



**Riverstone Networks Switch Router  
System Firmware Version 8.0.3.13  
October 2003**

**INTRODUCTION:**

This document provides specific information for version 8.0.3.13 and 8.0.3.13L of the system firmware for the Riverstone Networks RS Switch Router family of products.

It is recommended that one thoroughly review this release note prior to the installation or upgrade of this product.

**FIRMWARE SPECIFICATION:**

Before installing the 8.0.3.13 firmware, upgrade the Boot PROM image on the RS Switch Router to Boot PROM version 2.0.1.3. Refer to the RS Switch Router Getting Started Guide for instructions on loading the boot PROM software. The 8.0.3.13 code release will not fit onto an 8 MB PCMCIA Flash Card. The 8.0.3.13L release will fit onto an 8-MB flash, but does not support CMTS or ATM OC-12 line cards. If you do not have 16 MB of flash memory, do not attempt downloading the 8.0.3.13 software. It is highly recommended that the system be upgraded to 16 MB of flash memory at a minimum.

Firmware Image Name	Version No.	Type	Release Date
ros80313(L)	8.0.3.13(L)	Patch (Lite)	October 2003
ros80312(L)	8.0.3.12(L)	Patch (Lite)	June 2003
ros80311(L)	8.0.3.11(L)	Patch (Lite)	February 2003
ros80310(L)	8.0.3.10(L)	Patch (Lite)	December 2002
ros8039(L)	8.0.3.9(L)	Patch (Lite)	October 2002
ros8038(L)	8.0.3.8(L)	Patch (Lite)	September 2002
ros8037(L)	8.0.3.7(L)	Patch (Lite)	July 2002
ros8036(L)	8.0.3.6(L)	Patch (Lite)	May 2002
ros8035(L)	8.0.3.5(L)	Patch (Lite)	April 2002
ros8034(L)	8.0.3.4(L)	Patch (Lite)	March 2002
ros8033(L)	8.0.3.3(L)	Patch (Lite)	February 2002
ros8032(L)	8.0.3.2(L)	Patch (Lite)	February 2002
ros8031	8.0.3.1	Patch	January 2002
ros8030(L)	8.0.3.0(L)	Maintenance (Lite)	December 2001

Version numbers explained	
Version number	Description
ros 8 0 3 x - A 0 1	Five part version number (ros - Rapid Operating System, commonly known as RapidOS)
└	Test release version number (digit 2)
└	Test release version number (digit 1)
└	Test Phase: A = Alpha, B = Beta, C = Control Release, S = Special, Blank = Released, Generally Available (GA)
└	Patch releases number - Bug fixes- fully supported for production network environments.
└	Maintenance releases number - Bug fixes and minor functionality changes - fully supported for production network environments. (Extensive regression testing of all bug fixes in prior patch releases).
└	Minor release number - significant functional changes and performance improvements. (Beta testing and Extensive regression testing of all bug fixes in prior patch releases).
└	Major release number - Major functional / architectural changes. (Beta testing and Extensive regression testing of all bug fixes in prior patch releases).

**Alpha Test Code** - Riverstone Internal use only, Not supported for ANY Customer environment.

**Beta Test Code** - This firmware should be used in a test environment, by official Beta test sites only. This Firmware is not for production use.

**Controlled Release Code** - For use in production networks (supported for 2-4 weeks from date of build). This firmware is for customers with pre-arranged agreement with Riverstone to use the controlled release.

**Special Release** - Customer solution verification only - supported by Riverstone Engineering for specific customer network environment, no other installations will be supported!



#### ADDITIONAL INFORMATION:

Visit the Riverstone Networks Support page to view the most current hardware compatibility matrix, phase of the firmware life cycle, feature release matrix and other information can be found at:

[http://www.riverstonenet.com/support/support\\_docs.shtml](http://www.riverstonenet.com/support/support_docs.shtml)

#### FIRMWARE CHANGES AND ENHANCEMENTS AND NOTES:

##### Note: New Rate Limit commands

Addition to 8.0.3 user docs... The 'system set rate-limit-range' and 'system show rate-limit-range' commands have been added to the 8.0.3.9 release.

##### Note: Adding new system images to the RS Flash Memory

When upgrading the system image on the RS flash, using the command "system image add ...", it is normal for the CPU to run at 100% utilization. The task used to download the new image and write it to the Flash memory runs at a relatively low priority; therefore it consumes all available CPU time that is not required for any other router operations.

##### Features and Enhancements in 8.0.3.6 Firmware:

A new CLI configuration mode command was added in 8.0.3.5 but is officially supported in this release, the command is:

```
rs(configs)# ip enable local-proxy-arp interface xyz
```

This command is used to configure the router to provide Proxy-ARP services when the source and destination IP addresses are on the same interface. This feature can be used in the event some client system can only be configured with a default gateway, but is unable to determine the extent of the subnet of which it is a part.

##### Features and Enhancements in 8.0.3.4 Firmware:

Command: The command "wan set message-log..." can be used to define and limit the number of console / syslog messages that are reported by the WAN cards.

wan set message-log - Set message log parameters

- level - Minimum message reporting level (default info)
  - error - Report Fatal and Error messages only
  - fatal - Report Fatal messages only
  - info - Report ALL messages
  - warning - Report Fatal, Error and Warning messages only
- mode - Message logging mode (default enable)
  - disable - Disable message logging
- slot - Number of the slot
  - number - Value between 1 and 16, inclusive
- suppression - Message logging suppression (default enable)
  - disable - Disable message logging suppression

Customer Use:



## CUSTOMER RELEASE NOTES

The "wan set message-log" command allows the Riverstone WAN customer more granular control over the message logging facility for Riverstone WAN cards. This command controls the events that are logged to the Riverstone Control Module (CM) which can be further processed by the CM with existing facilities such as "system set console level", "system set console limit" and "system set syslog level."

### Level Control:

By default, all categories of messages are streamed from the WAN card to the CM including fatal, error, warning and informational message types. Using the "wan set message-log level" command, the customer can limit which types of messages are processed by the CM. It is recommended that error and fatal messages are never suppressed, suggesting that the level should normally be set to either info (default), warning, or error.

### Mode Control:

By default, the mode of the message logging facility is enabled, but if the customer wishes to turn it off completely, the mode should be set to disable. It is recommended that this be used in a temporary fashion, meaning the mode should be returned to enable when the need to disable the facility has passed.

### Suppression Control:

By default, message suppression, also referred to as summarization, is enabled. Suppression is used to limit the number of the same messages from being streamed to the CM. When messages are sent to the CM, they are checked against previous messages sent. If the same message is constantly being sent, the first three messages are sent, followed by a five minute summarization of the number of these same messages that are sent. After the five minute interval, the process is repeated (i.e. another three messages are sent followed by a five minute summarization.) If the customer wishes to see all of the messages in a non-summarized fashion, then the suppression option should be set to disable.

## Features and Enhancements in 8.0.3.3 Firmware:

### New Hardware Routing Table (HRT) show commands

#### 1. hrt show summary

```
rs# hrt show summary
HRT Summary:
-----
HRT is globally enabled
This RS platform is operating in HRT v1
HRT Memory Size : 7936 KB
HRT Memory Free : 7912 KB
```

#### 2. hrt show ports all-ports

```
rs# hrt show ports all-ports

HRT Port Information:
-----
This RS platform supports HRT v1
HRT is administratively enabled on slots: None
Legend:
NA: HRT feature not available on this port
```

Port	HRT Ver Supported	Ver Running	HRT Enabled	Reason Disabled
gi.6.1	--NA--	-	-	-
gi.6.2	--NA-	-	-	-
so.11.1	HRT v1	HRT v1	NO	Administratively
so.11.2	HRT v1	HRT v1	NO	Administratively
et.12.1	--NA--	-	-	-
et.12.2	--NA--	-	-	-
et.12.3	--NA--	-	-	-
et.12.4	--NA--	-	-	-

## Features and Enhancements in 8.0.3.2 Firmware:

### Changes to Custom Forwarding

In this release, custom forwarding wildcards are not applied to flows sent to the CPU for processing. Wildcards are applied only to flows that reside on line cards. Because of this, service ACLs can now be used with custom forwarding.

### Changes to IP DOS

The **ip dos rate-limit** command now supports additional protocol types. These additional types are:

- HTTP
- SSH
- SNMP
- Telnet

### Changes to Per VLAN Spanning Tree (PVST)

### Change in default behavior

There is a change in the behavior of PVST, default destination MAC address used by PVST BPDU's has changed. For backward compatibility with previous versions of the ROS firmware, the command

“pvst set special-encap”

can be used to force the use of the old PVST BPDU destination MAC address.

