic that must move from one module to another module within the Stinger is still managed by the ASIC on the primary controller in the unit, and therefore is still factored into the total ASIC switch capacity of 32,768. The traffic is also handled by the ASIC of any TRAM through which it passes. (Although traffic may pass through multiple ASICs on a Stinger equipped with TRAMs, it is not necessary to manually configure each of these switch-to-switch connections. These intermediate switch-to-switch connections within the Stinger are handled transparently by the TAOS operating system.)

A TRAM, which supports four DS3 and two OC3 trunk ports, allows a maximum of 49,152 (48K) virtual connections. The same limitations apply as for the controller ASIC—performance and memory constraints limit the actual number of virtual connections to a lower number, but the full ASIC capacity affects VPI-VCI assignment on the TRAM interfaces. The sum of `vpi-vci-range` values in all `oc3-atm` and `ds3-atm` profiles for the TRAM card must not exceed 48K.

Note When a TRAM is used in combination with a standard trunk module, the trunk module should consume no more than half of the 32,768 virtual connection capacity (16,384), because 16,384 capacity is used for the internal links between controller and TRAM ASICs.

VPI-VCI configuration for LIM slots and interfaces

Table 3-2 shows VPI-VCI assignments for LIM slots, with default settings shown in bold type.

Table 3-2. Valid VPI and VCI assignments on LIM slot

VCCs		VPCs	
VPI	VCI	VPI	VCI
0-3	32-511	One VPI from 1 to 3[1]	32-511[2]
0-7	32-255	One VPI from 1 to 7	32-255
0-15	**32-127**	One VPI from 1 to **15**	32-127
0-31	32-63	One VPI from 1 to 31	32-63

1. Within the valid VPI range, it is recommended that you use the highest possible value for VP switching. Otherwise, VPIs with a higher value within the range cannot be used for VCCs.

2. Although the VCI assigned to a connection is not used for switching purposes for a VPC, the VCI number still must be within the VCI range configured for the slot.

All ports in a LIM slot use the same specified range of valid VPIs and VCIs.

Note On ATM interfaces, VCI 0 through 31 are typically reserved for signaling and management. However, because LIM interfaces in Stinger units do not currently support ATM signaling and management operations, VCI 0 through 31 are available for assignment to subscriber connections.

Configuring `atm-config` with a VPI-VCI range for a LIM slot

You configure the valid VPI-VCI range for a LIM slot in the `atm-config` profile. Following are the parameters (shown with their default values for a Stinger FS) for modifying the VPI-VCI range of a LIM slot:

```
[in ATM-CONFIG:slot-vpi-vci-range]
slot-vpi-vci-range[1] = vpi-0-15-vci-32-127
slot-vpi-vci-range[2] = vpi-0-15-vci-32-127
```

```
slot-vpi-vci-range[3] = vpi-0-15-vci-32-127
slot-vpi-vci-range[4] = vpi-0-15-vci-32-127
slot-vpi-vci-range[5] = vpi-0-15-vci-32-127
slot-vpi-vci-range[6] = vpi-0-15-vci-32-127
slot-vpi-vci-range[7] = vpi-0-15-vci-32-127
slot-vpi-vci-range[8] = not applicable
slot-vpi-vci-range[9] = not applicable
slot-vpi-vci-range[10] = vpi-0-15-vci-32-127
slot-vpi-vci-range[11] = vpi-0-15-vci-32-127
slot-vpi-vci-range[12] = vpi-0-15-vci-32-127
slot-vpi-vci-range[13] = vpi-0-15-vci-32-127
slot-vpi-vci-range[14] = vpi-0-15-vci-32-127
slot-vpi-vci-range[15] = vpi-0-15-vci-32-127
slot-vpi-vci-range[16] = vpi-0-15-vci-32-127
```

Parameter	Setting	
`slot-vpi-vci-range[`*n*`]`	Valid range of VPI and VCI numbers for LIM slot *n*. All ports on a LIM use the same VPI-VCI range. Following are the allowed settings:	
	`vpi-0-1-vci-32-1023`	VPIs 0 to 1 and VCIs 32 to 1023 are valid.
	`vpi-0-3-vci-32-511`	VPIs 0 to 3 and VCIs 32 to 511 are valid.
	`vpi-0-7-vci-32-255`	VPIs 0 to 7 and VCIs 32 to 255 are valid.
	`vpi-0-15-vci-32-127`	VPIs 0 to 15 and VCIs 32 to 127 are valid. This is the default value.
	`vpi-0-31-vci-32-63`	VPIs 0 to 31 and VCIs 32 to 63 are valid.
	VPI 0 is always reserved for VCCs. By default, the system reserves VPI 15 for VPCs. For more information, see “Configuring a LIM port for VP switching” on page 3-10.	

Valid `slot-vpi-vci-range` values are constrained by the fact that 11 bits are available for VPI-VCI ranges on LIM slots. If you increase the valid VCI range for a LIM slot (which increases the number of bits used for that identifier), the VPI range must be decreased at the same time, and vice versa. Figure 3-1 shows the default allocation, with VPI numbers from 0 to 15 (4 bits) and VCI numbers from 32 to 127 (7 bits).

Figure 3-1. Bit sizes of default VPI-VCI range on a LIM slot

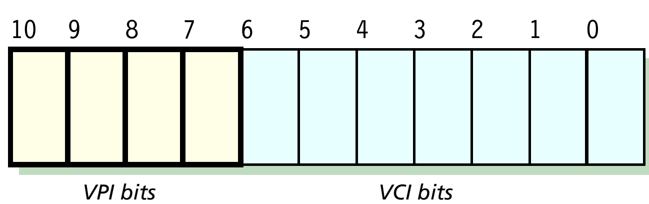


Table 3-3 lists `slot-vpi-vci-range` values and the corresponding VPI-VCI bit sizes for each value.

Table 3-3. VPI-VCI ranges and corresponding bit sizes on LIM slot

VPI-VCI range values	VPI bits	VCI bits
`vpi-0-1-vci-32-1023`	1 bit	10 bits
`vpi-0-3-vci-32-511`	2 bits	9 bits
`vpi-0-7-vci-32-255`	3 bits	8 bits
`vpi-0-15-vci-32-127`	4 bits	7 bits
`vpi-0-31-vci-32-63`	5 bits	6 bits

For example, the following commands configure the LIM in slot 1 to support VPIs from 0 to 7 and VCIs from 32 to 255:

```
admin> read atm-config
ATM-CONFIG read

admin> set slot-vpi-vci-range 1 = vpi-0-7-vci-32-255

admin> write -f
ATM-CONFIG written
```

With this sample configuration, the default VPI used for VP switching (VPI 15) is not within the valid VPI range. To configure a VPC on a LIM port, you must specify a new VPI for VP switching on that interface, as described in "Configuring a LIM port for VP switching" on page 3-10.

Enabling VP switching for a LIM slot

LIM-LIM VP switching is not supported, but you can configure VPCs between LIM and trunk interfaces. VPCs provide a useful way to aggregate traffic to and from a remote device.

LIMs that do not require the VP switching workaround

Many Stinger LIMs support the same set of cell-processing hardware, which requires that the system reserve backplane resources for VP switching. This requirement has introduced a VP switching workaround configuration in the `slot-static-config` profile, as described in "Configuring the LIM VP switching workaround" on page 3-9.

The following LIMs support a different chip set and do *not* require the VP switching workaround:

- STGR-LIM-AD-12
- STGR-LIM-SH-48
- STGR-LIM-AD-72
- STGR-LIM-SL-48
- STGR-LIM-SL-72

For these LIMs, a maximum of 12 LIM-trunk VPCs are supported per slot, with no `slot-static-config` settings required.

VP switching restrictions on LIM slots

The following limitations apply to VP switching on a LIM port:

- The VPI used for a VPC on a LIM port must fall within the VPI range configured for the slot.
- Even though the VCI is not used for switching purposes for the VPC, it must also fall within the VCI range configured for the slot.
- For LIMs other than STGR-LIM-AD-12 and STGR-LIM-SH-48, VPCs must originate from and terminate on the first 24 ports of the module.
- For LIMs that do not require the VP switching workaround, the maximum number of VPCs is 12.

Configuring the LIM VP switching workaround

Stinger LIMs that are not listed in "LIMs that do not require the VP switching workaround" on page 3-8 require reserved backplane resources to support VPCs from the LIM slot. When these LIMs support LIM-trunk VPCs, LIM-LIM functionality is disabled.

Note To allow reservation of the required backplane resources, when you write the `slot-static-config` profile after configuring the workaround, the system terminates and then reestablishes all connections on the slot. This also occurs for any later changes to the `use-vp-switching-workaround` or `need-max-vpswitching-vpis` setting.

Following are the parameters, shown with default settings for a LIM in slot 3:

```
[in SLOT-STATIC-CONFIG/{ shelf-1 slot-3 0 }]
use-vp-switching-workaround = no
need-max-vpswitching-vpis = no
```

Parameter	Setting
`use-vp-switching-workaround`	Enables/disables LIM-trunk VP switching on the slot. With the default `no` value, LIM-trunk VP switching is not supported. With the `yes` value, LIM-trunk VPCs and VCCs are supported, but LIM-LIM functionality is disabled. This parameter does not apply to LIMs with the following product codes: STGR-LIM-AD-12, STGR-LIM-SH-48, STGR-LIM-AD-72, STGR-LIM-SL-48, or STGR-LIM-SL-72.
`need-max-vpswitching-vpis`	Specifies whether to reserve the maximum number of 12 VPIs available for VP switching on a LIM slot. With the default `no` value, the system allocates 6 VPIs for a LIM in slot 1 to 7, or 5 VPIs for a LIM in slots 10 to 16. If you set this parameter to `yes`, up to 12 VPCs can originate from the slot, but F4-OAM functionality is disabled for switch-through connections to and from the slot. This parameter does not apply if the `use-vp-switching-workaround` parameter is set to `no`.

For example, the following commands enable LIM-trunk VP switching for up to 6 VPCs on the ports of a 48-port SDSL LIM (STGR-LIM-SQ-48) in slot 3:

```
admin> read slot-static-config { 1 3 0 }
SLOT-STATIC-CONFIG/{ shelf-1 slot-3 0 } read

admin> set use-vp-switching-workaround = yes

admin> write -f
SLOT-STATIC-CONFIG/{ shelf-1 slot-3 0 } written
```

Configuring a LIM port for VP switching

To support VP switching on any LIM, you must verify that the slot complies with VP switching restrictions (see “VP switching restrictions on LIM slots” on page 3-9) and then configure VPCs on the LIM ports.

If the VPI to be used for VP switching on a LIM port is outside the configured VPI range for the port, you must specify a different VPI by setting the following parameter:

```
[in SDSL/{ shelf-1 slot-3 22 }:line-config]
vp-switching-vpi = 15
```

Parameter	Setting
`vp-switching-vpi`	VPI to use for VP switching on the LIM port. The lowest VPI value is 1, because VPI 0 is always reserved for VC switching. The highest VPI value is the maximum VPI value specified in the `slot-vpi-vci-range` parameter for the LIM slot. For T1/E1 LIM interfaces, which can be used singly or in aggregation as trunk bandwidth, the meaning of this setting is slightly different from that for all other LIMs. For details, please see the *Stinger T1 and E1 Modules Guide*. You should use the highest value within the valid VPI range. Otherwise, VPIs with a higher value than this cannot be used for VCCs.

For example, the following commands determine the configured VPI-VCI range for LIM slot 3 and then reserve VPI 13 for VP switching on a LIM interface:

```
admin> get atm-config slot-vpi-vci-range 3
slot-vpi-vci-range[3] = vpi-0-3-vci-32-511

admin> read sdsl { 1 3 22 }
SDSL/{ shelf-1 slot-3 22 } read

admin> set line-config vp-switching-vpi = 13

admin> write -f
SDSL/{ shelf-1 slot-3 22 } written
```

The following commands configure a LIM-trunk VPC. The ingress LIM port {1 3 22} uses VPI 13 for VP switching and nailed group 122. The egress VPI is 15 on DS3 trunk port {1 18 1}, which uses nailed group 851.

```
admin> read connection lim-trunk
CONNECTION/lim-trunk read
admin> set active = yes
admin> set atm-options nail = 122
admin> set atm-options vpi = 13
admin> set atm-options vp-switching = yes
admin> set atm-connect-options nail = 851
admin> set atm-connect-options vpi = 15
admin> set atm-connect-options vp-switching = yes
admin> write -f
CONNECTION/lim-trunk written
```

For more information about configuring switch-through circuits, see Chapter 6, “ATM Circuit Configuration.”

ATM interface profile and statistics

RFC 2515, *ATM Management Objects*, defines SNMP management objects in support of the ATM cell layer on an interface, including objects that specify the maximum VPI-VCI bits for each ATM interface. For units managed by SNMP utilities, these objects are defined in the `atmInterfaceConfTable` of the RFC 2515 MIB. In the command-line interface, the maximum VPI-VCI bits for an interface are also represented as read-only values in the `atm-if-config` profile, but are defined elsewhere in the system. Following are the relevant settings, shown with default values:

```
[in ATM-IF-CONFIG/{ { any-shelf any-slot 0 } 0 }:base-config]
max-vpcs = 255
max-vccs = 8192
max-active-vpi-bits = 8
max-active-vci-bits = 13
```

Parameter	Setting
`max-vpcs`	Maximum number of VPCs supported on the interface. This value is read-only.
`max-vccs`	Maximum number of VCCs supported on the interface. This value is read-only.
`max-active-vpi-bits`	Maximum number of VPI bits in VPI-VCI pairs on the ATM interface. This value is read-only.
`max-active-vci-bits`	Maximum number of active VCI bits configured for use at this ATM interface. This value is read-only.

When the Private Network-to-Network Interface (PNNI) software has been licensed, ATM interfaces support signaling and routing protocols that are not required for standard ATM operations. Most of the settings in the `atm-if-config` profile are related to PNNI operations, and are read-only in units that do not support PNNI. If you are using PNNI, see the *Stinger Private Network-to-Network Interface (PNNI) Supplement*.

The Stinger unit creates an `atm-if-stat` profile for each of its ATM interfaces. The profiles provide information about the state of the physical and logical interfaces. Following is a sample `atm-if-stat` profile:

```
[in ATM-IF-STAT/{ { shelf-1 slot-1 20 } 0 }]
address* = { { shelf-1 slot-1 20 } 0 }
if-number = 159
nailed-group = 20
port-state = down
signalling-state = not-configured
pnni-link-state = not-configured
```

Parameter	Setting
`if-number`	Interface number.
`nailed-group`	Nailed group of the physical port's bandwidth. The system assigns a default nailed group for each physical interface. You can determine the nailed group associated with an interface by using the `which -n` command followed by the physical address of the interface.
`port-state`	State of the physical port. The state can be `not-configured`, `up`, or `down`.
`signalling-state`	Signaling state of the port. The signaling state can be `not-configured`, `up`, or `down`. For systems that do not support PNNI, the signaling state reports `not-configured`.
`pnni-link-state`	PNNI link state of the port. The link state can be `not-configured`, `up`, or `down`. For systems that do not support PNNI, the link state reports `not-configured`.

For example, following is a sample profile for an active ATM trunk interface in slot 17:

```
admin> get atm-if-stat { { 1 17 1 } 0 }
[in ATM-IF-STAT/{ { shelf-1 trunk-module-1 1 } 0 }]
address* = { { shelf-1 trunk-module-1 1 } 0 }
if-number = 11
nailed-group = 801
port-state = up
signalling-state = not-configured
pnni-link-state = not-configured
```

Configurable Quality of Service 4

Stinger units support configurable quality-of-service (QoS) contracts, which specify an ATM service category and related traffic management parameters. A QoS contract can apply to any number of virtual links. You apply a contract to upstream traffic, downstream traffic, or both.

In the Stinger command-line interface, you define QoS contracts in `atm-qos` profiles, which are indexed by the profile name. In the SNMP MIBs, the same parameters are specified as entries in the `atmTrafficDescrParamTable` defined in RFC 2514, *Definitions of Textual Conventions and OBJECT-IDENTITIES for ATM Management.* Entries in the traffic descriptor table are indexed by number. When you create an `atm-qos` profile, a corresponding entry is created in the `atmTrafficDescrParamTable`, and vice versa, as described in Chapter 8, "SNMP MIB Support."

Default `atm-qos` profiles

The system always creates at least one default `atm-qos` profile. If PNNI has been enabled on any port, the system creates a total of three default QoS contracts in `atm-qos` profiles.

```
admin> dir atm-qos
   33  01/04/2003 17:12:21  default
   22  01/04/2003 17:12:21  default-ctl
   43  01/04/2003 18:29:34  default-rcc
```

The `default` profile or profiles can be modified, but cannot be deleted.

The profile with the `default` index (traffic descriptor 1) is an unspecified bit rate contract applied by default to all virtual links that do not explicitly specify another contract.

The profiles with the `default-ctl` index (traffic descriptor 2) and the `default-rcc` index (traffic descriptor 3) are non-real-time variable bit rate contracts applied, respectively, to the PNNI signaling channel (VCI 5) and PNNI routing control channel

(VCI 18). See the *Stinger Private Network-to-Network Interface (PNNI) Supplement* for details.

Traffic management overview

The *ATM Forum Traffic Management Specification Version 4.0* defines service categories for different types of traffic that must have particular characteristics. For example, voice traffic requires a constant amount of bandwidth and cannot tolerate delays, whereas file transfer can tolerate delay and variable bandwidth. ATM switches use these categories and related traffic management settings to alter the characteristics of a cell stream to meet service requirements.

ATM service categories in Stinger units

In a Stinger unit, QoS contracts and traffic descriptor entries can specify one of the following service categories:

- Constant bit rate (CBR).
- Real-time variable bit rate (rtVBR).
- Non-real-time variable bit rate (nrtVBR).
- Unspecified bit rate (UBR). This is the category specified in the `default` contract.
- None. If the `connection` profile specifies a null contract name, the level of service is set to UBR with no policing.

CBR is used for applications that do not tolerate delay (for example, voice or video transmission). It guarantees that a static amount of bandwidth, known as the peak cell rate (PCR) is always available to the circuit. The source system can send cells at or below the specified PCR without compromising the quality of service. A value for cell delay variation tolerance (CDVT) relevant to the desired PCR must also be specified. Sustainable cell rate (SCR) and maximum burst size (MBS) values are not relevant to CBR service.

Real-time VBR is used for applications such as compressed audio or interactive multimedia, which do not tolerate significant delay but can tolerate some delay variance (*jitter*). Real-time VBR allows a variable amount of bandwidth, characterized by a PCR and CDVT, and an SCR, and MBS. The source system can send cells at a rate that varies (and might include bursts) but is within the boundaries defined by these settings.

Non-real-time VBR is used for applications such as transaction processing, which can tolerate delay but not cell loss. The bandwidth must remain within the boundaries of the PCR and CDVT and the SCR and MBS.

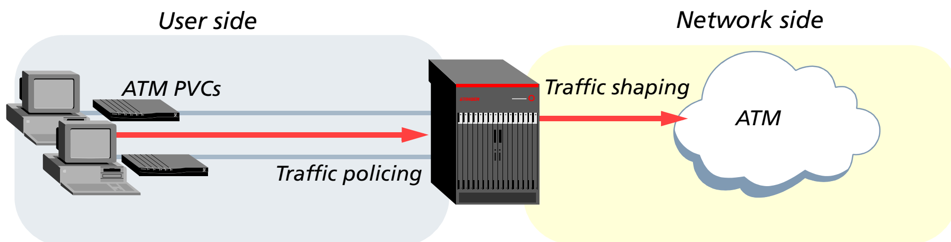
UBR is the lowest level of service. It makes no service or bandwidth guarantees. UBR is the default service category applied to all virtual links that do not explicitly specify another contract. UBR is useful for applications that do not require time dependency and can tolerate retransmissions of lost data. Applications such as telecommuting or background data transfer, which can tolerate delay, are good candidates for UBR service.

Traffic policing and shaping

A Stinger unit monitors ingress traffic on its LIMs to verify that the traffic does not exceed the bandwidth specified in the QoS contract (*traffic policing*). If the LIM is receiving traffic at too high a rate, the unit buffers the cells.

The unit can tag or discard traffic, if necessary, to ensure that its egress traffic conforms to the QoS contract (*traffic shaping*). Figure 4-1 illustrates traffic policing and shaping.

Figure 4-1. Traffic policing and shaping



Note Traffic policing applies only to upstream traffic. For a LIM interface, the QoS contract for downstream traffic is currently used to determine the service category. Other traffic management settings that describe downstream traffic are not currently used on LIM interfaces.

Stinger units implement a "dual leaky bucket" algorithm to regulate SCR and PCR. For a description of the algorithm, see the *ATM Forum Traffic Management Specification Version 4.0*. The unit also uses the virtual scheduling algorithm described in the *ATM Forum UNI Specification Version 3.1*. This algorithm calculates the expected arrival time of the next cell, compares that time to the actual arrival time with allowance for burst tolerance (or cell delay variation for PCR), and determines whether the cell is conforming. A cell that does not conform to the SCR part of the QoS contract can be tagged by changing its cell loss priority (CLP) bit to 1, or discarded. Cells that do not conform to the specified PCR are discarded.

