Asynchronous Transfer Mode (ATM) Module Installation and User Guide
©2001 Extreme Networks, Inc. All rights reserved. Extreme Networks and BlackDiamond are registered trademarks of Extreme Networks, Inc. in the United States and certain other jurisdictions. ExtremeWare, ExtremeWare Vista, ExtremeWorks, ExtremeAssist, ExtremeAssist1, ExtremeAssist2, PartnerAssist, Extreme Standby Router Protocol, ESRP, SmartTraps, Alpine, Summit, Summit1, Summit4, Summit4/FX, Summit7i, Summit24, Summit48, Summit Virtual Chassis, SummitLink, SummitGbX, SummitRPS, and the Extreme Networks logo are trademarks of Extreme Networks, Inc., which may be registered or pending registration in certain jurisdictions. The Extreme Turbodrive logo is a service mark of Extreme Networks, which may be registered or pending registration in certain jurisdictions. Specifications are subject to change without notice.

All other registered trademarks, trademarks, and service marks are property of their respective owners.
Asynchronous Transfer Mode (ATM) Module Installation and User Guide

Contents

Preface

Introduction xi
  Terminology xii
Conventions xii
Related Publications xiii

1 Overview

BlackDiamond 6800 Series Switch Overview 1-1
  BlackDiamond I/O Modules 1-2
About the ATM Module 1-3
  Physical Description 1-4
  Feature Summary 1-6
  Function Summary 1-7

2 Installing or Replacing an ATM Module

Preparing for Installation 2-1
  Software and Hardware Version Requirements 2-2
  Cables and Connectors 2-3
  Safety Information 2-3
  Tools 2-4
  I/O Module Slot Locations 2-4
Inserting and Securing a Module 2-7
Configuring the Section Trace Identifier 3-18
Configuring the Path Trace Identifier 3-18
Configuring the Signal Label 3-19
Resetting SONET Configuration Parameter Values 3-20
Displaying SONET Status Information on ATM ports 3-20
SONET Events on ATM Ports 3-21

Configuring VLAN-Related Attributes 3-24
  Summary of VLAN-Related Commands 3-24
  Configuring Tagged VLAN 802.1p and 802.1Q Functions 3-25
  Generic VLAN Registration Protocol Functions 3-28

Configuring Forwarding Database Attributes 3-28

Configuring Spanning Tree Attributes 3-28

Configuring QoS Functions 3-29
  Summary of QoS-Related Commands 3-29
  Configuring a QoS Profile 3-30
  Classification and Replacement Policies 3-31
  Configuring DiffServ 3-33
  Enhanced RED Support 3-36
  QoS Monitor 3-44
  Intra-Subnet QoS 3-44

Additional ATM Module Support Topics 3-45
  Configuring General Switch Attributes 3-45
  Configuring Port Attributes 3-46
  Configuring IGMP Attributes 3-48
  Configuring Layer 2 and 3 Switching Attributes 3-49
  Configuring Access List Attributes 3-49
  Changing Image and Configuration Attributes 3-49

A ExtremeWare Command Compatibility Information Related to the ATM Module

New Commands A-1
  New ExtremeWare Commands A-2

Changed Commands A-3

Commands and Functions Not Supported A-6
B  Supported MIBs and Standards

ATM Support
  MIBs Supported for ATM B-2

SONET/SDH Support
  Standards Supported for SONET/SDH B-2
  MIBs Supported for SONET/SDH B-2

QoS and DiffServ Support
  Standards Supported for DiffServ B-3

Index

Index of Commands
# Figures

<table>
<thead>
<tr>
<th>Figure</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1-1</td>
<td>ATM module</td>
<td>1-4</td>
</tr>
<tr>
<td>1-2</td>
<td>Front panel view of the ATM module</td>
<td>1-6</td>
</tr>
<tr>
<td>2-1</td>
<td>Slot locations in a BlackDiamond 6800 series chassis</td>
<td>2-6</td>
</tr>
<tr>
<td>2-2</td>
<td>Inserting and securing an ATM module</td>
<td>2-8</td>
</tr>
<tr>
<td>3-1</td>
<td>Bridging over ATM ports</td>
<td>3-6</td>
</tr>
<tr>
<td>3-2</td>
<td>Routing over ATM ports</td>
<td>3-7</td>
</tr>
<tr>
<td>3-3</td>
<td>Comparisons of RED and WRED operation</td>
<td>3-38</td>
</tr>
</tbody>
</table>
## Tables

<table>
<thead>
<tr>
<th>Table</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Notice Icons</td>
<td>xii</td>
</tr>
<tr>
<td>2</td>
<td>Text Conventions</td>
<td>xiii</td>
</tr>
<tr>
<td>2-1</td>
<td>ATM Module and Port LEDs</td>
<td>2-12</td>
</tr>
<tr>
<td>3-1</td>
<td>Summary of ATM Receive Statistics</td>
<td>3-11</td>
</tr>
<tr>
<td>3-2</td>
<td>Summary of ATM Transmit Statistics</td>
<td>3-11</td>
</tr>
<tr>
<td>3-3</td>
<td>SONET Parameters and Values</td>
<td>3-14</td>
</tr>
<tr>
<td>3-4</td>
<td>SONET Features on ATM Ports Commands</td>
<td>3-15</td>
</tr>
<tr>
<td>3-5</td>
<td>Summary of SONET Statistics</td>
<td>3-21</td>
</tr>
<tr>
<td>3-6</td>
<td>SONET Events</td>
<td>3-21</td>
</tr>
<tr>
<td>3-7</td>
<td>VLAN-related Commands</td>
<td>3-24</td>
</tr>
<tr>
<td>3-8</td>
<td>QoS-Related Commands</td>
<td>3-29</td>
</tr>
<tr>
<td>3-9</td>
<td>Default Code Point-to-QoS Profile Mapping</td>
<td>3-33</td>
</tr>
<tr>
<td>3-10</td>
<td>Assured Forwarding Classes and Three-Level Drop Precedence</td>
<td>3-41</td>
</tr>
<tr>
<td>3-11</td>
<td>Assured Forwarding Classes and Two-Level Drop Precedence</td>
<td>3-41</td>
</tr>
<tr>
<td>3-12</td>
<td>Mapping PHBs to QoS Profiles</td>
<td>3-41</td>
</tr>
<tr>
<td>3-13</td>
<td>Changes to General Switch Commands</td>
<td>3-45</td>
</tr>
<tr>
<td>3-14</td>
<td>Changes to Port Commands</td>
<td>3-47</td>
</tr>
<tr>
<td>3-15</td>
<td>Changes to Image Commands</td>
<td>3-49</td>
</tr>
<tr>
<td>A-1</td>
<td>New ExtremeWare Commands</td>
<td>A-2</td>
</tr>
<tr>
<td>A-2</td>
<td>Summary of Commands with Enhanced Syntax</td>
<td>A-4</td>
</tr>
<tr>
<td>A-3</td>
<td>Summary of Commands with Augmented Implementation</td>
<td>A-5</td>
</tr>
<tr>
<td>A-4</td>
<td>Summary of Commands Not Supported for ATM Ports</td>
<td>A-6</td>
</tr>
</tbody>
</table>
Preface

This preface provides an overview of this guide, describes guide conventions, and lists other publications that may be useful.

Introduction

This guide provides the required information to install the ATM module in a BlackDiamond® 6800 series switch from Extreme Networks and perform the initial module configuration tasks.

This guide is intended for use by network administrators who are responsible for installing and setting up network equipment. It assumes a basic working knowledge of:

- Local area networks (LANs)
- Ethernet concepts
- Asynchronous Transfer Mode (ATM)
- Ethernet switching and bridging concepts
- Routing concepts
- Internet Protocol (IP) concepts
- Routing Information Protocol (RIP) and Open Shortest Path First (OSPF)
- Simple Network Management Protocol (SNMP)
If the information in the release notes shipped with your module differs from the information in this guide, follow the release notes.

Terminology

When features, functionality, or operation is specific to the ATM module, the ATM module name is used.

Switches and switch modules that use naming conventions ending in “i” have additional capabilities that are documented throughout this user guide. For the most current list of products supporting the “i” chipset, consult your release notes.

Unless otherwise specified, a feature requiring the “i” chipset requires the use of both an “i” chipset-based management module, such as the MSM64i, and an “i” chipset-based I/O module, such as the G8Xi.

Conventions

Table 1 and Table 2 list conventions that are used throughout this guide.

**Table 1: Notice Icons**

<table>
<thead>
<tr>
<th>Icon</th>
<th>Notice Type</th>
<th>Alerts you to...</th>
</tr>
</thead>
<tbody>
<tr>
<td>![Note Icon]</td>
<td>Note</td>
<td>Important features or instructions.</td>
</tr>
<tr>
<td>![Caution Icon]</td>
<td>Caution</td>
<td>Risk of personal injury, system damage, or loss of data.</td>
</tr>
<tr>
<td>![Warning Icon]</td>
<td>Warning</td>
<td>Risk of severe personal injury.</td>
</tr>
</tbody>
</table>
Table 2: Text Conventions

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Screen displays</strong></td>
<td>This typeface indicates command syntax, or represents information as it appears on the screen.</td>
</tr>
<tr>
<td><strong>Screen displays bold</strong></td>
<td>This typeface indicates how you would type a particular command.</td>
</tr>
<tr>
<td>The words “enter” and “type”</td>
<td>When you see the word “enter” in this guide, you must type something, and then press the Return or Enter key. Do not press the Return or Enter key when an instruction simply says “type.”</td>
</tr>
<tr>
<td>[Key] names</td>
<td>Key names are written with brackets, such as [Return] or [Esc].</td>
</tr>
<tr>
<td></td>
<td>If you must press two or more keys simultaneously, the key names are linked with a plus sign (+). Example: Press [Ctrl]+[Alt]+[Del].</td>
</tr>
<tr>
<td>Words in <em>italicized</em> type</td>
<td>Italics emphasize a point or denote new terms at the place where they are defined in the text.</td>
</tr>
</tbody>
</table>

Related Publications

The publications related to this one are:

- ExtremeWare™ release notes
- ExtremeWare Software User Guide
- BlackDiamond 6800 Series Switch Hardware Installation Guide
- BlackDiamond Module Installation Note

Documentation for Extreme Networks products is available on the World Wide Web at the following location:

http://www.extremenetworks.com/
The Asynchronous Transfer Mode (ATM) module is an I/O module for the BlackDiamond 6800 series chassis-based system. The ATM module connects a BlackDiamond 6800 series switch to the ATM infrastructure used by service providers or enterprise customers.

This chapter includes information on the following topics:

- BlackDiamond 6800 Series Switch Overview on page 1-1
- About the ATM Module on page 1-3

**BlackDiamond 6800 Series Switch Overview**

The BlackDiamond 6800 series switch is a chassis-based switch designed to be placed in the core of your network. The BlackDiamond 6800 series switch is flexible and scalable, making it easy for you to meet the changing requirements of your network. The combination of BlackDiamond™, Alpine™, and Summit™ switches delivers a consistent end-to-end network solution that provides a nonblocking architecture, wire-speed switching, wire-speed IP routing, and policy-based Quality of Service (QoS).
Overview

BlackDiamond I/O Modules

In addition to the ATM module described in this guide, the BlackDiamond 6800 series switch supports a variety of I/O modules that offer a choice of port connections over different media types and distances. For more information, see the BlackDiamond 6800 Series Switch Hardware Installation Guide.

BlackDiamond 6800 series I/O modules can be inserted or removed at any time, without causing disruption of network services. No configuration information is stored on the I/O modules; all configuration information is stored on the MSM64i modules.

When the BlackDiamond 6800 series switch is powered on, the ExtremeWare software determines which slots are occupied by I/O modules, detects whether it has a configuration for each module, and generates a default configuration for each slot that is occupied by an I/O module that has not yet been configured. The default configuration is the minimal set of configuration parameter settings that will allow the I/O module and its ports to function. The default configuration for the I/O module is not preserved unless you explicitly save the information to nonvolatile RAM (NVRAM).

You can also use ExtremeWare commands to configure the I/O module after installing it in the BlackDiamond chassis, or you can preconfigure the parameters of a module that has not yet been inserted into the chassis.

If you preconfigure a slot for a particular module, the preconfigured information is used when the module is inserted. You must select a module type for the slot before you can preconfigure the parameters. If you have preconfigured a slot for a specific module type and then insert a different type of module, you must explicitly overwrite the existing configuration with a new configuration, or use the ExtremeWare unconfig slot <slot> command to clear the existing slot configuration. If you enter a new configuration for the new module, the module uses that configuration. If you clear the slot configuration, the new module type can use the default configuration ExtremeWare creates.

For information on configuring I/O modules, see the ExtremeWare Software User Guide.
About the ATM Module

Key applications for the ATM module are: interconnecting metropolitan area networks across an ATM network infrastructure, interconnecting server co-location network sites directly using ATM links, and providing connectivity between a legacy Enterprise ATM network and an Ethernet backbone.

In the first application, the metropolitan area network service provider can build service network sites in various cities, then use ATM modules in a BlackDiamond 6800 series switch to connect those cities to a carrier’s ATM infrastructure.

In the second application, operators of server co-location networks can use ATM modules in BlackDiamond 6800 series switches to create an ATM-based connection between server co-location sites. The result is that their network is simpler to manage, and problems can be isolated and resolved more expediently.

In the third application, a service provider can provide Ethernet-based services by using ATM modules in a BlackDiamond 6800 series switch to connect their Enterprise ATM network to an Ethernet backbone.

Extreme Networks offers the ATM module in the following configuration:

- A3cSi: four OC-3c/STM-1 single-mode, intermediate-reach optical interfaces

The A3cSi (single-mode version) operates in the 1310 nanometer (nm) wavelength window, but at a typical maximum cable distance of 15 km or 9.32 (mi). The ATM module uses industry-standard duplex SC optical fiber connectors.
Physical Description
The ATM module consists of a printed circuit board mounted on a metal carrier that acts as the insertion vehicle in a BlackDiamond 6800 series switch (see Figure 1-1). The module carrier also includes ejector/injector handles and captive retaining screws at each end of the module front panel. The module occupies one slot in a BlackDiamond 6800 series switch.

Figure 1-1: ATM module
The ATM module has the following key components:

- Two high-performance network processors
- A General Purpose Processor (GPP) subsystem

The network processors are programmable devices that participate with the Extreme “i” chipset to support expanded functionality, features, and flexibility.

The GPP subsystem handles system control and I/O module management functions. The GPP subsystem resides outside of the I/O module data path to optimize performance.

**ATM Module LED Indicators**

The ATM module is equipped with two module-level LED indicators (STATUS and DIAG) and one port-level LED indicator for each network interface port on the ATM module (see Figure 1-2).

The STATUS LED indicator is located near the top end of the ATM module front panel, near the ejector/injector handle. This LED indicator is a bi-color LED (displaying in either green or amber) that signals the operating status of the module as a whole.

The DIAG LED indicator is located beside the STATUS LED. This LED is a single-color LED (displaying in amber only) that flashes amber when diagnostics are running on the module, and is solid amber if the module fails the diagnostics.

The port-level LED is an LED next to the port number identifying each fiber optic network interface connector on the front panel of the module. The port LED is a bi-color LED (displaying in either green or amber) that signals the operating status of that network interface port.

For more information on ATM module LED states and their use in troubleshooting ATM module problems, see “Verifying the Module Installation” on page 2-10.

**Service Ports**

The ATM module is equipped with two front-panel service ports: one port is a DB-9 connector; the other is a micro HD-15 connector (see Figure 1-2). Both ports are reserved for use only by Extreme Networks technical support personnel for diagnostic purposes.
Overview

Feature Summary

The ATM module supports the following key networking functions:

- Synchronous Optical Network (SONET) and Synchronous Digital Hierarchy (SDH) modes of operation
- IP routing via the Logical Link Control (LLC) Encapsulation for Routed Protocols compatible with RFC 2684/RFC 1483
- Transparent LAN Services (TLS) over Asynchronous Transfer Mode (ATM) via the LLC Encapsulation Bridged Protocols compatible with RFC 2684/RFC 1483
- Permanent Virtual Circuits (PVCs) may be associated with one or more VLANs
- Routed and bridged encapsulations on the same PVC
- Jumbo frames
- Quality of Service (QoS) and Differentiated Services (DiffServ) features, including support for:
  - Eight ingress queues and eight egress queues per interface

Figure 1-2: Front panel view of the ATM module
About the ATM Module

— Ingress and egress rate shaping and limiting
— IEEE 802.1p VLAN priorities
— Weighted RED (WRED) congestion avoidance algorithm
— Assured Forwarding and Expedited Forwarding RFCs

• Service provider specific features, such as:
  — Flexible remapping of DiffServ codepoints
  — Flexible remapping of IEEE 802.1Q VLAN IDs
  — VLAN tunneling via nested 802.1Q tags

Function Summary
The following sections provide brief descriptions of the key functions provided by the ATM module. Each of these sections is expanded into greater detail in Chapter 3.

Asynchronous Transfer Mode (ATM)
ATM is a connection-oriented packet transmission technique that is widely used in existing telecommunications networks to transport voice, video, and data. ATM uses fixed size data packets called “cells” which are 53-bytes long and have a header that includes a connection identifier. The connection identifier makes it possible to support more than one point-to-point connection on a single physical ATM connection. The switches in an ATM network use the connection identifier in each cell to forward the cell to the next hop.

Synchronous Optical Network (SONET) and Synchronous Digital Hierarchy (SDH)
SONET and SDH are the two terms used to identify a time division multiplexing technology that is optimized for transporting voice traffic across a digital optical network, but that is also capable of providing high-speed capacity for transporting data.

The term SONET is used to identify the technology used within the North American digital network. Its standards are published by Bellcore and the American National Standards Institute (ANSI). The term SDH is used to identify the equivalent standard approved by the International Telecommunication Union (ITU) for use in Europe and elsewhere in the global digital network. Because SDH evolved out of SONET, the two standards are closely related and have been widely accepted as a dominant choice for implementations requiring high transport capacity and resistance to failure. The term
SONET is used throughout this guide. In instances where there are differences between SONET and SDH, the differences are explicitly called out.