## Features and Enhancements in 8.0.3.0 Firmware:

This document contains information regarding new RS Switch Router software and hardware features associated with release 8.0.3.0.

1. VLAN Translation
2. BOOT BACKUP FILE
3. BACKUP SYSTEM IMAGE
4. BACKUP CONFIGURATION FILE
5. BOOTPROM ESCAPE CHARACTER
6. SYSLOG FEATURES
7. DHCP Relay Agent for Flat Layer-4 Bridged VLANs
8. New WAN Rate Shaping Feature
9. New Command to Display MAC Addresses Stored on WAN Line Cards
10. Support for IGMP and DVMRP on ATM OC-3c Ports
11. New Command for Tracing Frame Relay Connections
12. New Command for Changing Mastership of Redundant Control Modules
13. Change in Statistics Show Port-Errors Command
14. OSPF Commands for Multicast Compatibility
15. Non-MPLS Gigabit Ethernet GBIC Line Card
  - a. GBIC modules
16. Additional new commands and output
  - a. `bgp set bad-aspath <discard | ignore>`
  - b. `ip-router show filter name <expression>`
  - c. `l2-tables show port-macs port`
17. Bootprom Variables – Change in default functionality
18. OSPF Reference Bandwidth

## 1. VLAN Translation

Metro service providers are often faced with the need to translate one VLAN ID (VID) to another. On the RS, you can configure a VLAN translation filter to translate a frame's VID to another VID, and forward traffic to a specified set of ports.

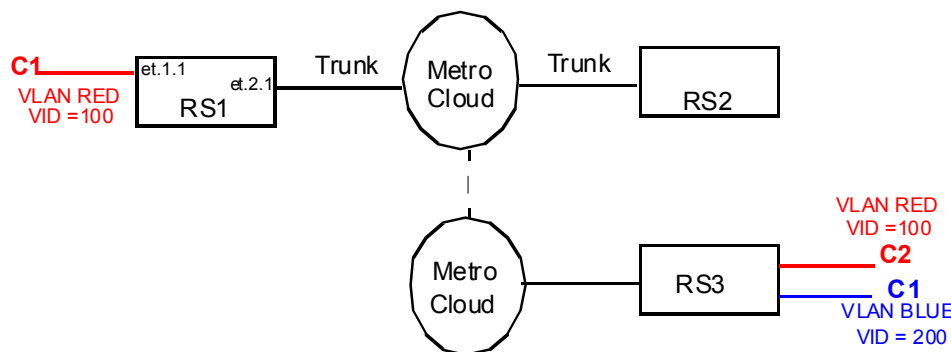
The VLAN translation filter specifies the input port(s) and input VLAN ID, the output port(s) and the output VLAN ID, and the destination and/or source MAC address. VLAN translation filters are configured and applied at the input port. Then when the input port receives a frame to be bridged that matches the filter, it switches the frame's VID to the output VID and forwards the frame to the specified output port(s).

When you configure the filter, you can also specify that the reverse mapping be applied to traffic flowing in the opposite direction (i.e., the input port becomes the output port and the input VLAN becomes the output VLAN), enabling the reverse traffic to be forwarded accordingly.

### Configuration Examples

Following are typical scenarios in which VLAN translation is used. In the first example, one VLAN translation filter is used to translate the VID of frames flowing in both directions of traffic. In the second example, a different filter is applied in each direction of traffic.

In the following diagram, the metro provider assigned Customer 1 (C1) to VLAN RED (VID = 100) on RS1 and to VLAN BLUE (VID = 200) on RS3. The metro provider previously assigned Customer 2 (C2) to VLAN RED on RS3.



The two metro clouds are then connected, resulting in the provider having two different customers (C1 and C2) with the same VID on the same MAN. The metro provider could reassign the VIDs so they do not overlap. But this would require the customers to change their configurations. The more efficient alternative is to configure a VLAN translation filter and apply it to port et.1.1 on RS1.

Following is the configuration for RS1:

*Configure VLAN RED and add ports to it.*

```
rs(config)# vlan create red ip id 100
rs(config)# vlan make trunk port et.2.1
rs(config)# vlan add ports et.1.1,et.2.1 to red
```

*Configure the VLAN translation filter.*

```
rs(config)# filters add vlan-switching name c1 input-port-list et.1.1 output-port-list et.2.1 input-vlan 100 output-vlan 200 dest-mac any reverse-mapping policy-id 100
```

## CUSTOMER RELEASE NOTES

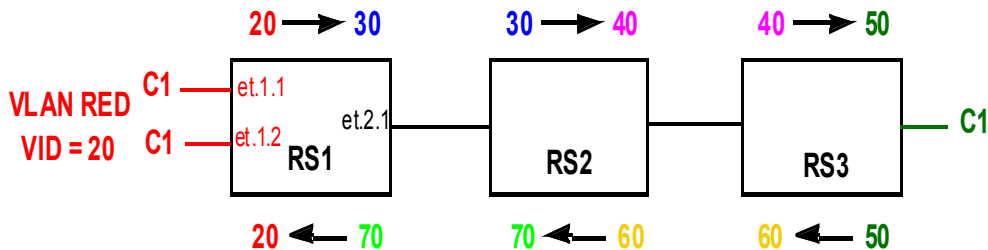
When port et.1.1 receives frames that match the configured filter, it switches the frames' VID from 100 to 200 and forwards the frames to et.2.1. The reverse mapping parameter in the filters add vlan-switching command specifies that VLAN translation is also applied to the traffic in the reverse direction. Thus, when port et.2.1 receives frames to be bridged with a VID of 200, it switches the VID to 100 and forwards it to port et.1.1.

Use the filter show vlan-switch command to display information about the translated VLANs.

```
rs# filters show vlan-switch in-vlan 100
```

```
Name:      100
-----
Direction: flow
Restriction: allow-to-go
In VLAN:   100
Out VLAN:  200
Mac VLAN:  4195
Source MAC: any
Dest MAC:  any
In-List ports: et.1.1
Out-List ports: et.2.1
```

In the following example, the VIDs are treated similar to MPLS transport labels. On RS1, ports et.1.1 and et.1.2 belong to VLAN RED, which has a VID of 20. The VID of incoming frames on these ports is translated from 20 to 30, while the VID of the reverse traffic coming in on port et.2.1 is translated from 70 to 20.



In the example, a different VLAN translation filter is applied to each direction of traffic; traffic flowing in one direction uses a VLAN translation scheme that is different from the one used in the reverse direction. Following is the configuration for RS1:

**Configure the VLANs and add ports to them.**

```
rs(config)# vlan create red ip id 20
rs(config)# vlan add ports et.1.(1,2) to red
rs(config)# vlan add ports et.2.1 to red
rs(config)# vlan make trunk port et.2.1
```

**Configure the VLAN translation filters; one for each direction of traffic. In this case, the reverse-mapping parameter is not specified.**

```
rs(config)# filters add vlan-switching name c100a input-port-list et.1.(1,2) output-port-list et.2.1 input-vlan 20 output-vlan 30
policy-id 100
rs(config)# filters add vlan-switching name c100b input-port-list et.2.1 output-port-list et.1.(1,2) input-vlan 70 output-vlan 20
policy-id 200
```

### Restrictions

Note the following restrictions on configuring and using VLAN translation:

1. VLAN translation and VLAN stacking cannot be implemented on the same ports.
2. You cannot enable L4 bridging on a VLAN to which a VLAN translation filter is applied.
3. VLAN translation is not supported on ports that are running MPLS.
4. When used with other L2 filters, the L2 filters are applied to the input VID only, and not to the

translated VID.

5. VLAN translation is supported on Ethernet line cards only.
6. VLAN translation filters cannot translate customer BPDUs.
7. You cannot apply to the same input port two or more VLAN translation filters mapped to the same translated VLAN.

## 2. Boot Backup File

The RS can boot from the **PC flash card**, from a **TFTP server**, or from a **BootP/TFTP server**. When you set the RS to boot from a TFTP server, you can specify both a primary and a backup TFTP server. Use the system set bootprom command in Enable mode to set the IP address for both servers. When you reboot the RS, it first tries to boot from the primary TFTP server. If that server is unavailable, the RS automatically tries to boot from the backup TFTP server.