If the call is based on AAL5 frames, the system can use partial packet discard (PPD) and early packet discard (EPD) to ensure that it manages the connection's packets rather than individual cells. PPD can be applied only to upstream packets, while EPD can be applied only to downstream packets.

QoS limitations of earlier Stinger LIMs

The12-port ADSL LIM (STGR-LIM-AD-12) and the earlier 48-port SDSL LIM (STGR-LIM-SH-48) have the following limitations on QoS functionality:

- No traffic policing
- Limited downstream ATM service categories

  In the upstream direction, all four categories are available. In the downstream direction, only two ATM service categories are available: constant bit rate (CBR) and non-CBR. Any category other than CBR—rtVBR, nrtVBR, and UBR—provide equivalent QoS performance.

QoS contract requirements

An `atm-qos` profile contains parameters that are relevant to any one of the supported service categories. Not all parameters are relevant to each one of the categories.

If your subscribers require service categories other than UBR, you must specify and least one QoS contract and apply it to the subscribers' connections. For example, if subscribers use transaction processing across the ATM network, you need a contract that specifies nrtVBR service. For details about service categories, see the *ATM Forum Traffic Management Specification Version 4.0*. For information about creating a traffic descriptor by using an SNMP utility, see the *Stinger SNMP Management of the ATM Stack*.

Overview of `atm-qos` settings

To define a QoS contract, you configure an `atm-qos` profile. Following are the parameters, shown with default values:

```
[in ATM-QOS/""]
contract-name* = ""
traffic-descriptor-index = 0
traffic-descriptor-type = noclp-noscr
atm-service-category = cbr
peak-rate-kbits-per-sec = 16
peak-cell-rate-cells-per-sec = 37
sustainable-rate-kbits-per-sec = 16
sustainable-cell-rate-cells-per-sec = 37
ignore-cell-delay-variation-tolerance = yes
cell-delay-variation-tolerance = 20
ignore-max-burst-size = yes
max-burst-size = 4
aal-type = aal-0
early-packet-discard = no
partial-packet-discard = no
tag-or-discard = discard
external-change = no
sub-channel = 1
```

Parameter	Setting
`contract-name`	Text name of the QoS contract, up to 31 characters. The name is used to apply the contract to any number of connections.
`traffic-descriptor-index`	Read-only numeric index of the traffic descriptor entry in the `atmTrafficDescrParamTable` that corresponds to the `atm-qos` profile. For details, see Chapter 8, "SNMP MIB Support."
`traffic-descriptor-type`	Traffic descriptor type as defined in RFC 2514. This setting must be compatible with the `atm-service-category` value. See "Parameters required to police specific service categories" on page 4-7.

Parameter	Setting
`atm-service-category`	ATM service category. Supported values are `cbr` (constant bit rate), `real-time-vbr`, `non-real-time-vbr`, and `ubr` (unspecified bit rate). This setting must be compatible with the `traffic-descriptor-type` value. See "Parameters required to police specific service categories" on page 4-7.
`peak-rate-kbits-per-sec`	PCR in kilobits per second. The default value is 16Kbps. The range is 0 to 148598Kbps.
`peak-cell-rate-cells-per-sec`	Read-only PCR value expressed in cells per second.
`sustainable-rate-kbits-per-sec`	SCR in kilobits per second. The default value is 16Kbps. The range is 0 to 148598Kbps.
`sustainable-cell-rate-cells-per-sec`	Read-only SCR value expressed in cells per second.
`ignore-cell-delay-variation-tolerance`	When this parameter is set to `yes` (the default), CDVT is ignored. For details, see "CDVT and MBS requirement checking" on page 4-6.
`cell-delay-variation-tolerance`	CDVT in microseconds. The range is 0 to 65535 microseconds.
`ignore-max-burst-size`	When this parameter is set to `yes` (the default), MBS is ignored. For details, see "CDVT and MBS requirement checking" on page 4-6.
`max-burst-size`	MBS, expressed relative to the PCR, as a cell rate. The default value is 4 cells. The range is 1 to 256 cells.
`aal-type`	ATM adaptation layer (AAL) type. Stinger units support AAL5 and AAL0 types. AAL0 (the default) is used for all traffic that is not packet. You can accommodate specific AAL types other than 5 by using the AAL0 setting with the appropriate service category setting. Because AAL5 circuits always handle packet traffic, the system must monitor the cells for the end-of-packet flag, thereby ensuring that packets rather than individual cells are discarded or tagged when necessary.
`early-packet-discard`	Enable/disable early packet discard (EPD). The default value is `no`. When the parameter is set to `yes`, the unit discards the entire downstream packet if it detects buffer congestion on the first cell of the packet. This parameter applies only to AAL5 circuits.

Parameter	Setting
`partial-packet-discard`	Enable/disable partial packet discard (PPD). The default value is `no`. If the parameter is set to `yes`, and the system detects buffer congestion after some cells of a packet have been queued, it discards the remaining cells of an upstream packet except the last cell (which contains the end-of-packet flag). In addition, if congestion occurs when the system is receiving the last cell of a packet, it discards the entire next packet. PPD relies on a higher layer to reject the partial packet when it is received. This parameter applies only to AAL5 circuits.
`tag-or-discard`	Enable/disable tagging of cells that do not conform to the SCR part of the QoS contract, by changing the cell loss priority (CLP) bit to 1. Cells not conforming to PCR are discarded. The default is `discard`. For information about how this value corresponds to the `traffic-descriptor-type` setting, see "" on page 4-7.
`sub-channel`	For LIMs that support dual latency, which of the multiple sub-channels will use the QoS contract. This setting applies only if dual latency has been enabled in the `al-dmt` line profile. When the DMT line is not configured for dual latency, the default sub-channel is always 1, regardless of the setting of this parameter. For details, see the *Stinger ADSL Line Interface Module Guide*.

CDVT and MBS requirement checking

CDVT and MBS values are required for policing of certain service categories. Following are the relevant parameters, shown with default settings:

```
[in ATM-QOS/""]
ignore-cell-delay-variation-tolerance = yes
cell-delay-variation-tolerance = 20
ignore-max-burst-size = yes
max-burst-size = 4
```

With the default `yes` value for `ignore-cell-delay-variation-tolerance` and `ignore-max-burst-size`, the system internally sets a value for the `cell-delay-variation-tolerance` and `max-burst-size` parameters that is high enough to make policing almost ineffective. This default behavior ensures that the Stinger does not discard cells from a bursty CPE device that does not use traffic shaping.

For CPE devices that support traffic shaping, you must change these defaults to enable the system to enforce contracts for certain service categories. For example, the following commands configure a rtVBR contract that allows the system to evaluate CDVT and MBS in the traffic stream:

```
admin> new atm-qos rt-vbr1
ATM-QOS/rt-vbr1 read

admin> set traffic-descriptor-type = noclp-scr

admin> set atm-service-category = real-time-vbr

admin> set peak-rate-kbits-per-sec = 1024
```

```
admin> set sustainable-rate-kbits-per-sec = 512
admin> set ignore-max-burst-size = no
admin> set max-burst-size = 20
admin> set ignore-cell-delay-variation-tolerance = no
admin> set cell-delay-variation-tolerance = 10
admin> write -f
ATM-QOS/rt-vbr1 written
```

If you attempt to write an `atm-qos` profile that specifies a `traffic-descriptor-type` value which requires CDVT, MBS, or both, and the value of the `ignore-cell-delay-variation-tolerance` or `ignore-max-burst-size` parameter (or both) is set to `yes`, the system issues warnings such as the following:

```
ignore-cell-delay-variation-tolerance should be set to NO for specified
traffic type unless dealing with bursty CPE.
ignore-max-burst-size should be set to NO for specified traffic type unless
dealing with bursty CPE.
```

Parameters required to police specific service categories

Allowable combinations of traffic descriptor types and ATM service categories are described in Table A9-2 in Annex 9 of the *ATM User-Network Interface (UNI) Signalling Specification Version 4.0*. If you configure an `atm-qos` profile with the `traffic-descriptor-type` and `atm-service-category` parameters set to incompatible values, the system refuses to write the profile and generates the following message:

```
ERROR: Inconsistent traffic type and atm-service-category field
```

Table 4-1shows traffic descriptors and service categories, and applicable parameters for policing traffic.

Table 4-1. Traffic descriptors, service categories, and applicable parameters

Traffic descriptor type	Service category	Applicable Parameters			
		PCR	CDVT	SCR	MBS
`unknown-traffic-desc`	*Not used*	N/A	N/A	N/A	N/A
`noclp-noscr`	CBR[1] UBR[1]	Y	N	N	N
`noclp-scr`	VBR[1]	Y	N	Y	Y[3]
`clp-notagging-scr`	VBR[1]	Y	N	Y	Y[3]
`clp-tagging-scr`	VBR[1]	Y	Y[3]	Y	Y[3]
`clp-transparent-noscr`	CBR.1[2]	Y	Y[3]	N	N
`clp-transparent-scr`	VBR.1[2]	Y	Y[3]	Y	Y[3]
`noclp-tagging-noscr`	UBR.2[2]	Y	Y[3]	N	N
`noclp-noscr-cdvt`	CBR[1] Similar to UBR.1[2]	Y	Y[3]	N	N

Table 4-1. Traffic descriptors, service categories, and applicable parameters (Continued)

Traffic descriptor type	Service category	Applicable Parameters			
		PCR	CDVT	SCR	MBS
noclp-scr-cdvt	VBR[1]	Y	Y[3]	Y	Y[3]
clp-notagging-scr-cdvt	VBR.2[2]	Y	Y[3]	Y	Y[3]
clp-tagging-scr-cdvt	VBR.3[2]	Y	Y[3]	Y	Y[3]

1. Service categories specified in accordance with the *ATM User-Network Interface Specification V3.0* (UNI 3.0) and *ATM User-Network Interface Specification V3.1* (UNI 3.1).

2. Service categories specified in accordance with the *ATM Forum Traffic Management Specification Version 4.0*.

3. To enable the system to use CDVT and MBS values to police traffic, you must set the values of the `ignore-cell-delay-variation-tolerance` and `ignore-max-burst-size` parameters to `no`.

Tagging or discarding nonconforming cells

The `traffic-descriptor-type` setting in an `atm-qos` profile determines whether the system tags or discards cells that do not conform to the QoS contract. If its value conflicts with the value of the `tag-or-discard` field in the same profile, the `traffic-descriptor-type` setting overrides the `tag-or-discard` action. Table 4-2 lists the compatible settings for the `traffic-descriptor-type` and `tag-or-discard` parameters in an `atm-qos` profile.

Table 4-2. Compatible settings for traffic descriptors and CLP tagging

traffic-descriptor-type	tag-or-discard
noclp-noscr	discard
noclp-scr	discard
clp-notagging-scr	discard
clp-tagging-scr	tag
clp-transparent-noscr	discard
clp-transparent-scr	discard
noclp-tagging-noscr	tag
noclp-noscr-cdvt	discard
noclp-scr-cdvt	discard
clp-notagging-scr-cdvt	discard
clp-tagging-scr-cdvt	tag

If you modify an `atm-qos` profile that has already been applied to one ore more active links, and the modification results in inconsistent `traffic-descriptor-type` and `tag-or-discard` settings, the system refuses to write the profile and generates the following message:

```
Inconsistent traffic type and tag-or-discard field
```

However, if you create an inconsistent `atm-qos` profile that has not been applied to any active links, the system modifies the `tag-or-discard` setting to a value that is compatible with the specified `traffic-descriptor-type` and generates a message such as the following:

```
Inconsistent tag-or-discard field, setting to discard
```

QoS recommendation for management PVCs

The profile with the `default` index (traffic descriptor 1) is a UBR contract applied by default by all virtual links that do not explicitly specify another contract.

If you use the `default` QoS contract for a management PVC, you could lose management access to Stinger unit through a trunk interface that becomes saturated. To retain management access even in congested conditions, Lucent Technologies recommends using a QoS contract specifying a higher level of service, such as CBR, for management PVCs.

Sample QoS contracts

This section provides a sample CBR, rtVBR, and UBR contract, and describes typical uses of these service categories.

Configuring a CBR contract

A CBR contract demands a static amount of bandwidth, which is characterized by a PCR value. The CDVT value can also be relevant to CBR service. CBR is the highest-priority service category, and is typically used for high-demand applications such as voice or video transmission. For CBR traffic, bandwidth is reserved for the PVC even if traffic requirements drop.

The following commands define a contract for CBR traffic with a bit rate of 1Mbps and a CDVT of 10 microseconds:

```
admin> new atm-qos cbr1
ATM-QOS/cbr1 read

admin> set peak-rate = 1024

admin> set ignore-cell = no

admin> set traffic-descriptor-type = clp-transparent-noscr

admin> set cell-delay = 10

admin> write -f
ATM-QOS/cbr1 written

admin> list
[in ATM-QOS/cbr1]
contract-name* = cbr1
traffic-descriptor-index = 6
traffic-descriptor-type = clp-transparent-noscr
atm-service-category = cbr
peak-rate-kbits-per-sec = 1024
peak-cell-rate-cells-per-sec = 2415
sustainable-rate-kbits-per-sec = 1024
sustainable-cell-rate-cells-per-sec = 2415
ignore-cell-delay-variation-tolerance = no
cell-delay-variation-tolerance = 10
ignore-max-burst-size = yes
```

```
max-burst-size = 4
aal-type = aal-0
early-packet-discard = no
partial-packet-discard = no
tag-or-discard = discard
sub-channel = 1
```

This contract allows the default discard actions (both early and partial packet discard are allowed when congestion occurs). Maximum burst size does not apply. Notice that the system sets the SCR equal to PCR for CBR service.

Configuring a VBR contract

VBR contracts specify a variable amount of bandwidth, characterized by the PCR and the CDVT, as well as by SCR and MBS values. The source system can send cells at a rate that varies, and might include bursts, but is within the boundaries defined by these settings. Real-time VBR can be used in place of CBR for voice or video. It can also be used for applications such as compressed audio or interactive multimedia. Although the bandwidth is allowed to vary, rtVBR does not allow long delays in the cell stream.

The following commands define a contract for real-time traffic with a peak bit rate of 1Mbps, a sustainable bit rate of 512Kbps, and a maximum of 20 consecutive cells at the peak rate before cells become candidates for discard:

```
admin> new atm-qos rt-vbr1
ATM-QOS/rt-vbr1 read

admin> set atm-service = real-time-vbr

admin> set traffic-descriptor-type = clp-transparent-scr

admin> set peak-rate = 1024

admin> set sustainable-rate = 512

admin> set ignore-max = no

admin> set max-burst-size = 20

admin> set ignore-cell = no

admin> set cell-delay = 10

admin> write -f
ATM-QOS/rt-vbr1 written

admin> list
[in ATM-QOS/rt-vbr1]
contract-name* = rt-vbr1
traffic-descriptor-index = 7
traffic-descriptor-type = clp-transparent-scr
atm-service-category = real-time-vbr
peak-rate-kbits-per-sec = 1024
peak-cell-rate-cells-per-sec = 2415
sustainable-rate-kbits-per-sec = 512
sustainable-cell-rate-cells-per-sec = 1207
ignore-cell-delay-variation-tolerance = no
cell-delay-variation-tolerance = 10
ignore-max-burst-size = no
max-burst-size = 20
```

```
aal-type = aal-0
early-packet-discard = no
partial-packet-discard = no
tag-or-discard = discard
sub-channel = 1
```

The virtual link that applies this contract is initially established at a bit rate of 512Kbps. It can then accommodate bursts of up to 20 cells at double its bit rate (up to 1Mbps).

UBR traffic policing

You can specify UBR contracts for applications that are not time dependent and can tolerate retransmissions of lost data. UBR contracts are policed unless policing has been specifically disabled, as described in "Settings that disable UBR policing" on page 4-12.

Policing action of UBR-compatible traffic descriptor types

The `traffic-descriptor-type` and `tag-or-discard` settings are used to determine the proper policing action (to tag or discard cells). Table 4-3 shows the policing action that will be performed for non-zero values of peak cell rate (PCR):

Table 4-3. Traffic descriptor and CLP settings for UBR contracts

traffic-descriptor-type	tag-or-discard	Traffic policing action
`noclp-tagging-noscr`	`tag`	Cells violating the generic cell rate algorithm (GCRA) for the PCR are tagged. CDVT should be specified, however if `ignore-cell-delay-variation-tolerance` (ignore-CDVT) is set to `yes`, the system displays a warning but accepts the parameter change.
`noclp-noscr-cdvt`	`discard`	Cells violating GCRA for the PCR are discarded. Cell delay variation tolerance (CDVT) should be specified, however if ignore-CDVT is set to `yes`, the system displays a warning but accepts the parameter change.
`noclp-noscr`	`discard`	Cells violating GCRA on the PCR are discarded. The ignore-CDVT setting can be `yes` or `no`. If set to `no`, the provisioned CDVT value is used.

Sample UBR contract

The following commands define an `atm-qos` profile settings specify a UBR contract with traffic policing in which the system discards cells that are not conforming to the GCRA for PCR:

```
admin> new atm-qos ubr1
```

```
ATM-QOS/ubr1 read
admin> set atm-service = ubr
admin> set traffic-descriptor-type = noclp-noscr-cdvt
admin> set peak-rate = 150
admin> set ignore-cell = no
admin> set cell-delay = 500
admin> write -f
ATM-QOS/ubr1 written
admin> list
[in ATM-QOS/ubr1]
contract-name* = ubr1
traffic-descriptor-index = 8
traffic-descriptor-type = noclp-noscr-cdvt
atm-service-category = ubr
peak-rate-kbits-per-sec = 150
peak-cell-rate-cells-per-sec = 353
sustainable-rate-kbits-per-sec = 16
sustainable-cell-rate-cells-per-sec = 37
ignore-cell-delay-variation-tolerance = no
cell-delay-variation-tolerance = 500
ignore-max-burst-size = yes
max-burst-size = 4
aal-type = aal-0
early-packet-discard = no
partial-packet-discard = no
tag-or-discard = discard
sub-channel = 1
```

Settings that disable UBR policing

To turn off policing in a UBR contract, the PCR must be set to zero. If the `traffic-descriptor-type` parameter is set to `noclp-tagging-noscr` or `noclp-noscr-cdvt` in the UBR contract, you must also set CDVT to zero to disable traffic policing for the contract.

The `default` `atm-qos` profile, which is applied to all virtual links that do not apply a different contract, is a UBR contract with no traffic policing. For example:

```
admin> get atm-qos default
[in ATM-QOS/default]
contract-name* = default
traffic-descriptor-index = 1
traffic-descriptor-type = noclp-noscr
atm-service-category = ubr
peak-rate-kbits-per-sec = 0
peak-cell-rate-cells-per-sec = 0
sustainable-rate-kbits-per-sec = 0
sustainable-cell-rate-cells-per-sec = 0
ignore-cell-delay-variation-tolerance = yes
cell-delay-variation-tolerance = 0
ignore-max-burst-size = yes
```

```
max-burst-size = 4
aal-type = aal-0
early-packet-discard = no
partial-packet-discard = no
tag-or-discard = discard
sub-channel = 1
```

Note The preceding profile contents show the sustainable rates set to zero, but those values are not used for UBR traffic contracts.

Applying a QoS contract to a `connection` profile

The way the system handles and prioritizes traffic for a virtual link is determined by the QoS contract or contracts applied in the `connection` or RADIUS profile. For some connections, the requirements differ for upstream and downstream traffic. For example, a connection used to receive video transmissions might have constant bit-rate downstream requirements and relatively few upstream requirements. You control these differing requirements by applying two QoS contracts in the profile, one for upstream and another for downstream traffic.

Note For a LIM interface, the QoS contract for downstream traffic is currently used to determine the service category. Other traffic management settings for downstream traffic are not currently used on LIM interfaces.

Following are the relevant parameters, shown with default values:

```
[in CONNECTION/"":atm-qos-options]
usr-up-stream-contract = default
usr-dn-stream-contract = default
```

Parameter	RADIUS attribute	Setting
`usr-up-stream-contract`	`Ascend-QOS-Upstream` (59)	Name of the `atm-qos` profile to be applied to upstream traffic on the virtual link: a text string of up to 31 characters. For information about the `default` contract, which is applied to all virtual links that have no explicit contract assignment, see "Default atm-qos profiles" on page 4-1.
`usr-dn-stream-contract`	`Ascend-QOS-Downstream` (60)	Name of the `atm-qos` profile to be applied to downstream traffic on the virtual link: a text string of up to 31 characters. For information about the `default` contract, which is applied to all virtual links that have no explicit contract assignment, see "Default atm-qos profiles" on page 4-1.