**Jumbo Frames**

The ATM module ports provide jumbo frame support that is similar to that provided by Ethernet ports on a BlackDiamond 6800 series switch.

Jumbo frames are Ethernet frames that are larger than 1522 bytes, including four bytes used for the cyclic redundancy check (CRC). Extreme products that use the “i” chipset support switching and routing of jumbo frames at wire-speed on all ports.

Jumbo frames are used between endstations that support larger frame sizes for more efficient transfers of bulk data. Both endstations involved in the transfer must be capable of supporting jumbo frames.

**QoS and Differentiated Services**

The ATM module supports eight ingress queues and eight egress queues per port. The scheduling parameters for these queues (minimum bandwidth, maximum bandwidth, priority level, etc.) are controlled by QoS profiles that you can customize for individual ingress or egress queues on a specific ATM port.

You can assign frames to queues based on IEEE 802.1p priorities, Differentiated Services Code Points (DSCPs), or by configuring a QoS profile for the port or VLAN. You can tailor the DSCP-to-queue mapping on a per-port basis. Most of the existing ingress classification functions, along with the DiffServ replacement functions, are also supported for ATM ports.

The supported DiffServ functions maximize user flexibility while providing all of the features needed to support the standard per-hop behaviors (PHBs), including:

- Default
- Class Selector
- Assured Forwarding
- Expedited Forwarding

The ATM module also provides flexible support for the well-known Weighted RED (WRED) congestion avoidance algorithm.
Service Provider Features

The ATM module provides the following features for service provider environments:

- DSCP mapping
- VLAN ID (VID) tag mapping
- VLAN ID (VID) tag nesting
- VLAN to PVC mapping

**DSCP Mapping.** You can use the `diffserv dscp-mapping` command to configure a mapped relationship between an input DSCP and an associated output DSCP. Each ATM port supports three DSCP mapping tables: one of the tables is used in the ingress direction; two are used for egress flows (onto the ATM link). The two egress tables are for the congested and noncongested states, as determined by the RED algorithm. If RED is not enabled on the ATM port, the egress congested-state mapping table is not used.

In the ingress direction, the input DSCP of a packet received from the ATM link is replaced by an output DSCP before the packet is forwarded. In the egress direction, the operation is similar, except that the DSCP mapping occurs before the packet is transmitted onto the ATM link.

One potential use of the DSCP mapping capability is to reconcile varying DiffServ policies at the boundary between autonomous systems, such as at the boundary between two ISPs. The availability of different tables for the congested and noncongested states is useful in marking operations that increase the probability of packets being dropped during times of congestion, as discussed in the DiffServ Assured Forwarding RFC (RFC 2597).

**VLAN ID (VID) Tag Mapping.** An analogous feature has been added for the managing of 802.1Q tags. The `dot1q tagmapping` command provides support for VLAN ID (VID) mapping tables. Each ATM port supports two VID tables: one table is used in the ingress direction; the other is used in the egress direction. Each of the tables enables an input VID to be mapped to an output VID. This feature is useful in reconciling policy differences at the boundary between the customer and the service provider.

**VLAN ID (VID) Tag Nesting.** Another related enhancement provides support for nested 802.1Q tags by allowing a `tag push` or `tag pop` attribute to be associated with a VID. The `push` attribute indicates that a new tag is to be added to the frame, while the `pop` attribute indicates that the top-level tag is to be removed from the frame. This capability is augmented by an option that allows the 802.1p priority of the frame to be either preserved or set to a user-configurable value when a new tag is pushed. These
Overview

functions make it possible for service providers to tunnel customer-specific VLANs across a common ATM backbone in a very simple manner.

**VLAN to PVC Mapping.** VLAN to PVC mapping can be used by service providers to isolate and provision a customer’s traffic using different VLANs and PVCs for each customer. Thus, a service provider can securely transport a customer’s Ethernet traffic across an ATM backbone or vice-versa.
Installing or Replacing an ATM Module

This chapter includes information on the following topics:

- Preparing for Installation on page 2-1
- Inserting and Securing a Module on page 2-7
- Making Network Interface Cable Connections on page 2-9
- Verifying the Module Installation on page 2-10
- Troubleshooting on page 2-10
- Removing and Replacing an I/O Module on page 2-17

Preparing for Installation

This section describes the preparation steps that you must perform before inserting and securing an ATM module. This section includes information on the following topics:

- Software and Hardware Version Requirements on page 2-2
- Cables and Connectors on page 2-3
- Safety Information on page 2-3
- Tools on page 2-4
- I/O Module Slot Locations on page 2-4
Software and Hardware Version Requirements

The ATM module is compatible with “i”-series MSM modules and Summit and “i”-series I/O modules. For the most current list of I/O modules supported for use with the ATM module, consult your release notes.

Software support for the ATM module is provided in an ExtremeWare technology release, which is a software release providing specialized hardware support and/or additional functionality not found in the current mainstream ExtremeWare releases.

The ExtremeWare technology release that supports the ATM module includes multiple software packages. One software package runs on the MSM module, while another package runs on each ATM module. These software packages are downloaded independently using the ExtremeWare download image command. Each software package has an associated version number that you can display by using the show version command. As a recommendation (not a requirement), the MSM software package and the ATM module software package should be the same version. To ensure compatibility, the MSM performs an automatic compatibility check before an ATM module is activated. In case of incompatibility, the ATM ports on the module will not come up and the show slot command will indicate that the software on the ATM module is incompatible with the software on the MSM.

You can also verify compatibility by comparing the version of the MSM software package with the version of the ATM module software package. The format of the software version field of the ExtremeWare software version identifier has been extended to support technology releases. The following example of the ExtremeWare software version identifier illustrates the extended version format:

```
ExtremeWare V6.1.8 (Build 12) Project IP_SERV_TECH_REL V4.1.40
```

In this example, the technology release-specific version information Project IP_SERV_TECH_REL V4.1.40 is added to the base ExtremeWare version identifier ExtremeWare V6.1.8 (Build 12) to form the extended version identifier format. The first field of the version identifier, ExtremeWare V6.1.8 (Build 12), identifies the ExtremeWare software version on which this technology release is based. The second field in the extended version identifier, Project IP_SERV_TECH_REL, is the name of the technology release. The final field, V4.1.40 is a three-part number that identifies the version of the technology release. In the example, the first part of the number, 4, is the extended major version number; the second part of the number, 1, is the extended minor version number; the third part of the number, 40, is the extended build version number.
Preparing for Installation

The MSM software package is compatible with the ATM module software package when the following conditions are true:

- Base ExtremeWare version numbers match
- Technology release names match
- Extended major version numbers match
- Extended minor version number of the MSM software package is equal to or greater than the extended minor version of the ATM module software package

⚠️ The extended build number is ignored for compatibility comparisons.

For example, MSM software package ExtremeWare V6.1.8 (Build 12) Project IP_SERV_TECH_REL V4.2.60 is compatible with ATM module software package ExtremeWare V6.1.8 (Build 12) Project IP_SERV_TECH_REL V4.1.50, but is not compatible with ATM module software package ExtremeWare V6.1.8 (Build 12) Project IP_SERV_TECH_REL V4.3.60.

Cables and Connectors

Extreme Networks offers the ATM module in the following configuration:
- A3cSi: four OC-3c/STM-1 single-mode, intermediate-reach optical interfaces

The A3cSi (single-mode version) operates in the 1310 nanometer (nm) wavelength window, but at a typical maximum cable distance of 15 km or 9.32 (mi). The ATM module uses industry-standard duplex SC optical-fiber connectors.

Use the appropriate type of optical-fiber cable to connect the ATM ports of your BlackDiamond 6800 series switch to another switch or router.

Safety Information

Before you begin the process of installing or replacing an ATM module in a BlackDiamond 6800 series system, read the safety information in this section.

⚠️ Failure to observe the necessary safety guidelines can lead to personal injury or damage to the equipment.

In addition, observe the following safety guidelines:
Installing or Replacing an ATM Module

- All service to components of a BlackDiamond 6800 series switch, including I/O modules, should be performed by trained service personnel only. Service personnel are persons having appropriate technical training and experience necessary to be aware of the hazards to which they are exposed in performing a task and of measures to minimize the danger to themselves or other persons.

  The ATM module uses electronic components that are sensitive to static electricity. Electrostatic discharge (ESD) originating from you or from objects around you can damage these components. Exercise every possible precaution to prevent ESD when working around printed circuit assemblies.

  Keep all printed circuit assemblies in protective ESD-preventive sacks or place them on antistatic mats until you are ready to install them. Wear an ESD-preventive wrist strap and ensure that the leash is securely grounded before handling a bare printed circuit assembly.

- This device contains fiber optic ports. To protect your eyes, you should never look at the fiber optic ports while they are on, or look directly at the fiber cable ends when they are on.

- This module is a Class 1 laser device.

Tools

You need the following tools to install an Extreme Networks I/O module in a BlackDiamond 6800 series chassis.

- ESD-preventive wrist strap and grounding leash that is provided with the BlackDiamond 6800 series chassis.
- Number 1 Phillips-head screwdriver.
- Optical-fiber cable of the type appropriate to the I/O module version you plan to install (see “Cables and Connectors” on page 2-3 for more information about cable and connector requirements).

I/O Module Slot Locations

Figure 2-1 shows the I/O module slot locations in the BlackDiamond 6800 series chassis. You can install the ATM module in any of the numbered slots labeled 1 through 8. I/O modules do not fit in slots A or B. When you are installing a new ATM module, you must first remove the blank filler from the available slot.
Preparing for Installation

To ensure a sufficient flow of cooling air across the component side of the ATM module, install the ATM module in the BlackDiamond 6800 series chassis so that another module, a blank filler, or the far right chassis wall covers the component side of the module.
Installing or Replacing an ATM Module

Figure 2-1: Slot locations in a BlackDiamond 6800 series chassis
Inserting and Securing a Module

This section describes the procedures for inserting and securing an ATM module.

Caution: I/O modules must be installed in any of the numbered chassis slots labeled 1 through 8. I/O modules do not fit in slots A or B. Forceful insertion can damage the I/O module.

1 Before you install modular cards in the BlackDiamond 6800 series chassis, put on the ESD-preventive wrist strap that is provided with the chassis, and connect the metal end of the grounding leash to the ground receptacle located on the top-left corner of the BlackDiamond 6800 series switch front panel.

Leave the ESD-preventive wrist strap permanently connected to the BlackDiamond 6800 series chassis so that it is always available when you need to handle ESD-sensitive switch components.

2 Identify the chassis slot for the module. If necessary, remove the blank filler from the slot to make room for the ATM module.

Any unoccupied module slot in the chassis should have a blank filler installed for electromagnetic compatibility (EMC) and to ensure adequate airflow through the chassis.

3 To insert an ATM module, use Figure 2-2 as a reference and follow these steps:

To prevent ESD damage, handle the ATM module by the metal card carrier edges only. Never touch components on the printed circuit board or pins on any of the connectors. Never attempt to lift or hold the module by using the heat sinks on either of the network processors.

a Grasp the module by its front panel with one hand and place your other hand under the edge of the metal card carrier to support the weight of the module.

b Ensure that the module is right side up (printed circuit board, or PCB, facing to the right) and that the ejector/injector handles are fully extended.

c Carefully align the upper and lower edges of the metal card carrier in the chassis slot and slide the module slowly into the slot, taking particular care that the heat sinks on the two network processors are not obstructed in any way.

d Continue sliding the module into the chassis slot until the ejector/injector handles make contact with the front edges of the chassis slot, then stop.
Figure 2-2: Inserting and securing an ATM module

When the module is pushed into the chassis slot, the ejector/injector handles will begin pivoting to their closed position.

To seat the module in the backplane connectors, completely close the module ejector/injector handles by pushing them toward the center of the module front panel.
Use a #1 Phillips-head screwdriver to tighten the captive screw on each end of the module front panel to prevent the module from being dislodged from the backplane connectors and to ensure satisfactory protection from EMI.

Repeat this procedure for additional modules, if applicable.

Making Network Interface Cable Connections

Use the appropriate type of optical-fiber cable—single-mode—to connect the ATM ports of your BlackDiamond 6800 series switch to another switch or router.

Kinks and sharp bends can destroy or impair the cable’s ability to convey light pulses accurately from one end of the cable to the other. Use care in dressing the optical-fiber cables: provide satisfactory strain relief to support the cable and maintain an adequate bend radius at all cable turns, particularly where the cable connects to the I/O module.

Working carefully, one port at a time, follow these steps:

1. Verify that you have identified the correct optical-fiber cable for the ATM module port.
2. Use an alcohol wipe or other appropriate cleaning agent to clean the fiber element on the cable connectors to be sure they are free of dust, oil, and other contaminants.
3. Align the transmit (Tx) and receive (Rx) connectors on the optical-fiber cable with the correct corresponding connectors on the ATM module.
   On the ATM module, the transmit (Tx) connector on each port is the top connector.
4. Press the cable connectors into their mating connectors on the ATM module until the cable connector is firmly seated.
5. Repeat steps 1 through 4 for the remaining cables on this or other ATM modules.
6. Dress and secure the cable bundle to provide appropriate strain relief and protection against bends and kinks.
Verifying the Module Installation

After you have installed the ATM module and connected the fiber optic cables, verify that the I/O module is working correctly. Check the LEDs on the front panel of the I/O module and use the command-line interface (CLI) `show slot <slot>` command to display slot-specific information about the newly installed module.

LED Indicators

When the ATM module and its ports are configured and operating normally, the front-panel LED indicators should appear as follows:

- **STATUS LED indicator**: green blinking
- **DIAG LED indicator**: off
- **Port status LED indicators** (per port):
  - Green: The link is operational.
  - Green blinking: The link is disabled.
  - Amber blinking, returning to green: There is activity on the link.
  - Amber blinking: The link is down (SONET error).
  - Off: No signal was received.

Displayed Slot Status Information

Assuming that there are no other problems with the ATM module, the command `show slot n` (where *n* is the number of the slot where you installed the module) will show that ExtremeWare has detected the module and set it to the OPERATIONAL state.

As the module progresses through its initialization, the `show slot n` command will show the GPP subsystem change state to OPERATIONAL, and then each of the network processors will change state to OPERATIONAL.

Troubleshooting

This section describes how to isolate module-specific problems and determine when it is appropriate to remove and replace an ATM module. This section includes information on the following topics:
• Identifying Problem Categories on page 2-12
• Fixing Configuration Errors on page 2-13
• Upgrading the Switch Software Image on page 2-14
• Upgrading the ATM Module Software Image on page 2-14
• Upgrading the ATM Module BootROM on page 2-15
• Fixing Power-Related Problems on page 2-15
• Fixing Link Down Problems on page 2-16
• Identifying Conditions for Replacing an I/O Module on page 2-16

⚠️ The information in this section should be used in conjunction with the “Troubleshooting” appendix in the ExtremeWare Software User Guide and the release notes that accompanied your Extreme Networks product. If you encounter a problem that is not discussed in one of these resources, contact Extreme Networks technical support.
# Identifying Problem Categories

Table 2-1 lists the color states of ATM module and port LEDs and describes their associated meanings. The STATUS and DIAG LEDs apply to the module as a whole; the port status LED for each port provides status information about that port.

**Table 2-1: ATM Module and Port LEDs**

<table>
<thead>
<tr>
<th>LED</th>
<th>Color</th>
<th>Indicates</th>
<th>Corrective action</th>
</tr>
</thead>
<tbody>
<tr>
<td>STATUS</td>
<td>Green blinking</td>
<td>Normal operation</td>
<td>(No action required.)</td>
</tr>
<tr>
<td></td>
<td>Amber blinking</td>
<td>Configuration error (configured slot type is different than inserted module type)</td>
<td>See “Fixing Configuration Errors” on page 2-13.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Version error (ExtremeWare version does not recognize inserted module)</td>
<td>See “Upgrading the Switch Software Image” on page 2-14.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Version error (the ATM module image version is not compatible with the MSM image version)</td>
<td>See “Upgrading the ATM Module Software Image” on page 2-14.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Hardware error (module failed diagnostics)</td>
<td>See “Identifying Conditions for Replacing an I/O Module” on page 2-16.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Network processor or GPP down (as detected by network processor heartbeat protocol)</td>
<td>Reboot slot. If condition persists, run diagnostics.</td>
</tr>
<tr>
<td></td>
<td>Off</td>
<td>No power</td>
<td>See “Fixing Power-Related Problems” on page 2-15.</td>
</tr>
<tr>
<td>DIAG</td>
<td>Amber blinking</td>
<td>Diagnostics in progress</td>
<td>(No action required.) Use the <code>show diagnostics {&lt;slot&gt;}</code> command to see test status.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Diagnostics failed</td>
<td>See “Identifying Conditions for Replacing an I/O Module” on page 2-16.</td>
</tr>
<tr>
<td></td>
<td>Off</td>
<td>No diagnostics in progress</td>
<td>(No action required.)</td>
</tr>
</tbody>
</table>
Fixing Configuration Errors

If the STATUS LED on the ATM module turns amber and blinks, use the show slot command to display the configured slot type. The output from this command also displays information about the module state, including the CARD MISMATCH message. This message indicates that the slot was previously configured for a module type different than the one you just installed.

Use one of the following commands to reset the slot configuration:

- `clear slot <slot>`
- `unconfig slot <slot>`
- `config slot <slot> module [a3c | f32t | f32f | f48t | g4x | g6x | g8x | g12x | p3c | p12c | wdm]`

⚠️ The first two commands listed above clear the slot of a previously assigned module type. The third command replaces the existing module type configuration with a new module type configuration.
Upgrading the Switch Software Image

If the STATUS LED on the ATM module turns amber and blinks, use the `show slot` command to display the configured slot type. The output from this command also displays information about the module state, including the CARD UNKNOWN message. This message indicates that the installed ExtremeWare software image version does not recognize the module type.