The following example specifies the IP addresses of the primary and backup TFTP servers.

```
rs# system set bootprom tftp-server 192.128.172.5 backup-tftp-server 192.128.178.5
```

To view the boot PROM parameters and verify the IP addresses of the TFTP servers, use the system show bootprom command as shown in the following example

```
rs# system show bootprom
Boot Prom's parameters for TFTP network booting:
Network address       : 192.128.172.30
Network mask         : 255.255.255.0
TFTP server          : 192.128.172.5
Gateway to reach TFTP server : 0.0.0.0
Backup TFTP server    : 192.128.178.5
Primary bootsource    : /ros8030
Backup bootsource     : /backup/ros8030
```

*The following example shows the messages displayed on the console as the RS boots up. It tries to boot from the primary TFTP server (192.128.172.5). When it is unable to do so, it boots from the backup TFTP server (192.128.178.5).*

```
Autoboot in 2 seconds - press RETURN to abort and enter prom
```

```
primary source: tftp://192.128.172.5/backup/ros8030
couldn't open 192.128.172.5:backup/ros8030 for reading
Kernel not found or lost in transmission
secondary source: tftp://192.128.178.5/backup/ros8030
File: version (874 bytes)
Build location: host 'cmbuild0' by 'mhaydt'

Version: 8.0.3.0
```

For even greater redundancy, you can specify a primary and backup system image. Use the system set bootprom command in Enable mode to specify both the primary and secondary system image files. When you reboot the RS, it tries to boot the primary system image from the primary and backup TFTP servers. If that fails, the RS tries to boot the backup system image from the primary and backup TFTP servers.

The following example specifies the primary and backup system images.

```
rs# system set bootprom primary-image rs8030
rs# system set bootprom backup-image /backup/ros8030
```

Use the system show bootprom command to display your settings:

```
rs# system show bootprom
Boot Prom's parameters for TFTP network booting:
Network address       : 192.128.172.30
Network mask         : 255.255.255.0
TFTP server          : 192.128.123.3
```



```
Gateway to reach TFTP server      : 0.0.0.0
Backup TFTP server                : 192.128.178.5
Primary bootsource                : /rs8030
Backup bootsource                 : /backup/ros8030
```

The following example shows the messages the RS displays on the console as it tries to boot the system image software.

```
Autoboot in 2 seconds - press RETURN to abort and enter prom
primary source: tftp://192.128.123.3/rs8030
couldn't open 192.128.123.3:rs8030 for reading
  Kernel not found or lost in transmission
secondary source: tftp://192.128.178.5/rs8030
couldn't open 192.128.178.5:rs8030 for reading
  Kernel not found or lost in transmission
primary source: tftp://192.128.123.3/backup/ros8030
couldn't open 192.128.123.3:backup/ros8030 for reading
  Kernel not found or lost in transmission
secondary source: tftp://192.128.178.5/backup/ros8030
File: version (874 bytes)
Build location: host 'cmbuild0' by 'mhaydt'
Version: 8.0.3.0
```

As shown in the example, the RS tried to boot the primary system image (rs8030) from the primary TFTP server (192.128.123.3), and then from the backup TFTP server (192.128.178.5). When the RS was unable to boot the primary image, it tried to boot the backup system image (qa/ros8030) from the primary TFTP server, and then from the backup TFTP server.

Note1: If the RS has a backup Control Module (CM), changes made to the primary CM using the **system set bootprom** command are not automatically propagated to the backup CM. You must specify this command on the backup CM as well.

Note2: There is a slight change in the boot procedure in 8.0.3.x and boot PROM 2.0.1.3, if the "startup" file is missing, then the system will use "startup.bak", if one is present in int-flash. This is a change from previous behavior, in which if "startup" was missing, the system boots with no config.

This affects the password recovery procedure – when attempting to boot the router it will be necessary to delete both "startup" and "startup.bak" files.

The names of those config files (primary and backup) can now be specified, using

```
system set sys-config primary <primary_config_file>
system set sys-config secondary <backup_config_file>
```

### 3. Backup System Image

Use the system image choose command to specify the system software image on the PC card that the RS will use the next time you reboot the system. Use the **system image secondary-choose** command to specify a secondary system image. When the RS boots, it will try to use the primary software image on the PC card. If for some reason the RS cannot use that file, then it automatically uses the secondary software image file. The following example specifies the secondary image in the backup Control Module:

```
rs# system image secondary-choose rs90c backup-cm
```

Note: If the RS has a backup CM, changes made to the primary CM using the **system image** command are not automatically propagated to the backup CM. You must specify this command on the backup CM as well.

### 4. Backup Configuration File

When the RS boots up, it uses the startup configuration file to configure itself. Use the system set sys-config command in Enable mode to specify both a primary and secondary configuration file. When the RS boots, it will try to use the primary

configuration file. If for some reason the RS cannot use the file, then it automatically uses the secondary configuration file. Following is an example:

```
rs# system set sys-config primary config_a secondary config_b
```

## 5. Bootprom Escape Character

When you boot the RS, you can interrupt the normal boot process and enter Boot mode. By default, you would do this by pressing the “Esc” key. You can change this default and use a character instead of the “ESC” key to interrupt the boot process. Use the **system set bootprom** command in Enable mode to specify the character, then save the command to the startup configuration file. In the following example, the character “x” is specified.

```
rs# system set bootprom esc-char x
```

Therefore, when the RS reboots and the character “x” is typed, the RS will interrupt its boot process and enter Boot mode. To change back to the default, enter the system set bootprom command with the keyword **ESC** as shown in the following example:

```
rs# system set bootprom esc-char ESC
```

## 6. SYSLOG Features

Normally, the RS does not save a copy of the SYSLOG messages in the internal flash of the RS. Specify the local\_copy parameter of the **system set syslog** command to save the last n messages in internal flash.

```
rs(config)# system set syslog local_copy
```

The RS stores a certain number of SYSLOG messages in its local buffer. Use the **buffer-size** parameter of the **system set syslog** command to specify how many messages the RS should store. The RS can store from 10 to 200 SYSLOG messages in its local buffer. The following example specifies that the RS should store 125 messages:

```
rs(config)# system set syslog buffer size 125
```

## 7. DHCP Relay Agent for Flat Layer-4 Bridged VLANs

The RS switch routers support DHCP relay agent (also known as Option 82) functionality across layer-2 bridged VLANs, which are also running layer-4 bridging.

On a VLAN where the relay agent is enabled, a *circuit ID* is attached to the packets. The circuit ID consists of the RS’ base MAC address, the port number on which the packet was received, and the VLAN on which the packet was received.

When the relay agent is enabled, packets that already contains relay agent information are dropped on the assumption that the information was fabricated by the DHCP client. Also, if the packet will become too large if the relay agent information is added, the packet is forwarded without adding the relay agent information.

Relay agent information contained within DHCP OFFER and DHCP ACK packets is stripped off to keep the DHCP client from seeing it.

The following is an example of activating the DHCP relay agent on a newly created VLAN:

```
rs(config)# vlan create op82 ip
rs(config)# vlan add port et.5.1 to op82
rs(config)# vlan enable l4-bridging on op82
rs(config)# ip helper-address relay-agent-info circuit-id mac-port-vlan vlan op82
```

Note: Notice that layer-4 bridging must be enabled on the VLAN for the relay agent to work.

## 8. New WAN Rate Shaping Feature

Support has been added in this release to allow WAN rate shaping parameters to be applied collectively to several source IP addresses, destination IP addresses, or VLANs.

**CUSTOMER RELEASE NOTES**

For example, prior to this release, the following command lines configure 10.1.1.1 and 10.1.1.2 to both use a CIR of 128 Kbps:

```
rs(config)# wan define rate-shape-parameters RS1 cir 128000
rs(config)# wan apply rate-shape-parameters RS1 port se.2.1 source-ip-address 10.1.1.1
rs(config)# wan apply rate-shape-parameters RS1 port se.2.1 source-ip-address 10.1.1.2
```

In the example above, line-1 (10.1.1.1) and line-2 (10.1.1.2) are each rate shaping a separate CIR of 128 Kbps.

The new rate shaping parameter, **bandwidth-shared**, provides a way to make line-1 and line-2 collectively rate shape a CIR of 128 Kbps.

For example:

```
rs(config)# wan define rate-shape-parameters RS1 cir 128000 bandwidth-shared
rs(config)# wan apply rate-shape-parameters RS1 port se.2.1 source-ip-address 10.1.1.1
rs(config)# wan apply rate-shape-parameters RS1 port se.2.1 source-ip-address 10.1.1.2
```

In the example above, the keyword, **bandwidth-shared**, causes line-1 (10.1.1.1) and line-2 (10.1.1.2) to share a CIR of 128 Kbps, and collectively rate shape the bandwidth across the two lines.