For example, the following command lists defined `atm-qos` profiles:

```
admin> dir atm-qos
33 02/11/2002 11:21:04 default
22 02/11/2002 11:21:04 default-ctl
26 02/11/2002 11:21:04 default-ilmi
43 02/11/2002 11:21:04 default-rcc
18 02/11/2002 14:01:21 rt-vbr1
```

For example, the following commands configure a switch-through PVC (an ATM circuit) and apply a rtVBR contract to both upstream and downstream traffic:

```
admin> new connection pvc1
CONNECTION/pvc1 read

admin> set active = yes

admin> set encapsulation-protocol = atm-circuit

admin> set atm-options nailed-group = 801

admin> set atm-options vci = 36

admin> set atm-connect-options nailed-group = 802

admin> set atm-connect-options vci = 36

admin> set atm-qos-options usr-up-stream-contract = rt-vbr1

admin> set atm-qos-options usr-dn-stream-contract = rt-vbr1

admin> write -f
CONNECTION/pvc1 written
```

Following is a comparable RADIUS profile:

```
permconn-ST-1 Password = "ascend"
    Service-Type = Outbound,
    Framed-Protocol = ATM-CIR,
    User-Name = "pvc1",
    Ascend-ATM-Group = 801,
    Ascend-Route-IP = Route-IP-No,
    Ascend-ATM-Vpi = 0,
    Ascend-ATM-Vci = 36,
    Ascend-ATM-Connect-Vpi = 0,
    Ascend-ATM-Connect-Vci = 36,
    Ascend-ATM-Connect-Group = 802,
    Ascend-QOS-Upstream = "rt-vbr1",
    Ascend-QOS-Downstream = "rt-vbr1"
```

For details about defining `connection` and RADIUS profiles, see Chapter 6, "ATM Circuit Configuration" and Chapter 7, "Terminating PVC Configuration." For general information about RADIUS profiles, see the *TAOS RADIUS Guide and Reference*.

Queues and VP Shaping

5

The controller's ATM ASIC uses outgoing queues for scheduling traffic flows within a class of service. You can assign priority and weight to queues to cause the system to handle traffic flows at a higher or lower priority. You can also activate a new queue and associate it with a virtual path (VP) shaper to shape trunk-side bandwidth usage, a feature typically used with subtending.

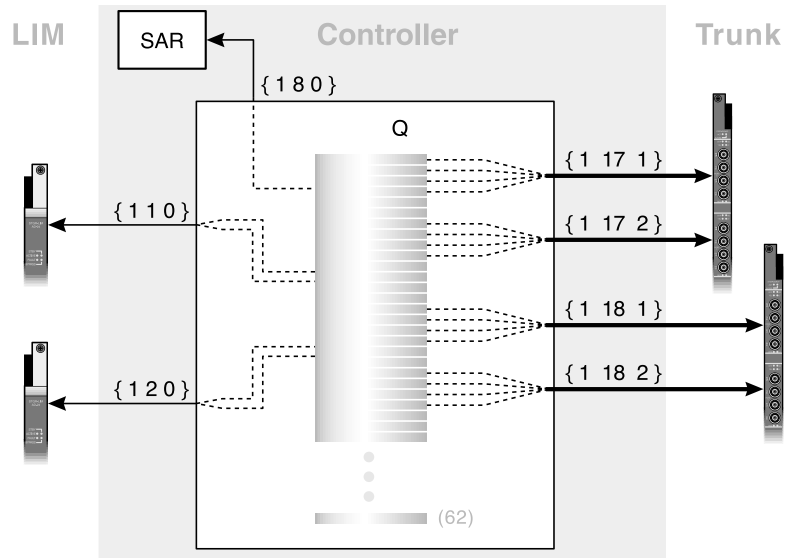
Overview of queue management

The Stinger controller ASIC supports 62 outgoing queues for temporary buffering and scheduling of cells.

Figure 5-1 shows sample outgoing queues allocated to the system's slots and interfaces.The system associates two outgoing queues with each LIM slot, and one queue with each controller. (Traffic to a controller typically consists of ATM management cells.) These queues are shown at the left side of Figure 5-1.

The system associates four outgoing queues with each trunk interface, one for each service category other than available bit rate (ABR). These queues and interfaces are shown at the right side of Figure 5-1.

Figure 5-1. Allocation of queues in the ASIC



Queues and classes of service

The system creates default active queue configurations to handle ATM service categories efficiently and fairly on its LIM slots, controllers, and trunk ports. The number of default active queues configured by a system is platform-specific, depending on the number of LIMs and other interfaces supported in the unit.

The default system-generated queue configurations provide at least one queue that can be used for each service category to each LIM and trunk port, and assigns values for processing traffic flows at an appropriate priority for each service category. CBR traffic is processed at the highest priority, followed by real-time VBR traffic, non-real-time VBR traffic, and UBR traffic at the lowest priority.

Outgoing queue priority and weight

The ASIC has both a low-priority and high-priority scheduler for queue processing. Each outgoing queue is assigned a weight that determines which scheduler to use for processing the queue and how much of the scheduler's work cycle is dedicated to the queue relative to other queues using the same scheduler. A queue must be processed by at least one scheduler, and can be processed by both schedulers.

The weight assigned to a queue is used to set up the scheduler of the ASIC such that the appropriate relative priorities are given to different queues in the system. To provide fairness among different traffic sources, you can configure multiple queues that correspond to the same service category and same output port and have the same weights on the scheduler.

Special features for subtending applications

In a subtending application, where a DSLAM is connected to another DSLAM through a trunk interface to create a tiered network, the system has to be able to selectively assign data from a particular source (ingress) port to a desired output queue. Further, when multiple levels of subtending are supported, different queues might be needed for Stinger nodes at various levels in the tiered network to provide fairness in allocation of bandwidth.

To provide the queuing flexibility needed for subtending applications, the system enables you to configure outgoing queues to admit traffic only from a specific source port and to admit traffic only from a subtended switch a specified number of hops away from the Stinger unit performing the subtending function.

Trunk-side VP bandwidth shaping

After the system has generated the active queue configurations it requires for the physical slots and interfaces supported by the unit, a number of inactive queues remain and are available for use with VP shapers. The number of inactive queues differs depending on the type of Stinger platform. The system supports up to 10 VP shapers for managing bandwidth usage of trunk-side virtual path links. To shape bandwidth usage for a trunk-side VPC, you activate a queue that is not already assigned to a slot or interface, configure it for a specific trunk port, and associate it with a VP shaper. The shaper specifies a VPI and the desired bandwidth for the uplink VPC. Only traffic with the specified VPI will be admitted to the queue.

You can also use VP shapers to shape bandwidth usage for multiple VCCs that share the same VPI on the trunk side. The VCCs *share* the bandwidth specified in the shaper definition. The cumulative output of the queue (not the individual VCCs within the virtual path) is shaped. The system does not place a limit on the number of VCCs each shaper can manage in this way.

Setting incoming traffic priority

Incoming traffic on a LIM, controller, and trunk interface has an associated priority setting that, together with the QoS requirements of the incoming traffic and its outgoing interface, affects which queue is used to process the traffic. By default, all incoming traffic has a low-priority setting.

Overview of `incoming-priority` settings

You set the priority for incoming traffic on LIMs and controllers by setting the following parameter, shown with the default value for the first LIM slot in the unit:

```
[in SLOT-STATIC-CONFIG/{ shelf-1 slot-1 0 }:atm-parameters]
incoming-priority = low-priority
```

For trunk interfaces, you set the priority for incoming traffic by setting the following parameter, shown with the default value for the first trunk interface in the unit:

```
[in HIGH-SPEED-SLOT-STATIC-CONFIG/{ shelf-1 trunk-module-1 1 }:
atm-parameters]
incoming-priority = low-priority
```

Parameter	Setting
`incoming-priority`	Priority at which traffic on the slot or interface is scheduled. With the default `low-priority` setting, the ASIC assigns the traffic flow to a low-priority outgoing queue with the same ATM service category. If you set the parameter to `high-priority`, and an outgoing queue with the same ATM service category is configured for high-priority scheduling, that queue is selected instead. If the connection's outgoing interface is assigned only one queue for a given ATM service category, than that queue is used regardless of the value of this parameter. For LIM and controllers, the same priority is shared by all incoming traffic received on any one of the slot's ports. Each trunk interface is assigned its own priority setting.

Typical high-priority LIM configuration

Specifying a high priority for incoming traffic can result in faster throughput for traffic received on that slot or interface. For example, the following set of commands specifies high-priority processing for traffic received on any interface of the LIM in slot 2:

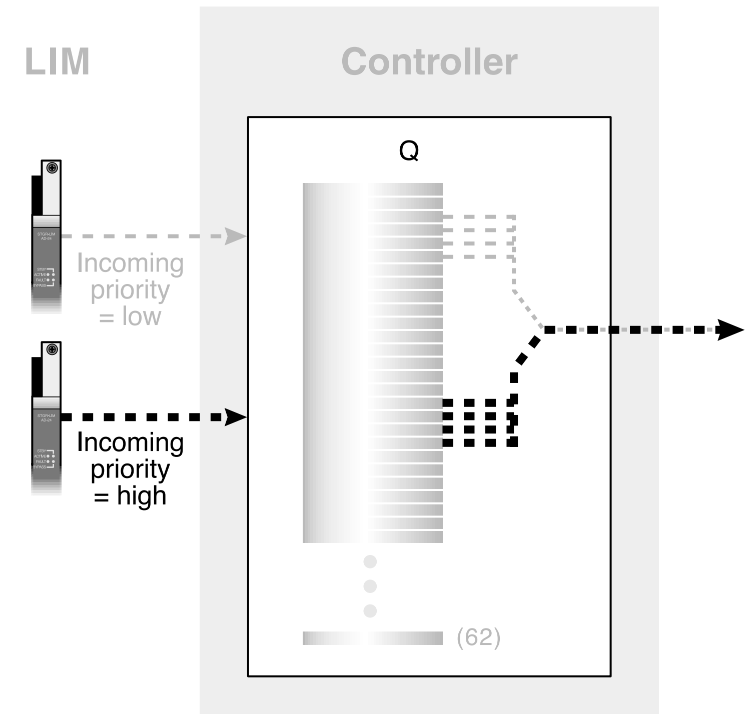
```
admin> read slot-static-config { 1 2 0 }
SLOT-STATIC-CONFIG/{ shelf-1 slot-2 0 } read

admin> set atm-parameters incoming-priority = high-priority

admin> write -f
SLOT-STATIC-CONFIG/{ shelf-1 slot-2 0 } written
```

Figure 5-2 shows two LIMs, slot 1 with the default low-priority setting for incoming traffic, and slot 2 with a high-priority setting. The traffic from both LIMs exits the unit on the same trunk interface, but is processed at different priorities.

If the system has two queues associated with the same egress port and both queues support the required ATM service categories, the system chooses the lower-priority queue for traffic from slot 1 and a queue that has either a high priority, or a low priority with a higher weight value, for traffic from slot 2.

The system selects the outgoing queue on the basis of a number of requirements, but if possible it selects a queue for the high-priority LIM that results in faster throughput for incoming traffic on that LIM.

Figure 5-2. High-priority LIM



System-generated active outgoing queues

The default queue configuration is stored in the `switch-config` profile. A trunk aggregation module (TRAM) supports its own ATM ASIC and default queues, stored in its own `switch-config` profile. For example, the following command shows the `switch-config` profiles created on a system with a TRAM installed in slot 17:

```
admin> dir switch-config
   633  09/12/2002 20:48:12  controller
  1976  09/12/2002 20:48:06  tram-17
```

In the following Tables showing default values assigned to the system-generated active configurations, queues are labeled `Qn` through `Qn+m` to represent the sets of queues allocated for each port or slot. For example, because each trunk port supports four active queues, the queues are labeled `Qn` through `Qn+3`. Each LIM slot is allocated two active queues, so the queues are labeled `Qn` and `Qn+1`. By default, each controller is assigned one queue.

Trunk port outgoing queues (`switch-config controller`)

Table 5-1. Defaults for OC3, DS3, or E3 active outgoing queues

Parameter	Q *n* default	Q *n*+1 default	Q *n*+2 default	Q *n*+3 default
active	yes	yes	yes	yes
physical-address	*port address*	*port address*	*port address*	*port address*
cbr	yes	no	no	no
real-time-vbr	no	yes	no	no
non-real-time-vbr	no	no	yes	no
ubr	no	no	no	yes
high-priority-weight	12	5	0	0
low-priority-weight	0	0	4	1
source-port	any	any	any	any
hop-level	any-level	any-level	any-level	any-level

Table 5-2. Defaults for Stinger MRT T1/E1 active outgoing queues

Parameter	Q *n* default	Q *n*+1 default	Q *n*+2 default	Q *n*+3 default
active	yes	yes	yes	yes
physical-address	*port address*	*port address*	*port address*	*port address*
cbr	yes	no	no	no
real-time-vbr	no	yes	no	no
non-real-time-vbr	no	no	yes	no
ubr	no	no	no	yes
high-priority-weight	5	2	0	0
low-priority-weight	0	0	4	1
source-port	any	any	any	any
hop-level	any-level	any-level	any-level	any-level

Table 5-3. Defaults for OC12 active outgoing queues

Parameter	Q *n* default	Q *n*+1 default	Q *n*+2 default	Q *n*+3 default
active	yes	yes	yes	yes
physical-address	*port address*	*port address*	*port address*	*port address*
cbr	yes	no	no	no
real-time-vbr	no	yes	no	no
non-real-time-vbr	no	no	yes	no
ubr	no	no	no	yes

Table 5-3. Defaults for OC12 active outgoing queues (Continued)

Parameter	Q *n* default	Q *n*+1 default	Q *n*+2 default	Q *n*+3 default
`high-priority-weight`	12	6	0	0
`low-priority-weight`	0	0	5	4
`source-port`	`any`	`any`	`any`	`any`
`hop-level`	`any-level`	`any-level`	`any-level`	`any-level`

Notice about default values when an OC12 trunk module is installed

When an OC12 trunk module is installed, the system assigns defaults to support full duplex throughput (599040Mbps) on a single OC12 port.

Note If you use multiple OC12 trunk ports, the total bandwidth must still be within 599040Mbps. In addition, when multiple OC12 trunk ports are in use, the total throughput supported by the system is reduced to approximately 95% of the capacity it supports when one OC12 port is in use.

OC12 VP shaper limitation

To support 599040Mbps bandwidth for an OC12 trunk module, the system assigns a higher weight to the ASIC's high-priority queues. As a tradeoff to the increased traffic processing achieved with higher weight assignments, the number of VP shapers the system can support is reduced from 10 to 8 if one OC12 module is installed, and from 10 to 6 VP shapers if two OC12 modules are installed.

Workaround for VP shaper limitation with OC12

If you must use up to 10 VP shapers with OC12, you can reduce the weight of the high-priority scheduler from 4 to 3 on any trunk port that is not being used, and/or on queue 31 (the queue used for the primary controller in slot 8), and/or on queue 32 (the queue for the secondary controller in slot 9). For example, the following commands change the weight of the high-priority scheduler on queues 31 and 32:

```
admin> read switch-config controller
SWITCH-CONFIG/controller read

admin> set atm outgoing-queue 31 high-priority-weight = 3

admin> set atm outgoing-queue 32 high-priority-weight = 3

admin> write -f
SWITCH-CONFIG/controller written
```

Reducing the `high-priority-weight` value from 4 to 3 increases the number of supported VP shapers by 2. However, reducing the weight of queues used for the controllers also reduces the throughput to support intrashelf traffic from OC12 to the controller (for example, to the Gigabit Ethernet port of an IP2000 controller) from approximately 98% to approximately 70% of 599040Mbps.

Controller outgoing queues (`switch-config controller`)

Table 5-4. Defaults for controller active outgoing queues

Parameter	Controller 1 Q defaults		Controller 2 Q defaults	
active	yes		yes	
physical-address	{ 1 8 0 }		{ 1 9 0 }	
cbr	yes		yes	
real-time-vbr	yes		yes	
non-real-time-vbr	yes		yes	
ubr	yes		yes	
high-priority-weight	3	(4 with OC12)	3	(4 with OC12)
low-priority-weight	0	(5 with OC12)	0	(5 with OC12)
source-port	any		any	
hop-level	any-level		any-level	

LIM slot outgoing queues (`switch-config controller`)

Table 5-5. Defaults for LIM slot active outgoing queues

Parameter	Q *n* default	Q *n*+1 default
active	yes	yes
physical-address	*slot address*	*slot address*
cbr	yes	no
real-time-vbr	yes	no
non-real-time-vbr	no	yes
ubr	no	yes
high-priority-weight	3	0
low-priority-weight	0	3
source-port	any	any
hop-level	any-level	any-level

TRAM port outgoing queues (`switch-config tram`)

For each OC3 port on a TRAM, the system creates one queue for each QoS service category for each of the other possible TRAM source port addresses. Table 5-6 shows some sample default values for outgoing queues on the first OC3 port on a TRAM for inbound traffic from the first DS3 port on the same TRAM. (The system creates similar queues that specify the `source-port` address of the other three DS3 interfaces.)

Table 5-6. Defaults for TRAM OC3 queues for traffic from TRAM DS3 ports

Parameter	Q *n* default	Q *n*+1 default	Q *n*+2 default	Q *n*+3 default
active	yes	yes	yes	yes
physical-address	{ 1 18 1 }	{ 1 18 1 }	{ 1 18 1 }	{ 1 18 1 }
cbr	yes	no	no	no
real-time-vbr	no	yes	no	no
non-real-time-vbr	no	no	yes	no
ubr	no	no	no	yes
high-priority-weight	6	2	0	0
low-priority-weight	0	0	2	1
source-port	{ 1 18 3 }	{ 1 18 3 }	{ 1 18 3 }	{ 1 18 3 }
hop-level	any-level	any-level	any-level	any-level

For each OC3 port on a TRAM, the system also creates two queues that can take traffic corresponding to any service category and from any source port (traffic from internal channels, such as LIM traffic, are mapped to these queues). Table 5-7 shows the default values for outgoing queues on the first OC3 port on a TRAM for traffic from internal channels. (The system creates similar queues for the second OC3 port.)

Table 5-7. Defaults for TRAM OC3 queues for traffic from internal channels

Parameter	Q *n* default	Q *n*+1 default
active	yes	yes
physical-address	{ 1 18 1 }	{ 1 18 1 }
cbr	yes	no
real-time-vbr	yes	no
non-real-time-vbr	no	yes
ubr	no	yes
high-priority-weight	2	0
low-priority-weight	0	2
source-port	any	any
hop-level	any-level	any-level

For each DS3 port on a TRAM, the system creates one queue for each QoS service category and sets the `source-port` value for each queue set to the wildcard value. Table 5-8 shows some sample default values for outgoing queues on the first DS3 port on a TRAM.

Table 5-8. Defaults for TRAM DS3 active outgoing queues

Parameter	Q *n* default	Q *n*+1 default	Q *n*+2 default	Q *n*+3 default
`active`	`yes`	`yes`	`yes`	`yes`
`physical-address`	`{ 1 18 3 }`	`{ 1 18 3 }`	`{ 1 18 3 }`	`{ 1 18 3 }`
`cbr`	`yes`	`no`	`no`	`no`
`real-time-vbr`	`no`	`yes`	`no`	`no`
`non-real-time-vbr`	`no`	`no`	`yes`	`no`
`ubr`	`no`	`no`	`no`	`yes`
`high-priority-weight`	`5`	`2`	`0`	`0`
`low-priority-weight`	`0`	`0`	`2`	`1`
`source-port`	`any`	`any`	`any`	`any`
`hop-level`	`any-level`	`any-level`	`any-level`	`any-level`

For more details about TRAM queues, see the Stinger *Trunk Aggregation Module (TRAM) Guide*.

TRAM default weight requirement for improved throughput

To take advantage of improved interface payload throughput for TRAM interfaces, when the system is running the 9.4-185.2 software version or later, the `high-priority-weight` of the following outgoing queues must be set to `6`:

- outgoing-queue 1
- outgoing-queue 5
- outgoing-queue 9
- outgoing-queue 13
- outgoing-queue 19
- outgoing-queue 23
- outgoing-queue 27
- outgoing-queue 31

Enabling the system to generate new defaults for TRAM queues

If the TRAM `switch-config` profile was created under a software version earlier than 9.4-185.2 and the default queue settings are in use, you can simply delete the old profile(s) and create a new one. The new profile will use the weights required for increased TRAM throughput. The following commands accomplish this for a TRAM in slot 17. (If the system also supports a TRAM in slot 18, you must perform the same procedure for that module.)

```
admin> delete switch-config tram-17
Delete profile SWITCH-CONFIG/tram-17? [y/n] y
SWITCH-CONFIG/tram-17 deleted

admin> new switch-config tram-17
SWITCH-CONFIG/tram-17 read
```

```
admin> write -f
SWITCH-CONFIG/tram-17 written
```

Setting the weights for improved TRAM throughput

If the TRAM `switch-config` profile was created under a software version earlier than 9.4-185.2 and a customized queue configuration is in use, first save the configuration to an external server, and then apply the required `high-priority-weight` values manually. The following commands apply the new `high-priority-weight` values for a TRAM in slot 17. (If the system also supports a TRAM in slot 18, you must perform the same procedure for that module.)

```
admin> read switch-config tram-17
SWITCH-CONFIG/tram-17 read

admin> set atm-parameters outgoing-queue 1 high-priority-weight = 6

admin> set atm-parameters outgoing-queue 5 high-priority-weight = 6

admin> set atm-parameters outgoing-queue 9 high-priority-weight = 6

admin> set atm-parameters outgoing-queue 13 high-priority-weight = 6

admin> set atm-parameters outgoing-queue 19 high-priority-weight = 6

admin> set atm-parameters outgoing-queue 23 high-priority-weight = 6

admin> set atm-parameters outgoing-queue 27 high-priority-weight = 6

admin> set atm-parameters outgoing-queue 31 high-priority-weight = 6

admin> write -f
SWITCH-CONFIG/tram-17 written
```

Configuring inactive outgoing queues

The controller ASIC supports 62 outgoing queues. The number of outgoing queues with inactive configurations, which can be used for VP shaping, depends on the type of Stinger platform. For example, Stinger FS controller ASICs support 16 inactive queues (queue 46 through 62), and Stinger MRT controller ASICs support up to 36 inactive queues, depending on how the unit is configured physically.