To correct this problem, you will need to upgrade the ExtremeWare software image. To perform this task, see the “Software Upgrade and Boot Options” chapter in the ExtremeWare Software User Guide.

Upgrading the ATM Module Software Image

The ATM module software image file contains the executable code that runs on the ATM module. The image file is preinstalled on the ATM module at the factory. As new versions of the image are released, they can be downloaded to the ATM module.

⚠️ When you upgrade the ATM module software image, you might also be required to upgrade the image for associated MSM modules to maintain software compatibility.

To download an ATM software image, use the following command:

```
download image [<ipaddress> | <hostname>] <filename> {primary | secondary}
  slot <slot>
```

This command is the same command used to download ExtremeWare images to MSM modules, but you use the `slot <slot>` option to download the specified image file to the ATM module in the specified slot rather than to one of the switch’s image partitions.

Like the MSM module, the ATM module can store up to two images: a primary and a secondary image. When you download a new image, you can specify the image space—primary or secondary—where the new image is to be stored. If you do not specify the image space, the new image is downloaded to the image space that will be used as the load source on the next reboot.

To select which image—primary or secondary—the ATM module will load on the next reboot, use the following command:

```
use image [primary | secondary] slot <slot>
```
Upgrading the ATM Module BootROM

Like the MSM module, the ATM module has its own BootROM image.

To view the ATM module BootROM version, use the following command:

```
show slot {<slot>}
```

This command is the same command used to display slot information for other I/O and MSM modules, but the command is augmented to display data about the software images loaded on the ATM module.

To upgrade the ATM module BootROM image, use the following command:

```
download bootrom [<ipaddress> | <hostname>] <filename> {slot <slot>}
```

This command is the same command used to download BootROM images to MSM modules, but you use the `slot <slot>` option to download the specified image file to the ATM module in the specified slot rather than to one of the switch’s MSM modules.

⚠️ **Note:** Do not power off the switch while the BootROM is being upgraded. If the BootROM upgrade is interrupted, the module will be unable to boot up until the BootROM upgrade is completed. If you experience a problem with the BootROM upgrade, contact Extreme Networks Technical Support.

See Chapter 3 for more information about changing images and configuration attributes.

Fixing Power-Related Problems

If the LEDs on all other modules are off, verify that the BlackDiamond 6800 series switch is connected to an appropriate power source and is turned on.

If the LEDs on the new module are off, but the LEDs on other modules are on, try ejecting and reseating the unpowered module. If the module still does not power up, it is possible that the available system power is not sufficient to handle the power requirements of the added module. To test this condition, temporarily eject another I/O module to see whether that frees enough power to power up the new card. If it does, you may need to upgrade the power supply configuration in this BlackDiamond 6800 series switch. For more information on system power configuration, see the BlackDiamond 6800 Series Switch Hardware Installation Guide.
Fixing Link Down Problems

A flashing green port status LED can indicate the following conditions:

- Port is disabled.
- Port is not configured as a member of a VLAN.

To enable a port, use the following command:

`enable ports <portlist>`

To add a port to a VLAN, use the following command:

`config vlan <name> add port <portlist> {tagged | untagged} {nobroadcast}`

A flashing amber port status LED indicates that a signal has been detected, but that one or more SONET alarms exist. Use the `show sonet detail` command to display SONET status information.

If the port status LED is off, suspect a loss-of-signal condition caused by a optical-fiber cable or connector problem. Check for one or more of the following conditions:

- The transmit (Tx) and receive (Rx) cable connectors are reversed in the module port connector. Remove and reinsert the connectors in their correct positions.
- The optical-fiber cable is not terminated. Verify that the connectors on both ends of the cable are plugged in correctly and firmly seated.
- The optical-fiber cable is damaged. Replace the cable with a cable known to be good and try again.

Identifying Conditions for Replacing an I/O Module

If the STATUS LED on the ATM module turns amber and blinks, use the `show slot` command to display the slot status information. If the output of the command shows that the module state is not OPERATIONAL, use the following commands to run the diagnostics on the module and display the results:

`run diagnostics [normal | extended] slot <slot>`
`show diagnostics slot {<slot>}`

The displayed results list each test that was run, and indicate whether that test passed or failed. If the diagnostics fail, replace the ATM module with another module of the same type.
Removing and Replacing an I/O Module

I/O modules can be installed only in any of the BlackDiamond 6800 series chassis slots labeled 1 through 8. I/O modules do not fit in slots A or B. Forceful insertion can damage the I/O module.

I/O modules can be extracted from the BlackDiamond 6800 series chassis, or inserted into the chassis at any time, without disrupting network services.

Tools and Equipment

You will need the following items to remove and replace an I/O module:

- ESD-preventive wrist strap and leash
- Number 1 Phillips-head screwdriver
- Replacement I/O module

Removing an I/O Module

To remove an I/O module, follow these steps:

1. Put on the ESD-preventive wrist strap that is provided with the chassis, and verify that the metal end of the leash is connected to the ground receptacle located on the top-left corner of the BlackDiamond 6800 series switch front panel.

2. Identify the I/O module to be replaced and write down the following information for later use:
   - The chassis slot number and the type of I/O module. When you install the replacement I/O module, install it in the same chassis slot.
   - The optical-fiber cable connections to the I/O module connectors. You must reconnect the cables to the same connectors on the replacement I/O module.
Installing or Replacing an ATM Module

3 Disconnect all of the optical-fiber cables from the I/O module and set them carefully aside.

   Be very careful in handling optical-fiber cables: kinks and sharp bends can destroy or degrade the cable’s ability to convey light pulses accurately.

4 Use the #1 Phillips-head screwdriver to loosen the captive screw at each end of the I/O module front panel.

5 Grasp both ejector/injector handles and pivot them simultaneously away from each other to unseat the module from the chassis backplane.

6 Use the ejector/injector handles to pull the module part way out of the chassis slot. Do not touch the printed circuit board or any connector pins.

   There is an EMI-preventive gasket attached to one edge of the module front panel. To prevent diminished EMI protection, handle the module carefully and avoid damage to this gasket.

7 Grasp the module front panel with one hand and place your other hand under the metal card carrier to support the weight of the module. Slide the module completely out of the chassis slot. Place the module immediately into an antistatic sack to protect it from ESD damage and prevent dust from collecting on the module’s optical-fiber connectors.

8 Install and secure the replacement module as described in the “Inserting and Securing a Module” on page 2-7.

9 Check your notes on the slot assignment and cable connection information that you wrote down before removing the defective I/O module, then reconnect the network interface cables to their assigned ports on the I/O module.
3 Configuring the ATM Module

This chapter describes the ExtremeWare commands that support the ATM module. Other commands and background information used to configure I/O modules and switch behavior in a network are documented in the ExtremeWare Software User Guide. For hardware installation information on the BlackDiamond 6800 series switch, see the BlackDiamond Hardware Installation Guide.


This chapter includes information on the following topics:

- Basic ATM Module Configuration Information on page 3-2
- Configuring and Monitoring ATM Ports on page 3-9
- Configuring and Monitoring SONET on page 3-14
- Configuring VLAN-Related Attributes on page 3-24
- Configuring Forwarding Database Attributes on page 3-28
- Configuring Spanning Tree Attributes on page 3-28
- Configuring QoS Functions on page 3-29
- Additional ATM Module Support Topics on page 3-45
Basic ATM Module Configuration Information

This section uses several typical usage and configuration schemes to provide a brief overview of the ATM module configuration process as a general context for the detailed command description sections that follow.

ATM Module Characteristics

ATM is a packet transmission technique that uses fixed size data frames called “cells”. Each cell is 53-bytes long and includes a 5-byte ATM header and 48-byte payload. The ATM header includes a Virtual Path Identifier (VPI) and a Virtual Circuit Identifier (VCI). The VPI/VCI pair uniquely identifies a Virtual Circuit (VC) which is a logical connection configured on a physical ATM link. Each VC is a separate point-to-point connection and the ATM network uses the VPI/VCI in each ATM cell to determine how to forward the cell. Intermediate ATM switches in the network may change the VPI/VCI values for a VC so the same VC may be identified by a different VPI/VCI at the termination point. Multiple VCs can be configured on a single physical ATM link. The ATM module supports Permanent Virtual Circuits PVCs which are VCs that have been pre-provisioned by the ATM service provider. To connect to a service provider’s ATM network using a PVC, the VPI and VCI values must be obtained from the ATM service provider. The ATM module does not support Switched Virtual Connections (SVCs) which are VCs that are dynamically established using a signalling protocol.

The ATM module segments each outbound packet into ATM cells before transmitting and conversely re-assembles received cells into packets. Before segmenting a packet, the ATM module encapsulates the packet in an ATM Adaption Layer (AAL-5) format as defined in IETF RFC 2648/1483. The ATM module supports two types of encapsulations as defined in IETF RFC 2648/1483: LLC Encapsulation for Routed Protocols and LLC Encapsulation for Bridged Protocols. After the packets are segmented into ATM cells, the cells are transported inside a SONET payload.

The contents of ATM cells can be scrambled to randomize the pattern of 1s and 0s carried in the cells. Randomizing the bits can prevent long strings of all 1s and 0s. Transitions between 1s and 0s are used by the physical layer to maintain clocking and achieve signal synchronization which can improve the performance of delineating received ATM cells. The ATM module supports cell scrambling.

The ATM module responds to Operations, Administrations and Maintenance (OAM) F5 loopback cells but does not generate them. Loopback can be used to detect if the remote device is still active.
Default ATM Module Configurations

When the BlackDiamond 6800 series switch is powered on, the ExtremeWare software determines which slots are occupied by I/O modules, determines whether it has a configuration for each module, and generates a default configuration for each slot that is occupied by an I/O module that has not yet been configured. The default configuration is the minimal set of configuration parameter settings that will allow the I/O module and its ports to function.

By default, only ports 1 and 3 on the ATM module are assigned to the default VLAN, while ports 2 and 4 are not assigned to a VLAN. By default, ATM scrambling is enabled for all ATM ports. Before any data can be forwarded across an ATM port, PVCs must be configured on the port and mapped to a VLAN. Use the `config atm add pvc` command to configure PVCs on the port and map PVCs to a VLAN. See “Configuring PVCs” on page 3-9 for more details.

Bridging and Routing Over ATM Ports

The ATM module supports bridging and routing across ATM PVCs. Frames can be forwarded across ATM PVCs using either bridged or routed protocol encapsulations as defined in IETF RFC 2648/1483. When using the bridged protocol encapsulation, the ATM module forwards the entire Ethernet frame (except the Frame Check Sequence) across an ATM PVC. The ATM PVC looks like an Ethernet segment to the rest of the switch. The Ethernet frame can carry any protocol including IP, IPX, and MPLS, and it can also include 802.1Q and 802.1p tags. The ATM module can also use the routed protocol encapsulation for sending IP packets across an ATM PVC. When using the routed protocol encapsulation, the ATM module strips the Ethernet header and only forwards the IP datagram across the ATM PVC, resulting in improved throughput for IP packets.

Before packets can be forwarded over ATM ports, at least one PVC must be configured on the port and mapped to a VLAN using the `config atm add pvc` command. Each PVC must be mapped to one or more VLANs and each mapping must be designated to use the bridged protocol encapsulation (using the `encap l2` keywords in the `config atm add pvc` command) or the routed protocol encapsulation (using the `encap ip` keywords in the `config atm add pvc` command). Both encapsulations can be simultaneously used on a PVC as long as they are associated with different VLANs. ExtremeWare supports up to 500 routed VLANs and 3000 total VLANs in the

Note: The ATM module can support one PVC per port for each VLAN. The BlackDiamond 6800 series switch can support 3000 VLANs.
Configuring the ATM Module

BlackDiamond switch. When a routed VLAN is configured, the total number of VLANs supported in the BlackDiamond switch is 1500. If no routed VLANs are configured, and you want to support more than 1500 VLANs, you must set the CPU transmit priority to normal using the `config cpu-transmit-priority normal` command.

Each ATM port can support the previously described VLAN limits, and the following rules govern the association of PVCs with VLANs:

- Each PVC configured on a given ATM port must be associated with one or more VLANs.
- The same VLAN cannot be associated with multiple PVCs on the same ATM port.
- Ports 1 and 2 on the same ATM module may not be bridged together; similarly, ports 3 and 4 on the same ATM module may not be bridged together. Ports 1 and 2 or ports 3 and 4 may not be members of the same VLAN.
- Ports 1 and 2 on the same ATM module may not use the same VPI/VCI for a PVC; similarly, ports 3 and 4 on the same ATM module may not use the same VPI/VCI for a PVC.
- Both encapsulation types may be carried on the same PVC as long as they are associated with different VLANs.
- Multiple tagged VLANs may be configured to use the L2 encapsulation on the same PVC.
- Only one VLAN may be configured to use the IP encapsulation on a given PVC.
- Only one untagged VLAN may use the L2 encapsulation on a given PVC.
- When the IP encapsulation is configured, the ATM port must be the only member of the associated VLAN, and the IP address of the peer router must be configured using the `peer-ipaddress <ipaddress>` parameter in the `config atm add pvc` command.

Frames received on an ATM port for VLANs that the ATM port is not a member of are discarded. Additionally, frames received from a PVC that contain a VLAN ID which does not match the VLAN ID associated with any of the VLANs configured for that PVC are discarded. Similarly, a frame received from the switch backplane is only forwarded on a PVC when the VLAN ID in the frame matches the VLAN ID associated with one of the VLANs configured for that PVC.

The ATM module supports all of the Spanning Tree Protocol (STP) commands. STP Bridge Protocol Data Units (BPDUs) are sent on a PVC when an L2 encapsulated VLAN associated with the PVC has been added to an STP domain. STP BPDUs are always transmitted as untagged frames on ATM PVCs. The `enable ignore-stp vlan`
command can be used to indicate that the spanning tree forwarding state should be ignored for a particular VLAN.

**Bridging Over ATM ports**

Figure 3-1 displays multiple BlackDiamonds being used by an Ethernet Service Provider to provide point-to-point connectivity between their customer’s Ethernet networks using ATM PVCs. In this example, CustomerA has an Ethernet network in two different locations, one connected to BlackDiamond switch 1 via port 1:1 and the other connected to BlackDiamond switch 2 via port 8:1. Similarly, CustomerB is connected to BlackDiamond switch 1 via port 1:16 and BlackDiamond switch 3 via port 8:1. On BlackDiamond switch 1, the service provider has configured PVC 5/101 on ATM port 8:1 to connect to BlackDiamond switch 2 and PVC 5/102 on ATM port 8:1 to connect to BlackDiamond switch 3. The following configuration commands describe the basic steps necessary to configure the network displayed in Figure 3-1.
Figure 3-1: Bridging over ATM ports

Commands for configuring BlackDiamond switch 1:

create vlan customerA
config vlan customerA tag 101
config vlan customerA add ports 1:1, 8:1 tagged
config atm add pvc 5/101 encap 12 vlan customerA port 8:1

create vlan customerB
config vlan customerB tag 102
config vlan customerB add ports 1:16, 8:1 tagged
config atm add pvc 5/102 encap 12 vlan customerB port 8:1
Commands for configuring BlackDiamond switch 2:

```plaintext
create vlan customerA
config vlan customerA tag 101
config vlan customerA add ports 1:1, 8:1 tagged
config atm add pvc 5/101 encap l2 vlan customerA port 1:1
```

Commands for configuring BlackDiamond switch 3:

```plaintext
create vlan customerB
config vlan customerB tag 102
config vlan customerB add ports 1:1, 8:1 tagged
config atm add pvc 5/102 encap l2 vlan customerB port 1:1
```

**Routing Over ATM Ports**

Figure 3-2 displays multiple BlackDiamonds being used to inter-connect server co-location sites using an ATM PVC. In this example, the customer has leased an ATM PVC between the different server co-location sites. The following configuration commands describe the basic steps necessary to configure the network displayed in Figure 3-2.

**Figure 3-2:** Routing over ATM ports
Configuring the ATM Module

Commands for configuring BlackDiamond switch 1:

create vlan Serverfarma
config vlan Serverfarma add ports 1:1
config vlan Serverfarma ipaddress 192.168.9.1/24

create vlan wanLink
config vlan wanLink add ports 8:1
config vlan wanLink ipaddress 192.168.10.1/24
config atm add pvc 5/101 encap ip peer-ipaddress 192.168.10.2 vlan wanLink
    port 8:1
enable ipforwarding

Commands for configuring BlackDiamond switch 2:

create vlan Serverfarmb
config vlan Serverfarmb add ports 8:1
config vlan Serverfarmb ipaddress 192.168.11.1/24

create vlan wanLink
config vlan wanLink add ports 1:1
config vlan wanLink ipaddress 192.168.10.2/24
config atm add pvc 5/101 encap ip peer-ipaddress 192.168.10.1 vlan wanLink
    port 1:1
enable ipforwarding
Configuring and Monitoring ATM Ports

In addition to the ExtremeWare commands for configuring slot and port behavior that are described in the *ExtremeWare Software User Guide*, this section describes the commands used to configure ATM ports.

This section provides information on the following topics:

- Configuring PVCs on page 3-9
- Deleting PVCs on page 3-9
- Displaying ATM Port Status Information on page 3-10
- Displaying PVC Status Information on page 3-11
- Configuring ATM Scrambling on page 3-12

### Configuring PVCs

This section describes how to configure a PVC on an ATM port.

The following command is used to define a PVC on an ATM port:

```plaintext
config atm add pvc <vpi/vci> encap [l2 | ip peer-ipaddress <ipaddress>] vlan <name> ports <portlist>
```

Where the following is true:

- The PVC is identified by the specified vpi and vci parameters. The vpi parameter is an integer in the range of 0 through 15. The vci parameter is an integer in the range of 17 through 4095. Both parameters are defined in RFC 2648/1483.
- The encap parameter indicates the type of encapsulation that is to be used on the PVC for traffic from the associated VLAN. The l2 keyword is an abbreviation for Layer-2 and indicates the LLC Encapsulation for Bridged Protocols (defined in RFC 2684). The ip keyword indicates that the VLAN will carry only routed IP traffic and that the LLC Encapsulation for Routed Protocols (defined in RFC 2684) should be used.