## 9. New Command to Display MAC Addresses Stored on WAN Line Cards

A new WAN command (**mac-table**) has been added to display the contents of the layer-2, MAC addresses table on the WAN line-cards. To use this command, the slot within which the WAN line card resides must be specified.

The following is an example of the **mac-table** command applied to a T3 module residing in slot 4:

```
rs# wan show mac-table slot 4
-----
Id      MAC          VLAN  Source Port  VC
-----
1  00:02:02:02:02:02  2    t3.4.1.1    102
2  00:01:01:01:01:01  2    t3.4.1.1    101
```

## 10. Support for IGMP and DVMRP on ATM OC-3c Ports

Support has been added to allow IGMP and DVMRP to be enabled on an interface whose members include ATM OC-3c ports. Subsequently, ATM OC-3c ports and their VCLs now appear within the **igmp show membership** command output.

## 11. New Command for Tracing Frame Relay Connections

Support has been added in Enable mode that allows the RS to trace Frame Relay control packets (LMI and DCP) on specified ports. The **frame-relay show trace** command is useful for debugging frame-relay circuits. By enabling packet tracing, traffic on a specified frame relay link is displayed on the console.

The following, lists the keywords and parameters used with the **frame-relay show trace** command.

- **ctl-packet-trace** – Specifies tracing on control packets (supports LMI and DCP only).
  - **on** – Keyword, enables control packet tracing.
  - **off** – Keyword, disables control packet tracing.
- **max-packets-displayed** – Optional field that specifies how many control packets to display. Once the maximum is reached (default value is 60 packets), the packet tracing feature disables itself. If a 0 is entered, the trace runs continuously until the user turns it off.
- **packet-trace-level** – Optional field that specifies the level of detail that gets displayed to the user.
  - **normal** – Compresses important information to a couple of lines.
  - **verbose** – Decodes all information and formats it on separate lines.
  - **hex-only** – Shows only the raw hex data of the packets.
- **ports** – Required field that specifies on which ports to trace.

The following is an example of the output from the frame-relay show trace command:

```
rs# frame-relay show trace ctl-packet-trace on ports t1.4.3:1

Port 3 vc 0 FR Ingress, Unicast, DLCI 0, Status Enquiry, Full, Annex D, Tx Seq 7, Rx Seq 6
Port 3 vc 0 FR Egress, Unicast, DLCI 0, Status, Full, Annex D, Tx Seq 7, Rx Seq 7
  DLCI 100: N=1 A=0
  DLCI 200: N=1 A=0
Port 3 vc 0 FR Ingress, Unicast, DLCI 0, Status Enquiry, LIV, Annex D, Tx Seq 8, Rx Seq 7
Port 3 vc 0 FR Egress, Unicast, DLCI 0, Status, LIV, Annex D, Tx Seq 8, Rx Seq 8
Port 3 vc 0 FR Ingress, Unicast, DLCI 0, Status Enquiry, LIV, Annex D, Tx Seq 9, Rx Seq 8
Port 3 vc 0 FR Egress, Unicast, DLCI 0, Status, LIV, Annex D, Tx Seq 9, Rx Seq 9
Port 3 vc 0 FR Ingress, Unicast, DLCI 0, Status Enquiry, LIV, Annex D, Tx Seq 10, Rx Seq 9
Port 3 vc 0 FR Egress, Unicast, DLCI 0, Status, LIV, Annex D, Tx Seq 10, Rx Seq 10
Port 3 vc 0 FR Ingress, Unicast, DLCI 0, Status Enquiry, LIV, Annex D, Tx Seq 11, Rx Seq 10
Port 3 vc 0 FR Egress, Unicast, DLCI 0, Stat LIV, Annex D, Tx Seq 11, Rx Seq 11
```

## 12. New Command for Changing Mastership of Redundant Control Modules

Entering the Enable mode command, system redundancy change-mastership immediately changes the backup Control Module (CM) to the primary CM. The original CM is rebooted and is brought back up as the backup CM.

## 13. Change in Statistics Show Port-Errors Command

The Enable mode command, **statistics show port-errors**, displays **N/A** (Not Applicable) for the parameter, **Input VLAN dropped frames** for all 10/100 Ethernet ports, HSSI ports, 2-port and 4-port serial cards, and CMTS ports.

The following is an example of the output of the statistics show port-errors command:

```
rs# statistics show port-errors et.1.4

Port: et.1.4
----
Error Stats                               Error Stats
CRC errors                                0          Carrier sense errors          0
Single collision (tx OK)                   0          Many collisions (tx OK)     0
Many collisions (drop)                     0          Late collisions               0
Long frames >1518 bytes                    0          Invalid long frames          0
Short frames <64 bytes                     0          Alignment errors             0
Deferred transmissions                     0          Transmit underruns           0
IP - bad version                           0          IP - bad checksum            0
IP - bad header                           0          IP - small datagram          0
IP - expand TTL ring                       0          IPX - bad header             0
Non-IP/IPX protocol                       0          Invalid MAC encap.           0
Internal frame tx error                    0          Internal frame rx error       0
Input buffer overflow                      0          Packet request overflow       0
Out buffer (low) ovflow                    0          Out buffer (med) ovflow       0
Out buffer (high) ovflow                   0          Out buffer (ctrl) ovflow      0
Input VLAN dropped frames N/A              0          Output VLAN dropped frames    0

Error stats cleared * Never Cleared *
```

Note: the **N/A** for **Input VLAN dropped frames**, near the bottom of the display.

## 14. OSPF Commands for Multicast Compatibility

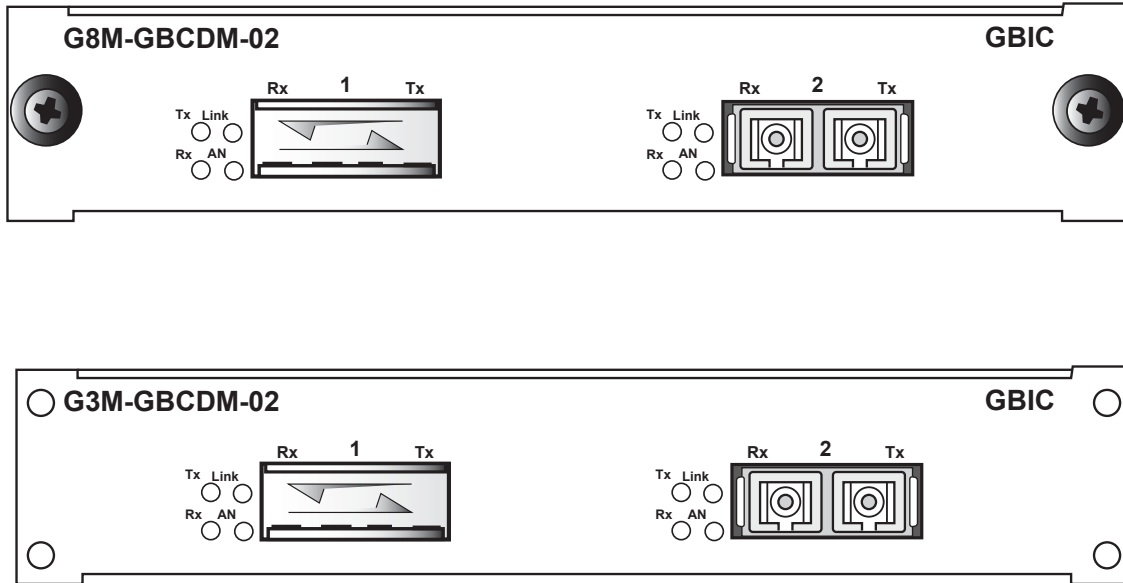
Two CLI commands have been added to provide compatibility with other vendor's equipment that use multicast to communicate between OSPF neighbors. By default, the RS receives packets only from configured neighbors, and sends out unicast packets only. The following two OSPF commands alter the RS' behavior.

The **ospf set interface <interface name> strict-routers off** command enables the RS to receive packets on the interface from any neighbor, and to receive multicast packets.

The **ospf set interface <interface name> do-multicast on** command enables the RS to send multicast packets on the specified interface.