Note If you modify an outgoing queue configuration while the system is actively processing traffic, the queues are reconfigured dynamically. This process causes a reset of the ATM switching fabric, which might cause some cell loss but does not terminate active connections.

Caveat about modifying system-generated active queues

Although you can modify the default priorities of system-generated outgoing queues if your environment requires it, you cannot remove support for an ATM service category on a LIM or trunk port. Reconfiguring the system-generated outgoing queues for the controller ASIC must be done with caution, because the default outgoing queues are distributed among the slots and ports to handle ATM service categories efficiently and fairly.

How the system selects a queue

The system selects a queue for a particular connection by comparing the source address, outgoing port, quality of service (QoS) of the queue, priority of the source interface, and the subtending hops between the Stinger unit and the virtual circuit end point. If a trunk aggregation module (TRAM) is installed, the comparison process is run on each ASIC in the system independently. Further, for each leg of a cross-connection, the output queue is determined in each direction.

The procedure works by performing several comparison passes and selectively narrowing the set of available queues. Wildcard `source-port` or `hop-level` values (such as the following) match any value, so queues with these values remain in the list of possible queues for the next comparison pass.

```
source-port = {any-shelf any-slot 0}
hop-level = any-level
```

Note For user-defined queues associated with a VP shaper, the system ignores the QoS of the VPC and the QoS of the queue when selecting the queue to use for VPC traffic. For more details, see "Configuring VP shaping for VPCs" on page 5-15.

Overview of `outgoing-queue` settings

If the unit does not support an optional TRAM, the system creates a single `switch-config` profile for configuring the controller ASIC. For example:

```
admin> dir switch-config
603 03/02/2002 15:04:14 controller
```

Note Do not modify the profile index name (`controller` in this example) assigned by the system.

Following are the `switch-config` parameters for configuring the inactive queues, shown with default values for queue 47:

```
[in SWITCH-CONFIG/controller:atm-parameters:outgoing-queue[47]]
active = no
name = ""
physical-address = { shelf-1 any-slot 0 }
cbr = no
real-time-vbr = no
non-real-time-vbr = no
ubr = no
high-priority-weight = 0
low-priority-weight = 0
source-port = { any-shelf any-slot 0 }
hop-level = any-level
```

Parameter	Setting
`active`	Enable/disable the queue for use. By default queues 1 through 46 are active. If a queue is active, at least one service category must be set to `yes`.
`name`	Text name of the slot or interface. With the current software version, this value is read-only.

Parameter	**Setting**
physical-address	Physical address of the slot or interface in the Stinger unit to which outgoing traffic using this queue is directed. If active is yes, then the value of this parameter must be the valid address of a LIM, controller, or trunk port. The interface associated with each queue is identified in the physical-address field associated with the queue.
cbr	Enable/disable the queue for CBR traffic. At least one of the active queues assigned to a LIM, controller, or trunk port must be enabled for CBR traffic. This setting is not used by the system in selecting a user-defined queue associated with a VP shaper for VPC traffic.
real-time-vbr	Enable/disable the queue for real-time VBR traffic. At least one of the active queues assigned to a LIM, controller, or trunk port must be enabled for real-time VBR traffic. This setting is not used by the system in selecting a user-defined queue associated with a VP shaper for VPC traffic.
non-real-time-vbr	Enable/disable the queue for non-real-time VBR traffic. At least one of the active queues assigned to a LIM, controller, or trunk port must be enabled for non-real-time VBR traffic. This setting is not used by the system in selecting a user-defined queue associated with a VP shaper for VPC traffic.
ubr	Enable/disable the queue for UBR traffic. At least one of the active queues assigned to a LIM, controller, or trunk port must be enabled for UBR traffic. This setting is not used by the system in selecting a user-defined queue associated with a VP shaper for VPC traffic.
high-priority-weight	Weight on the high-priority scheduler (a number from 0 to 15). The higher the number, the more of the scheduler's work cycle is dedicated to processing this queue relative to other queues on the same scheduler. The sum of all high-priority-weight settings in all outgoing queues must be less than or equal to 128. For related information, see "Outgoing queue priority and weight" on page 5-2. Either this parameter or low-priority-weight must be nonzero if the queue is active. If both this parameter and the low-priority-weight parameter are assigned nonzero values, the queue appears on both schedulers, which can result in even higher scheduler priority.

Parameter	Setting
low-priority-weight	Weight on the low-priority scheduler (a number from 0 to 15). The higher the number, the more of the scheduler's work cycle is dedicated to processing this queue relative to other queues on the same scheduler. The sum of all low-priority-weight settings in all outgoing queues must be less than or equal to 128. For related information, see "Outgoing queue priority and weight" on page 5-2. Either this parameter or high-priority-weight must be nonzero if the queue is active. If both this parameter and the high-priority-weight parameter are assigned nonzero values, the queue appears on both schedulers, which can result in even higher scheduler priority.
source-port	Physical address of a LIM slot or trunk port from which data is permitted into the queue. This parameter is used to restrict a configured queue to a specific local port or slot. The default wildcard address { any-shelf any-slot 0 } indicates that data from any LIM slot or trunk port is permitted into this queue.
hop-level	Number of hops (ATM switches) between the Stinger unit and a virtual circuit end point that is permitted to use the queue. This parameter is used to restrict a configured queue for use by virtual circuits originating a certain distance away. With the default any-level setting, a virtual circuit that originated from a node that is any number of hops away from the Stinger unit is permitted into this queue. Other possible values are 0-level (virtual circuits originating from a node that is zero hops away), 1-level, 2-level, or 3-level.

Overview of outgoing-shaper settings

The controller ASIC supports up 10 configured VP shapers for shaping virtual path bandwidth on trunk interfaces. Each shaper must be associated with a dedicated user-defined outgoing queue that is associated with a trunk port.

Following are the switch-config parameters for configuring a VP shaper (shaper 1 through 10), shown with default values:

```
[in SWITCH-CONFIG/controller:atm-parameters:outgoing-shaper[1]]
queue-index = 0
vpi = 0
bandwidth = 0
```

Parameter	Setting
`queue-index`	Index of a dedicated user-defined outgoing queue associated with a trunk port. The valid range of this setting is from 0 to 62, but Lucent Technologies recommends that you use VP shaping only with a user-defined queue. The specified queue is available only for traffic with the VPI value specified in the shaper definition (the `vpi` setting). With the default zero value, the shaper is not active.
`vpi`	VPI of the virtual path to be shaped. The valid range is 1 to 1023.
`bandwidth`	Shaped bandwidth in kilobits per second. The valid range is 8000 to 155520Kbps. Note that the minimum rate for shaping traffic is 8Mbps.

Configuring VP shaping for VPCs

VP shaping is intended for use only with a dedicated user-defined queue. To shape bandwidth usage for a trunk-side VPC, you must define both a dedicated queue and a VP shaper. The queue and shaper definitions work together to admit only traffic with the specified VPI and send it out on a specified trunk port with the configured bandwidth requirements.

Note For virtual path traffic only, when a shaper has been applied to the queue, the system does not examine the class of service assigned to the VPC or the class of service settings in the queue definition when selecting the queue to use. For shaped VPCs only, class of service is ignored in queue selection.

Shaping egress virtual path bandwidth

In this example, a queue is configured to forward traffic to the first trunk port in the system. Because the queue is associated with a VP shaper, it will accept only traffic with the specified VPI. The VP shaper sets the maximum bandwidth for this traffic stream to 12Mbps. The following set of commands configures queue 47 for egress to the first trunk port in slot 17:

```
admin> read switch-config controller
SWITCH-CONFIG/controller read

admin> list atm-parameters outgoing-queue 47
[in SWITCH-CONFIG/controller:atm-parameters:outgoing-queue[47]]
active = no
name = ""
physical-address = { shelf-1 any-slot 0 }
cbr = no
real-time-vbr = no
non-real-time-vbr = no
ubr = no
high-priority-weight = 0
low-priority-weight = 0
```

```
source-port = { any-shelf any-slot 0 }
hop-level = any-level
```

admin> **set active = yes**

admin> **set physical-address = { 1 17 1 }**

The next commands configure the weight of this queue in the scheduler and write the profile:

admin> **set low-priority-weight = 12**

admin> **write -f**
SWITCH-CONFIG written

The next set of commands configures a VP shaper and associates it with queue 47:

admin> **list .. .. outgoing-shaper 1**

```
[in SWITCH-CONFIG:atm-parameters:outgoing-shaper[1]]
queue-index = 0
vpi = 0
bandwidth = 0
```

admin> **set queue-index = 47**

admin> **set vpi = 20**

admin> **set bandwidth = 12000**

admin> **write -f**
SWITCH-CONFIG written

Shaping egress bandwidth for traffic originating from slot 5

In this example, a queue is configured to accept traffic originating on slot 5 and forward the traffic to the first trunk port in the system. Because the queue is associated with a VP shaper, it will accept only traffic with the specified VPI. The VP shaper sets the maximum bandwidth for this traffic stream to 12Mbps. The following commands configure queue 52 for egress to the first trunk port in slot 18, and to admit traffic from slot 5 into the queue:

admin> **list .. .. outgoing-queue 52**

```
[in SWITCH-CONFIG/controller:atm-parameters:outgoing-queue[52]]
active = no
name = ""
physical-address = { shelf-1 any-slot 0 }
cbr = no
real-time-vbr = no
non-real-time-vbr = no
ubr = no
high-priority-weight = 0
low-priority-weight = 0
source-port = { any-shelf any-slot 0 }
hop-level = any-level
```

admin> **set active = yes**

admin> **set physical-address = { 1 18 1 }**

admin> **set source-port = { 1 5 0 }**

The next commands configure the weight of this queue in the scheduler and write the profile:

```
admin> set low-priority = 1

admin> write -f
SWITCH-CONFIG/controller written
```

The next set of commands configures a VP shaper and associates it with queue 52:

```
admin> list .. .. outgoing-shaper 2
[in SWITCH-CONFIG:atm-parameters:outgoing-shaper[2]]
queue-index = 0
vpi = 0
bandwidth = 0

admin> set queue-index = 52

admin> set vpi = 36

admin> set bandwidth = 8000

admin> write -f
SWITCH-CONFIG written
```

Configuring VP shaping for VCCs

Stinger units can use the VP shaper mechanism to shape bandwidth usage for multiple VCCs that share the same VPI on the trunk side. The VCCs *share* the bandwidth specified in the shaper definition. The cumulative output of the queue (not the individual VCCs within the virtual path) is shaped. The system does not place a limit on the number of VCCs a shaper can manage in this way.

Required trunk interface settings for VCC shaping

You cannot bind a VP shaper to VPI 0 (zero), the default VPI used for virtual channel switching. So, you must define an additional VPI for virtual channel switching on the trunk port used for egress. For example, the following commands reserve VPI 101 for virtual channel switching:

```
admin> read ds3-atm { 1 17 1 }
DS3-ATM/{ shelf-1 trunk-module-1 1 } read

admin> set line-config vc-switching-vpi 1 = 101

admin> set line-config vpi-vci-range = vpi-0-255-vci-32-4095

admin write
DS3-ATM/{ shelf-1 trunk-module-1 1 } written
```

For details about VPI and VCI allocation, see "VPI-VCI configuration for trunk interfaces" on page 3-2.

Required LIM interface settings for VCC shaping

Because of the internal algorithms used by the ASIC when queuing cell streams, you must include certain settings in the atm-qos profile used by ingress VCCs on LIM interfaces. For the queue to be in a stable state, the LIM interfaces for all the incoming VCCs must police traffic and tag cells that exceed the SCR before forwarding the cell stream to the switch. This enables the shaper to manage the bandwidth of the component VCCs equally. Without these settings, variations in dropped cells will occur across the component VCCs.

Example ATM-QOS for component VCCs

For the purposes of this example, suppose 10 VCCs are destined to the same trunk port with the same VPI, and the VP shaper's desired output for the VPI is to be limited to 8Mbps. To enable the system to shape the component VCCs equally, it is recommended that all of the VCC `connection` profiles specify the same `atm-qos` profile, as shown in the following commands. In this example, the `atm-qos` profile specifies real-time VBR service.

```
admin> new atm-qos
ATM-QOS/"" read
admin> set contract-name = rtvbr
admin> set atm-service-category = real-time-vbr
```

The following command sets the PCR to the SDSL port rate:

```
admin> set peak-rate-kbits-per-sec = 2320
```

The following command sets the SCR for each VCC to be 800Kbps (8000 divided by the number of VCCs multiplexed through the shaper):

```
admin> set sustainable-rate-kbits-per-sec = 800
```

The following commands change the default behavior of dropping cells that exceed the SCR, which instructs the LIM to tag the cells with a CL) of 1, and write the profile.

```
admin> set tag-or-discard = tag
admin> write -f
ATM-QOS/rtvbr written
```

For details about `atm-qos` profiles, see Chapter 4, "Configurable Quality of Service."

The following commands apply this profile to a VCC in a local `connection` profile:

```
admin> new connection vcc-1
CONNECTION/vcc-1 read
admin> set active = yes
admin> set encapsulation-protocol = atm-circuit
admin> set ip-options ip-routing-enabled = no
admin> set atm-options nailed-group = 155
admin> set atm-options vci = 32
admin> set atm-connect-options nailed-group = 801
admin> set atm-connect-options vpi = 101
admin> set atm-connect-options vci = 33
admin> set atm-qos-options usr-up-stream-contract = rtvbr
admin write
CONNECTION/vcc-1 read
```

Caveats about ATM-QOS settings and shaping

If all sources are sending data that is already tagged with CLP = 1, there will be unequal drops of cells across component shaped VCCs. This behavior is generally acceptable because when cells are coming in with CLP = 1, no guarantees are made regarding the transport of those cells through the network.

Recommendations for use in a subtended configuration

When this feature is used in a subtended Stinger configuration, the subtended Stinger must be set up to do the CLP tagging. This method is recommended because the controller ASIC does not have the capability to police at SCR rate and tag cells that exceed it. Keep this requirement in mind if you use this feature on subtended units.

Class of service considerations

Although the system permits VCCs with different classes of service to use the same VP shaper, for best results, ensure that all VCCs going into the queue associated with a shaper use the same class of service.

The system does not shape bandwidth for the component VCCs of a virtual path, so if the `atm-qos` settings for the VCCs are very different, one VCC can consume a large amount of the shaped bandwidth. For example, if the VP shaper specifies 10Mbps bandwidth, and one of the component VCCs is carrying traffic at a rate close to 10Mbps with a high-priority class of service, the remaining VCCs have almost no available bandwidth. In addition, if the VCCs use different classes of service, bursty traffic from one of the VCCs can result in queue processing problems such as potential head-of-line blocking.

To address the potential problems that can occur when VCCs with different classes of service share a VP shaper, you can configure multiple shapers that specify the same VPI but different criteria for admission into their queues. For example, you can configure one shaper to admit only CBR connections from a certain LIM port, and another shaper to admit only real-time VBR and non-real-time VBR connections from any source port. Admission to a queue can be decided on the basis of any combination of the following:

- Source port or source slot of the traffic stream in the system. (See the sample configuration in “Shaping UBR VCCs from LIM slot 6, port 5” on page 5-22.)
- Priority of the source port of the traffic stream. (See “Setting incoming traffic priority” on page 5-3.)
- Class of service of the traffic stream

Shaping VCCs irrespective of class of service

The following set of sample commands configure the Stinger unit to shape the cumulative bandwidth of all VCCs with an egress VPI of 100 on the first trunk port in slot 17 to 9Mbps. All VCCs with that egress VPI and port will be affected by this shaper.

The following commands open the first VP shaper configuration in the controller’s `switch-config` profile:

```
admin> read switch-config controller
SWITCH-CONFIG/controller read

admin> list atm-parameters outgoing-shaper 1
[in SWITCH-CONFIG/controller:atm-parameters:outgoing-shaper[1]]
queue-index = 0
vpi = 1
bandwidth = 8000
```

The next set of commands specifies that traffic in queue 50 with VPI 100 will be shaped to 9Mbps:

```
admin> set queue-index = 50

admin> set vpi = 100

admin> set bandwidth = 9000
```

The next commands configure queue 50 for egress to the first trunk port in slot 17, and to admit traffic with any class of service into the queue:

```
admin> list .. .. outgoing-queue 50
[in SWITCH-CONFIG/controller:atm-parameters:outgoing-queue[50]]
active = no
name = ""
physical-address = { shelf-1 any-slot 0 }
cbr = no
real-time-vbr = no
non-real-time-vbr = no
ubr = no
high-priority-weight = 0
low-priority-weight = 0
source-port = { any-shelf any-slot 0 }
hop-level = any-level

admin> set active = yes

admin> set physical-address = { 1 17 1 }

admin> set cbr = yes

admin> set real-time-vbr = yes

admin> set non-real-time-vbr = yes

admin> set ubr = yes
```

The next commands configure the weight of this queue in the scheduler and write the profile:

```
admin> set high-priority = 4

admin> write -f
SWITCH-CONFIG/controller written
```

Shaping only unspecified and non-real-time VBR VCCs

The following set of sample commands configure the Stinger unit to shape the cumulative bandwidth of UBR and non-real-time VBR VCCs with an egress VPI of 101 on the first trunk port in slot 17 to 8Mbps.

With this configuration, a VCC with an egress VPI of 101 but a different class of service is not admitted to the queue and will not be shaped. If no other shapers have been configured, the system uses the default queues for those VCCs.

The following commands open the second VP shaper configuration:

```
admin> read switch-config controller
SWITCH-CONFIG/controller read

admin> list atm-parameters outgoing-shaper 2
[in SWITCH-CONFIG/controller:atm-parameters:outgoing-shaper[2]]
queue-index = 0
vpi = 1
bandwidth = 8000
```

The next set of commands specifies that traffic in queue 51 with VPI 101 will be shaped to 8Mbps:

```
admin> set queue-index = 51
```

```
admin> set vpi = 101
```

```
admin> set bandwidth = 8000
```

The next commands configure queue 51 for egress to the first trunk port in slot 17, and admit UBR and non-real-time VBR VCCs into the queue:

```
admin> list .. .. outgoing-queue 51
[in SWITCH-CONFIG/controller:atm-parameters:outgoing-queue[51]]
active = no
name = ""
physical-address = { shelf-1 any-slot 0 }
cbr = no
real-time-vbr = no
non-real-time-vbr = no
ubr = no
high-priority-weight = 0
low-priority-weight = 0
source-port = { any-shelf any-slot 0 }
hop-level = any-level
```

```
admin> set active = yes
```

```
admin> set physical-address = { 1 17 1 }
```

```
admin> set non-real-time-vbr = yes
```

```
admin> set ubr = yes
```

The next commands configure the weight of this queue in the scheduler and write the profile:

```
admin> set low-priority = 4
```

```
admin> write -f
SWITCH-CONFIG/controller written
```

Shaping only UBR VCCs from LIM slot 5

The following set of sample commands configure the Stinger unit to shape the cumulative bandwidth of UBR VCCs that originate from the LIM in slot 5, and that have an egress VPI of 102 on the first trunk port in slot 18, to 16Mbps.