### Deleting PVCs

The following command is used to delete a PVC configuration on an ATM port:
Configuring the ATM Module

```
config atm delete pvc [<vpi / vci> | all] {vlan <name>} ports <portlist>
```

This command deletes the specified PVC configuration on the specified ATM port(s). The optional `vlan` parameter may be used to limit the scope of the command to the specified VLAN. The PVC may still exist following command execution if multiple VLANs have been configured to use the PVC. If the `vlan` parameter is omitted, the PVC configuration is deleted for all VLANs on the specified ATM port(s).

The command can be used to delete configuration information for the PVC identified via the `vpi` and `vci` parameters for all PVCs defined for the specified VLAN(s) or port(s). The all keyword may also be used as the portlist parameter to indicate that the command should be applied to all ATM ports. A PVC is completely deleted when there are no longer any VLANs configured for the PVC on a given ATM port.

---

**All associated PVCs must be deleted before an ATM port can be removed from a VLAN.**

Displaying ATM Port Status Information

To display status information for the ATM ports, use the following command:

```
show atm {<portlist>}
```

You can use the optional `portlist` parameter to narrow the range of status information the command displays; otherwise, the command displays the status information for all ports.

By default, the command displays a summary of status information for the specified ports.

The summary of status information includes the following information for each port:

- Values of all port configuration parameters
- Port state
- ATM statistics

The detailed status information includes the summary information plus any ATM statistics. Table 3-1 describes the ATM receive statistics, and Table 3-2 describes the ATM transmit statistics.
Table 3-1: Summary of ATM Receive Statistics

<table>
<thead>
<tr>
<th>Receive Statistics</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cells Received</td>
<td>Number of cells received.</td>
</tr>
<tr>
<td>Cells OAM</td>
<td>Number of Operations, Administration, and Maintenance (OAM) cells received.</td>
</tr>
<tr>
<td>Cells Dropped (Congestion)</td>
<td>Number of cells dropped due to insufficient buffers.</td>
</tr>
<tr>
<td>Cells Dropped (Invalid VCC)</td>
<td>Number of cells dropped due to invalid VPI/VCI or AAL-5 header.</td>
</tr>
<tr>
<td>Cells Dropped (HEC)</td>
<td>Number of cells dropped with Header Error Control (HEC) errors. HEC is an 8 bit cyclic redundancy check (CRC) computed on all fields in an ATM header and capable of detecting bit errors. HEC is used for cell delineation.</td>
</tr>
<tr>
<td>PDUs Received</td>
<td>Number of PDUs received.</td>
</tr>
<tr>
<td>PDUs Dropped (CRC)</td>
<td>Number of PDUs discarded due to CRC-32 errors.</td>
</tr>
<tr>
<td>PDUs Dropped (Oversized)</td>
<td>Number of PDUs discarded because they were too large. See &quot;Jumbo Frame Support&quot; on page 3-47 for more details.</td>
</tr>
<tr>
<td>PDUs Dropped (Other)</td>
<td>PDUs dropped due to an invalid VLAN ID, Spanning Tree Protocol (STP) state, or invalid encapsulation.</td>
</tr>
</tbody>
</table>

Table 3-2 describes the ATM transmit statistics.

Table 3-2: Summary of ATM Transmit Statistics

<table>
<thead>
<tr>
<th>Receive Statistics</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cells Transmitted</td>
<td>Number of cells transmitted.</td>
</tr>
<tr>
<td>Cells Dropped (Congestion)</td>
<td>Number of cells dropped due to insufficient buffers.</td>
</tr>
<tr>
<td>PDUs Transmitted</td>
<td>Number of PDUs transmitted.</td>
</tr>
</tbody>
</table>

Displaying PVC Status Information

To display status information for a PVC, use the following command:

```
show atm pvc [<vpi / vci | all] {vlan <name>} {<portlist>}
```

You can specify a particular PVC to display information for, or you can specify that information for all PVCs be displayed.
Configuring the ATM Module

You can use the optional `vlan` parameter to narrow the range of status information the command displays; otherwise, the command displays status information for all VLANs.

You can use the optional `portlist` parameter to narrow the range of status information the command displays; otherwise, the command displays the status information for all PVCs associated with all ATM ports.

By default, the command displays a summary of status information for the specified PVC.

The summary of status information includes the following information for each PVC:

- Port number
- VPI/VCI
- VLAN IDs on this PVC
- Type of PVC (L2 or IP)
- Peer IP address (for IP PVCs)
- Received octets
- Received packets
- Transmitted octets
- Transmitted packets

The following command example displays all of the PVC status information for a PVC configured on an ATM port in a BlackDiamond switch:

```
show atm pvc 5/101 port 1:1
```

**Configuring ATM Scrambling**

To enable or disable payload data scrambling on the specified port, use the following command:

```
config atm scrambling [on | off] ports <portlist>
```

Choose either `on` or `off`. Scrambling is enabled by default.

Scrambling is used to improve signal synchronization and the performance of the ATM cell delineation process.
The following command example turns off the scrambling function for port 1 of the ATM module installed in slot 8 of the BlackDiamond switch.

```
config atm scrambling off ports 8:1
```
Configuring and Monitoring SONET

In addition to the ExtremeWare commands for configuring slot and port behavior that are described in the ExtremeWare Software User Guide, this section describes the commands used to configure and monitor SONET specific attributes on ATM ports.

This section provides information on the following topics:

- SONET Parameters and Values on page 3-14
- Commands for Configuring and Monitoring SONET Features on ATM Ports on page 3-15
- Configuring SONET Framing on page 3-16
- Configuring SONET Clocking on page 3-16
- Configuring the Signal Fail Threshold on page 3-17
- Configuring the Signal Degrade Threshold on page 3-17
- Configuring the Section Trace Identifier on page 3-18
- Configuring the Path Trace Identifier on page 3-18
- Configuring the Signal Label on page 3-19
- Resetting SONET Configuration Parameter Values on page 3-20
- Displaying SONET Status Information on ATM ports on page 3-20
- SONET Events on ATM Ports on page 3-21

SONET Parameters and Values

This section describes the configurable SONET parameters and values. Table 3-3 describes the SONET parameters and values.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Possible Values</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Framing</td>
<td>SONET or SDH</td>
<td>SONET</td>
</tr>
<tr>
<td>Clock source</td>
<td>internal or line</td>
<td>internal</td>
</tr>
<tr>
<td>Signal Failure threshold</td>
<td>$10^{-3}$ through $10^{-5}$</td>
<td>$10^{-5}$</td>
</tr>
<tr>
<td>Signal Degrade threshold</td>
<td>$10^{-5}$ through $10^{-9}$</td>
<td>$10^{-6}$</td>
</tr>
<tr>
<td>J0 Section Trace byte</td>
<td>0 through 255</td>
<td>1</td>
</tr>
</tbody>
</table>
Table 3-3: SONET Parameters and Values (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Possible Values</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>J0 Section Trace string(^a)</td>
<td>Maximum of 15 characters</td>
<td>15 NULL characters</td>
</tr>
<tr>
<td>J1 Path Trace identifier string(^b)</td>
<td>Maximum of 62 characters</td>
<td>NULL characters</td>
</tr>
<tr>
<td>C2 Signal Label(^c)</td>
<td>0 through xFF</td>
<td>auto</td>
</tr>
</tbody>
</table>

1. B2 bit error rate (BER) threshold; a Signal Failure (SF) event is generated if the BER exceeds the specified threshold.
2. B2 bit error rate (BER) threshold; a Signal Degrade (SD) event is generated if the BER exceeds the specified threshold.
3. The default value of 1 is per ANSI T1.105-1995. This parameter applies only when SONET framing is configured on the port.
4. This parameter applies only when SDH framing is configured on the port.
5. When SDH framing is configured on the port, only the first 15 characters of the string are applied.
6. Set automatically based on synchronous payload envelope (SPE) payload type.

Commands for Configuring and Monitoring SONET Features on ATM Ports

Table 3-4 describes the ExtremeWare commands for configuring and monitoring SONET related attributes on ATM ports. Each command is described in detail in the sections that follow.

Table 3-4: SONET Features on ATM Ports Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>config sonet clocking [line</td>
<td>internal] ports &lt;portlist&gt;</td>
</tr>
<tr>
<td>config sonet framing [sonet</td>
<td>sdh] ports &lt;portlist&gt;</td>
</tr>
<tr>
<td>config sonet signal label [auto</td>
<td>&lt;hex_octet&gt;] ports &lt;portlist&gt;</td>
</tr>
<tr>
<td>config sonet threshold signal degrade &lt;error_rate&gt; ports &lt;portlist&gt;</td>
<td>Configures the Signal Degrade threshold for the specified ATM ports.</td>
</tr>
<tr>
<td>config sonet threshold signal fail &lt;error_rate&gt; ports &lt;portlist&gt;</td>
<td>Configures the Signal Failure threshold for the specified ATM ports.</td>
</tr>
<tr>
<td>config sonet trace path &lt;id_string&gt; ports &lt;portlist&gt;</td>
<td>Configures the Path Trace Identifier string for the specified ATM ports.</td>
</tr>
<tr>
<td>config sonet trace section [&lt;id_byte&gt;</td>
<td>string &lt;id_string&gt;] ports &lt;portlist&gt;</td>
</tr>
</tbody>
</table>
Configuring the ATM Module

Configuring SONET Framing

You can configure each port for framing that complies with either the SONET standard or the SDH standard. SONET is primarily an American standard; SDH is the international version. The default is SONET.

To configure the framing for the specified SONET feature on an ATM port, use the following command:

```
config sonet framing [sonet | sdh] ports <portlist>
```

The following command example selects SDH framing for port 1 of the ATM module installed in slot 8 of the BlackDiamond switch.

```
config sonet framing sdh ports 8:1
```

Configuring SONET Clocking

You can configure each port on the ATM module to use either line clocking, where the clock source is recovered from the received bit stream, or internal clocking, where the clock source is based on an internal clock. The default is internal.

To configure the clocking source for the specified ATM port, use the following command:

```
config sonet clocking [line | internal] ports <portlist>
```

The following command example selects line clocking for port 1 of the ATM module installed in slot 8 of the BlackDiamond switch.

```
config sonet clocking line ports 8:1
```
Configuring the Signal Fail Threshold

A Signal Failure (SF) event is generated if the bit error rate (BER) for the SONET line exceeds the configured threshold. An SF event brings the port down.

To configure the Signal Fail threshold for the specified ATM port, use the following command:

```
config sonet threshold signal fail <error_rate> ports <portlist>
```

The `error_rate` parameter is an integer in the range from 3 to 5, where the SF BER is $10^{-error_rate}$. The default value of the `error_rate` parameter is 5, which equates to an SF bit error rate of $10^{-5}$, or 1 per hundred thousand.

The following command example sets the Signal Fail threshold value to 3 for port 1 of the ATM module installed in slot 8 of the BlackDiamond switch.

```
config sonet threshold signal fail 3 ports 8:1
```

You might set the signal fail threshold to a value different than the default value of 5 if your particular application has a very low tolerance for errors. In general, you should not change the default setting unless you are an expert and have a specific reason for the change.

Configuring the Signal Degrade Threshold

A Signal Degrade (SD) event is generated if the BER for the SONET line exceeds the configured Signal Degrade threshold.

To configure the Signal Degrade threshold for the specified ATM port, use the following command:

```
config sonet threshold signal degrade <error_rate> ports <portlist>
```

The `error_rate` parameter is an integer in the range from 5 to 9, where the SD bit error rate is $10^{-error_rate}$. The default value of the `error_rate` parameter is 6, which equates to an SD bit error rate of $10^{-6}$, or 1 per million.

The following command example sets the Signal Degrade threshold value to 8 for port 1 of the ATM module installed in slot 8 of the BlackDiamond switch.

```
config sonet threshold signal degrade 8 ports 8:1
```
Configuring the ATM Module

You might set the signal degrade threshold to a different value than the default value of 6 depending on your particular application’s tolerance for errors. In general, you should not change the default setting unless you are an expert and have a specific reason for the change.

Configuring the Section Trace Identifier

Section trace is a maintenance feature of SONET. One byte of the Section Overhead associated with each SONET frame is used to carry information identifying the transmitting equipment.

To configure the Section Trace identifier for the specified ATM port, use the following command:

```
config sonet trace section [id_byte | string id_string] ports <portlist>
```

In this command, the Section Trace identifier can take one of two forms: an ID byte (id_byte) or an ID string (id_string).

The id_byte parameter is an integer in the range from 1 to 255, with a default value of 1. This parameter applies only when SONET framing is configured, in which case, the configured id_byte value is transmitted in each SONET frame.

The id_string parameter is a string of up to 15 characters. By default, the <id_string> parameter contains 15 NULL characters. This parameter applies only when SDH framing is configured, in which case the SDH framing cycles repetitively through a 15-character string, sending one character per frame. If the configured string contains fewer than 15 characters, it is padded to full length by NULL characters.

The following command example sets the Section Trace identifier to the string “1800wombat” for port 1 of the ATM module installed in slot 8 of the BlackDiamond switch.

```
config sonet trace section string 1800wombat ports 8:1
```

Configuring the Path Trace Identifier

Path trace is a maintenance feature of SONET. One byte of the Path Overhead associated with each SONET frame is used to carry information identifying the originating Path Terminating Equipment (PTE).
To configure the Path Trace identifier for the specified ATM port, use the following command:

```
config sonet trace path <id_string> ports <portlist>
```

The `id_string` parameter defaults to a string of 62 NULL characters.

When SONET framing is configured, a 62-character string is transmitted repetitively, one character per frame. If the configured string consists of fewer than 62 characters, it is padded to its full length with NULL characters.

When SDH framing is configured, the maximum length of the `id_string` parameter is 15 characters. If the configured string consists of more than 15 characters, it is truncated to 15 characters.

The following command example sets the Path Trace identifier to the string “parador” for port 1 of the ATM module installed in slot 8 of the BlackDiamond switch.

```
config sonet trace path parador ports 8:1
```

### Configuring the Signal Label

The Signal Label field occupies one byte (C2) of the Path Overhead associated with each SONET frame. It is used to indicate the type of contents carried in the Synchronous Payload Envelope (SPE). For example, 0x13 indicates that the SONET SPE contains ATM cells.

To configure the C2 Signal Label value for the specified ATM port, use the following command:

```
config sonet signal label [auto | <hex_octet>] ports <portlist>
```

The `hex_octet` parameter is specified as a hexadecimal integer in the range from 00 to FF. It may be necessary to specify a particular Signal Label value in order to interoperate with implementations that do not follow the standard conventions for the Signal Label field.

To determine whether you need to specify a particular Signal Label value, perform the following tasks:

1. Use the `show sonet` command to display SONET status information on ATM ports.
2. Look for a Path Payload Label Mismatch (PLM-P) event indicating that the received payload type does not match the expected payload.
Configuring the ATM Module

3 Compare the contents of the received C2 field (Signal Label value) with the contents of the transmitted C2 field.

If no Signal Label value is specified, the command defaults to auto, which causes the value of the Signal Label field to be set automatically based on standard conventions for the given payload type.

The following command example sets the Signal Label to the hexadecimal value CF for port 1 of the ATM module installed in slot 8 of the BlackDiamond switch.

`config sonet signal label CF ports 8:1`

**Resetting SONET Configuration Parameter Values**

To reset the SONET configuration parameters for the specified ATM ports to their default values, use the following command:

`unconfig sonet ports <portlist>`

**Displaying SONET Status Information on ATM ports**

To display SONET status information for the ATM ports, use the following command:

`show sonet {<portlist>} {detail}`

You can use the optional `portlist` parameter to narrow the range of status information the command displays; otherwise, the command displays the status information for all ports.

By default, the command displays a summary of status information for the specified ports. You can use the optional `detail` keyword to display detailed status information for the specified ports.

The summary of status information includes the following information for each port:

- Values of all port configuration parameters
- Port state
- Any active events

The detailed status information includes the summary information plus any SONET statistics (listed and described in Table 3-5).
Configuring and Monitoring SONET

SONET Events on ATM Ports

The ATM module can detect and report a variety of error and alarm conditions, some of which also trigger actions on the SONET link. Table 3-6 describes these events and their associated actions. Syslog messages are output for these events. For more information about Syslog, see the ExtremeWare Software User Guide.