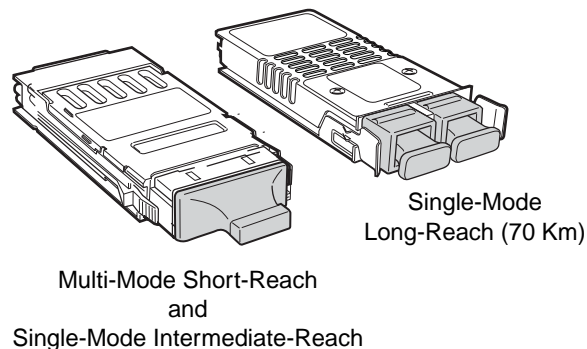
## 15. Non-MPLS Gigabit Ethernet GBIC Line Card

The following figure shows the front panels of the 2-port non-MPLS activated Gigabit Interface Converter (GBIC) line cards. The G8M-GBCDM-02 is used with the RS 8000 and RS 8600 switch routers. The G3M-GBCDM-02 is used with the RS 3000 and RS 1000 switch routers.



Front panels of the Gigabit GBIC line cards with one GBIC installed

GBIC modules provide the media-specific portion of the Gigabit GBIC line-card, which support Gigabit Ethernet connectivity across multiple media types and distances. The Gigabit GBIC line cards provide the power, initialization, and control for each GBIC module. Any combination of GBICs can be used on a single Gigabit GBIC line card.



### 15.a. GBIC modules

The Gigabit GBIC line cards accept the GBIC modules described in the following table.

#### 1. GBIC modules media specification

Port type	Specification
-----------	---------------

GBIC SX (MMF)	<ul style="list-style-type: none"> <li>Multi-mode fiber interface</li> <li>50 or 62.5 125-mm multi-mode fiber cable terminated with SC connectors</li> <li>Maximum of 300 m of cable</li> </ul>
GBIC LX (SMF-IR)	<ul style="list-style-type: none"> <li>Single-mode fiber (intermediate range) interface</li> <li>8 or 9 125-mm single-mode fiber cable terminated with SC connectors</li> <li>Maximum of 10 km of cable</li> </ul>
GBIC LH (SMF-LR)	<ul style="list-style-type: none"> <li>Single-mode fiber (long range) interface</li> <li>8 or 9 125-mm single-mode fiber cable terminated with SC connectors</li> <li>Maximum of 70 km of cable</li> </ul>

The Gigabit GBIC line cards use the LEDs as described in the following table.

## 2. Gigabit GBIC line card LEDs

LED	Description
Online	When lit, this green LED indicates that the line card is online and is ready to receive, process, and send packets if configured to do so.
Offline	When lit, this amber LED indicates that the line card is offline (powered off) and is ready for hot swap. The Offline LED also is lit briefly during a reboot or reset of the RS and goes out as soon as the Control Module discovers and properly initializes the line card.
Per-GBIC RX	<b>Green</b> indicates when the GBIC's transceiver receives packets <b>Amber</b> indicates when the GBIC's transceiver receives flow-control packets
Per-GBIC TX	<b>Green</b> indicates when the GBIC's transceiver transmits packets <b>Amber</b> indicates when the GBIC's transceiver transmits flow-control packets
Per-GBIC AN	<b>Green</b> indicates that the port hardware has auto negotiated the operating mode of the link between full-duplex and half-duplex. <b>Orange (intermittent)</b> indicates that auto negotiation is in process. <b>Orange (solid)</b> indicates a problem with auto negotiation configuration. <b>Red</b> indicates an auto negotiation failure. This fault may occur if the link partner does not support full duplex. <b>Off</b> indicates that auto negotiation has been disabled or the link is down.
Per-GBIC LINK	<b>Green</b> indicates that the port hardware detects a cable plugged into the port and a good link is established. <b>Red (intermittent)</b> indicates that port hardware received an error during operation. <b>Red (solid)</b> indicates that the port hardware detects a cable plugged into the port, however, a bad link is established. <b>Off</b> indicates that no link from the port exists.

## 16. Additional new commands and output

### 16.a bgp set bad-aspash <discard | ignore>

This option allows you to define the manner in which the router handles and/or responds to a bad BGP ASPATH prefix. Unless this option is configured, the default action is to reset the peering session.

The following is an example of how to configure the RS to ignore bad ASPATH prefix attributes:

```
rs(config)# bgp set bad-aspash ignore
```

### 16.b. ip-router show filter [name <expression>]

When BGP is configured, this command will display the given matching filter name or will display all filters if the name is omitted.

```
rs# ip-router show filter
Filter [FilterDefault]: 0.0.0.0/0 Exact
Filter [FilterStatic]: 10.0.1.0/24 Refine
```

```
rs# ip-router show filter name FilterDefault
Filter [FilterDefault]: 0.0.0.0/0 Exact
```

### 16.c. I2-tables show port-macs port ab.X.Y verbose



**CUSTOMER RELEASE NOTES**

When MPLS is enabled, this command displays the extra field, "Label", which identifies the LSP a mac address is received from.

```
rs# I2-tables show port-macs port gi.2.1 verbose
Id      MAC      VLAN  Type  Frames  Age  Label  Exit Ports
-----
00001  01:80:C2:00:00:00  4095  Dst    0       0    -    CPU
```

**17. Bootprom Variables (change in the default behavior)**

The commands to set the bootprom variables were originally settable via configuration mode. These commands have now been moved to enable mode. Customer upgrading from previous releases of firmware need to remove bootprom commands from the startup.cfg file. If not, the redundant commands in the RS configuration, for setting tftp server and the router's IP address via en0 port in boot mode, will override the commands executed in enable mode. The result will be the Primary and Backup CMs will both have the same IP address, which would likely interrupt the boot process.

**18. OSPF Support for reference bandwidth**

By default, the OSPF interface cost is calculated as:  $Cost = 2 \times 10^9 / \text{Interface speed (in bps)}$ . It is now possible to override this by specifying a reference bandwidth to replace the  $10^9$  component in the above formula. The reference bandwidth is specified in Mbps, i.e. the following command line:

```
RS(config)#ospf set ref-bw 10000
```

Specifies the reference bandwidth to be 10Gbps, resulting in the following calculation of OSPF interface costs:

Cost	Default Reference bandwidth ( $10^9$ )	Reference bandwidth ( $10^{10}$ )
2	1 Gigabit per second	10 Gigabits per second
20	100 Megabits per second	1 Gigabit per second
200	10 Megabits per second	100 Megabits per second
2000	1 Megabits per second	10 Megabits per second

and so on.