The following commands open the third VP shaper configuration:

```
admin> read switch-config controller
SWITCH-CONFIG/controller read
```

```
admin> list atm-parameters outgoing-shaper 3
[in SWITCH-CONFIG/controller:atm-parameters:outgoing-shaper[3]]
queue-index = 0
vpi = 1
bandwidth = 8000
```

The next set of commands specifies that traffic in queue 52 with VPI 102 will be shaped to 16Mbps:

```
admin> set queue-index = 52
```

```
admin> set vpi = 102
admin> set bandwidth = 16000
```

The next commands configure queue 52 for egress to the first trunk port in slot 18, and to admit only UBR VCCs from slot 5 into the queue:

```
admin> list .. .. outgoing-queue 52
[in SWITCH-CONFIG/controller:atm-parameters:outgoing-queue[52]]
active = no
name = ""
physical-address = { shelf-1 any-slot 0 }
cbr = no
real-time-vbr = no
non-real-time-vbr = no
ubr = no
high-priority-weight = 0
low-priority-weight = 0
source-port = { any-shelf any-slot 0 }
hop-level = any-level
admin> set active = yes
admin> set physical-address = { 1 18 1 }
admin> set ubr = yes
admin> set source-port = { 1 5 0 }
```

The next commands configure the weight of this queue in the scheduler and write the profile:

```
admin> set low-priority = 1
admin> write -f
SWITCH-CONFIG/controller written
```

Shaping UBR VCCs from LIM slot 6, port 5

The following set of sample commands configures the Stinger unit to shape the cumulative bandwidth of UBR VCCs that originate from port 5 of the LIM in slot 6, and that have an egress VPI of 103 on the first trunk port in slot 18, to 10Mbps:

The following commands open the fourth VP shaper configuration:

```
admin> read switch-config controller
SWITCH-CONFIG/controller read
admin> list atm-parameters outgoing-shaper 4
[in SWITCH-CONFIG/controller:atm-parameters:outgoing-shaper[4]]
queue-index = 0
vpi = 1
bandwidth = 8000
```

The next set of commands specifies that traffic in queue 53 with VPI 103 will be shaped to 10Mbps.

```
admin> set queue-index = 53
admin> set vpi = 103
admin> set bandwidth = 10000
```

The next commands configure queue 53 for egress to the first trunk port in slot 18, and to admit only UBR VCCs originating from port 5 on LIM slot 6 into the queue:

```
admin> list .. .. outgoing-queue 53
[in SWITCH-CONFIG/controller:atm-parameters:outgoing-queue[53]]
active = no
name = ""
physical-address = { shelf-1 any-slot 0 }
cbr = no
real-time-vbr = no
non-real-time-vbr = no
ubr = no
high-priority-weight = 0
low-priority-weight = 0
source-port = { any-shelf any-slot 0 }
hop-level = any-level

admin> set active = yes

admin> set physical-address = { 1 18 1 }

admin> set ubr = yes

admin> set source-port = { 1 6 5 }
```

The next commands configure the weight of this queue in the scheduler and write the profile:

```
admin> set low-priority = 4

admin> write -f
SWITCH-CONFIG/controller written
```

Subtending applications

In a subtending application, virtual circuits from a number of Stinger units that are connected through trunk modules (subtended units) all converge onto a single unit (the subtending unit) for transmission onto an ATM core network. The subtended units can be geographically remote.

The only constraint on where the units are located is the distance limitation imposed by the type of cable used to link the units. Because all traffic converges on the subtending unit, the maximum number of PVCs in a subtending configuration is the same as the maximum number of PVCs supported in the subtending unit.

Using trunk aggregation with subtending

A Stinger unit with a TRAM installed is a likely candidate for a subtending unit because its multiple interfaces and local ASIC make it ideal for aggregation applications. If one or more TRAMs are installed, the system creates `switch-config` profiles for those modules. For example:

```
admin> dir switch-config
603 02/02/2002 15:04:14 controller
1964 02/02/2002 15:08:22 tram-17
1770 02/02/2002 15:05:37 tram-18
```

Because the TRAM ASIC does the local switching among its ports, a much larger number of queues can be allocated on the TRAM's local ASIC to provide a substantially better quality of service for subtended applications. In the TRAM `switch-config` profiles, 54 of the 62 outgoing queues supported by the ASIC are configured by the system for handling outbound traffic. You can configure the remain 8 queues to any desired output port.

For details about using a TRAM for subtending, see the Stinger *Trunk Aggregation Module (TRAM) Guide.*

Specifying subtending hops

The following parameters can be used to restrict the ingress traffic accepted by a queue to traffic originating a specific number of hops (ATM switches) away, and to configure `connection` profiles to fulfill that requirement by setting a hop level. These settings are particularly useful in configuring a subtending unit to handle traffic from remote units. The parameters are shown here with default settings:

```
[in SWITCH-CONFIG/controller:atm-parameters:outgoing-queue[47]]
hop-level = any-level
```

```
[in CONNECTION/"":atm-qos-options]
subtending-hops = 0-level
```

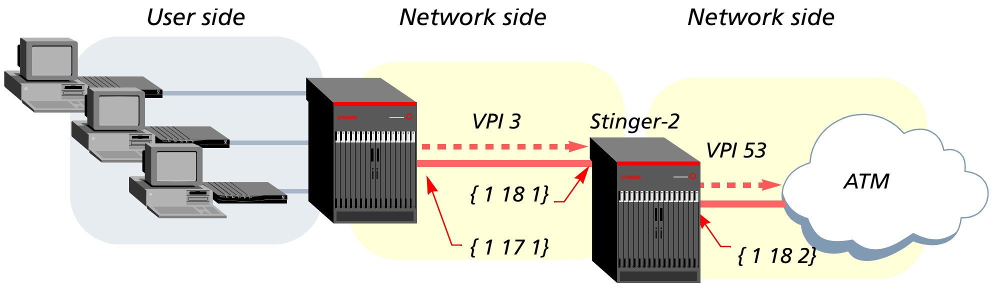
Parameter	Setting
`hop-level`	Number of hops (ATM switches) between the Stinger unit and a virtual circuit end point that is permitted to use the queue. For more details, see the description of this parameter under "Overview of outgoing-queue settings" on page 5-12.
`subtending-hops`	Number of hops (ATM switches) between the subtending Stinger unit and the virtual circuit end point represented in the `connection` profile. This parameter is currently supported only for PVCs or PVPs. With the default `0-level` setting, the virtual circuit end point is zero number of hops away from the subtending unit. Other possible values are `1-level`, `2-level`, or `3-level`.

For examples of how to use these settings in a subtending configuration, see the Stinger *Trunk Aggregation Module (TRAM) Guide.*

Sample subtending configuration

In the sample subtending configuration shown in Figure 5-3, two units are linked together by an OC3 cable, and connect to the ATM network by a single OC3 trunk interface. The unit labeled Stinger-1 is the subtended unit. The unit labeled Stinger-2 is the subtending unit, which is directly connected to the ATM backbone.

Figure 5-3. Stinger units in a subtending configuration



In this example, the two units are connected by the first port of an OC3-ATM trunk module in each unit. The subtending unit (Stinger-2) connects to the ATM network by the second port of its OC3-ATM trunk module.

The subtended unit (Stinger-1) switches traffic from its subscribers on LIM interfaces to its trunk port 1 in slot 17, where it is transmitted to the Stinger-2 unit's trunk port 1 in slot 18 with VPI 3.

The subtending unit switches the traffic received with VPI 3 on its subtending ingress trunk port (trunk port 1 in slot 18) to trunk port 2 in slot 18 with VPI 53. Trunk port 2 is the subtending egress port, which connects to the backbone.

Configuring the subtended unit (Stinger-1)

The subtended unit requires standard subscriber LIM-to-trunk ATM circuits using virtual channel switching. On the trunk side, each connection must use the same VPI (VPI 3 in this example) and must use the subtended trunk port.

The following commands configure the subtended trunk to support VPI 3 for virtual channel switching:

```
admin> read oc3-atm { 1 17 1 }
OC3-ATM/{ shelf-1 trunk-module-1 1 } read

admin> set line-config vc-switching-vpi 2 = 3

admin> write -f
OC3-ATM/{ shelf-1 trunk-module-1 1 } written
```

The next commands determine the nailed-group associated with the subtended trunk:

```
admin> which -n {1 17 1}
Nailed group corresponding to port { shelf-1 trunk-module-1 1 } is 801
```

The following commands configure two sample `connection` profiles for LIM-to-trunk ATM circuits. The egress port for these circuits is the subtended trunk.

```
admin> new connection subtend-1
CONNECTION/subtend-1 read

admin> set active = yes

admin> set encapsulation-protocol = atm-circuit

admin> set ip-options ip-routing-enabled = no

admin> set atm-options vci = 35

admin> set atm-options vpi = 8
```

```
admin> set atm-options nailed-group = 155
admin> set atm-connect-options vci = 32
admin> set atm-connect-options vpi = 3
admin> set atm-connect-options nailed-group = 801
admin> set atm-qos-options usr-up-stream-contract = nrt-vbr-1
admin> set atm-qos-options usr-dn-stream-contract = nrt-vbr-1
admin write
CONNECTION/subtend-1 read
admin> new connection subtend-2
CONNECTION/subtend-2 read
admin> set active = yes
admin> set encapsulation-protocol = atm-circuit
admin> set ip-options ip-routing-enabled = no
admin> set atm-options vci = 36
admin> set atm-options vpi = 8
admin> set atm-options nailed-group = 156
admin> set atm-connect-options vci = 33
admin> set atm-connect-options vpi = 3
admin> set atm-connect-options nailed-group = 801
admin> set atm-qos-options usr-up-stream-contract = nrt-vbr-1
admin> set atm-qos-options usr-dn-stream-contract = nrt-vbr-1
admin write
CONNECTION/subtend-2 read
```

Configuring the subtending unit (Stinger-2)

The following commands determine the nailed groups associated with the ingress and egress trunk ports in the subtending unit:

```
admin> which -n {1 18 1}
Nailed group corresponding to port { shelf-1 trunk-module-2 1 } is 851
admin> which -n {1 18 2}
Nailed group corresponding to port { shelf-1 trunk-module-2 2 } is 852
```

The following set of commands configures a VPC between the ingress and egress trunk interfaces:

```
admin> new connection subtend-trunk
CONNECTION/subtend-trunk read
admin> set active = yes
admin> set ip-options ip-routing-enabled = no
admin> set atm-options vpi = 3
admin> set atm-options nailed-group = 851
admin> set atm-options vp-switching = yes
admin> set atm-connect-options vpi = 53
```

```
admin> set atm-connect-options nailed-group = 852
admin> set atm-connect-options vp-switching = yes
admin> write -f
CONNECTION/subtend-trunk written
```

The following commands configure an outgoing queue for trunk port 2 with a low-priority scheduler weight of 5:

```
admin> read switch-config controller
SWITCH-CONFIG/controller read
admin> list atm-parameters outgoing-queue 53
[in SWITCH-CONFIG/controller:atm-parameters:outgoing-queue[53]]
name = ""
physical-address = { shelf-1 any-slot 0 }
cbr = no
real-time-vbr = no
non-real-time-vbr = no
ubr = no
high-priority-weight = 0
low-priority-weight = 0
source-port = { any-shelf any-slot 0 }
hop-level = any-level
admin> set active = yes
admin> set physical-address = { 1 18 2 }
admin> set real-time-vbr = yes
admin> set low-priority-weight = 5
```

The following set of commands configures a VP shaper that allocates a maximum rate of 53Mbps for queue 53, and writes the profile:

```
admin> list .. .. outgoing-shaper 3
[in SWITCH-CONFIG/controller:atm-parameters:outgoing-shaper[3]]
queue-index = 0
vpi = 0
bandwidth = 0
admin> set queue-index = 53
admin> set vpi = 53
admin> set bandwidth = 53000
admin> write -f
SWITCH-CONFIG/controller written
```

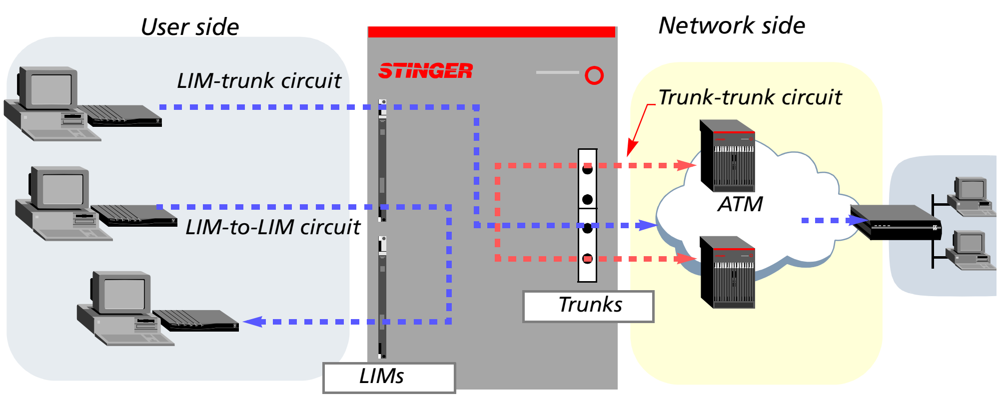
ATM Circuit Configuration

6

An ATM circuit is a cross-connection of two virtual links from one interface to another within the system. The ATM circuits described in this chapter are permanent virtual circuits (PVCs), which means that both sides of the circuit are manually configured in the `connection` or RADIUS profile.

The most widely used circuits are LIM-trunk circuits for DSLAM operations. However, LIM-to-LIM circuits and trunk-to-trunk circuits are also supported. Figure 6-1 shows an example of each type of circuit.

Figure 6-1. ATM circuits on LIM and trunk interfaces



Each LIM interface connects to a single CPE device. However, that physical connection can support up to eight circuits. Configuring more than one PVC on a LIM port enables the system to manage different types of ATM traffic at the same time for the same subscriber.

Overview of ATM circuit settings

ATM circuits are not password authenticated. You configure both sides of the circuit in one `connection` or RADIUS profile. The profile must specify `atm-circuit` encapsulation to make use of the system's circuit management software.

When the system establishes an ATM circuit, it places a call on one side of the circuit and then uses its circuit management software to handle the switch-through to the other side of the circuit. In the descriptions that follow, the side on which the call is placed is referred to as the *first side* of the circuit, which the system builds using the settings in the `atm-options` subprofile. The other side is referred to as the *second side* of the circuit, which the system builds using the settings in the `atm-connect-options` subprofile.

ATM circuits can use either VC switching or VP switching. For an introduction to VC and VP switching operations, and for a list of current limitations for VP switching, see "ATM switching operations" on page 1-1.

General `connection` profile settings for ATM circuits

The following basic `connection` parameters (shown with default settings) are used for ATM circuits. Some of these settings have counterparts in RADIUS profiles. For details about each RADIUS attribute, see the *TAOS RADIUS Guide and Reference*.

For information about other general ATM-related parameters, see the *Stinger Reference*.

```
[in CONNECTION/""]
station* = ""
active = no
encapsulation-protocol = atm-circuit
```

```
[in CONNECTION/"":ip-options]
ip-routing-enabled = yes
```

Parameter	RADIUS attribute	Setting
station	User-Name (1)	Name of the PVC. Because a subscriber can have up to eight configured PVCs, a common convention is to use the name of the subscriber device followed by a number (for example, `kam-1`, `kam-2`, and so forth).
active	N/A	Enable/disable the profile for active use.
encapsulation-protocol	Framed-Protocol (7)	Encapsulation protocol to use for the circuit. Must be set to `atm-circuit` (the default) for switch-through connections.
ip-routing-enabled	Ascend-Route-IP (228)	Enable/disable IP routing for the interface. IP routing is not used for ATM circuits. For best results, set this parameter to `no`.

The `atm-options` and `atm-connect-options` settings

The `atm-options` subprofile configures the first side of the circuit (the side on which the call is placed). For DSLAM operations, the first side of the circuit must be the subscriber side (a LIM port).

The `atm-connect-options` subprofile configures the second side of the circuit. For DSLAM operations, the second side of the circuit must be the trunk side. These two subprofiles contain more options than are listed below. Many of those parameters are for use with a specific LIM or software license. For details about those settings, see the *Stinger Reference* or the individual LIM guide.

Note The `atm-qos-options` subprofile enables you to apply a defined quality of service (QoS) contract to the circuit. For details about defining these contracts and applying them to one or both sides of a circuit, see Chapter 4, "Configurable Quality of Service."

Following are the parameters, shown with default values, for defining the two sides of an ATM circuit:

```
[in CONNECTION/"":atm-options]
atm1483type = aal5-llc
vpi = 0
vci = 35
nailed-group = 1
conn-kind = pvc
vp-switching = no
```

```
[in CONNECTION/"":atm-connect-options]
atm1483type = aal5-llc
vpi = 0
vci = 35
nailed-group = 1
vp-switching = no
```

Parameter	RADIUS attribute	Setting
`atm1483type`	`N/A`	*Not used for circuit configurations*. (See Chapter 7, "Terminating PVC Configuration.")
`vpi`	`Ascend-ATM-Vpi` (94) `Ascend-ATM-Connect-Vpi` (61)	In the `atm-options` subprofile, the VPI for the first side of the circuit. In the `atm-connect-options` subprofile, the VPI for the second side of the circuit. The default zero value means the circuit uses VC switching. For a discussion of valid values, see "Assigning valid VPI-VCI pairs" on page 6-5. *VP switching is not currently supported in RADIUS profiles.*
`vci`	`Ascend-ATM-Vci` (95) `Ascend-ATM-Connect-Vci` (62)	In the `atm-options` subprofile, the VCI for the first side of the circuit. In the `atm-connect-options` subprofile, the VCI for the second side of the circuit. For a discussion of valid values, see "Assigning valid VPI-VCI pairs" on page 6-5.
`nailed-group`	`Ascend-ATM-Group` (64) `Ascend-ATM-Connect-Group` (63)	In the `atm-options` subprofile, the nailed-group number of the interface used by the first side of the circuit. In the `atm-connect-options` subprofile, the nailed-group number of the interface used by the second side of the circuit. For a command that displays a port's nailed-group number, see "Identifying a circuit's ports with the which command" on page 6-4.

Parameter	RADIUS attribute	Setting
`vp-switching`	`N/A`	Enable/disable VP switching. The default value is `no`. If this parameter is set to `yes`, you must enable VP switching on both sides of the circuit and specify a valid VPI number for each side. *VP switching is not supported for LIM-to-LIM circuits and is not supported in RADIUS profiles.* (For related information, see "Assigning valid VPI-VCI pairs" on page 6-5.)

How circuits are established

A Stinger unit makes only one call in establishing an ATM circuit. It places the call on the *first side* of the circuit, which is built with the settings in the `atm-options` subprofile. After the system has placed the call to establish the initial nailed connection, switch-through to the second side of the circuit is handled internally. The unit generates `Call-Info` log information only for the side of the circuit on which it placed the call.

For LIM-trunk circuits (DSLAM), the call must be placed on the LIM port rather than the trunk port. For LIM-to-LIM and trunk-to-trunk circuits, either port can be used for the call that initiates a circuit.

Identifying a circuit's ports with the `which` command

The `which` command enables you to look up the nailed group associated with the ports to be used for an ATM connection. The command has the following syntax:

```
admin> help which
translate between nailed group and actual physical port

usage: which [-p|n] port|group
example: which -p 55
or:      which -n { 1 3 7 }
```

When used with the `-p` flag and a nailed-group number, the command displays the port address associated with that number. When used with the `-n` flag and a port address, the command displays the nailed group assigned to that port.

For examples of how to use the `which` command to find a port's nailed-group assignment for use in an ATM connection, see "Typical ATM circuits using VC switching" on page 6-6. You can also use the `which` command to determine which port is in use when you have the nailed-group assignment of a `connection` profile. For example, if the circuit uses nailed-group 296:

```
admin> which -p 296
The port corresponding to nailed group 296 is: { shelf-1 slot-6 46 }
```

If the argument specifies a slot that is not populated, or a nailed group that is not assigned, the command returns a message that the number was not found. For example:

```
admin> which -p 43
The port corresponding to nailed group 43 is:
NONE!
```

If more than one port has the same nailed group associated with it (which is illegal), the `which` command returns all the ports that have this nailed group. Consequently, the command provides a convenient way to find duplicate nailed-groups. For example:

```
admin> read sdsl {1 6 46}
SDSL/{ shelf-1 slot-6 46 } read

admin> set line-config nailed-group = 801

admin> write -f
SDSL/{ shelf-1 slot-6 46 } written

admin> which -p 801
The port corresponding to nailed group 801 is:
{ shelf-1 slot-6 46 }
{ shelf-1 trunk-module-1 1 }
```

Duplicate nailed-group assignments can occur only when the administrator changes default nailed-group numbers. To correct the problem, change the nailed-group assignments in one or more profiles, and then verify the change by using the `which` command again.

Assigning valid VPI-VCI pairs

You must be sure to use a VPI-VCI pair that is within the valid range assigned to both physical interfaces of an ATM circuit. A VPI-VCI assignment that is not compatible with a port's configuration causes the connection to fail with an error message.

For details about VPI-VCI assignments on LIMs, see "VPI-VCI configuration for trunk interfaces" on page 3-2. For details about VPI-VCI assignments on trunk interfaces, see "VPI-VCI configuration for trunk interfaces" on page 3-2.

Table 6-1 summarizes the assignment of VPI-VCI values for a PVC that uses VC switching and one that uses VP switching on a LIM interface.

Table 6-1. LIM interface VPI-VCI values

Switching type	VPI value	VCI value
Virtual channel	A VPI within the valid VPI range on the LIM slot, other than the VPI allocated for VP switching on the LIM interface.	Must be a VCI within the valid VCI range for the LIM slot.
Virtual path	VPI allocated for VP switching on the LIM interface.	Must be a VCI within the valid VCI range for the LIM slot, even though the VCI number is not significant in the VP switching process.