**Table 3-6: SONET Events**

<table>
<thead>
<tr>
<th>Event</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Loss of Signal (LOS)</td>
<td>Loss of Signal is detected by the Section Terminating Equipment (STE) when an all-zeros pattern on the incoming SONET signal lasts 100 microseconds or longer. This condition can be caused by loss of light on the fiber. SONET Action: Send RDI-L upon LOS detection.</td>
</tr>
</tbody>
</table>
### Table 3-6: SONET Events (continued)

<table>
<thead>
<tr>
<th>Event</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Loss of Frame (LOF)</td>
<td>Loss of Frame is detected by the STE when a Severely Errored Framing (SEF) defect on the incoming signal persists for 3 milliseconds.</td>
</tr>
<tr>
<td></td>
<td>Related SONET Overhead: A1, A2 (framing pattern).</td>
</tr>
<tr>
<td></td>
<td>SONET Action: Send RDI-L upon LOF detection.</td>
</tr>
<tr>
<td>Loss of Pointer (LOP)</td>
<td>The Path Loss Of Pointer event is detected as a result of excess New Data Flags (NDFs) or invalid pointers in the H1/H2 fields of the received signal.</td>
</tr>
<tr>
<td></td>
<td>Related SONET Overhead: H1,H2 contain NDF and pointer.</td>
</tr>
<tr>
<td></td>
<td>SONET Action: Send RDI-P upon LOP detection.</td>
</tr>
<tr>
<td>Alarm Indication Signal—Line (AIS-L)</td>
<td>The Line Alarm Indication Signal is sent by the upstream STE to inform the LTE that a LOS or LOF defect has been detected. Extreme's SONET module never sends AIS-L. AIS-L was formerly known as Line Far End Receive Failure (FERF).</td>
</tr>
<tr>
<td></td>
<td>Related SONET Overhead: K2 carries AIS-L.</td>
</tr>
<tr>
<td></td>
<td>SONET Action: Send RDI-L upon reception of AIS-L.</td>
</tr>
<tr>
<td>Alarm Indication Signal—Path (AIS-P)</td>
<td>The Path Alarm Indication Signal is sent by the upstream LTE to inform the PTE that a LOS, LOF, AIS-L, or LOP defect has been detected. Extreme's SONET module never sends AIS-P. AIS-P was formerly known as Path Far End Receive Failure (FERF).</td>
</tr>
<tr>
<td></td>
<td>Related SONET Overhead: H1,H2,H3 = 0 when indicating AIS-P.</td>
</tr>
<tr>
<td></td>
<td>SONET Action: Send RDI-P upon receiving AIS-P.</td>
</tr>
<tr>
<td>Remote Defect Indicator—Line (RDI-L)</td>
<td>The Line Remote Defect Indication is sent by the downstream LTE when a LOS, LOF, or AIS-L defect is detected.</td>
</tr>
<tr>
<td></td>
<td>Related SONET Overhead: K2 carries RDI-L.</td>
</tr>
<tr>
<td>Remote Defect Indicator—Path (RDI-P)</td>
<td>The Path Remote Defect Indication is sent by the downstream PTE when a LOP or AIS-P defect is detected.</td>
</tr>
<tr>
<td></td>
<td>Related SONET Overhead: G1 carries RDI-P.</td>
</tr>
<tr>
<td>Remote Error Indicator—Line (REI-L)</td>
<td>The Line Remote Error Indicator conveys a count of detected B2 parity errors from the peer LTE.</td>
</tr>
<tr>
<td></td>
<td>Related SONET Overhead: M1 carries REI-L.</td>
</tr>
<tr>
<td>Remote Error Indicator—Path (REI-P)</td>
<td>The Path Remote Error Indicator conveys a count of detected B3 parity errors from the peer PTE.</td>
</tr>
<tr>
<td></td>
<td>Related SONET Overhead: G1 carries REI-P.</td>
</tr>
</tbody>
</table>
Configuring and Monitoring SONET

Table 3-6: SONET Events (continued)

<table>
<thead>
<tr>
<th>Event</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Path Payload Label Mismatch (PLM-P)</td>
<td>The Path Payload Label Mismatch event occurs when the received payload type does not match the expected payload. This event is commonly caused by a Signal Label or scrambling mode mismatch configuration error. Related SONET Overhead: C2 carries the Signal Label.</td>
</tr>
<tr>
<td>Signal Failure Bit Error Rate (SF BER)</td>
<td>The Signal Failure BER event occurs when the B2 bit error rate exceeds the configured SF threshold. Related SONET Overhead: B2 carries line parity. SONET Action: Send RDI-L upon detecting SF BER event.</td>
</tr>
<tr>
<td>Signal Degraded Bit Error Rate (SD BER)</td>
<td>The Signal Degraded BER event occurs when the B2 bit error rate exceeds the configured SD threshold. This event is used for APS switching. Related SONET Overhead: B2 carries line parity.</td>
</tr>
</tbody>
</table>
Configuring VLAN-Related Attributes

The ExtremeWare software and the Extreme Networks switch architecture provide a range of Virtual Local Area Network (VLAN) features, which are described in detail in the ExtremeWare Software User Guide. This section describes how these features are supported on the ATM module.

This section assumes some familiarity with the Extreme Networks implementation of VLAN features as described in the ExtremeWare Software User Guide. For more information about VLAN-related features supported by ExtremeWare, see the ExtremeWare Software User Guide.

This section provides information on the following topics:

- Summary of VLAN-Related Commands on page 3-24
- Configuring Tagged VLAN 802.1p and 802.1Q Functions on page 3-25
- Generic VLAN Registration Protocol Functions on page 3-28

Summary of VLAN-Related Commands

Table 3-7 lists the ExtremeWare VLAN-related commands that support the ATM module. Each command is described in detail in the sections that follow.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>config dot1q tagmapping &lt;input_vlanid/output_vlanid&gt; ports &lt;portlist&gt; {egress {priority &lt;priority&gt;}}</td>
<td>Configures the VLAN tag mapping tables for an ATM port.</td>
</tr>
<tr>
<td>config dot1q tagnesting {&lt;vlanid&gt;</td>
<td>&lt;vlanid_range&gt;} [off</td>
</tr>
</tbody>
</table>

ATM module ports do not support protocol-based VLANs or MAC address VLANs. Thus, there are restrictions on the use of the following commands:

- `config vlan <name> [add | delete] ports <portlist> {tagged | untagged} {nobroadcast}`
• config vlan <name> protocol [<protocol_name> | any]
• enable mac-vlan mac-group [any | group_number] ports <portlist>

The restrictions are as follows:

• An ATM port cannot be added to a VLAN if the VLAN is a protocol-based VLAN.
• A VLAN cannot be configured to be a protocol-based VLAN if the VLAN contains an ATM port.
• A MAC address VLAN cannot be enabled on an ATM port.

The config vlan <name> protocol any command is supported, because it can be used to configure the default VLAN for ATM ports.

In the config vlan <name> [add | delete] ports <portlist> {tagged | untagged} {nobroadcast} command, ATM ports support the optional tagged and untagged keywords when LLC encapsulation for bridged protocols is enabled, and ignore them when LLC encapsulation for routed protocols is enabled.

Configuring Tagged VLAN 802.1p and 802.1Q Functions

The dot1q tag mapping and tag nesting commands are supported only by ATM ports and apply only when LLC encapsulation for bridged protocols is enabled on the ATM port.

The following ExtremeWare commands are supported for the ATM module:

• config dot1q ethertype <ethertype>
• config dot1p type dot1p_priority <priority> qosprofile <qosprofile>

If an ATM port receives a frame with a priority value “n” that is not mapped to a profile in the range from qp1 through qp8, the frame is assigned to QoS profile \( qpn+1 \).

The following commands provide ATM module support for managing 802.1Q tags:

• config dot1q tagmapping
• config dot1q tagnesting
Configuring VLAN Tag Mapping Tables

The `config dot1q tagmapping` command provides support for VLAN ID (VID) mapping tables. Each ATM port supports two VID tables: one table is used in the ingress direction; the other is used in the egress direction. These tables make it possible to map an input VID to an output VID, which can be useful in reconciling policy differences at the boundary between the customer and the service provider. The tables also allow the option of preserving the 802.1p priority or overwriting the priority with a configured value.

To configure the VLAN tag mapping tables for an ATM port, use the following command:

```
config dot1q tagmapping <input_vlanid/output_vlanid> ports <portlist>
    {egress {priority <priority>} | ingress {priority <priority>}}
```

The `input_vlanid` and `output_vlanid` parameters are both integers in the range from 1 to 4095 and must be separated by a slash character.

The `priority` parameter is an integer in the range from 0 to 7.

Use the `egress` keyword to apply the mapping of the input VLAN ID to the output VLAN ID to frames received from the switch backplane prior to transmitting them onto the ATM link. Use the `ingress` keyword to apply the mapping to input frames received from the ATM link. The mappings are applied after they are classified to a QoS profile. Frames containing the VLAN ID specified in `input_vlanid` are changed so that the VLAN ID is set to the value specified in `output_vlanid` before the frame is forwarded.

If you omit both the `egress` and the `ingress` keywords, the command automatically applies the specified mapping to the egress direction, and also applies a symmetrical mapping (with the `input_vlanid` and `output_vlanid` values reversed) to the ingress direction.

These tables also give you the option of preserving the 802.1p priority or overwriting the priority with a user-configured value. Using the `priority` keyword in the command indicates that the 802.1p priority field is to be set to the value specified in `priority`. To preserve the 802.1p priority, do not enter the `priority` keyword and value when using this command.

The default behavior is that the tables are initialized such that VLAN IDs are not altered by the mapping operations, and frame priority is preserved. For example, an input VLAN ID of \( n \) is always mapped to an output VLAN ID of \( n \), and the 802.1p priority field is not changed.
Configuring VLAN Tag Nesting Attributes

The config dot1q tagnesting command provides support for 802.1Q tags by allowing a tag push or pop attribute to be associated with a VLAN ID. The push attribute indicates that a new tag is to be added to the frame, while the pop attribute indicates that the top-level tag is to be removed from the frame. The command also gives you the option to preserve the 802.1p priority of the frame or set it to a configured value when a new tag is added (pushed) to the frame. VLAN ID (VID) mapping occurs before a new tag is pushed, and after a nested tag is popped.

To configure the VLAN tag nesting attributes for an ATM port, use the following command:

```
cfg dot1q tagnesting {<vlanid> | <vlanid_range>} [off | pop | push <new_vlanid> {priority <priority>}] ports <portlist> {egress | ingress}
```

The `vlanid` parameter is an integer in the range from 1 to 4095. The `vlanid_range` parameter is specified in the form `start_vlanid-end_vlanid`, where the start and end values are both integers in the range from 1 to 4095 and must be separated by a hyphen.

The `push` keyword indicates that a new tag is to be added to frames containing the VID specified in `vlanid` or to one of the VIDs in the range specified in `vlanid_range`. The new tag added to frames contains the value specified in `new_vlanid`. The `pop` keyword indicates that the top-level tag is to be removed from frames when that tag contains either the VID specified in `vlanid` or any one of the VIDs in the range specified in `vlanid_range`.

If you do not specify a VID or a range of VIDs, the command settings are applied to all VIDs.

Tag operations can be performed in either the egress direction (to the ATM link) or the ingress direction (from the ATM link). If you do not specify a direction, the default behavior is that tag operations are performed in the egress direction. If you do not use either the `egress` or `ingress` keyword and tag pushing is configured, a corresponding tag pop operation is automatically configured for the ingress direction. If you do not use either the `egress` or `ingress` keyword and tag nesting is disabled using the `off` keyword, tag nesting is disabled in both directions.

The optional `priority` keyword provides a way to overwrite the 802.1p priority with a user-configured value when a new tag is pushed. Using the `priority` keyword in the command indicates that the 802.1p priority field is to be set to the value specified in
Configuring the ATM Module

**priority**, which is an integer in the range from 0 to 7. To preserve the 802.1p priority, do not enter the **priority** keyword and value when using this command.

Default behavior is that tag nesting is disabled (off) for all VLAN IDs.

Tag push operations apply to egress frames only when the port is configured to transmit tagged frames for the associated VLAN. Tag nesting operations apply only to ingress frames that contain a VLAN tag. Tag nesting operations are applied after classification to a QoS profile.

![The DiffServ and RED functions are not performed by ATM ports when frames contain nested tags (more than one tag).](image)

**Generic VLAN Registration Protocol Functions**

The Generic VLAN Registration Protocol (GVRP) is not supported on ATM module ports, so the following command will not work if you specify an ATM port:

```
config gvrp {listen | send | both | none} ports <portlist>
```

**Configuring Forwarding Database Attributes**

ATM ports support all of the existing ExtremeWare forwarding database (FDB) commands. For more information on these commands, see the *ExtremeWare Software User Guide*.

**Configuring Spanning Tree Attributes**

ATM ports support all of the existing ExtremeWare Spanning Tree commands.
Configuring QoS Functions

The ExtremeWare software and the Extreme Networks switch architecture provide a number of Quality of Service (QoS) functions, which are described in detail in the ExtremeWare Software User Guide. This section describes how these QoS functions, such as Differentiated Services (DiffServ) and Random Early Detection (RED) are supported on the ATM module.

This section assumes some familiarity with the Extreme Networks implementation of QoS and DiffServ features as described in the ExtremeWare Software User Guide. For more information about QoS and DiffServ features supported by ExtremeWare, see the ExtremeWare Software User Guide.

This section contains information on the following topics:

- Summary of QoS-Related Commands on page 3-29
- Configuring a QoS Profile on page 3-30
- Classification and Replacement Policies on page 3-31
- Configuring DiffServ on page 3-33
- Enhanced RED Support on page 3-36

Summary of QoS-Related Commands

Table 3-8 contains an alphabetical list of the QoS-related commands that support the ATM module. Commands with keywords or parameters shown in italic typeface are existing ExtremeWare commands that have been enhanced to support the ATM module. Each command is described in detail in the sections that follow.

Table 3-8: QoS-Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>config diffserv dscp-mapping &lt;input_codepoint&gt;/&lt;output_codepoint&gt; ports &lt;portlist&gt; {egress {no-congestion</td>
<td>congestion}</td>
</tr>
<tr>
<td>config diffserv examination code-point &lt;code_point&gt; qosprofile &lt;qosprofile&gt; ports &lt;portlist&gt; {low-drop-probability</td>
<td>high-drop-probability}</td>
</tr>
</tbody>
</table>
Configuring the ATM Module

Configuring a QoS Profile

The ATM module supports eight ingress queues and eight egress queues per port. The scheduling parameters (minimum bandwidth, maximum bandwidth and priority level) for these queues are controlled by QoS profiles qp1 through qp8, which are defined using the existing ExtremeWare config qosprofile command.

This command has been enhanced to allow you to configure more module-specific parameters on a port-by-port basis, including the ability to customize the QoS profile parameters for individual ingress or egress queues on a specific ATM port.

The syntax and description of the enhanced config qosprofile command are described below.

Table 3-8: QoS-Related Commands (continued)

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>config red [drop-probability</td>
<td>low-drop-probability</td>
</tr>
<tr>
<td>config red min-threshold &lt;percent&gt; ports &lt;portlist&gt;</td>
<td>Configures the minimum queue length threshold for RED operation on the specified ATM ports.</td>
</tr>
<tr>
<td>config qosprofile &lt;qosprofile&gt; (minbw &lt;percent&gt;) {maxbw &lt;percent&gt;} (priority &lt;level&gt;) (minbuf &lt;percent&gt;) (maxbuf &lt;percent&gt;) {egress} {ingress} &lt;portlist&gt;</td>
<td>Configures a QoS profile. Added optional egress and ingress keywords.</td>
</tr>
<tr>
<td>disable red ports &lt;portlist&gt; {queue &lt;queue#&gt;}</td>
<td>Disables RED on the specified ATM ports. Added optional keyword and argument to specify the queue number.</td>
</tr>
<tr>
<td>enable red ports &lt;portlist&gt; {queue &lt;queue#&gt;}</td>
<td>Enables RED on the specified ATM ports. Added optional keyword and argument to specify the queue number.</td>
</tr>
<tr>
<td>show ports info detail</td>
<td>Displays detailed system-related information. Command output enhanced to display RED configuration information.</td>
</tr>
<tr>
<td>unconfig diffserv dscp-mapping ports &lt;portlist&gt;</td>
<td>Resets the DSCP mapping tables for the specified ATM ports to their default values.</td>
</tr>
</tbody>
</table>
To configure the scheduling parameters for a specified QoS profile, use the following command:

```
config qosprofile <qosprofile> {minbw <percent>} {maxbw <percent>}
   (priority <level>) {minbuf <percent>} {maxbuf <percent>} {<portlist>}
   (egress | ingress)
```

The optional `egress` and `ingress` keywords apply only to ATM ports. As stated earlier, the ATM module supports eight egress queues and eight ingress queues per port, and the scheduling parameters for these queues are controlled by QoS profiles qp1-qp8, which means queue #0 is controlled by qp1, queue #1 is controlled by qp2, and so on.

The optional `portlist` parameter allows QoS profiles to be customized on a port-by-port basis for the ATM module. The `egress` and `ingress` keywords allow you to fine-tune the customization (down to a particular egress or ingress queue on a given port). If you do not enter either the `egress` or `ingress` keyword in the command, the configured parameters apply to the egress queue associated with the specified QoS profile by default.

The `minbw` parameter specifies the minimum percentage of the bandwidth guaranteed to be available to the specified queue for transmissions from the QoS profile. The value is an integer in the range from 0 through 100. The default value is 0. The sum of the minimum bandwidth parameters across all eight QoS profiles cannot exceed 90%.

The `maxbw` parameter specifies the maximum percentage of the bandwidth that the specified queue can use for transmissions from the QoS profile. The value is an integer in the range from 1 through 100. The default value is 100.

The optional `priority` keyword and `level` parameter specify the service priority for the specified queue. The service priority determines which traffic is scheduled when bandwidth is still available after the minimum requirements of all profiles have been satisfied. Settings for `level` include: low, lowHi, normal, normalHi, medium, mediumHi, high, or highHi. The default setting is low.

> The `minbuf` and `maxbuf` keywords do not apply to ATM ports.

**Classification and Replacement Policies**

This section deals primarily with classification operations performed by the ATM module.

Most of the existing ingress classification functions are supported for LLC Encapsulation for Routed Protocols or LLC Encapsulation for Bridged Protocols.
configured ATM ports. Functions such as access list and destination MAC address QoS policies are supported, as is the `enable diffserv replacement` command.

Egress frames are always assigned to a QoS profile based on their 802.1p priority. Thus, when an ATM port receives a frame from the switch fabric with a priority value \( n \), that frame is assigned to egress QoS profile \( qp_{n+1} \).

The existing `enable diffserv examination ports` and `disable diffserv examination ports` commands are used on ATM ports to control whether the DiffServ code point (DSCP) is examined for ingress classification purposes.

When you enable the LLC Encapsulation for Bridged Protocols on an ATM port, non-IP frames that contain a VLAN tag are assigned to an ingress QoS profile based on their 802.1p priority value. You can configure this assignment using the `config dot1p type` command, which is used to specify the mappings between 802.1p priority values and QoS profiles. However, if an ATM port receives a frame with a priority value \( n \), for which there is no mapping to one of the eight profiles (qp1-qp8), that frame is assigned to ingress QoS profile \( qp_{n+1} \).