**ISSUES RESOLVED:**

Issues Resolved in version 8.0.3.13	ID
<p>ATM - In some ATM configurations the following error messages can be output by syslog on a regular basis.</p> <p>%ATM_OC12-E-MSG, ATM module 4: -ATM-CANTENCAP,can't do encapsulation for etype 2 on at.4.1.1.100. %ATM_OC12-E-MSG, ATM module 4: -ATM-CANTENCAP, can't do encapsulation for etype 2 on at.4.1.1.110.</p> <p>This issue is due to invalid traffic consuming buffer for a longer period of time than valid traffic would need, to resolve this issue the small buffer head room size has been increased by ~150% to provide the necessary tome to ride through these events.</p>	49815
<p>ATM-OC12 - In the Lite version of the 8.0.3.xL software, there is no support for ATM OC-12. If an attempt is made to boot the RS with an ATM OC12 installed the RS will crash. Although this is not a supported configuration, modifications have been made so the RS will no longer crash, the ATM card will be left offline.</p>	46336
<p>ATM-OC3 - On an ATM OC-3 port the priority bit on UBR circuits is set to the wrong value. The RS internal priority bit was not being set correctly for outbound UBR traffic. This condition was limited to the Low priority, which is the most abundant, the result was that this traffic was then interfering with higher priority traffic exiting the same port on a different VC. This condition has now been corrected.</p>	51016
<p>MLP - In an ML-PPP configuration a condition can occur where the WAN card on the RS can get into a degenerative state that will eventually lead to the WAN card crashing and restarting. Before the crash occurs the following error and warning messages may be output by syslog.</p> <p>%L2TM-W-INVALID_WAN_VLAN, WAN Module in slot number 5 is receiving frames from non-member VLAN (56). Possible misconfiguration. %L2TM-W-INVALID_VLAN, Port et.2.3 receiving frames from non-member VLAN (1). Possible misconfiguration. %WAN-W-MSG, Loadable module 5: -SERIAL-CTL_ERROR_QUEUE_SEND, control: Cannot send message to control task (repeated 189 times in 5 minutes) %WAN-E-MSG, Loadable module 5: -SYS-INVALID_GROUP, tmr_recurring: NU_Set_Events: invalid group 300 times in 5 minutes) %L2TM-W-INVALID_WAN_VLAN, WAN Module in slot number 5 is receiving frames from non-member VLAN (1). Possible misconfiguration. %WAN-W-MSG, Loadable module 5: -SERIAL-CTL_ERROR_QUEUE_SEND, control: Cannot send message to control task ...</p> <p>This problem was a result of MLP fragment reassembly, in an ML-PPP environment, some vendors fragment all IP traffic before it is transmitted on the MLP link. The result can be increased over head on the down stream devices. There was a negative impact on the WAN card, which has now been corrected in this release.</p>	45044
<p>MLPPP - In an MLPPP configuration (two T1s) between two RSs, if one of the T1 links is pulled, all traffic on one direction will stop. If the opposite link is disconnected traffic in the opposite direction will stop. This issue has now been corrected, when one of the links goes down, traffic will continue on the remaining link.</p>	48538 47925
<p>NTP - In some environments it has been reported that the system clock slips after NTP synchronization. The problem is that sometimes, the response packets, from the NTP server, take a long time to reach the RS and by the time the packet arrives the RS has timed out. These packets which came for a previous sync requests are queued in the receive queue. Now, when the next sync request is sent, the previous reply was read from the queue, and the time was set based on this stale reply. A modification has been made to check the originate time of the response received with the transmit time of the request. If these don't match, the response is quietly discarded and the RS will wait for the next response.</p>	48008
<p>PVST - The configuration of PerVLAN Spanning Tree does not operate as expected without the "special encaps" qualifier. When PVST is configured without the "special encaps" qualifier, a BPDU received is treated as if it were an STP BPDU being received on the default VLAN. If STP has not been enabled on the default VLAN, the BPDU is discarded. In this release, modifications have been made to not use the destination MAC address to distinguish between a PVST BPDU and an STP BPDU. If both STP and PVST are enabled on the same port, then special encaps is needed for PVST, otherwise the correct VLAN must be used to identify the PVST context.</p>	43813 35017
<p>SYSINIT – A new "RAPIDOS" banner has been added to boot time output.</p>	49984
<p>WAN - A condition can occur on an RS configured with a Channelized T3 card, where a port lockup can occur. The lockup is usually proceeded by a series of the following error messages:</p> <p>%WAN-E-MSG, Loadable module 5: -SERIAL-EGRESS_FR_DEC_FAIL, egress: failed to forward from vc 35 on port 1 channel 7 %WAN-E-MSG, Loadable module 5: -SERIAL-EGRESS_FR_DEC_FAIL, egress: failed to forward from vc 35 on port 1 channel 6 ...</p> <p>The problem was caused by an incoming PPP frame with a valid PPP header but no data. During the receive path processing, as the WAN port strips away parts of the packet such as PPP header and CRC, the data length value becomes smaller than the value being subtracted, the result is a negative value for the length. The length variable unsigned, so this negative number in turn becomes a very large positive number. Now, as the data packet is sent to the DEC21143 Ethernet controller to transmit the data to the backplane, it is sent with this very large data length. The DEC transmitter can lock up when it attempts to send 2027 bytes or more. This issue has now been resolved in this release.</p>	45916



CUSTOMER RELEASE NOTES

Issues Resolved in version 8.0.3.13	ID
<p>WAN - Due to lack of interest the IMUX feature for WAN interfaces has been deprecated in this release. The ability to configure IMUX on an MLP bundle has been removed, the CLI no longer contains the command "ppp set mlp-imux-mode ports &lt;mp.x port list&gt;". In addition, the associated statistics have been removed from the output of the "ppp show stats" command.</p>	51357
<p>ATM – When hot-swapping out an ATM OC3 line card and in and ATM OC12 line card, a Port Bus write and a spurious interrupt error may be displayed by syslog.            %SYS-E-PORTBUSWRITE, Port bus write error at address 0x5bcfffe0            %SR-W-SPURIOUSINT, spurious interrupt, unknown reason 0x0 (0x8 0x400)            %STP-I-PORT_STATUS, Port status change detected: at 6.1 - Port Down            %SYS-I-HOTSWAPIN, module in slot 6 has been hotswapped in</p>	52006
<p>The Hotswap will complete and the card will be operational, in any case this issue has been corrected in this release.</p>	

Issues Resolved in version 8.0.3.12	ID
<p>System – Drop-flow programming and custom mode forwarding, there are cases where certain types of traffic need to be discarded. These cases are usually the implementation of an ACL or in reaction to a DOS attack. The RS has several layer 3 flow modes (Application, host, destination and Custom) each of these modes has different latitude when making the decision to install a flow to drop traffic. Application flow mode has the highest resolution of flow definition and therefore, is the safest for the installation of drop flows. Where Destination flow mode has the least resolution and requires the greatest care when making the decision to install a drop flow. In this release of the ROS software, drop flow protection has been added for the Custom Forwarding Mode.</p>	35891
<p>SYSLOG - Undocumented WAN warning message:            %WAN-W-MSG, Loadable module 8: -SERIAL-EGRESS_MLP_PID, egress: invalid PPP proto id(2330) on port 1 channel 26 in mp.8            %WAN-W-MSG, Loadable module 8: -SERIAL-EGRESS_MLP_PID, egress: invalid PPP proto id(3d22) on port 1 channel 26 in mp.8            %WAN-W-MSG, Loadable module 8: -SERIAL-EGRESS_MLP_PID, egress: invalid PPP proto id(4500) on port 1 channel 24 in mp.8            %WAN-W-MSG, Loadable module 8: -SERIAL-EGRESS_MLP_PID, egress: invalid PPP proto id(4500) on port 1 channel 24 in mp.8            %WAN-W-MSG, Loadable module 8: -SERIAL-EGRESS_MLP_PID, egress: invalid PPP proto id(7939) on port 1 channel 24 in mp.8</p> <p>This message is the result of the RS receiving PPP packets with invalid PID's.            The recommended action is to verify that the device that connects to the RS is not corrupting packets or using proprietary protocols.</p>	34519
<p>DOS - SQL worm attack sends IP multicasts and causes L2 hash collisions leading to high CPU utilization. This attack consisted of IP multicast traffic with random destination MAC addresses and random ip addresses. In this release of the ROS software additional protection of this type of attack has been added. A new CLI configuration mode command has been added:</p> <pre>ip dos disable ip-multicast bridging ports</pre> <p>This command inserts an entry, in the routing address table, that matches any IP multicast MAC address. This means that any valid IP multicast packets received on that port will bypass L2 processing and be sent directly for L3 processing. This will allow the RS to bypass the L2 processing and avoid filling the L2 table with unnecessary data caused by IP Multicast DOS attacks.</p> <p><u>Caveats:</u></p> <ul style="list-style-type: none"> <li>Note that this fix does not help with L3 processing. It is still possible to have high CPU utilization due to a large number of L3 misses, L3 hash collisions etc. To mitigate this, we will have to play with deep hashing, different hash variants, and forwarding modes.</li> <li>Note that NO IP multicast traffic will be bridged on ports which are configured with the above command. So the customer may not be able to use this command if they are bridging IP multicast traffic. Or this command could be used temporarily to stop/slow an attack, and then removed when the attack is over.</li> </ul> <p><u>Better fixes:</u></p> <ul style="list-style-type: none"> <li>In cards with Gen 5 ASICs, L2 and L3 misses can be rate limited. This will hopefully be very effective against these attacks.</li> </ul>	46486