Note The `atm-config` profile specifies the valid VPI-VCI range specification for a LIM slot. Although the parameter settings in that profile show a VCI range that starts with 32, the VCI numbers from 0 through 31 can be used for subscriber connections on LIM interfaces, because LIMs do not support the ATM signaling and OAM functions that typically reserve those VCI numbers on ATM interfaces.

Table 6-2 summarizes the assignment of these values for a trunk interface.

Table 6-2. Trunk interface VPI-VCI values

Switching type	VPI value	VCI value
Virtual channel	VPI 0 (which is always allocated for VC switching on trunk interfaces) or another VPI configured for VC switching on the trunk interface.	Must be a VCI within the valid VCI range for the trunk interface.
Virtual path	Any VPI other than those configured for VC switching on the trunk interface.	Any value. Circuits that use VP switching have no restriction on the VCI number or on the number of VCCs switched on the virtual path.

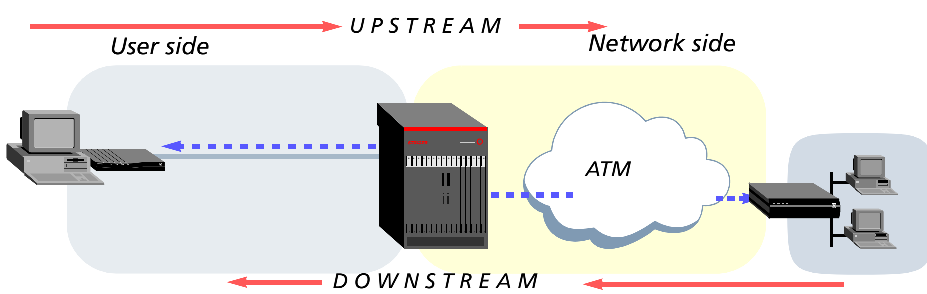
Typical ATM circuits using VC switching

When configuring a DSLAM ATM circuit, the user (LIM) side of the circuit must be defined in the `atm-options` subprofile, and the network (trunk) side of the circuit must be defined in the `atm-connect-options` subprofile. LIM-to-LIM and trunk-to-trunk circuits have no restriction on which side of the circuit must be specified in the `atm-options` subprofile. (For related information, see "How circuits are established" on page 6-4.)

Configuring a LIM-trunk circuit (DSLAM)

Figure 6-2 shows a sample digital subscriber line access multiplexer (DSLAM) configuration in which a Stinger unit receives ATM traffic from an ADSL subscriber and switches it onto a high-speed ATM backbone.

Figure 6-2. LIM-trunk circuit (DSLAM operations)



For DSLAM operations, data transmitted from the CPE to the Stinger unit is *upstream traffic.* Data transmitted from the Stinger unit to the CPE is *downstream traffic.*

The first side of the circuit (the side specified in the `atm-options` subprofile) must be the subscriber side. The following commands create a local `connection` profile and assign both of the ATM circuit's VCI numbers:

```
admin> new connection simon-1
CONNECTION/simon-1 read
```

```
admin> set active = yes
admin> set encapsulation-protocol = atm-circuit
admin> set ip-options ip-routing-enabled = no
admin> set atm-options vci = 32
admin> set atm-connect-options vci = 33
```

The following commands display the nailed-group number of an AL-DMT interface (slot 4, port 5) and assign it to the first side of the circuit:

```
admin> which -n {1 4 5}
Nailed group corresponding to port { shelf-1 slot-4 5 } is 155
admin> set atm-options nailed-group = 155
```

The following commands display the nailed-group number of an OC3-ATM interface (trunk module 1, port 2) and assign it to the second side of the circuit:

```
admin> which -n {1 17 2}
Nailed group corresponding to port { shelf-1 trunk-module-1 2 } is 802
admin> set atm-connect-options nailed-group = 802
```

The following commands assign an upstream and downstream QoS contract and write the profile:

```
admin> set atm-qos-options usr-up-stream-contract = abr-1
admin> set atm-qos-options usr-dn-stream-contract = cbr-1
admin write
CONNECTION/simon-1 read
```

For details about QoS, see Chapter 4, "Configurable Quality of Service."

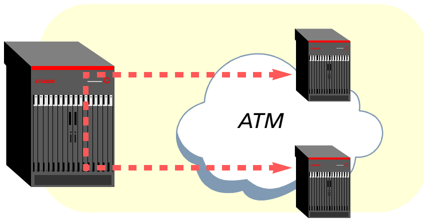
Following is a comparable circuit definition in a RADIUS profile:

```
permconn-ST-2 Password = "ascend"
    Service-Type = Outbound,
    Framed-Protocol = ATM-CIR,
    User-Name = "simon-1",
    Ascend-ATM-Group = 155,
    Ascend-Route-IP = Route-IP-No,
    Ascend-ATM-Vpi = 0,
    Ascend-ATM-Vci = 32,
    Ascend-ATM-Connect-Vpi = 0,
    Ascend-ATM-Connect-Vci = 33,
    Ascend-ATM-Connect-Group = 802,
    Ascend-QOS-Upstream = "abr-1",
    Ascend-QOS-Downstream = "cbr-1"
```

Configuring a trunk-to-trunk circuit

Figure 6-3 shows a sample configuration in which a Stinger unit receives ATM traffic from an ATM switch on one trunk interface and switches it through to a switch on another trunk interface.

Figure 6-3. Trunk-to-trunk circuit



For a trunk-to-trunk circuit, the system can place the call on either interface, so either side of the circuit can be specified in the `atm-options` subprofile.

The following commands create a local `connection` profile for the trunk-to-trunk circuit:

```
admin> new connection kai-1
CONNECTION/kai-1 read
```

```
admin> set active = yes
```

```
admin> set encapsulation-protocol = atm-circuit
```

```
admin> set ip-options ip-routing-enabled = no
```

The following commands assign VCI numbers to each side of the circuit:

```
admin> set atm-options vci = 100
```

```
admin> set atm-connect-options vci = 200
```

The following commands display the nailed-group number of a trunk interface (trunk module 1, port 1) and assign it to the first side of the circuit:

```
admin> which -n {1 17 1}
Nailed group corresponding to port { shelf-1 trunk-module-1 1 } is 801
```

```
admin> set atm-options nailed-group = 801
```

The following commands display the nailed-group number of a different trunk interface (trunk module 2, port 2) and assign it to the second side of the circuit:

```
admin> which -n {1 18 2}
Nailed group corresponding to port { shelf-1 trunk-module-2 2 } is 852
```

```
admin> set atm-connect-options nailed-group = 852
```

The following commands assign an upstream and downstream QoS contract and write the profile:

```
admin> set atm-qos-options usr-up-stream-contract = nrt-vbr
```

```
admin> set atm-qos-options usr-dn-stream-contract = cbr-1
```

```
admin write
CONNECTION/kai-1 read
```

For details about QoS, see Chapter 4, “Configurable Quality of Service.”

Following is a comparable circuit definition in a RADIUS profile:

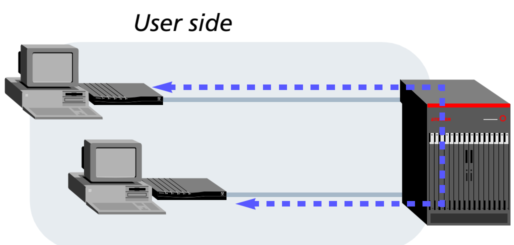
```
permconn-ST-4 Password = "ascend"
    Service-Type = Outbound,
    Framed-Protocol = ATM-CIR,
    User-Name = "kai-1",
```

```
Ascend-ATM-Group = 801,
Ascend-Route-IP = Route-IP-No,
Ascend-ATM-Vpi = 0,
Ascend-ATM-Vci = 100,
Ascend-ATM-Connect-Vpi = 0,
Ascend-ATM-Connect-Vci = 200,
Ascend-ATM-Connect-Group = 852,
Ascend-QOS-Upstream = "nrt-vbr",
Ascend-QOS-Downstream = "cbr-1"
```

Configuring a LIM-to-LIM circuit

Figure 6-4 shows a sample configuration in which a Stinger unit receives ATM traffic from a CellPipe unit on one SDSL interface and switches it through to another SDSL interface.

Figure 6-4. LIM-to-LIM circuit



For a LIM-to-LIM circuit, the system can place the call on either interface, so either side of the circuit can be specified in the `atm-options` subprofile.

Note VP switching is not supported for LIM-to-LIM circuits.

The following commands create a local `connection` profile and assign both of the ATM circuit's VCI numbers:

```
admin> new connection jintao-1
CONNECTION/jintao-1 read

admin> set active = yes

admin> set encapsulation-protocol = atm-circuit

admin> set ip-options ip-routing-enabled = no

admin> set atm-options vci = 42

admin> set atm-connect-options vci = 43
```

The following commands display the nailed-group number of an SDSL interface (slot 2, port 5) and assign it to the first side of the circuit:

```
admin> which -n {1 2 5}
Nailed group corresponding to port { shelf-1 slot-2 5 } is 55

admin> set atm-options nailed-group = 55
```

The following commands display the nailed-group number of another SDSL interface (slot 10, port 3) and assign it to the second side of the circuit:

```
admin> which -n {1 10 3}
Nailed group corresponding to port { shelf-1 slot-10 3 } is 803
```

```
admin> set atm-connect-options nailed-group = 803
```

The next commands assign upstream and downstream QoS contracts and write the profile:

```
admin> set atm-qos-options usr-up-stream-contract = cbr-1

admin> set atm-qos-options usr-dn-stream-contract = cbr-1

admin write
CONNECTION/jintao-1 read
```

For details about QoS, see Chapter 4, "Configurable Quality of Service."

Following is a comparable circuit definition in a RADIUS profile:

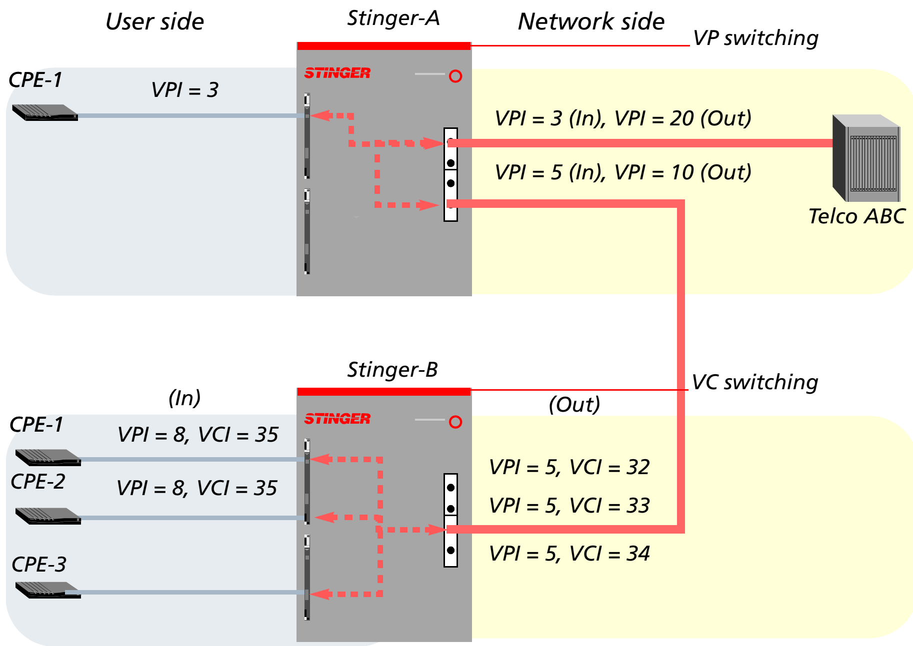
```
permconn-ST-5 Password = "ascend"
    Service-Type = Outbound,
    Framed-Protocol = ATM-CIR,
    User-Name = "jintao-1",
    Ascend-ATM-Group = 55,
    Ascend-Route-IP = Route-IP-No,
    Ascend-ATM-Vpi = 0,
    Ascend-ATM-Vci = 42,
    Ascend-ATM-Connect-Vpi = 0,
    Ascend-ATM-Connect-Vci = 43,
    Ascend-ATM-Connect-Group = 803,
    Ascend-QOS-Upstream = "cbr-1",
    Ascend-QOS-Downstream = "cbr-1"
```

Typical VP switching configuration

Figure 6-5 shows two Stinger units. The unit labeled Stinger-B is concentrating multiple incoming VCCs to a single outgoing VPC that uses VPI 5 with a range of VCIs starting with VCI 32.

The unit labeled Stinger-*A* is performing two VP switching operations. One VP switching operation is a LIM-trunk circuit from CPE-1 to the Telco switch using VPI 20. Another VP switching operation is a trunk-to-trunk circuit on which the unit switches the VPC from Stinger-B to the Telco switch using VPI 10.

Figure 6-5. Sample VP and VC switching configuration



For information about current VP switching limitations, see "VP switching" on page 1-2.

Stinger-A configuration using VP switching

The following examples show how to configure the LIM port, trunk ports, and `connection` profiles in the command-line interface of the unit labeled Stinger-A.

Sample LIM port configuration

The VPI-VCI ranges for LIM slots must be configured to support the VPI selected for VP switching on LIM ports (see "VPI-VCI configuration for LIM slots and interfaces" on page 3-6). The following commands configure a LIM port on Stinger-A for VP switching using VPI 3:

```
admin> read sdsl { 1 5 5 }
SDSL/{ shelf-1 slot-5 5 } read

admin> set enabled = yes

admin> set line-config vp-switching = 3

admin> write -f
SDSL/{ shelf-1 slot-5 5 } written
```

Sample trunk port configuration

The following commands enables the first port of the first trunk module and the second port of the second trunk module on Stinger-A. The profiles retain their default settings, which allows the ports to use VP switching using any VPI other than zero:

```
admin> read ds3-atm {1 trunk-module-1 1}
DS3-ATM/{ shelf-1 trunk-module-1 1 } read
```

```
admin> set enabled = yes

admin> write -f
DS3-ATM/{ shelf-1 trunk-module-1 1 } written

admin> read ds3-atm {1 trunk-module-1 2}
DS3-ATM/{ shelf-1 trunk-module-1 2 } read

admin> set enabled = yes

admin> write -f
DS3-ATM/{ shelf-1 trunk-module-1 2 } written
```

Sample CPE `connection` profile

The following commands create a `connection` profile for the CPE-1 connection to Stinger-A:

```
admin> new connection cpe-1
CONNECTION/cpe-1 read

admin> set active = yes

admin> set encapsulation-protocol = atm-circuit

admin> set ip-options ip-routing-enabled = no

admin> set atm-options vpi = 3

admin> set atm-options nailed-group = 155

admin> set atm-options vp-switching = yes

admin> set atm-connect-options vpi = 20

admin> set atm-connect-options nailed-group = 801

admin> set atm-connect-options vp-switching = yes

admin write
CONNECTION/cpe-1 read
```

The first side of the circuit uses the SDSL port in slot 5, port 5. That port has the nailed group 155, which has been configured for VP switching using VPI 3. The second side uses the first trunk port (nailed-group 801) with VPI 20.

Note The CPE connection must use a VCI within the valid VCI range configured for the LIM port, even when VP switching is used. However, the value is not used for switching.

Sample trunk-to-trunk `connection` profile for traffic from Stinger-B

The following commands create a `connection` profile for the trunk-to-trunk connection from Stinger-B to the Telco switch:

```
admin> new connection stinger-b
CONNECTION/stinger-b read

admin> set active = yes

admin> set encapsulation-protocol = atm-circuit

admin> set ip-options ip-routing-enabled = no

admin> set atm-options vpi = 5

admin> set atm-options nailed-group = 852

admin> set atm-options vp-switching = yes
```

```
admin> set atm-connect-options vpi = 20
admin> set atm-connect-options nailed-group = 801
admin> set atm-qos-options usr-up-stream-contract = ubr-1
admin> set atm-qos-options usr-dn-stream-contract = ubr-1
admin write
CONNECTION/stinger-b read
```

The first side of the circuit uses the second port of the second trunk module (nailed group 852) with VPI 5. The second side uses the first port of the first trunk module (nailed group 801) with VPI 20.

Stinger-B CPE `connection` profiles using VC switching

The following commands create three `connection` profiles for the CPEs connecting to Stinger-B in Figure 6-5:

```
admin> new connection cpe-1
CONNECTION/cpe-1 read
admin> set active = yes
admin> set encapsulation-protocol = atm-circuit
admin> set ip-options ip-routing-enabled = no
admin> set atm-options vpi = 8
admin> set atm-options vci = 35
admin> set atm-options nailed-group = 122
admin> set atm-connect-options vpi = 5
admin> set atm-connect-options vci = 32
admin> set atm-connect-options nailed-group = 851
admin write
CONNECTION/cpe-1 read
admin> new connection cpe-2
CONNECTION/cpe-2 read
admin> set active = yes
admin> set encapsulation-protocol = atm-circuit
admin> set ip-options ip-routing-enabled = no
admin> set atm-options vpi = 8
admin> set atm-options vci = 35
admin> set atm-options nailed-group = 142
admin> set atm-connect-options vpi = 5
admin> set atm-connect-options vci = 33
admin> set atm-connect-options nailed-group = 851
admin write
CONNECTION/cpe-2 read
admin> new connection cpe-3
CONNECTION/cpe-3 read
admin> set active = yes
```

```
admin> set encapsulation-protocol = atm-circuit
admin> set ip-options ip-routing-enabled = no
admin> set atm-options vpi = 8
admin> set atm-options vci = 35
admin> set atm-options nailed-group = 155
admin> set atm-connect-options vpi = 5
admin> set atm-connect-options vci = 34
admin> set atm-connect-options nailed-group = 851
admin write
CONNECTION/cpe-3 read
```

Checking the status of ATM connections

You can check the status of a VCC by using the `atmvcc-stat` profile or the `atmvccstat` command. You can also use TAOS commands to display information about an ATM virtual channel link (VCL) or virtual path link (VPL), and about ATM cross-connects. For details, see the *Stinger Adminstration Guide*.

Terminating PVC Configuration

7

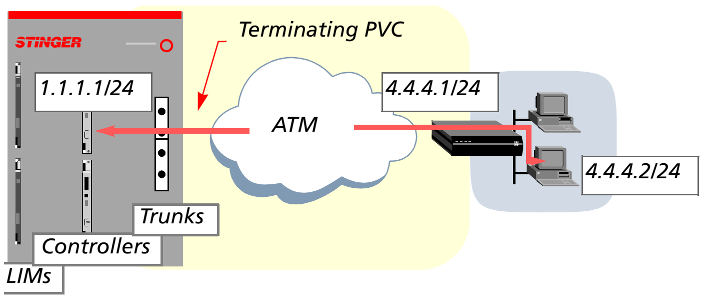
A terminating PVC is not switched through the system. It uses a single physical interface, such as the trunk interface shown in Figure 7-1, and carries IP packets, which are reassembled in the Stinger unit and then handled as regular IP traffic. The profile for a terminating PVC specifies both the IP routing and ATM characteristics of the connection.

For units with the standard controller, terminating PVCs are typically only used for logging in via `telnet` or SNMP to manage the system, and are also referred to as *management virtual circuits*.

For units with the IP2000 controller or a T1000 module, terminating PVCs can be any RFC 1483 IP-routed connection. For details about configuring RFC 1483 PVCs for subscribers, see the *Stinger IP2000 Configuration Guide* or the Stinger *T1000 Module Configuration Guide*.

Figure 7-1 shows an example of a management virtual circuit: an administrative `telnet` or SNMP login from a remote workstation (4.4.4.2/24) to the Stinger interface across an ATM trunk.

Figure 7-1. Terminating management virtual circuit on the trunk side



Overview of terminating `connection` settings

You configure a terminating PVC in a `connection` or RADIUS profile. The cells received on the connection are reassembled into IP packets. The connections are not password authenticated.

Following are the parameters (shown with default settings) for ATM terminating connections:

```
[in CONNECTION/""]
station* = ""
active = no
encapsulation-protocol = atm-circuit

[in CONNECTION/"":ip-options]
ip-routing-enabled = yes
remote-address = 0.0.0.0/0

[in CONNECTION/"":atm-options]
atm1483type = aal5-llc
vpi = 0
vci = 35
nailed-group = 1
vp-switching = no
```

Parameter	RADIUS attribute	Setting
`station`	`User-Name` (1)	Name of the far-end device.
`active`	N/A	Enable/disable the profile for active use.
`encapsulation-protocol`	`Framed-Protocol` (7)	Encapsulation protocol to use for the connection. Must be set to `atm` for terminating connections.
`ip-routing-enabled`	`Ascend-Route-IP` (228)	Enable/disable IP routing for the interface. IP routing must be enabled (as it is by default) for terminating connections.
`remote-address`	`Framed-IP-Address` (8) `Framed-IP-Netmask` (9)	IP address of the far-end device, which can include a subnet specification. If it does not include a subnet mask, the router software in the Stinger unit assumes a default subnet mask that is based on address class.
`atm1483type`	`Framed-Protocol` (7)	Method of multiplexing Layer-3 packets into ATM cells. Valid values are AAL5-LLC and AAL5-VC. (For details, see "AAL5 multiplexing for packet traffic (atm1483type)" on page 7-3.)
`vpi`	`Ascend-ATM-Vpi` (94)	VPI for the terminating PVC. For a discussion of valid values, see "Assigning valid VPI-VCI pairs" on page 6-5.
`vci`	`Ascend-ATM-Vci` (95)	VCI for the terminating PVC. For a discussion of valid values, see "Assigning valid VPI-VCI pairs" on page 6-5.
`nailed-group`	`Ascend-ATM-Group` (64)	Nailed-group number of the interface used by terminating PVC. For a command that displays a port's nailed-group number, see "Identifying a circuit's ports with the which command" on page 6-4.
`vp-switching`	N/A	*Not used for terminating connections. (*See "Typical VP switching configuration" on page 6-10.)