If `diffserv examination` is not enabled, then the preceding 802.1p priority classification rules are applied to tagged IP frames as well.

In both cases, untagged frames are assigned to a single ingress QoS profile (provided that the port is an untagged member of a VLAN; if that is not the case, then untagged frames are discarded). This QoS profile defaults to qp1, but you can assign it to another profile using the `config ports <portlist> qosprofile <qosprofile>` command or the `config vlan <name> qosprofile <qosprofile>` command (where the port-based QoS configuration has higher precedence than VLAN-based QoS).

Additionally, if you enable the LLC Encapsulation for Routed Protocols on an ATM port and do not enable `diffserv examination` on the port, then all ingress frames (received from the SONET link) are assigned to a single ingress QoS profile. The profile defaults to qp1, but you can configure it to another profile using the `config ports <portlist> qosprofile <qosprofile>` command or the `config vlan <name> qosprofile <qosprofile>` command.

If you enable `diffserv examination` on an ATM port, then ingress IP frames are assigned to a QoS profile based on the DiffServ code point (regardless of whether you enabled either LLC Encapsulation for Bridged Protocols or LLC Encapsulation for Routed Protocols on the port). The existing `config diffserv examination code-point` command maps DiffServ code points to QoS profiles. This command has been enhanced for use with ATM ports. The syntax and description of the enhanced `config diffserv examination code-point` command are given below.
Also note that, in all cases, the 802.1p priority bits of ingress frames forwarded to the switch backplane are set based on the ingress QoS profile classification. More specifically, the 802.1p priority value is set to qp# – 1. For example, if the packet is classified to qp5, then the 802.1p priority value is set to 4.

**Configuring DiffServ**

All of the existing ExtremeWare DiffServ commands are supported by ATM ports with IP frames that are encapsulated for bridged or routed protocols. ATM ports also support a DiffServ code point (DSCP) mapping function that you configure using the `config diffserv dscp-mapping` command, which is described below. The DSCP is a 6-bit value in the IP-TOS byte of the IP packet header. For more information on DSCPs, see “Configuring DiffServ” in the *ExtremeWare Software User Guide*.

**DiffServ Classification**

When a packet arrives at the switch on an ingress port, the switch examines the first six of eight TOS bits, called the code point. The switch can assign the QoS profile used to subsequently transmit the packet based on the code point. The QoS profile controls a hardware queue used when transmitting the packet out of the switch, and determines the forwarding characteristics of a particular code point. The examination of DiffServ information is disabled by default. To enable examination of DiffServ information, use the command:

```
enable diffserv examination ports [<portlist> | all]
```

**Changing DiffServ Code Point Assignments in the QoS Profile**

Because the code point uses six bits, it has 64 possible values ($2^6 = 64$). By default, the values are grouped and assigned to the default QoS profiles listed in Table 3-9.

<table>
<thead>
<tr>
<th>Code Point</th>
<th>QoS Profile</th>
</tr>
</thead>
<tbody>
<tr>
<td>0-7</td>
<td>Qp1</td>
</tr>
<tr>
<td>8-15</td>
<td>Qp2</td>
</tr>
<tr>
<td>16-23</td>
<td>Qp3</td>
</tr>
<tr>
<td>24-31</td>
<td>Qp4</td>
</tr>
<tr>
<td>32-39</td>
<td>Qp5</td>
</tr>
</tbody>
</table>

*Table 3-9: Default Code Point-to-QoS Profile Mapping*
Configuring the ATM Module

Table 3-9: Default Code Point-to-QoS Profile Mapping (continued)

<table>
<thead>
<tr>
<th>Code Point</th>
<th>QoS Profile</th>
</tr>
</thead>
<tbody>
<tr>
<td>40-47</td>
<td>Qp6</td>
</tr>
<tr>
<td>48-55</td>
<td>Qp7</td>
</tr>
<tr>
<td>56-63</td>
<td>Qp8</td>
</tr>
</tbody>
</table>

To configure the mapping between a DiffServ code point and a specified QoS profile, use the following command:

```config
diffserv examination code-point <code_point>
qosprofile <qosprofile> ports <portlist>
{low-drop-probability | high-drop-probability}
```

The mapping is applied in the ingress direction—for IP packets received from the ATM link.

The optional `low-drop-probability` and `high-drop-probability` keywords apply only to ATM ports. If you do not enter either of these keywords in the command, the command uses `low-drop-probability` as the default.

The `low-drop-probability` and `high-drop-probability` keywords are useful in conjunction with the Weighted RED (WRED) implementation provided by ATM ports. This implementation supports two different drop probabilities: one for DiffServ code points designated as having low drop-probability; another for DiffServ code points designated as having high drop-probability. These keywords give you complete flexibility in assigning DiffServ code points to these two drop-probability levels.

Configuring DiffServ Code Point Mapping Tables

You can use the `diffserv dscp-mapping` command to configure a mapped relationship between an input DSCP and an associated output DSCP. Each ATM port supports three DSCP mapping tables: one of the tables is used in the ingress direction; two are used for egress flows (onto the ATM link). The two egress tables are for the congested and noncongested states, as determined by the RED algorithm. If RED is not enabled on the ATM port, the egress congested-state mapping table is not used.

In the ingress direction, the input DSCP of a packet received from the ATM link is replaced by an output DSCP before the packet is forwarded. In the egress direction, the operation is similar, except that the DSCP mapping occurs before the packet is transmitted onto the ATM link.
One potential use of the DSCP mapping capability is to reconcile varying DiffServ policies at the boundary between autonomous systems, such as at the boundary between two ISPs. The availability of different tables for the congested and noncongested states is useful in marking operations that increase the probability of packets being dropped during times of congestion, as discussed in the DiffServ Assured Forwarding RFC (RFC 2597).

This command applies only to ATM ports with IP frames that are encapsulated for bridged or routed protocols. You should also be aware that DSCP mapping is performed even when the diffserv examination function is disabled on the port.

To configure the mapping between an input DSCP and an associated output DSCP, use the following command:

```
config diffserv dscp-mapping <input_codepoint>/<output_codepoint>
    ports <portlist> {egress {no-congestion | congestion} | ingress}
```

where:

- **input_codepoint** Specifies one of the 64 possible DiffServ code point values as the input code point.
- **output_codepoint** Specifies one of the 64 possible DiffServ code point values as the output code point.
- **egress** Applies the DSCP mapping to the egress direction.
- **no-congestion** Applies the DSCP mapping to the egress mapping table for the non-congested state.
- **congestion** Applies the DSCP mapping to the egress mapping table for the congested state.
- **ingress** Applies the DSCP mapping to the ingress direction.

If you omit the no-congestion and congestion keywords, the command applies the mapping to the tables for both states.

If you omit the egress and ingress keywords, the command applies the mapping to the egress direction, and automatically configures a symmetrical mapping (with the input_codepoint and output_codepoint values reversed) in the ingress direction.

By default, all the tables are initialized such that DSCPs are not altered by the mapping operations. For example, an input DSCP value of \( n \) is always mapped to an output DSCP value of \( n \).
**Configuring the ATM Module**

### Resetting DiffServ Code Point Mapping Tables

To reset the DSCP mapping tables for a specified ATM port to their default values, use the following command:

```bash
unconfig diffserv dscp-mapping ports <portlist>
```

### Replacing DiffServ Code Points

To replace DiffServ code points, you must use the following command to enable DiffServ replacement:

```bash
enable diffserv replacement ports [<portlist> | all]
```

You then change the 802.1p priority to DiffServ code point mapping to any code point value using the following command:

```bash
config diffserv replacement priority <vpri> code_point <code_point> ports [<portlist> | all]
```

By doing so, the hardware queue used to transmit a packet determines the DiffServ value replaced in the IP packet.

To verify the DiffServ configuration, use the command:

```bash
show ports <portlist> info detail
```

### Enhanced RED Support

Random Early Detection (RED) is a congestion avoidance mechanism. The basic idea behind RED is that most data transports detect packet loss and will, therefore, restrain transmission—if only temporarily—when they detect dropped packets. Consequently, if the switch needs to signal another device to slow transmission due to congestion, RED provides a way of intelligently dropping packets.

This section describes the changes and additions to ExtremeWare to support RED in conjunction with ATM modules that have IP frames encapsulated in bridged or routed protocols. The Extreme implementation of RED combines the functions of the RED algorithm with IP precedence to provide support for preferential traffic handling for higher-priority packets. This implementation provides weighted RED (WRED) functionality through two packet-drop probabilities (described below), so that a device can selectively drop lower-priority traffic when an interface begins to show signs of congestion. This capability is combined with DiffServ attributes to allow you to tailor performance characteristics for different classes of service.
Configuring RED Drop Probability

To configure the RED drop probability for a specified ATM port, use the following command:

```
config red [drop-probability | low-drop-probability | high-drop-probability] <percent> {ports <portlist>}
```

The optional low-drop-probability, high-drop-probability, and ports keywords are supported only for ATM ports.

If you omit the ports keyword, the command applies the setting to all ports.

The drop probability is specified as a percentage, where the percent parameter is an integer in the range from 1 to 100.

Weighted RED (WRED) functionality is supported through two different drop probabilities: a low-drop-probability and a high-drop-probability. The DiffServ code points of IP packets indicate whether the packet should be dropped with low probability or high probability, and the appropriate percentage is then applied if WRED is active.

WRED is applied only to IP packets. The `config diffserv examination code-point` command gives you complete flexibility in assigning DSCPs to the two different drop-probability levels. This configured mapping of DSCPs to drop-probability levels is used by WRED even if `diffserv examination` is disabled on the port.

The drop-probability keyword indicates that the specified percentage should be used for both the low and high drop-probabilities. This effectively disables WRED and reverts to standard RED operation. For ATM ports, both the low and high drop-probabilities default to 10%.

The role of the configured drop probability in RED operation on ATM ports is illustrated in Figure 3-3A. RED is active when the average queue length is between the minimum and maximum thresholds. In this region, the probability that a given packet is dropped increases in a straight line up to the configured drop probability at the maximum threshold. All packets are dropped when the average queue length exceeds the maximum threshold.

The operation of WRED on ATM ports is depicted in Figure 3-3B. In this case, the drop probability depends not only on the average queue length, but also upon whether the
DSCP indicates that the packet should be dropped with a low or high probability, which is to say, the DSCP of the packet controls which curve is used.

**A. RED Operation on ATM Ports**

- Packet drop probability
- Configured drop-probability
- Minimum threshold
- Maximum threshold
- Average queue length

**B. WRED Operation on ATM Ports**

- Packet drop probability
- High-drop-probability
- Low-drop-probability
- Minimum threshold
- Maximum threshold
- Average queue length

*Figure 3-3:* Comparisons of RED and WRED operation
Enabling and Disabling RED on ATM Ports

The existing ExtremeWare commands to enable and disable RED ports have been enhanced to provide RED configuration attributes for the ATM module. Because the ATM module supports eight egress queues per port, the commands were enhanced to allow the user a way to enable RED selectively on an individual port and queue basis. By default, RED is disabled.

To enable RED on a specified ATM port, use the following command:

```
enable red ports <portlist> {queue <queue#>}
```

To disable RED on a specified ATM port, use the following command:

```
disable red ports <portlist> {queue <queue#>}
```

The optional `queue` keyword applies only to ATM ports. You can use this keyword to enable or disable the RED function on an individual queue basis.

The `queue#` parameter is an integer in the range from 0 to 7, and identifies one of the eight egress queues. If you omit the `queue` keyword, the command applies to all of the queues for the ATM port.

Configuring the RED Minimum Queue Length Threshold

The packet drop probability is based, in part, on the RED minimum queue length threshold. When the average queue length exceeds this threshold, the RED algorithm is activated and begins dropping packets. The packet drop rate increases in a linear fashion as the average queue length increases or until the average queue length hits the maximum threshold.

This command applies only to PoS and ATM ports.

To configure the minimum queue length threshold for RED operation on a specified ATM port, use the following command:

```
cfg red min-threshold <percent> ports <portlist>
```

The threshold value is specified as a percentage in the range from 1 to 100. For ATM ports, the minimum threshold is a percentage of 1000 packet buffers, and the maximum threshold is set to the value calculated by the formula:

```
minimum ((3 * minimum threshold buffers), maximum available buffers)
```
By default, the minimum threshold for ATM ports is 10%, or 100 buffers; thus, the default maximum threshold is 300 buffers.

You can use the `show ports info detail` command to display the settings of the minimum and maximum thresholds, displayed in terms of the number of buffers.

Use the `ports` keyword to configure the threshold parameter on specific ATM ports.

**Support for Standard Per-Hop Behaviors**

The per-hop behavior (PHB) describes the externally observable packet forwarding handling (or “behavior”) to be applied by the receiving network element when there are competing requests for resources such as bandwidth and buffer space. In the packet forwarding path, differentiated services are identified by mapping the differentiated services code point (DSCP) contained in the IP packet header to a specific forwarding behavior at each network element along its path. The DSCP is 6 bits wide, and takes the form \( \text{xxxxxx} \), where \( x \) can be either 0 or 1. The DSCP field is capable of identifying one of 64 distinct code points. For purposes of code point allocation and management, the code point space is divided into three pools: one pool of 32 code points (pool 1) constitutes the recommended code points to be allocated as standards; a second pool of 16 code points (pool 2) is set aside for experimental or local use; a third pool of 16 code points (pool 3) that are initially set aside for experimental or local use, but that might be used for standard assignments if pool 1 is ever exhausted. The mapping of DSCPs to PHBs is a user-configurable function, as described below.

The current standards call for two PHBs: Assured Forwarding (AF) and Expedited Forwarding (EF). The EF PHB describes the required behavior for voice-over-IP service. The AF PHB consists of four independently forwarded AF classes: AF1, AF2, AF3, and AF4. Within each of these classes, an IP packet can be assigned to different levels of drop precedence (used to determine drop probability) depending on how many levels of drop precedence the implementation supports. RFC 2597 describes two schemes for drop-precedence levels: a three-level scheme (see Table 3-10) and a two-level scheme (see Table 3-11). The three-level scheme supports low, medium, and high drop-precedence levels for the AF classes; the two-level scheme supports low and high drop-precedence levels (and groups the medium drop-precedence code-points with the high drop-precedence code-points). The Extreme implementation for the ATM module supports the two-level drop-precedence scheme.
Configuring QoS Functions

In addition, a network element that complies with the DiffServ standards must also provide a recommended default code point, which must be unique for code points in the standard space. The default PHB describes the common, best-effort forwarding behavior offered by existing network elements, as defined in RFC 1812.

As an additional differentiation, a set of code points has been allocated for use as the Class Selector code points, which describe the minimum forwarding handling requirements needed to preserve compatibility with existing practices while respecting flexibility for the future.

Table 3-12 and the command examples that follow show how the standard per-hop behaviors (PHBs) might be mapped onto ExtremeWare QoS profiles qp1 through qp8.

Table 3-10: Assured Forwarding Classes and Three-Level Drop Precedence

<table>
<thead>
<tr>
<th>Drop-Precedence Level</th>
<th>AF1</th>
<th>AF2</th>
<th>AF3</th>
<th>AF4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low drop precedence</td>
<td>(AF11) 001010</td>
<td>(AF21) 010010</td>
<td>(AF31) 011010</td>
<td>(AF41) 100010</td>
</tr>
<tr>
<td>Medium drop precedence</td>
<td>(AF12) 001100</td>
<td>(AF22) 010100</td>
<td>(AF32) 011100</td>
<td>(AF42) 100100</td>
</tr>
<tr>
<td>High drop precedence</td>
<td>(AF13) 001110</td>
<td>(AF23) 010110</td>
<td>(AF33) 011110</td>
<td>(AF43) 100110</td>
</tr>
</tbody>
</table>

Table 3-11: Assured Forwarding Classes and Two-Level Drop Precedence

<table>
<thead>
<tr>
<th>Drop-Precedence Level</th>
<th>AF1</th>
<th>AF2</th>
<th>AF3</th>
<th>AF4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low drop precedence</td>
<td>(AF11) 001010</td>
<td>(AF21) 010010</td>
<td>(AF31) 011010</td>
<td>(AF41) 100010</td>
</tr>
<tr>
<td>High drop precedence</td>
<td>(AF12) 001100</td>
<td>(AF22) 010100</td>
<td>(AF32) 011100</td>
<td>(AF42) 100100</td>
</tr>
</tbody>
</table>

Table 3-12: Mapping PHBs to QoS Profiles

<table>
<thead>
<tr>
<th>PHB</th>
<th>Default</th>
<th>Class Selector</th>
<th>AF1</th>
<th>AF2</th>
<th>AF3</th>
<th>AF4</th>
<th>EF</th>
</tr>
</thead>
<tbody>
<tr>
<td>QoS Profile</td>
<td></td>
<td></td>
<td>qp1</td>
<td>qp2</td>
<td>qp3</td>
<td>qp4</td>
<td>qp5</td>
</tr>
<tr>
<td>DSCP</td>
<td></td>
<td></td>
<td>000000</td>
<td>001000</td>
<td>010000</td>
<td>001100</td>
<td>110000</td>
</tr>
</tbody>
</table>
The DSCPs associated with a PHB are assigned to the appropriate QoS profile using the config diffserv examination code-point command. For example, the following command sets up the mapping for the EF PHB:

```
config diffserv examination code-point 46 qosprofile qp8 ports 2:1-2:2
```

Additional configuration steps for ATM ports in this example are as follows:

- **Enable RED for all PHBs except the EF PHB.** For example:
  ```
  enable red ports 2:1-2:2
  disable red ports 2:1-2:2 queue 8
  ```

- **Configure a high drop-probability of 20% on the ATM ports.** For example:
  ```
  config red high-drop-probability 20 ports 2:1-2:2
  ```