CUSTOMER RELEASE NOTES

Issues Resolved in version 8.0.3.12	ID
<p>MLP - Multi-Link PPP fragmentation causes problems in the serial DEC driver. If MLP fragmentation is enabled, while sending traffic at a rate greater than the defined threshold (an oversubscribed rate), it causes problems in the serial DEC driver on the WAN card.</p> <p>With packet size of 768 bytes and a data rate of 100 Mbps, all MLP encapsulated frames would have the MLP sequence number added to the header at the time of transmission, and the sequence number is incremented only after a successful transmission. In the case of fragmentation, as the sequence numbers are used by the reassembly algorithm, along with the beginning and end bits, to determine a fully reassembled MLP frame.</p> <p>What was happening is that, with mixed fragmented/unfragmented frames, portions of a fragmented frame were getting held behind an unfragmented frame during transmission. Because of this, middle fragments of a different frame would arrive at the receiver before middle fragments of the original frame, so (since the MLP spec doesn't account for this scenario...i.e. there is no identifier reserved for "which frame does this fragment belong to") the receiver would assemble these middle fragments of different frames within a single frame. This would cause extremely large frames to be reassembled in error.</p> <p>The fix is to apply the MLP sequence number for fragmented frames "AT THE TIME THE FRAME IS FRAGMENTED" to preserve the fragment order when the fragments get reassembled by the receiver.</p>	45925
<p>SmartTrunk - The RS shows incorrect ports in the SmartTrunk when issuing the command "port show stats st.1". When executing this command on a RS38000, the RS doesn't report the correct ports as the members of the SmartTrunk. The problem is the "Show Ports" function is not handling the case for a SmartTrunk. Modifications have now been completed to accurately report the member ports of the SmartTrunk.</p>	45876
<p>CPU-Redundancy – After a CM failover, the RS crashed when attempting to free an L3 entry twice. This condition is timing related and is unlikely to occur in a production network. In the lab a specific RS configuration is required and the CMs must be failed-over repeatedly for a couple of hours to catch this condition. This issue has now been corrected.</p>	45455
<p>ACL – The RS can crash when attempting to modify or remove an ACL. The problem is that the Backup-CM was attempting to modify the flows that were effected by the ACL change, but the Primary-CM had already completed this task. This issue has now been corrected.</p>	44687
<p>BGP - There is a display issue in the output of the command "bgp show ip route", the netmask is displayed as /32768 instead of /16. This issue has now been corrected and the proper format of the netmask is displayed.</p>	44298
<p>HRT – when the RS is configured for HRT and OSPF with a Default Gateway , the RS can crash in HRT, when attempting to add an ARP entry for a directed broadcast address. The RS didn't account for the fact that it was configured for HRT, even though the RS was attempting to update the L3 entry used by HRT for the route in question. The L3 entry pointer was NULL in this case resulting corruption of the HRT and a crash. This problem has now been resolved.</p>	44048
<p>HRT – When the RS is configured with Hardware Routing (HRT) and Equal Cost Multi-Path (ECMP) the RS will crash is the diag mode command "debug l3 l3hrt x.x.x.x/y channel n" is issued. This command is not supported for use out side of Riverstone because of it's ability to cause an RS crash. In this instance the cause of this crash has been identified and corrected.</p>	43491
<p>IP-POLICY - BGP route-map will incorrectly affect the OSPF configuration. When the command "route-map xx permit 10 match-prefix network all between 8-24" is configured, the OSPF configuration in the configuration file ("ip-router show configuration-file") shows the route-map incorrectly affects the OSPF configuration.</p>	42444 43028
<p>WAN – There is a timer issue causing on some WAN modules that cause PPP and/or Cisco-HDLC messages to be sent at the wrong time intervals. The timer on the WAN module was programmed to run at 75 MHz, it should have been programmed for 66 MHz, the result was keep-alive messages were being sent at the wrong time intervals. This condition only effects the 4 port Serial and 2 port HSSI line cards and has now been resolved.</p>	42982
<p>HW - The command "system show hardware verbose" does not show the ASIC version clearly. Since many of the hardware based functions are referenced by the generation of the ASICs on the line card, the output of the "system show hardware verbose" command has been expanded to include the ASIC generation. Example: Slot 12, Module: 1-POS OC48 "T" Rev. 5.0 Service String: 1392582658_OC2.0_16_S13.0_16_SO2.2_32_64 (Gen 4)</p>	42217
<p>WAN – The command "statistics show port-stats" shows the incorrect values for the T1 ports. This has been an issue since the HDLC card was introduced, the "statistics show port-stats" shows the "1 minute traffic rates" on the T1 transmit link was 91 megabytes, on the adjacent port the traffic received was reported as 1.5 megabytes. These statistics have now been corrected.</p>	42179
<p>L2-Drivers – Layer 2 table corruption has been identified in specific RS configurations. When the RS is configured for both OSPF and PIM, once the PIM hello packets are exchanged all Ethernet ports installed in system will have invalid packet counts. This can be determined through the output of the "statistics show port-stats" command.</p>	41846 41241



CUSTOMER RELEASE NOTES

Issues Resolved in version 8.0.3.12	ID
WAN – It was identified that there exists some vulnerability, when accessing one of the data structures, in the WAN driver where WAN card will crash. Although the conditions that would lead to a crash are rare, additional protection for the access of this data structure has been implemented in this release of the ROS software.	41418
Drivers - Some port counters are not reset to zero when clearing the port statistics. When clearing the port stats for different card types, including 10/100, gigabit, ATM and POS it has been observed that not all of the counters are set back to their initial values. This issue has now been corrected.	41241
WAN - When adding a WAN port to an STP enabled VLAN, the RS may crash. This problem has now been corrected in this release of the ROS software.	40832
DHCP – If an IP interface name is changed the IP-Helper will no longer forward DHCP traffic until the RS is rebooted. DHCP relay agent stops forwarding traffic when the interface name is changed and the helper interface is changed, when the name is changed back, dhcp works fine. If the changes are saved to the configuration and then the RS is booted, the configuration works fine. This issue has now been resolved.	40791
PVST – In a Frame Relay configuration, PVST ports go into blocking when a PPP port is added to the VLAN. Adding an additional PPP port to a vian that contains a Frame Relay port running PVST causes the ports to go into a blocking state. This can only be alleviated by rebooting the RS. This issue has now been addressed in this version of the RSO software.	40624
MLP - Certain MLP commands remain errored out of the configuration after a hot-swap, PPP does not re-negotiate. When dual WIC module with T1s are configured for MLP and the WAN card is hot-swapped out and the back in, the commands associated with MLP remain marked as errored in the RS configuration. PPP does not re-negotiate, and reset as is required to complete the reconfiguration. The workaround is to negate and re-enter the MLP commands.	40522 25980
VLAN – There is a problem hot-swapping in a line card that has ports that will be part of an IEEE802.1q trunk, if the trunk was created with a single CLI command containing multiple ports, i.e. several trunks were created with the same CLI command. If a card is hot-swapped out, this line will become a partially executed command, and then if this card is hot-swapped back in, the line will be marked in "error". As a preventative measure, each VLAN trunk port should be created on a separate command line. This behavior has now been corrected in this release of the ROS software.	40160
HRT - Enabling/disabling HRT multiple times with ARP clear all can cause a gigabit port to lockup. The CPU shows packets are transmitted but the peer router is not receiving any packets. The only way to recover is to hot-swap the line card out and back in to the RS. This issue has now been resolved.	39973
HRT - On the RS16000, HRT returns an error if it is enabled on slot 1. there is no error reported if HRT is enabled on all of slots. A modification has been made to support HRT on the CM slots if the RS16000 with the extended HRT memory.	29038

Issues Resolved in version 8.0.3.11	ID
ATM - Non-ISO routed PDU's cause performance degradation, when these packets are received on an ATM OC-12 port containing a moderate to large number of VC's. Modification have been made to improve performance in this type of environment and a new command has been added to detect the presents of these types of packets: "atm set port pkt-err-msg"	35947
ATM – The IP fragmentation value is not properly set on the ATM OC-12 port. One of the symptoms is inability to establish OSPF adjacencies, because the RS can't properly receive packets with large IP fragments. This issue has now been corrected.	37290
CFM – High CPU utilization may occur when implementing Custom Forwarding Mode on the 10/100 ports on the Control Module of the RS16000. When enabling Custom Forwarding Mode on Ethernet ports on the Control module's 12 10/100 ports, the CPU utilization will go to 100% with just 1 bi-directional flow. When the Custom Forwarding commands are removed from the RS configuration the CPU utilization drops back to a low percent. This issue has now been corrected.	36428
CLI – The on line help for the "show" command displays the string "SSR" when it should be "RS", this modification has now been made.	38415
CLI – CLI on-line help states that the default SmartTrunk load policy is Round Robin, when it is now Link Utilization. The on-line help has now been changed to indicate that "link utilization" is now the default load policy for SmartTrunks and not round-robin.	37159
CLI – In some cases when negating commands from the RS configuration a core dump may occur. This condition occurs when the configuration changes are made through a telnet connection to the RS. The core dump is usually preceded by the following message being displayed on the RS console: %SYS-F-BLKFREE, memory free failed - block '0x81c48230' is already free(64) (by: 0x801a3630 0x8014aa98 0x800be7bc 0x800bb528 0x8003eacc ) This problem has now been resolved in the this release of the ROS software.	40484