Information in the `ip-options` subprofile

When a Stinger unit starts up, it creates a routing interface for terminating connections specified in local `connection` profiles. For those defined in RADIUS profiles, a Stinger unit creates a routing interface when a session becomes active.

The IP address of the far-end device is the minimum IP information that must be supplied in the profile. The default settings for the `ip-options` subprofile enable IP routing. They also enable Van Jacobson header compression and turn off RIP, which is appropriate for many IP connections. You can change these defaults, or set a variety of routing and service parameters (which are described in the *Stinger Reference*).

If the far-end device specifies the Stinger unit's soft interface IP address as its destination, the connection will be robust even if the unit switches over to its redundant controller. For information about the unit's soft interface, see your unit's *Getting Started Guide*.

AAL5 multiplexing for packet traffic (`atm1483type`)

Stinger units support the two encapsulation methods for carrying routed PDUs in the payload field of ATM adaptation layer (AAL) type 5, which are defined in RFC 1483, *Multiprotocol Encapsulation over ATM Adaptation Layer 5.*

The AAL5-LLC encapsulation method multiplexes multiple protocols on a single ATM virtual circuit. Each protocol is identified in the 802.2 LLC header of the packet. This is the default method for Stinger connections and is recommended for the current software version, in which only PVCs are supported.

The AAL5-VC method carries each protocol on a separate ATM virtual circuit (in effect, it multiplexes the circuits rather than the individual protocols). This method is sometimes used in private networks, in which PVC creation is very economical.

Notice about loading a system configuration across a management PVC

When you are logged into a Stinger unit across an ATM PVC, a `connection` profile and associated `atm-qos` profile define the characteristics of the management channel. If you use the `load config` command to load a configuration file, you must be sure that the profiles in that file do not differ from ones currently in use for the connection.

If the configuration file contains profiles for the management PVC that differ from the profiles currently in use for the connection, the management channel might be dropped during the load process. To avoid dropping the channel, you must delete those profiles from the configuration profile first. You can then load the file as usual, and manually modify the `connection` and `atm-qos` profiles for the management channel if necessary.

Typical terminating PVC configuration

A Stinger unit establishes a PVC to a far-end unit on the basis of the VPI-VCI assignment and other ATM parameters. For an IP-routed connection, the unit then validates the far-end device's IP address. After the connection has been established, users can Telnet across the connection or access the Stinger from an SNMP management station.

In the example illustrated in Figure 7-2, a Stinger unit has a `connection` or RADIUS profile for the DSLTNT® unit, and vice versa. The ATM PVC between the two units allows an administrator at the DSLTNT® side to connect to the Stinger unit, where he or she can authenticate the appropriate `user` profile for an administrative session.

Figure 7-2. Management connection from remote network

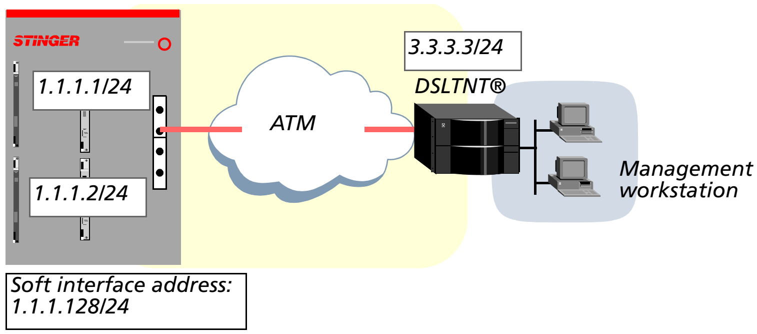


Figure 7-2 shows the IP addresses assigned to the Stinger unit's primary controller (1.1.1.1/24) and secondary controller (1.1.1.2/24), and a soft interface address of 1.1.1.128/24. Many sites use the soft interface as the Stinger unit's destination IP address because it enables the profile to reach the unit regardless of which controller is acting as the primary. For information about the soft interface, see your unit's *Getting Started Guide*.

Sample Stinger configuration

In Figure 7-2, the connection from the Stinger to the DSLTNT® unit uses an OC3-ATM interface. The following commands create a local `connection` profile and specify the IP address of the DSLTNT® unit:

```
admin> new connection dsltnt-1
CONNECTION/dsltnt-1 read

admin> set active = yes

admin> set encapsulation-protocol = atm

admin> set ip-options remote-address = 3.3.3.3/24
```

The following commands specify the AAL5 multiplexing method and assign VCI 101 to the link:

```
admin> set atm-options atm1483type = aal5-llc

admin> set atm-options vci = 101
```

The following commands display the nailed-group number of the OC3 trunk interface (trunk module 1, port 2) and assign it to the PVC:

```
admin> which -n {1 17 2}
Nailed group corresponding to port { shelf-1 trunk-module-1 1 } is 802

admin> set atm-options nailed-group = 802
```

The following commands assign an upstream and downstream QoS contract and write the profile:

```
admin> set atm-qos-options usr-up-stream-contract = cbr

admin> set atm-qos-options usr-dn-stream-contract = cbr
```

```
admin write
CONNECTION/dsltnt-1 read
```

Following is a comparable definition in a RADIUS profile:

```
permconn-ST-1 Password = "ascend"
    Service-Type = Outbound,
    Framed-Protocol = ATM-1483,
    User-Name = "dsltnt-1",
    Framed-IP-Address = 3.3.3.3,
    Framed-IP-Netmask = 255.255.255.0,
    Ascend-ATM-Group = 802,
    Ascend-Route-IP = Route-IP-Yes,
    Ascend-ATM-Vci = 101,
    Ascend-QOS-Upstream = "cbr",
    Ascend-QOS-Downstream = "cbr"
```

Sample far-end unit configuration

In this example, the DSLTNT® unit has a DS3 interface to the ATM network. The DSLTNT® unit is just used for the purposes of this example. The far-end unit could be any system that processes ATM across a DS3 interface. The following command displays the nailed-group value assigned to the DS3-ATM interface used for this connection:

```
admin> get atm-ds3 {1 7 1} line-config nailed-group
[in ATM-DS3/{ shelf-1 slot-7 1 }:line-config]
nailed-group = 70
```

The following commands on the DSLTNT® unit configure a `connection` profile for the Stinger connection using the Stinger unit's soft interface address and VCI 101:

```
admin> get connection stinger-1
CONNECTION/stinger-1 read

admin> set active = yes

admin> set encapsulation = atm

admin> set ip-options remote-address = 1.1.1.128/24

admin> set telco-options call-type = ft1

admin> set telco-options nailed-group = 70

admin> set atm-options vci = 101

admin> write
CONNECTION/stinger-1 written
```

Note The `connection` profile specifies the soft interface address as the remote address. For this reason, if the primary controllers fails, the terminating connection will be briefly dropped and then reestablished within a few seconds using the new primary controller.

For more details about creating `connection` profiles on DSLTNT® units, see the DSLTNT® documentation.

Multiple terminating PVCs on LIM ports

With previous software versions, the internal mechanism for allocating a VPI-VCI pair to a terminating PVC on a LIM port enforced a one-per-port limitation on terminating PVCs. With the current software version, that limitation has been removed. Now, the system supports a maximum of (`3 *` *`number-of-ports`*) terminating connections on a LIM. For example, a 48-port LIM can support a maximum of 144 user terminating connections. An individual port can support up to its maximum number of PVCs, but the entire module cannot exceed the LIM maximum.

Traffic shaping on management virtual circuits

Traffic shaping on management virtual circuits enables you to control burstiness of traffic transmitted from the Stinger controller, such as SNMP protocol data units (PDUs).

Overview of traffic shaper settings

You configure traffic shaping for transmissions generated by the Stinger unit in the `traffic-shaper` subprofiles of the `atm-config` profile. The subprofiles are numbered from 1 through 4. You apply a traffic shaper to a management virtual circuit by specifying the `traffic-shaper` subprofile number in the `session-options` subprofile of the virtual circuit's `connection` profile. Following are the relevant parameters, shown with default settings:

```
[in ATM-CONFIG:traffic-shapers[1]]
enabled = no
bit-rate = 1000
peak-rate = 1000
max-burst-size = 2
aggregate = no
priority-number = 1
```

```
[in CONNECTION/"":session-options]
traffic-shaper = 16
```

Parameter	Setting
`enabled`	Enable/disable the shaper for use. If a virtual circuit applies a traffic shaper that is disabled, the virtual circuit has a peak rate equal to the maximum line bandwidth.
`bit-rate`	Maximum sustainable effective bit rate in kilobits per second. The valid range is 1 through 135631. The default is 1000 (1Mbps). The Stinger unit verifies that the `bit-rate` value of a shaper does not exceed the effective line rate.
`peak-rate`	Maximum effective bit rate allowed, in kilobits per second. The valid range is 1 through 135631. The default is 1000 (1Mbps). The Stinger unit verifies that the `peak-rate` value of a shaper does not exceed the effective line rate.

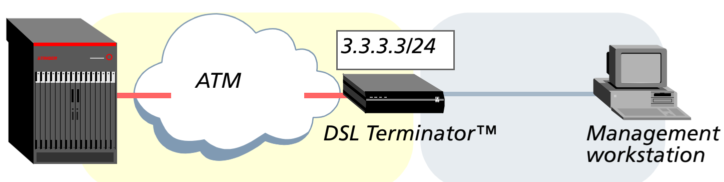
Parameter	Setting
`max-burst-size`	Maximum burst size (MBS) is the maximum number of cells that can be transmitted at the specified peak rate before the Stinger unit determines that the virtual circuit is exceeding the defined characteristics. The valid range is from 2 through 255. The default is 2.
`aggregate`	Enable/disable aggregation of virtual circuits using this traffic shaper. If the parameter set to `yes` and the traffic shaper is applied to more than one virtual circuit, the combined virtual circuits share the full bandwidth defined in the shaper.
`priority-number`	Read-only numeric value, set to the number of the traffic shaper.

`connection:`
`session-options:`
`traffic-shaper`
	Number of a defined traffic shaper (from 1 through 4) to apply to the virtual circuit. The default is shaper 16, which is an internal shaper that is not configurable and provides no bandwidth limitation. If the parameter specifies from 1 to 4, the specified traffic shaper in the `atm-config` profile is applied to the virtual circuit. If you specify a value higher than 4, the default settings (no bandwidth limitation) are applied.

Typical `atm-config` traffic shaper configuration

In the example shown in Figure 7-3, a management workstation on a remote IP network logs into the Stinger unit on a terminating (management) virtual circuit. The IP connection from the Stinger to the DSL Terminator™ unit uses an OC3-ATM interface.

Figure 7-3. Sample setup for traffic shaping on a management PVC



The following commands define a traffic shaper that limits the bit rate to less than 500Kbps:

```
admin> read atm-config
ATM-CONFIG read

admin> set traffic-shapers 1 enabled = yes

admin> set traffic-shapers 1 bit-rate = 500

admin> write -f
ATM-CONFIG written
```

Applying a traffic shaper in the `session-options` subprofile

The following command displays the nailed-group number of the OC3-ATM trunk interface (trunk module 1, port 2) to be used for the management virtual circuit:

```
admin> which -n { 1 17 2 }
Nailed group corresponding to port { shelf-1 trunk-module-1 2 } is 802
```

The following commands create a local `connection` profile to the remote DSL Terminator™ unit and apply the traffic shaper:

```
admin> new connection terminator-1
CONNECTION/terminator-1 read

admin> set active = yes

admin> set encapsulation-protocol = atm

admin> set ip-options remote-address = 3.3.3.3/24

admin> set atm-options atm1483type = aal5-llc

admin> set atm-options vci = 101

admin> set atm-options nailed-group = 802

admin> set session-options traffic-shaper = 1

admin write
CONNECTION/terminator-1 read
```

Following is a comparable definition in a RADIUS profile:

```
permconn-ST-1 Password = "ascend"
    Service-Type = Outbound,
    Framed-Protocol = ATM-1483,
    User-Name = "dsltnt-1",
    Framed-IP-Address = 3.3.3.3,
    Framed-IP-Netmask = 255.255.255.0,
    Ascend-ATM-Group = 802,
    Ascend-Route-IP = Route-IP-Yes,
    Ascend-ATM-Vci = 101,
    Ascend-Traffic-Shaper = 1
```

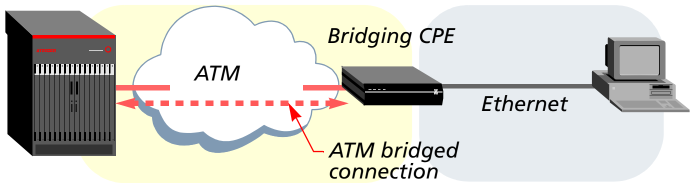
Because the traffic shaper in the `atm-config` profile in this example does not enable aggregation (the default setting), the actual transfer rate across the virtual circuit to the DSL Terminator™ is approximately 480Kbps, which is what the shaper permits.

If two management virtual circuits are configured on the same OC3-ATM interface, both using a traffic-shaper with `bit-rate` set to 500 and `aggregate` set to `yes`, each virtual circuit uses a transfer rate of about half the actual transfer rate, or 240Kbps.

Bridged IP routing terminating PVC

Bridged IP routing (BIR) enables the Stinger unit to process IP packets encapsulated in bridged frames, so a remote IP host can initiate an IP connection to the Stinger unit through CPE that supports bridging and ATM, but not IP routing. A sample setup is shown in Figure 7-4.

Figure 7-4. Access to the Stinger unit through a bridging CPE



The Stinger receives the bridged packets, decapsulates them, and passes them up the protocol stack to the IP router. To the remote host running `telnet` or SNMP, the session appears to be an ordinary IP connection.

Overview of `connection` BIR settings

BIR configurations require numbered interfaces, for which both the remote and local side of the connection is assigned a unique IP address. Typically, the local address for the Stinger unit is a unique address on the remote subnet.

A `connection` or RADIUS profile with BIR enabled uses all of the standard ATM and IP settings for a terminating PVC, as described in “Overview of terminating connection settings” on page 7-2. In addition, following are the parameters, shown with default values, that are specific to BIR interfaces:

```
[in CONNECTION/"":bir-options]
enable = no
proxy-arp = no
[in CONNECTION/"":ip-options]
ip-routing-enabled = yes
remote-address = 0.0.0.0/0
local-address = 0.0.0.0/0
```

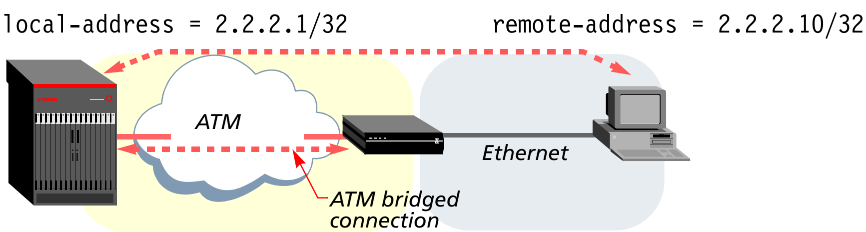
Parameter	RADIUS attribute	Setting
`enable`	`Ascend-BIR-Enable` (70)	Enable/disable BIR on this interface.
`proxy-arp`	`Ascend-BIR-Proxy` (71)	Enable/disable proxy ARP, which causes the controller to respond as proxy for ARP requests from local hosts for remote hosts on the far end of the link.
`ip-routing-enabled`	`Ascend-Route-IP` (228)	Enable/disable IP routing for the interface. IP routing must be enabled (as it is by default) for BIR connections.
`remote-address`	`Framed-IP-Address` (8) `Framed-IP-Netmask` (9)	IP address of the remote host or subnet. For a host route (an address with a 32-bit subnet mask), the system transmits bridged packets on this interface only when the full destination address in the packets matches this address. For a subnet route (an address with a subnet mask less than 32 bits), the system transmits bridged packets when the network bits of the destination address match the network bits of this address.

Parameter	RADIUS attribute	Setting
`local-address`	`Ascend-PPP-Address` (253) `Ascend-IF-Netmask` (153)	IP address assigned to the local side of a numbered-interface connection (a requirement for BIR interfaces). This is an address for the Stinger unit that has meaning only within the context of this connection. Typically, the local address for the Stinger unit is a unique address on the remote subnet.

Typical BIR configuration

In the sample setup shown in Figure 7-5, the host initiating a terminating PVC to the Stinger unit supports IP routing and an application such as `telnet` or an SNMP manager. The host connects to the Stinger unit through a DSL Terminator™ unit, which has a bridged connection to the Stinger unit on an OC3 trunk interface.

Figure 7-5. Sample BIR configuration for a bridging DSL Terminator™ unit



The following profiles are required:

- The Stinger unit requires a `connection` or RADIUS profile to the remote host, with BIR enabled.
- The DSL Terminator™ unit requires one `connection` or RADIUS profile to the Stinger unit, with bridging enabled.
- The PC must specify the proper host IP address and identify the Stinger unit's local address as the default gateway.

Stinger `connection` profile with BIR enabled

The following command displays the nailed group of an OC3 interface in the Stinger unit:

```
admin> which -n { 1 17 1 }
Nailed group corresponding to port { shelf-1 trunk-module-1 1 } is 801
```

The next commands configure an ATM PVC to the DSL Terminator™ across the OC3 interface, with BIR enabled:

```
admin> new connection stinger-bir
CONNECTION/stinger-bir read

admin> set active = yes

admin> set encapsulation-protocol = atm

admin> set ip-options remote-address = 2.2.2.10/32

admin> set ip-options local-address = 2.2.2.1/32

admin> set atm-options nailed-group = 801

admin> set bir-options enable = yes
```

```
admin> write
CONNECTION/stinger-bir written
```

When you write the profile, the connection comes up. For example:

```
LOG info, Shelf 1, Controller-1, Time: 20:16:58--
[1/17/1/1] LAN session up: <stinger-bir> [MBID 29] [stinger-bir]
```

Following is a comparable RADIUS profile:

```
permconn-ST-1 Password = "ascend"
    Service-Type = Outbound,
    Framed-Protocol = ATM-1483,
    User-Name = "stinger-bir",
    Ascend-Route-IP = Route-IP-Yes,
    Framed-IP-Address = 2.2.2.10,
    Framed-IP-Netmask = 255.255.255.255,
    Ascend-PPP-Addr = 2.2.2.1,
    Ascend-IF-Netmask = 255.255.255.255
    Ascend-ATM-Group = 801,
    Ascend-BIR-Enable = BIR-Enable-Yes
```

DSL Terminator™ configuration with bridging enabled

The following menu settings show a connection configured in the DSL Terminator™ unit to the Stinger unit, with bridging enabled:

```
Ethernet / Connections
    Station=bridge-to-stinger
    Active=Yes
    Route IP=No
    Bridge=Yes
    Bridge Options...
        Bridge Group=1
    Encaps options...
        vpi=0
        vci=35

Ethernet / Mod Config
    Ether2 Options..
        IP Adrs=0.0.0.0/0
        2nd Adrs=0.0.0.0/0
        Bridge Group = 1
```

IP configuration on initiating host

Following is a sample TCP/IP protocol configuration on the initiating PC:

```
IP address:            2.2.2.10
Subnet mask:           255.255.255.255
Default gateway:       2.2.2.1
```

SNMP MIB Support

8

Management information bases (MIBs) supported by the Stinger unit for ATM interface configuration and monitoring are closely related to TAOS command-line interface profiles and commands that have the same purpose. Changes made to a read-write MIB are reflected in the command-line interface, and vice versa.

For example, the `atm-qos` profile and the ATM-MIB traffic descriptor table are used to specify the quality of service (QoS) parameters of an ATM connection. From the command-line interface, you configure a service contract by creating a new `atm-qos` profile and setting parameters in the profile. The new profile becomes visible to SNMP utilities as an entry in the ATM-MIB traffic descriptor table. If you create a new entry in the traffic descriptor table by using an SNMP utility, the new entry becomes visible in the command-line interface as an `atm-qos` profile.

Note With the current software version, the `switch-config` profile configuration object, the `ASCEND-MIBSWITCHCONFIG-MIB`, which is indexed by name, is supported through the private `ASCEND-MIB`. The `controller-static-config` profile's MIB still shows as one of the configuration objects in `ASCEND-MIB` but with no associated instance.