- **Enable examination of DiffServ information.** For example:
  ```
  enable diffserv examination ports 2:1-2:2
  ```

- **Configure the default PHB.** For example:
  ```
  config diffserv examination code-point 0 qosprofile qp1 ports 2:1-2:2
  ```

- **Configure the Class Selectors.** For example:
  ```
  config diffserv examination code-point 8 qosprofile qp2 ports 2:1-2:2 high-drop-probability
  config diffserv examination code-point 16 qosprofile qp2 ports 2:1-2:2 high-drop-probability
  config diffserv examination code-point 24 qosprofile qp2 ports 2:1-2:2 high-drop-probability
  config diffserv examination code-point 32 qosprofile qp2 ports 2:1-2:2 low-drop-probability
  config diffserv examination code-point 40 qosprofile qp2 ports 2:1-2:2 low-drop-probability
  config diffserv examination code-point 48 qosprofile qp3 ports 2:1-2:2 high-drop-probability
  config diffserv examination code-point 56 qosprofile qp3 ports 2:1-2:2 low-drop-probability
  ```

- **Configure the drop-probability for the DSCPs assigned to AF1 through AF4.** For example, for AF1 (qp4):
  ```
  config diffserv examination code-point 10 qosprofile qp4 ports 2:1-2:2 low-drop-probability
  config diffserv examination code-point 12 qosprofile qp4 ports 2:1-2:2 high-drop-probability
  ```
config diffserv examination code-point 14 qosprofile qp4
   ports 2:1-2:2 high-drop-probability

For example, for AF2 (qp5):
config diffserv examination code-point 18 qosprofile qp5
   ports 2:1-2:2 low-drop-probability
config diffserv examination code-point 20 qosprofile qp5
   ports 2:1-2:2 high-drop-probability
config diffserv examination code-point 22 qosprofile qp5
   ports 2:1-2:2 high-drop-probability

For example, for AF3 (qp6):
config diffserv examination code-point 26 qosprofile qp6
   ports 2:1-2:2 low-drop-probability
config diffserv examination code-point 28 qosprofile qp6
   ports 2:1-2:2 high-drop-probability
config diffserv examination code-point 30 qosprofile qp6
   ports 2:1-2:2 high-drop-probability

For example, for AF4 (qp7):
config diffserv examination code-point 34 qosprofile qp7
   ports 2:1-2:2 low-drop-probability
config diffserv examination code-point 36 qosprofile qp7
   ports 2:1-2:2 high-drop-probability
config diffserv examination code-point 38 qosprofile qp7
   ports 2:1-2:2 high-drop-probability

- Configure the congested-state mappings for DSCPs 10 (AF1), 18 (AF2), 26 (AF3), and 34 (AF4). For example:
  config diffserv dscp-mapping 10/12 egress congestion
  config diffserv dscp-mapping 18/20 egress congestion
  config diffserv dscp-mapping 26/28 egress congestion
  config diffserv dscp-mapping 34/36 egress congestion

- Use the EF PHB to configure bandwidth reservation and rate limiting. For example:
  config diffserv examination code-point 46 qosprofile qp8 ports 2:1-2:2
  config qosprofile qp8 minbw 10 maxbw 20 2:1-2:2 egress
  config qosprofile qp8 minbw 10 maxbw 20 2:1-2:2 ingress
Displaying RED Configuration Information for ATM Module Ports

While the syntax of the existing `show ports info detail` command has not changed, the output of the command now displays the RED and DiffServ configuration parameters associated with ATM module ports.

To display QoS, RED, and DiffServ information for a specified ATM port, use the following command:

```
show ports info detail
```

For ATM ports, the existing `show ports qosmonitor` command has also been enhanced to display the number of packet transmissions and discards from each queue (in both egress and ingress directions).

QoS Monitor

The QoS Monitor utility is supported for ATM module ports. The QoS Monitor and its associated ExtremeWare commands are described in the *ExtremeWare Software User Guide*.

Intra-Subnet QoS

Intra-Subnet QoS (ISQ) is not supported on switches that use the “i” chipset; the ATM module is supported only on switches that use the “i” chipset.
Additional ATM Module Support Topics

This section describes additional command and configuration information related to the use of the ATM module. This section includes information on the following topics:

• Configuring General Switch Attributes on page 3-45
• Configuring Port Attributes on page 3-46
• Configuring IGMP Attributes on page 3-48
• Configuring Layer 2 and 3 Switching Attributes on page 3-49
• Configuring Access List Attributes on page 3-49
• Changing Image and Configuration Attributes on page 3-49

Configuring General Switch Attributes

Except as described below, the ATM module supports all of the general ExtremeWare switch commands. Table 3-13 describes the changes to existing ExtremeWare general switch commands to support the ATM module. Commands with keywords or parameters shown in italic typeface are existing ExtremeWare commands that have been enhanced to support the ATM module.

Table 3-13: Changes to General Switch Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description of Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>show slot {&lt;slot&gt;}</td>
<td><strong>Augmented implementation:</strong> For the ATM module, the information displayed by this command will include data about the software images loaded on the module, as well as network processor and GPP status.</td>
</tr>
<tr>
<td>config slot &lt;slot&gt; module [a3c</td>
<td>f32t</td>
</tr>
<tr>
<td>show version</td>
<td><strong>Augmented implementation:</strong> The information displayed by this command will include data about the ATM module and the bootrom version of the ATM module.</td>
</tr>
</tbody>
</table>
Configuring the ATM Module

**Table 3-13: Changes to General Switch Commands (continued)**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description of Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>reboot {time &lt;date&gt; &lt;time&gt;</td>
<td>cancel} (slot &lt;slot&gt;)</td>
</tr>
<tr>
<td>clear counters</td>
<td>Augmented implementation: For the ATM module, this command clears statistics for all of the ATM-related functions: SONET and DiffServ.</td>
</tr>
<tr>
<td>show diagnostics slot {&lt;slot&gt;}</td>
<td>Augmented implementation: This command displays the result of ATM module diagnostics.</td>
</tr>
<tr>
<td>run diagnostics [normal</td>
<td>extended] slot &lt;slot&gt;</td>
</tr>
</tbody>
</table>

**Configuring Port Attributes**

The following ExtremeWare port commands are not supported for the ATM module:

- show ports (<portlist>) collisions
- config ports <portlist> auto off {speed [10 | 100 | 1000]} duplex [half | full]
- config ports <portlist> auto on
- enable smartredundancy <portlist>
- enable sharing <port> grouping <portlist> {port-based | address-based | round-robin}
- enable mirroring to <port>
- disable learning ports <portlist>
- config mirroring add [vlan <name> | port <port> | vlan <name> ports <portlist>]

Except as described below, the ATM module supports the remainder of the ExtremeWare port commands. Table 3-14 describes the changes to the ExtremeWare port commands to support the ATM module. Commands with keywords or parameters shown in italic typeface are existing ExtremeWare commands that have been enhanced to support the ATM module.
Jumbo Frame Support

The jumbo frame size affects the size of the payload that can be transmitted or received on an ATM port.

If jumbo frame support is enabled on an ATM port, the following can occur:

---

### Table 3-14: Changes to Port Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description of Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>disable ports &lt;portlist&gt;</td>
<td><strong>Augmented implementation:</strong> For ATM modules, this command brings down the ATM link on the specified port, and changes the port status LED to blinking green.</td>
</tr>
<tr>
<td>enable ports &lt;portlist&gt;</td>
<td><strong>Augmented implementation:</strong> For ATM modules, this command enables the ATM link on the specified port, and changes the port status LED to solid green (if no other problems exist).</td>
</tr>
<tr>
<td>show ports {&lt;portlist&gt;} info {detail}</td>
<td><strong>Augmented implementation:</strong> The information displayed by this command includes DiffServ and RED configuration parameters for the ATM module ports.</td>
</tr>
<tr>
<td>show ports {&lt;portlist&gt;} qosmonitor {egress</td>
<td>ingress} {discards}</td>
</tr>
<tr>
<td>show ports {&lt;portlist&gt;} rxerrors</td>
<td><strong>Augmented implementation:</strong> Only a subset of the statistics displayed by this command are applicable to ATM ports. The fields that do not apply to ATM ports are displayed with values of all zeroes.</td>
</tr>
<tr>
<td>show ports {&lt;portlist&gt;} txerrors</td>
<td><strong>Augmented implementation:</strong> Only a subset of the statistics displayed by this command are applicable to ATM ports. The fields that do not apply to ATM ports are displayed with values of all zeroes.</td>
</tr>
</tbody>
</table>
Configuring the ATM Module

- No frames received from the switch backplane will be discarded due to being too large. Nor will any IP frames be fragmented.
- PDUs received from the ATM link with routed protocol encapsulation will be discarded if the size of the IP packet exceeds \((\text{configured JUMBO_FRAME_MTU} - 22)\) octets.
- PDUs received from the ATM link with bridged protocol encapsulation will be discarded if the size of the Ethernet frame (including a VLAN tag but excluding the LAN FCS) exceeds \((\text{CONFIGURED JUMBO_FRAME_MTU} - 4)\) octets. If the Ethernet frame does not include a VLAN tag field, then the frame will be discarded if the size of the Ethernet frame (excluding the LAN FCS) exceeds \((\text{CONFIGURED JUMBO_FRAME_MTU} - 8)\) octets.

If jumbo frame support is not enabled on an ATM port, the following can occur:

- Frames received from the switch backplane, whose size exceeds 1522 octets, will not be forwarded onto the ATM link. IP frames that meet this criteria will be sent to the MSM CPU for fragmentation/Path MTU Discovery processing. Non-IP frames that meet this criteria will be discarded.
- PDUs received from the ATM link with routed protocol encapsulation will be discarded if the size of the IP packet exceeds 1500 octets.
- PDUs received from the ATM link with bridged protocol encapsulation will be discarded if the size of Ethernet frame (including a VLAN tag but excluding the LAN FCS) exceeds 1518 octets. If the Ethernet frame does not include a VLAN tag field, then the frame will be discarded if the size of the Ethernet frame (excluding the LAN FCS) exceeds 1514 octets.

Consider these factors when configuring jumbo frame support on an ATM port:

- When the jumbo frame size is changed from a value of 6129 or less to a value greater than 6129, any ATM module that has ports with jumbo frame support enabled must be rebooted for the change to take effect.

For more information on the ExtremeWare jumbo frame commands, see the *ExtremeWare Software User Guide*.

**Configuring IGMP Attributes**

For more information on the ExtremeWare IGMP commands, see the *ExtremeWare Software User Guide*. 
Configuring Layer 2 and 3 Switching Attributes

All of the IP routing protocols are supported for either L2 encapsulation or IP encapsulation: RIP, OSPF, BGP, DVMRP, and PIM.

When L2 encapsulation is enabled on an ATM port, IPX RIP and SAP are supported.

Configuring Access List Attributes

For more information on the ExtremeWare access list commands, see the ExtremeWare Software User Guide.

On the ATM module, the access list functions apply to port pairs, where ports 1 and 2 are a pair, and ports 3 and 4 are a pair. This pairing scheme means that the ports in a given pair share the same access lists: ports 1 and 2 share the same lists, while ports 3 and 4 share their access lists. For example, if an access list is configured for port 1, that access list also applies to port 2, and vice versa.

Changing Image and Configuration Attributes

Except as described below, the ATM module supports all of the ExtremeWare commands associated with managing image and configuration attributes. For more information about these commands and operations, see the “Software Upgrade and Boot Options” appendix in the ExtremeWare Software User Guide. Table 3-15 describes the command changes to support the ATM module. Commands with keywords or parameters shown in italic typeface are existing ExtremeWare commands that have been enhanced to support the ATM module.

Table 3-15: Changes to Image Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description of Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>download bootrom [&lt;ipaddress&gt;</td>
<td>&lt;hostname&gt;] &lt;filename&gt; {slot &lt;slot&gt;}</td>
</tr>
</tbody>
</table>
Configuring the ATM Module

Table 3-15: Changes to Image Commands (continued)

<table>
<thead>
<tr>
<th>Command</th>
<th>Description of Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>download image [&lt;ipaddress&gt;</td>
<td>&lt;hostname&gt;]</td>
</tr>
<tr>
<td>filename&gt; [primary</td>
<td>secondary]</td>
</tr>
<tr>
<td>(slot &lt;slot&gt;)</td>
<td></td>
</tr>
<tr>
<td>use image [primary</td>
<td>secondary] (slot &lt;slot&gt;)</td>
</tr>
</tbody>
</table>
ExtremeWare Command Compatibility Information Related to the ATM Module

This appendix summarizes the ExtremeWare command changes and additions to support the ATM module, and includes information on the following topics:

- New commands added to support the ATM module on page A-1
- Commands changed to support the ATM module on page A-3
- Commands not supported by the ATM module on page A-6

New Commands

New commands have been added to ExtremeWare to support the following functions:

- ATM
- SONET
- QoS and DiffServ
- 802.1Q tag mapping and tag nesting
New ExtremeWare Commands

Table A-1 lists the new ExtremeWare commands that have been added to support the ATM module. For more information on these commands, see Chapter 3.

**Table A-1: New ExtremeWare Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>`config atm add pvc &lt;vpi</td>
<td>vci&gt; encap [l2</td>
</tr>
<tr>
<td>`config atm delete pvc [&lt;vpi</td>
<td>vci&gt;</td>
</tr>
<tr>
<td>`config atm scrambling [on</td>
<td>off] ports &lt;portlist&gt;`</td>
</tr>
<tr>
<td>`config diffserv dscp-mapping &lt;input_codepoint&gt;/&lt;output_codepoint&gt; ports &lt;portlist&gt; {egress {no-congestion</td>
<td>congestion}</td>
</tr>
<tr>
<td>`config dot1q tagmapping &lt;input_vlanid/output_vlanid&gt; ports &lt;portlist&gt; {egress {priority &lt;priority&gt;}</td>
<td>ingress {priority &lt;priority&gt;}}`</td>
</tr>
<tr>
<td>`config dot1q tagnesting (&lt;vlanid&gt;</td>
<td>&lt;vlanid_range&gt;) [off</td>
</tr>
<tr>
<td><code>config red min-threshold &lt;percent&gt; ports &lt;portlist&gt;</code></td>
<td>Configures the minimum queue length threshold for RED operation on the specified ATM ports.</td>
</tr>
<tr>
<td>`config sonet clocking [line</td>
<td>internal] ports &lt;portlist&gt;`</td>
</tr>
<tr>
<td>`config sonet framing [sonet</td>
<td>sdh] ports &lt;portlist&gt;`</td>
</tr>
<tr>
<td>`config sonet signal label [auto</td>
<td>&lt;hex_octet&gt;] ports &lt;portlist&gt;`</td>
</tr>
</tbody>
</table>
Changed Commands

Changes to existing ExtremeWare commands fall into two categories:

- Syntax enhancements to support the ATM module
- Implementation changes to support the ATM module

Syntax changes are visible: keywords or arguments may have been added or changed to make it possible to configure the behavior associated with the ATM module. Implementation changes may be visible, taking the form of different input behavior, such as blocking an attempt at specifying an ATM port for a given command, or in additional information in the results of a command, such as in a show ports command.

Commands not described in this section are supported by the ATM module as described in the ExtremeWare Software User Guide.
Table A-2 is an alphabetical list of the existing ExtremeWare commands whose syntax has been enhanced to support the ATM module. New keywords and arguments are shown in italic typeface.

### Table A-2: Summary of Commands with Enhanced Syntax

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>`config diffserv examination code-point &lt;code_point&gt; qosprofile &lt;qosprofile&gt; ports &lt;portlist&gt; {low-drop-probability</td>
<td>high-drop-probability}`</td>
</tr>
<tr>
<td>`config red [drop-probability</td>
<td>low-drop-probability</td>
</tr>
<tr>
<td>`config qosprofile &lt;qosprofile&gt; {minbw &lt;percent&gt;} {maxbw &lt;percent&gt;} {priority &lt;level&gt;} {minbuf &lt;percent&gt;} {maxbuf &lt;percent&gt;} {&lt;portlist&gt;} {egress</td>
<td>ingress}`</td>
</tr>
<tr>
<td>`config slot &lt;slot&gt; module [a3c</td>
<td>f32t</td>
</tr>
<tr>
<td><code>disable red ports &lt;portlist&gt; {queue &lt;queue#&gt;}</code></td>
<td>Added optional keyword and argument to specify the queue number.</td>
</tr>
<tr>
<td>`download bootrom [&lt;ipaddress&gt;</td>
<td>&lt;hostname&gt;] &lt;filename&gt; {slot &lt;slot&gt;}`</td>
</tr>
<tr>
<td>`download image [&lt;ipaddress&gt;</td>
<td>&lt;hostname&gt;] &lt;filename&gt; [primary</td>
</tr>
<tr>
<td><code>enable red ports &lt;portlist&gt; {queue &lt;queue#&gt;}</code></td>
<td>Added optional keyword and argument to specify the queue number.</td>
</tr>
<tr>
<td>`reboot {time &lt;date&gt; &lt;time&gt;</td>
<td>cancel} {slot &lt;slot&gt;}`</td>
</tr>
<tr>
<td>`show ports {&lt;portlist&gt;} qosmonitor {egress</td>
<td>ingress} {discards}`</td>
</tr>
<tr>
<td>`use image [primary</td>
<td>secondary] {slot &lt;slot&gt;}`</td>
</tr>
</tbody>
</table>
Table A-3 is an alphabetical list of the existing ExtremeWare commands whose implementation has been augmented to support the ATM module.

### Table A-3: Summary of Commands with Augmented Implementation

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear counters</td>
<td>For the ATM module, this command clears statistics for all ATM-related functions such as PVC counters and SONET events.</td>
</tr>
<tr>
<td>disable jumbo-frame ports [&lt;portlist&gt;</td>
<td>all]</td>
</tr>
<tr>
<td>disable ports &lt;portlist&gt;</td>
<td>For ATM modules, this command changes the port status LED to blinking green.</td>
</tr>
<tr>
<td>enable jumbo-frame ports [&lt;portlist&gt;</td>
<td>all]</td>
</tr>
<tr>
<td>enable ports &lt;portlist&gt;</td>
<td>For ATM modules, this command enables PVCs on the specified port, and changes the port status LED to solid green (if no other problems exist).</td>
</tr>
<tr>
<td>show diagnostics {&lt;slot&gt;}</td>
<td>This command displays results of diagnostics for the ATM module.</td>
</tr>
<tr>
<td>show ports {&lt;portlist&gt;} info {detail}</td>
<td>The information displayed by this command will include new DiffServ and RED configuration parameters.</td>
</tr>
<tr>
<td>show ports {&lt;portlist&gt;} rxerrors</td>
<td>Only a subset of the statistics displayed by this command are applicable to ATM ports. The fields that do not apply to ATM ports are displayed with values of all zeroes.</td>
</tr>
<tr>
<td>show ports {&lt;portlist&gt;} txerrors</td>
<td>Only a subset of the statistics displayed by this command are applicable to ATM ports. The fields that do not apply to ATM ports are displayed with values of all zeroes.</td>
</tr>
<tr>
<td>show slot &lt;slot&gt;</td>
<td>For the ATM module, the information displayed by this command will include data about the software images loaded on the module, as well as status information on the network processors and GPP.</td>
</tr>
<tr>
<td>show version</td>
<td>The information displayed by this command will include data about the ATM I/O module and the bootrom version of the ATM I/O module.</td>
</tr>
</tbody>
</table>
Commands and Functions Not Supported

None of the ExtremeWare commands associated with the following functions are supported for ATM ports:

- Extreme Standby Routing Protocol (ESRP)
- Dynamic Link Context System (DLCS)
- Intra-Subnet QoS™ (ISQ)
- Remote Monitoring (RMON)

Table A-4 is an alphabetical list of the existing ExtremeWare commands that are not supported for the ATM module.

**Table A-4: Summary of Commands Not Supported for ATM Ports**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>config gvrp [listen</td>
<td>send</td>
</tr>
<tr>
<td>config mirroring add [vlan &lt;name&gt;</td>
<td>port &lt;port&gt;</td>
</tr>
<tr>
<td>config ports &lt;portlist&gt; auto off [speed [10</td>
<td>100</td>
</tr>
<tr>
<td>config ports &lt;portlist&gt; auto on</td>
<td>This command is an Ethernet-specific command.</td>
</tr>
<tr>
<td>config vlan &lt;name1&gt; [add</td>
<td>delete] ports &lt;portlist&gt; {tagged</td>
</tr>
<tr>
<td>config vlan &lt;name2&gt; protocol &lt;protocol_name&gt;</td>
<td><strong>Usage restrictions apply.</strong> The command config vlan &lt;name&gt; protocol any is supported, because it can be used to configure the default VLAN for ATM ports.</td>
</tr>
<tr>
<td>disable learning ports &lt;portlist&gt;</td>
<td>Learning is always enabled.</td>
</tr>
<tr>
<td>enable dlcs ports &lt;portlist&gt;</td>
<td>No DLCS functions are supported for an ATM port when the port is a member of a VLAN.</td>
</tr>
<tr>
<td>enable esrp vlan &lt;name&gt;</td>
<td>Not supported when an ATM port is a member of the VLAN specified as &lt;name&gt;.</td>
</tr>
</tbody>
</table>
### Table A-4: Summary of Commands Not Supported for ATM Ports (continued)

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>enable isq &lt;name&gt;</code></td>
<td>Not supported when an ATM port is a member of the VLAN specified as <code>&lt;name&gt;</code>.</td>
</tr>
<tr>
<td>`enable mac-vlan mac-group [any</td>
<td>ATM I/O module ports do not support Protocol-Based VLANs or MAC Address VLANs.</td>
</tr>
<tr>
<td>group_number] ports &lt;portlist&gt;`</td>
<td></td>
</tr>
<tr>
<td><code>enable mirroring to &lt;port&gt;</code></td>
<td>Port mirroring is not supported on ATM module ports.</td>
</tr>
<tr>
<td><code>enable sharing &lt;port&gt; grouping &lt;portlist&gt;</code></td>
<td>Load-sharing port groups are not supported for ATM module ports.</td>
</tr>
<tr>
<td><code>enable smartredundancy &lt;portlist&gt;</code></td>
<td>This command is an Ethernet-specific command.</td>
</tr>
<tr>
<td><code>restart ports &lt;portlist&gt;</code></td>
<td>Restarting ports is not supported on ATM module ports.</td>
</tr>
<tr>
<td><code>show ports {&lt;portlist&gt;} collisions</code></td>
<td>This command is an Ethernet-specific command.</td>
</tr>
</tbody>
</table>

1. When `<name>` is a protocol-based VLAN.
2. When an ATM port is a member of the VLAN specified as `<name>`. 
Supported MIBs and Standards

This appendix lists the software standards and management information bases (MIBs) supported in relation to the ATM module.

For a broader list of the software standards supported by ExtremeWare as a whole, see the “Supported Standards” appendix in the ExtremeWare Software User Guide.

This appendix includes information on the following topics:

- ATM Support on page B-2
- SONET/SDH Support on page B-2
- QoS and DiffServ Support on page B-3
ATM Support

This section lists the ATM status and interface counters MIBs that are supported for the ATM module.

MIBs Supported for ATM

The interface counters in MIB-II (RFC 1213) are supported for ATM.

Support for read-only operations (GET operations, but not SET operations) is provided for selected objects in the standard ATM MIB (RFC 2515). Additional MIB objects to support ATM have also been added to the Extreme Networks private MIB.

SONET/SDH Support

This section lists the Synchronous Optical Network/Synchronous Digital Hierarchy (SONET/SDH) related standards and SNMP MIBs that are supported for the ATM module.

Standards Supported for SONET/SDH

The Extreme Networks SONET/SDH implementation complies with the following standards:

- ITU-T G.707 (03/96), Network Node Interfaces for the Synchronous Digital Hierarchy (SDH), March 1996.

MIBs Supported for SONET/SDH

A subset of RFC 2558, Definitions of Managed Objects for the SONET/SDH Interface Type, has been implemented. The Virtual Tributary (VT) group and the Section/Line/Path interval tables were not implemented. Read-only support (GET operations, but not SET operations) has been implemented for the remainder of the MIB.
QoS and DiffServ Support

This section lists the DiffServ-related software standards that are supported for the ATM module.

Standards Supported for DiffServ

The Extreme Networks implementation of RED is based on the well-known paper *Random Early Detection Gateways for Congestion Avoidance*, by Sally Floyd and Van Jacobson. The Extreme Networks implementation of RED also complies with the recommendations published in RFC 2309, *Recommendations on Queue Management and Congestion Avoidance in the Internet*.

The Extreme implementation of DiffServ complies with the following standards:

- RFC 2474: *Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers*
- RFC 2475: *An Architecture for Differentiated Services*
- RFC 2597: *Assured Forwarding PHB Group*
- RFC 2598: *An Expedited Forwarding PHB*
Index

Numerics
802.1p command support 3-25
802.1Q command support 3-25

A
AAL-5 3-2
access list support for ATM module 3-49
AIS-L event counter (SONET) 3-21
AIS-P event counter (SONET) 3-21
alarm indication signal—line (AIS-L) 3-22
alarm indication signal—path (AIS-P) 3-22
Assured Forwarding (AF) PHB 3-40
Asynchronous Transfer Mode. See ATM
ATM 3-2
overview 3-2
port status information, displaying 3-10
receive statistics, summary (table) 3-11
transmit statistics, summary (table) 3-11
ATM Adaption Layer. See AAL-5
ATM module feature summary 1-6
GPP subsystem 1-5
hot-swapping 1-2
installing 2-7
LED indicators 2-10, 2-12
network processors 1-5
troubleshooting 2-10
ATM scrambling, configuring 3-12
default slot configuration 1-2, 3-3
I/O modules 1-2
overview 1-1
slot preconfiguration 1-2
bootrom downloading 3-49

C
cables multimode 2-3
single-mode 2-3
code points assignments, changing 3-33
class selector 3-41
default 3-41
mapping tables, resetting 3-36
mapping, configuring 3-34
replacing 3-36
connectors diagnostic service ports 1-5
optical fiber 2-3
conventions notice icons, Preface xii
text, Preface xiii
CRC 1-8
Cyclic Redundancy Check. See CRC

D
default settings, SONET (table) 3-14
slot configuration 1-2, 3-3
diagnostics 2-12
Differentiated Services Code Points. See DSCP

B
BGP 3-49
BlackDiamond switch
Differentiated Services. See DiffServ

DiffServ

- code points
  - assignments, changing 3-33
  - Assured Forwarding 3-41
  - Class Selector 3-41
  - default 3-41
  - Expedited Forwarding 3-41
  - mapping tables, configuring 3-34
  - mapping tables, resetting 3-36
  - QoS profile mapping assignments (table) 3-33
  - replacement, enabling 3-36
  - commands (table) 3-29
  - configuring 3-33
  - mapping PHBs to QoS profiles (table) 3-41

DLCS A-6

- drop probability (RED), configuring 3-37
- DSCP 1-8
- DSCP mapping 1-9
- DVMRP 3-49

Dynamic Link Context System. See DLCS

E
electrostatic discharge (ESD), preventing damage 2-4

ESRP A-6

- Expedited Forwarding (EF) PHB 3-40
- Extreme Standby Routing Protocol. See ESRP

ExtremeWare
  - base version identifier 2-2
  - technology release versions 2-2

F

FDB 3-28

G

Generic VLAN Registration Protocol. See GVRP

GPP subsystem 1-5

GVRP 3-28, A-6

H

hardware version requirements 2-2

- high drop precedence 3-41

I

IGMP, support for ATM module image
  - commands, changed (table) 3-49
  - downloading 3-50
  - primary or secondary, using 3-50

installation
  - air-flow requirements and slot assignments 2-5
  - connecting network interface cables 2-9
  - inserting and securing a module 2-7
  - slot locations (figure) 2-6
  - tools 2-4
  - verifying operation 2-10
  - version requirements, software and hardware 2-2

Intra-Subnet QoS. See ISQ

IPX 3-49

ISQ A-6

J

jumbo frame support 1-8

L

LED indicators 2-10

- line parity errors (SONET) 3-21
- LOF event counter (SONET) 3-21
- Logical Link Control. See LLC
- LOP event counter (SONET) 3-21
- LOS event counter (SONET) 3-21
- loss of frame (LOF) 3-22
- loss of pointer (LOP) 3-22
- loss of signal (LOS) 3-21
- low drop precedence 3-41

M

MAC-based VLANs 3-24, A-6, A-7

- medium drop precedence 3-41
- minimum queue length threshold (RED), configuring 3-39

N

network processors 1-5

O

OAM 3-2

Operations, Administrations and Maintenance. See OAM

optical interfaces
  - Class 1 laser device (warning) 2-4
  - OC-3c/STM-1 single-mode 1-3, 2-3
  - optical safety precautions 2-4
  - optical-fiber cable connections 2-9
  - OSPF 3-49
  - Overview
    - ATM module (figure) 1-4
P

path parity errors (SONET) 3-21
path payload label mismatch (PLM-P) 3-23
payload data scrambling 3-12
payload data scrambling, configuring 3-12
per-hop behaviors. See PHBs
Permanent Virtual Circuits. See PVC
PHBs
   Assured Forwarding (AF) 3-40
   Assured Forwarding classes (table) 3-41
   Class Selector 3-41
   Default 3-41
   drop precedence levels (table) 3-41
   Expedited Forwarding (EF) 3-40
   support and configuration 3-40
PIM 3-49
PLM-P event counter (SONET) 3-21
   port
      commands, changed (table) 3-47
      SONET commands (table) 3-15
   precedence levels 3-41
   protocol-based VLANs 3-24, A-6, A-7
PVC
   port status information, displaying 3-11
Q

QoS
   802.1p and 802.1Q support 3-25
      configuring 3-29
      DiffServ support functions 1-8, 3-29
      profile, configuring 3-30
      RED support 3-29
      support overview 1-6
QoS monitor 3-44
Quality of Service. See QoS
R

Random Early Detection. See RED
RDI-L event counter (SONET) 3-21
RDI-P event counter (SONET) 3-21
RED
   commands (table) 3-29
   configuration information, displaying 3-44
   drop probability, configuring 3-37
   enhancements for ATM support 3-36
   minimum queue length threshold, configuring 3-39
   operation compared to WRED (figure) 3-37
   PHB support 3-40
   ports, enabling and disabling 3-39
REI-L event counter (SONET) 3-21
REI-P event counter (SONET) 3-21
remote defect indicator—line (RDI-L) 3-22
remote defect indicator—path (RDI-P) 3-22
remote error indicator—line (REI-L) 3-22
remote error indicator—path (REI-P) 3-22
Remote Monitoring. See RMON
RIP 3-49
RMON A-6
S

safety information 2-3
SAP 3-49
SD BER event counter (SONET) 3-21
SDH 1-7
section parity errors (SONET) 3-21
SF BER event counter (SONET) 3-21
signal degrade bit error rate (SD BER) 3-23
signal failure bit error rate (SF BER) 3-23
software
      checking version compatibility 2-2
      downloading packages 2-2
      technology release version identifier 2-2
      version requirements 2-2
SONET
      clock source 3-14, 3-16
      configuration parameter values, resetting 3-20
      configuration parameter values, summary (table) 3-14
      error and alarm events (table) 3-21
      framing type 3-14, 3-16
      overview 1-7
      Path Trace identifier 3-15, 3-18
      port configuration commands (table) 3-15
      port status information, displaying 3-20
      Section Trace byte 3-14, 3-18
      Section Trace identifier 3-15, 3-18
      Signal Degrade threshold 3-14, 3-17
      Signal Fail threshold 3-14, 3-17
      Signal Label 3-15, 3-19
      statistics (table) 3-21
Spanning Tree Protocol. See STP
STP
      ExtremeWare commands 3-28
      support 3-28
SVC 3-2
Switched Virtual Connection. See SVC
Synchronous Digital Hierarchy. See SDH
Synchronous Optical Network. See SONET
T

tag mapping 3-26
tag nesting 3-27
technology release version identifier 2-2
tools for installation 2-4
troubleshooting 2-10
U
upgrading the ATM module BootROM image 2-15
upgrading the ATM module image 2-14
upgrading the switch image 2-14

V
VC 3-2
virtual circuit identifier 3-2
Virtual Circuit. See VC
virtual path identifier 3-2
VLANs
configuration commands (table) 3-24
tag mapping 3-26
tag nesting 3-27
tagged VLAN 802.1p and 802.1Q functions 3-25

W
Weighted RED. See WRED
WRED
drop probability 3-34, 3-36, 3-37
operation compared to RED (figure) 3-37
# Index of Commands

| C | clear counters 3-46, A-5  
|   | config atm add pvc 3-9, A-2  
|   | config atm delete pvc 3-10, A-2  
|   | config atm scrambling 3-12, A-2  
|   | config diffserv dscp-mapping 3-29, 3-35, A-2  
|   | config diffserv examination code-point 3-29, 3-34, A-4  
|   | config diffserv replacement priority 3-36  
|   | config dot1p type 3-25  
|   | config dot1q ethertype 3-25  
|   | config dot1q tagmapping 3-24, 3-26, A-2  
|   | config dot1q tagnesting 3-24, 3-27, A-2  
|   | config gvrp 3-28, A-6  
|   | config mirroring add 3-46, A-6  
|   | config ports auto off 3-46, A-6  
|   | config ports auto on 3-46, A-6  
|   | config qosprofile 3-30, 3-31, A-4  
|   | config red 3-30, 3-37, A-4  
|   | config red min-threshold 3-30, A-2  
|   | config red min-threshold ports 3-39  
|   | config slot 3-45, A-4  
|   | config sonet clocking 3-15, 3-16, A-2  
|   | config sonet framing 3-15, 3-16, A-2  
|   | config sonet signal label 3-15, 3-19, A-2  
|   | config sonet threshold signal degrade 3-15, 3-17, A-3  
|   | config sonet threshold signal fail 3-15, 3-17, A-3  
|   | config sonet trace path 3-15, 3-19, A-3  
|   | config sonet trace section 3-15, 3-18, A-3  
|   | config vlan add ports A-6  
|   | config vlan delete ports A-6  
|   | config vlan protocol A-6  
|   | config vlan protocol any 3-25, A-6 |

| D | disable jumbo-frame A-5  
|   | disable learning ports 3-46, A-6  
|   | disable ports 3-47, A-5  
|   | disable red A-4  
|   | disable red ports 3-30, 3-39  
|   | download bootrom 3-49, A-4  
|   | download image 3-50, A-4 |

| E | enable diffserv examination ports 3-33  
|   | enable diffserv replacement ports 3-36  
|   | enable jumbo-frame A-5  
|   | enable mac-vlan A-7  
|   | enable mirroring 3-46  
|   | enable mirroring to A-7  
|   | enable ports 3-47, A-5  
|   | enable red A-4  
|   | enable red ports 3-30, 3-39  
|   | enable sharing 3-46, A-7  
|   | enable smartredundancy 3-46, A-7 |

| R | reboot 3-46, A-4  
|   | restart ports A-7  
|   | run diagnostics 3-46 |

| S | show atm 3-10, A-3  
|   | show atm pvc 3-11, A-3 |
show diag 3-46, A-5
show ports collisions 3-46, A-7
show ports info 3-36, 3-47, A-5
show ports info detail 3-30
show ports qosmonitor 3-47, A-4
show ports rxerrors 3-47, A-5
show ports txerrors 3-47, A-5
show slot 2-10, 3-45, A-5
show sonet 3-16, 3-20, A-3
show version 3-45, A-5

U
unconfig diffserv dscp-mapping 3-30, A-3
unconfig diffserv dscp-mapping ports 3-36
unconfig sonet A-3
unconfig sonet ports 3-16, 3-20
use image 3-50, A-4