Proprietary MIBs for Stinger trunk interfaces

Stinger units support the types of trunk modules shown in Table 8-1 for connecting to the ATM network. When the system initially starts up, it creates profiles for the physical interfaces it detects and configures them automatically to their default settings. Each physical interface has an associated ATM interface.

Table 8-1. Profiles and corresponding MIBs for physical trunk interfaces

Command-line interface profile	Proprietary MIB
ds1-atm	mibds1atmnet.mib
ds3-atm	mibds3atmnet.mib
e3-atm	mibe3atmnet.mib
oc3-atm	miboc3atmnet.mib

RFC 2515 ATM management objects (ATM MIB)

For ATM-specific interface configuration beyond what is supported in the `ifTable`, the Stinger unit supports the profiles and tables listed in Table 8-2 and defined in the ATM MIB (RFC 2515, *Definitions of Managed Objects for ATM Management*).

Table 8-2. Profiles and subprofiles and corresponding ATM MIB tables

Command-line interface profile	MIB table
`atm-if-config:base-config`	`atmInterfaceConfTable`
`atm-qos`	`atmTrafficDescrParamTable`
`atm-vcl-config`	`atmVclTable`
`atm-vpl-config`	`atmVplTable`
`connection:atm-options` `connection:atm-connect-options`	`atmVpCrossConnectTable` `atmVcCrossConnectTable`

The `atm-vcl-config` and `atm-vpl-config` profiles are created when an SNMP manager creates entries in the atmVclTable and atmVplTable. The profiles disappear when a `connection` profile using virtual links is created and reappear when the `connection` profile is deleted. For details about the contents of these profiles, see the `atmVclTable` and `atmVplTable` in RFC 2515.

Supplemental ATM management objects (AToM MIB)

For ATM interface configuration and monitoring information not defined in the atmInterfaceConfTable from the ATM MIB, the Stinger unit supports the profiles and tables listed in Table 8-3 and defined the AToM MIB in `draft-ietf-atommib-atm2-13.txt`.

Table 8-3. Profiles and subprofiles and corresponding AToM MIB tables

Command-line interface profile	MIB table
`atm-if-config:extension-config`	`atmInterfaceExtTable`

`connection:atm-options`
`connection:atm-connect-options`
`connection:cross-connect-index`
	`atmSvcVpCrossConnectTable`
	`atmSvcVcCrossConnectIndex`

CALEA Compliance

A

The Communications Assistance for Law Enforcement Act (CALEA) requires telecommunications carriers to support the types of electronic surveillance that law enforcement agencies are authorized to conduct. Specifically, section 103(a) of CALEA requires a carrier to ensure the following capabilities in its "equipment, facilities, or services that provide a customer or subscriber with the ability to originate, terminate, or direct communications":

- To isolate the content of targeted communications transmitted by the carrier within its service area
- To isolate information identifying the origin and destination of targeted communications
- To transmit intercepted communications and call identifying information to law enforcement agencies (LEAs) at locations away from the carrier's premises;
- To carry out intercepts unobtrusively, so that targets are not made aware of the interception, and in a manner that does not compromise the privacy and security of other communications.

These core functional requirements, referred to as the *assistance capability requirements* of CALEA, are supported in Stinger units with optional software.

Optional software license

For Stinger units, the CALEA optional software license enables a law enforcement agency (LEA) to nonintrusively intercept the traffic stream of specific targeted connections and transmit a copy of the data stream to a remote location, where it can be stored for analysis. The traffic stream of a targeted connection is not affected. This feature works only on ATM VCCs. It does not apply to VPCs.

When the CALEA license has been enabled in the system, the `base` profile shows the following setting:

```
[in BASE]
calea = yes
```

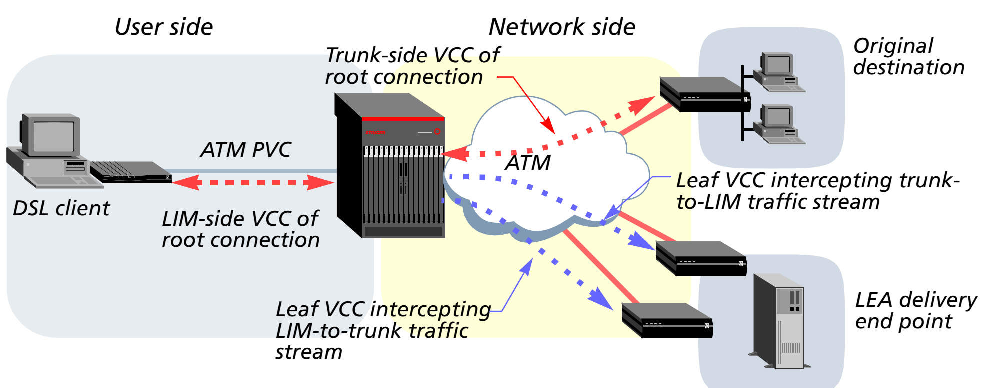
For information about obtaining and enabling Lucent Technologies software licenses, contact your Lucent sales representative.

How the CALEA software option works

Figure A-1 shows a sample CALEA setup in which an LEA is intercepting the bidirectional traffic of an ATM circuit connection. With this configuration, the LEA receives a copy of the data sent from the DSL client to the network, as well as the traffic sent back from the trunk-side connection to the DSL client.

The target connection (the one being intercepted) is referred to as the *root connection*. The connection to the LEA (the one on which the intercepted traffic is forwarded) is called the *CALEA leaf connection*.

Figure A-1. Sample CALEA interception of a switch-through connection

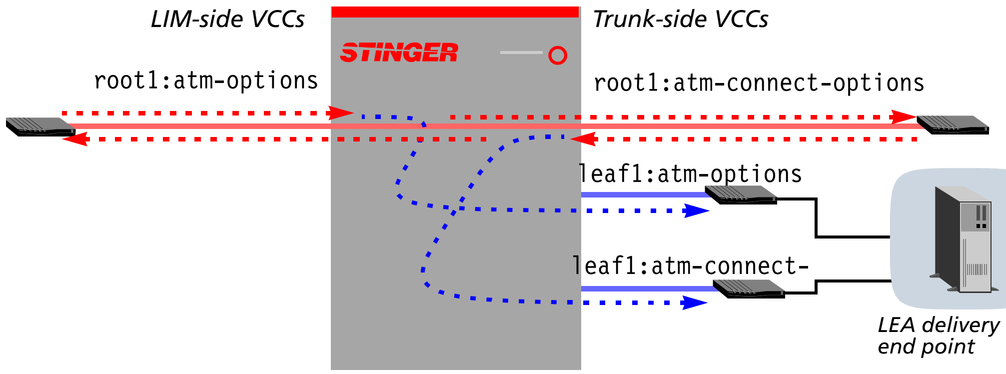


A root connection is a normal ATM connection, with bidirectional traffic between two end points. For an ATM circuit (switch-through) connection, the birdirectional traffic is switched between two VCCs on the ATM network. For a terminating connection, the bidirectional traffic is exchanged between a VCC on the ATM network and an internal VCC to the Stinger unit's controller.

The CALEA leaf connection is also a bidirectional ATM connection, but it has the additional capability of redirecting the traffic of an associated root connection to a LEA delivery end point. From the perspective of a root VCC, the redirected data transfer is unidirectional to the LEA delivery end point. No data is sent from a leaf VCC to the associated root VCC at any time.

Figure A-2 shows a root connection named `root1`, with the two sides of the connection specified in the `atm-options` and `atm-connect-options` subprofiles, as usual. The leaf connection, named `leaf1`, intercepts the traffic in one direction from each side of the root connection.

Figure A-2. Bidirectional traffic being intercepted on two leaf VCCs



Configuring root connections

The root connection of a CALEA interception can be an ATM circuit, a terminating PVC, or (in a PNNI-enabled unit) a soft PVC (SPVC) initiator. For details about how to configure these connection types, see the *Stinger ATM Configuration Guide* or (for PNNI-enabled systems) the *Stinger Private Network-to-Network Interface (PNNI) Supplement*.

CALEA interception works on the following types of root connections:

- ATM circuit between a LIM and legacy trunk interface
- ATM circuit between a LIM and TRAM interface
- Terminating PVC on a legacy trunk interface
- Terminating PVC on a TRAM interface

CALEA interception is not supported for root connections on the following types of interfaces:

- ATM circuit between two LIM interfaces
- Terminating PVC on a LIM interface
- ATM circuit between two trunk interfaces (legacy or TRAM, or both)

Configuring CALEA leaf connections

A CALEA leaf connection can be an ATM circuit, a terminating PVC, or (in a PNNI-enabled unit) an SPVC initiator connection. For details about how to configure these connection types, see the *Stinger ATM Configuration Guide* or (for PNNI-enabled systems) the *Stinger Private Network-to-Network Interface (PNNI) Supplement*.

Types of interfaces supported for leaf connections

CALEA leaf connections that receive intercepted traffic are supported on the following types of interfaces:

- ATM circuit between a LIM and legacy trunk interface
- ATM circuit between a LIM and TRAM interface
- ATM circuit between two legacy trunk interfaces
- ATM circuit between a legacy trunk interface and a TRAM interface

- ATM circuit between two TRAM interfaces (*interslot*)
- Terminating PVC on a legacy trunk interface (possible but not recommended)
- Terminating PVC on a TRAM interface (possible but not recommended)

Although you can configure a CALEA leaf connection as a terminating PVC, that configuration is typically not recommended. When a leaf connection terminates in the Stinger unit itself, the traffic from the `atm-connect-options` side of the root connection cannot be intercepted. Further, terminating PVCs are typically used for management connections, which should not be loaded with redirected data.

Types of interfaces *not* supported for leaf connections

The CALEA leaf connection cannot use the following types of interfaces:

- ATM circuit between two LIM interfaces
- Terminating PVC on a LIM interface
- ATM circuit between two TRAM interfaces (intraslot)
- Any ATM SPVC target circuit

CALEA leaf `connection` settings

A CALEA leaf connection is handled by the system in a unique way, unlike a normal ATM connection. The presence of a valid `connection` profile name in the `root` setting of the `atm-options` subprofile, `atm-connect-options` subprofile, or both, causes the system to recognize the current profile as a leaf connection.

Note Before you save the profile of the leaf connection with `active` set to `yes`, the root connection must already exist in the system. The leaf CALEA connection does not become operational until the root connection is operational.

Following are the parameters, shown with default values, for configuring a CALEA leaf connection:

```
[in CONNECTION/"":atm-options]
root = ""

[in CONNECTION/"":atm-connect-options]
root = ""
```

The `root` parameter can specify the name of a valid `connection` profile to be intercepted (the root profile). You can specify the root profile in the CALEA leaf profile's `atm-options` subprofile, `atm-connect-options` subprofile, or both.

When you write the CALEA leaf profile with a root profile name in the `atm-options` subprofile, the system creates a unidirectional connection from the VCC defined in the `atm-options` subprofile of the specified root profile to the VCC (the `nailed-group`, `vpi`, and `vci` values) defined in the `atm-options` subprofile of the leaf profile. The system then begins transmitting the intercepted traffic to the leaf end point.

Similarly, when you write the CALEA leaf profile with the name of a valid `connection` profile in the `atm-connect-options` subprofile, the system creates a unidirectional connection from the VCC defined in the `atm-connect-options` subprofile of the specified root profile to the VCC defined in the `atm-connect-options` subprofile of the leaf profile. The system then begins transmitting the intercepted traffic to the leaf end point.

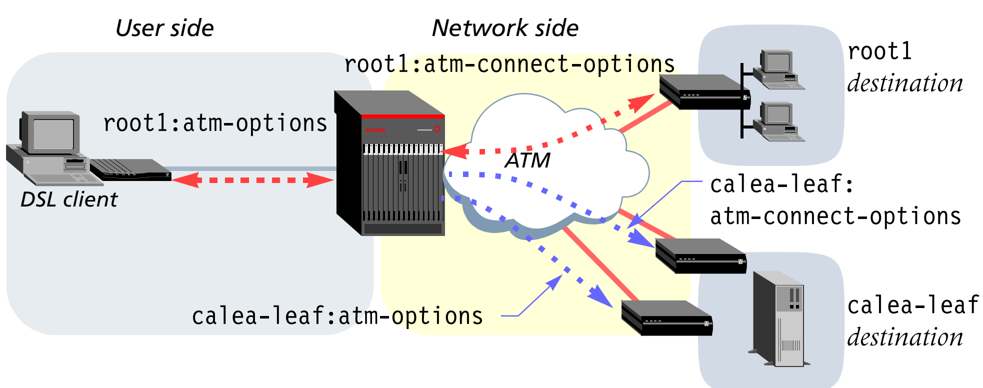
Note The system always uses the highest-priority queue for outbound intercepted traffic. In a leaf `connection` profile, the following settings are ignored:

```
[in CONNECTION/"":atm-qos-options]
usr-up-stream-contract = default
usr-dn-stream-contract = default
```

Sample CALEA interception of both sides of a LIM-to-trunk circuit

Figure A-3 shows a Stinger unit that receives ATM traffic from a DSL subscriber and switches it onto a high-speed ATM backbone. In this example, a CALEA leaf connection is configured to intercept the traffic in both directions and forward it to another site.

Figure A-3. Interception of both sides of a LIM-to-trunk circuit



The following commands configure the root connection:

```
admin> new connection root1
CONNECTION/root1 read
admin> set active = yes
admin> set encapsulation-protocol = atm-circuit
admin> set ip-options ip-routing-enabled = no
admin> set atm-options nailed-group = 155
admin> set atm-options vci = 32
admin> set atm-connect-options nailed-group = 802
admin> set atm-connect-options vci = 33
admin> write -f
CONNECTION/root1 written
```

The following commands configure the intercepting CALEA leaf connection:

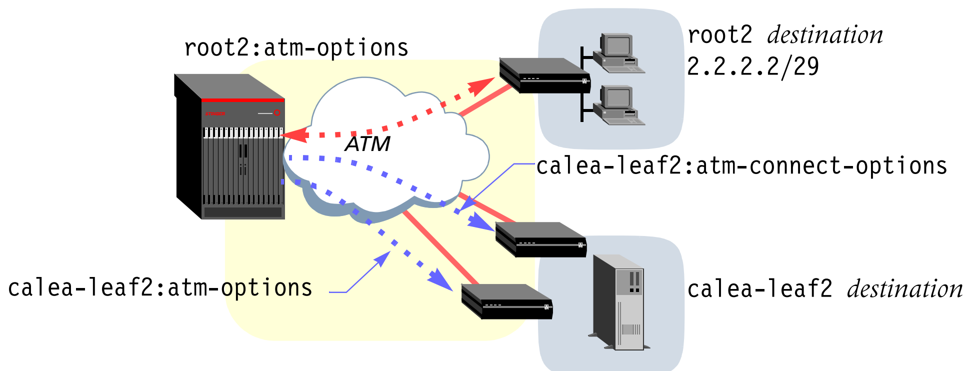
```
admin> new connection calea-leaf
CONNECTION/calea-leaf read
admin> set active = yes
admin> set encapsulation-protocol = atm-circuit
admin> set atm-options nailed-group = 801
```

```
admin> set atm-options vci = 101
admin> set atm-connect-options nailed-group = 801
admin> set atm-connect-options vci = 102
admin> set atm-options root = root1
admin> set atm-connect-options root = root1
admin> write -f
CONNECTION/calea-leaf written
```

Sample CALEA interception of terminating PVC

In the example shown in Figure A-4, the CALEA leaf connection is a trunk-to-trunk ATM circuit connection and the root connection is a terminating PVC. Terminating PVCs are typically used for a management connection on a Stinger trunk interface.

Figure A-4. Interception of a trunk-side terminating root connection



For any terminating connection, the `atm-connect-option` side of the `connection` profile represents an internal VCC to the system's controller. With the leaf configuration shown in Figure A-4, the VCC specified in the `atm-options` subprofile intercepts traffic sent from the ATM network to the Stinger unit on the trunk-side PVC. The VCC specified in the `atm-connect-options` subprofile intercepts traffic sent from the Stinger unit (the controller) back to the end point on the ATM network.

The following commands configure the terminating root connection:

```
admin> new connection root2
CONNECTION/root2 read
admin> set active = yes
admin> set encapsulation-protocol = atm
admin> set ip-options remote-address = 2.2.2.2/29
admin> set atm-options nailed-group = 801
admin> set atm-options vci = 32
admin> write -f
CONNECTION/root2 written
```

The following commands configure the CALEA leaf connection to intercept both directions of traffic on the terminating root PVC:

```
admin> new connection calea-leaf2
CONNECTION/calea-leaf2 read
```

```
admin> set active = yes
admin> set atm-options nailed-group = 151
admin> set atm-options vci = 100
admin> set atm-options root = root2
admin> set atm-connect-options nailed-group = 801
admin> set atm-connect-options vci = 100
admin> set atm-connect-options root = root2
admin> write -f
CONNECTION/calea-leaf2 written
```

SNMP objects for CALEA leaf connections

You can configure CALEA leaf connections in local `connection` profiles or via the `internetProfile` MIB. Following are the MIB objects for specifying CALEA leaf profiles:

```
internetProfile__atm_options__root OBJECT-TYPE
    SYNTAX DisplayString
    ACCESS read-write
    STATUS mandatory
    DESCRIPTION "The name of the root connection profile (must exist in the
    system while using it as root) from which the multicast will be
    originating towards this nailed-group/vpi/vci. If <NULL> is specified
    then this leg of the connection is not part of multicast. If both of the
    legs of the connection profile is specified as <NULL> then it is a
    normal PVC. The default value for this field is always <NULL>."
::= { mibinternetProfileEntry 486 }

internetProfile__atm_connect_options__root OBJECT-TYPE
    SYNTAX DisplayString
    ACCESS read-write
    STATUS mandatory
    DESCRIPTION "The name of the root connection profile (must exist in the
    system while using it as root) from which the multicast will be
    originating towards this nailed-group/vpi/vci. If <NULL> is specified
    then this leg of the connection is not part of multicast. If both of the
    legs of the connection profile is specified as <NULL> then it is a
    normal PVC. The default value for this field is always <NULL>."
::= { mibinternetProfileEntry 487 }
```

If the following SNMP objects are set in a leaf connection configured via SNMP, the values are ignored:

```
internetProfile__atm_qos_options__usr_up_stream_contract OBJECT-TYPE
    SYNTAX DisplayString
    ACCESS read-write
    STATUS mandatory
    DESCRIPTION "Quality of Service (QOS) contract for user up stream
    traffic"
::= { mibinternetProfileEntry 352 }

internetProfile__atm_qos_options__usr_dn_stream_contract OBJECT-TYPE
```

```
    SYNTAX DisplayString
    ACCESS read-write
    STATUS mandatory
    DESCRIPTION "Quality of Service (QOS) contract for user down stream
    traffic"
::= { mibinternetProfileEntry 353 }
```

Displaying information about CALEA connections

The `caleashow` command, which requires system-level permissions, displays information about all CALEA leaf connections and their associated root connections. The command uses the following syntax:

```
admin> caleashow
Calea Connection  Root Connection      This Side           Other Side
----------------  ---------------    -------------      -----------------
calea1            root1              {18/1 /0   /67   }    {18/1 /0   /68   }
calea2            root2                                   {18/1 /0   /67   }
```

Output field	Displays
`Calea Connection`	Name of the CALEA leaf `connection` profile.
`Root Connection`	Name of the root `connection` profile associated with the CALEA leaf connection.
`This Side`	Interface, VPI, and VCI specified in the `atm-options` subprofile of the root `connection` profile. If this field is empty, the VCC is not being intercepted by the CALEA connection.
`Other Side`	Interface, VPI, and VCI specified in the `atm-connect-options` subprofile of the root `connection` profile. If this field is empty, the VCC is not being intercepted by the CALEA connection.

CALEA log messages

The system displays the following log messages if a problem is detected in a CALEA configuration:

- `Warning: CALEA can not sniff atm-connect of root for terminating leaf connection.`

  This message is a warning that CALEA is operational only for the `atm-options` side. If the leaf is a terminating connection, only the `atm-options` side of the root connection can be intercepted. If the leaf connection specifies a `root` parameter setting in the `atm-connect-options` subprofile, it is ignored.

- `Warning: No internet profile found for root <root-profile-name>.`

  This message is generated if you attempt to write the CALEA leaf `connection` profile with a `root` setting that does not match an established connection. It is typically generated when the root connection is a target SPVC and it has not been created yet in the system, but the VPI-VCI pair for that SPVC is already known.

The CALEA leaf `connection` profile is saved but the connection does not become operational until the root target SPVC connection becomes operational.

- `Error: CALEA leaf <leaf-profile-name> not supported for trunk-to-trunk root <root-profile-name>.`

  A trunk-to-trunk root connection cannot be intercepted for CALEA. See "Configuring root connections" on page A-3 for details.

- `Error: CALEA is not supported for intra-TRAM leaf connection <leaf-profile-name>.`

  Configurations between two TRAM interfaces in the same TRAM slot are not supported for CALEA leaf connections. For details, see "Types of interfaces supported for leaf connections" on page A-3.

Index

C

D

E

H

I

J

L

M

N

O

P

Q

R

S

T

U

V

W