CUSTOMER RELEASE NOTES

Issues Resolved in version 8.0.3.11	ID
CLI – The CLI can become unresponsive if RS is used as a telnet client with pagination turned off (cli set terminal rows 0). The RS console task will now lower it's priority when executing commands (as opposed reading user input from the command line). This will insure other functions within the RS will run when the output of a command is long. This prevents long running CLI commands from keeping other tasks from running.	38203
HRT – In an HRT configuration of LAN ports and ATM VCs configured fro point-to-point, DHCP offers are not properly forwarded. If the ATM VCs are set for type point-to-point, then the next hop MAC in HRT is all zeros. In the ATM VCs are type broadcast, then DHCP works. Modifications have been made to properly program the appropriate MAC addresses for Point-to-Point interfaces.	40054
HRT – In an HRT configuration, all traffic across the gigabit ports will stop after a CPU failover. This problem will not occur unless performing CM failover with HRT previously enabled on gigabit cards. This problem was fixed by insuring the L2 filters for the system MAC addresses have been sent to the backup CM when the backup CM boots-up so that when the failover occurs, the backup CM already has the system MAC addresses.	37157
IP - If the routing task were to abort the ASSERT information not registered in syslog server. Additional functionality has been added to insure the appropriate information is sent to the syslog following these types of events.	38637
IP – in some cases it's not possible to successfully add a secondary IP interface to and interface on a CT-3 port. Changes have now been made to add the support for secondary IP addresses on CT-3 ports belonging to the same VLAN.	37871
OSPF - Equal-cost paths through an NSSA area is not being handled correctly. On a configuration with an OSPF equal cost multi-path through an NSSA area, if there is a failover, the "edge" router will correctly pick only one path. But on the "fail-back", the "edge router" still shows only one path, although all adjacencies are up. When a type-7 LSA is generated, the RS was setting the forwarding address within LSA to be any of the valid OSPF interface addresses. Since a router which receives these LSAs uses the forwarding address to compute the cost to the destination, and since RS could have different costs associated with each of its interfaces, more care in selecting the forwarding address was necessary. Now, If the router-id has been added as a stub-host, the RS will advertise the router-id in the forwarding address, otherwise the RS operate as it has originally.	36001
OSPF – in a redundant router configuration, the RS has poor failover timing for OSPF route updates. The RS takes about 30 seconds to update OSPF routes from the backup router after the primary failed. Modifications have been made to more quickly flush the LSA information to improve the failover/route update time.	36845
OSPF - OSPF does not come up when configured on ATM OC-3 port 2, the OSPF hello messages are sent on port 1. All other functions operate properly over the directly connected interface. This anomaly only occurs when the OSPF is specifically configured as interface type as point-to-point. The issue has now been resolved.	37560
OSPF - OSPF NSSA external routes cannot be redistributed as Type 1 routes. When redistributing static routes into an OSPF NSSA area, the option to set these routes as "type-1" is not working, the default "type-2" is still being sent. This issue has now been corrected routes specified as type-1 will be re-distributed as type-1.	38291
Port Mirroring – The module slot information is incorrectly updated, when port mirroring is negated from the RS configuration. ARP broadcasts will no longer be flooded on the target ports for which port mirroring was enabled/disabled (if monitor port on same slot). If the Target port and the Monitor port are on the same line card, when Port Mirroring is disabled, the slot information of the Monitor port is removed from the existing flows. Since the Target port and the Monitor port both share this parameter, the target port will no longer forward flooded traffic, such as ARP requests. This issue has now been corrected.	40234
QOS – The QOS TOS-rewrite is not working properly on routed interfaces. It turns out that the ACL that is used to define the Type of Service rewriting was not being interpreted properly, this problem has now been corrected.	36990
SSH – Under some circumstances running the SSHredder application against the RS can result in a system crash. It was determined that there was a small window of vulnerability during the SSH process cleanup where this problem can occur, this issue has now been corrected.	38396
WAN – The E1 wan statistics are incorrect – The byte counters for transmit / receive are considerably larger than they should be. Modification have been made to the "port byte" statistics to handle in/out bytes counters rolling over. The same modifications have been made for "port errors" and RMON port statistics as well.	38803

Issues Resolved in version 8.0.3.10	ID
ATM – On the ATM OC-12 line card there is a condition that can occur where the L2 table can become corrupted. When this occurs the ATP port hangs, the cause has been identified as a condition where the packet received is significantly larger than indicated by the SAR. This issue has been resolved in this release.	31215
ATM - Traffic lockup on ingress of the ATM OC-12 line card. It has been identified that this condition occurs where the ATM OC-12 transmitter can hang with the recipe of a minimum sized packet just prior to a maximum sized packet. This issue has been resolved in this release.	38212



CUSTOMER RELEASE NOTES

Issues Resolved in version 8.0.3.9	ID
ARP - When redundant ATM physical links are terminated over back to back connections between two RSs the ARP table can become corrupted resulting in a system crash when the ARP process is started. This issue has now been resolved.	35087
BGP-The command "bgp set peer-group local-pref xxx" doesn't operate properly. The output of the command "bgp show routes" does not display the specified local-pref information. This problem has now been corrected.	36755
HRT - On the RS-38000 with HRT enabled, the following error message may be displayed on the console: %SYS-E-PORTBUSWRITE, Port bus write error at address 0xc374000c. This issue has now been resolved.	31942
ISIS - It has been observed that ISIS SPF runs quite frequently when redistributing routes from RIP to ISIS on an ongoing basis. The source of this behavior has been identified as a result of LSP hold time being different for LSPs that contain these routes, this issue has now been corrected.	35431
NAT – The NAT DNS translation should be turned off by default. The command to enable the DNS translation exists in configuration mode. NAT DNS translation has been on by default, therefore there has been no way to disable it. NAT DNS Translation has now been disabled by default as it should have been.	36175
OSPF – In some cases the RS is incorrectly removing static ARP entries even though there was a peer address defined for the point to point interface. When OSPF is stopped and then restarted the ARP entries are recreated but ip connectivity between directly connected interfaces is not restored. This issue has now been resolved, the RS will not delete the ARP entry if the no-delete flag is set.	34080
Port – The "port force-link-up" command has been enhanced to support SmartTrunks. If the "port force-link-up" command is applied to a port and then the port is added to a SmartTrunk, the "port set" command will error out, this command must be applied to the SmartTrunk not the ports within the SmartTrunk.	35404
Port statistics – When the command "statistics clear port-stats" is issued on the 10/100 ports of the 16 port line card, the statistics are not completely cleared. This behavior has now been corrected, however, the statistics under "1 minute traffic rates" will not be cleared with "statistics clear port-stat" because they will average out with time.	33266
Rate Limit – The command "system set rate-limit-range" and it's associated functionality, has been added to this release.	36045
SNMP – When configuring a VLAN via SNMP, dot1qVlanStaticEgressPorts - adding a group of ports to a VLAN, all but the last port will be added to the VLAN. This condition has now been corrected.	35422
System – Packets are buffered, for later transmission, when a link in a SmartTrunk goes down. As the packet are buffered the system identifies the remaining available links of the SmartTrunk and then begins transmitting the packets and freeing the buffers. When all of the links of the SmartTrunk are down the system will not be able to find a link to transmit the buffered packets. When this occurs the buffers containing the packets are not freed before the function ends and the SmartTrunk is declared down. This problem has now been resolved.	35257
System – There is a condition where the RS can crash when attempting to free a network packet buffer that has already been freed. This condition has now been corrected.	37118
Telnet – A Telnet session can hang, when the command "wan show mac-table slot x" is executed through the telnet session and the command "frame relay show stats ports all-ports" is executed through the console at the same time. This condition has now been corrected.	35610
VRRP - When an ACL is edited the VRRP master changes to the "initialize" state. VRRP shuts off the interface status polling when an interface reaches the up state. In this state, VRRP can set the interface status to down again if it is unable to send a packet. If, during this time, the interface goes down the interface will be marked down for VRRP and polling will be left disabled. In this state VRRP will never recover. Modifications have been made to check the VRRP interface status right before shutting off the polling to insure is hasn't reached the up state.	35021
WAN – There is a memory leak when an MLP bundle disconnects. Whenever an alarm condition occurs on an MLP line approx 2000 bytes of memory is not freed as it should be. A crash can occur when all of the memory is consumed. This problem has now been resolved.	35158

Issues Resolved in version 8.0.3.8	ID
------------------------------------	----



CUSTOMER RELEASE NOTES

Issues Resolved in version 8.0.3.8	ID
ACL – For L4 bridging environments, if an input ACL has been defined to deny specific traffic, if it is necessary to update the flow information due to changing conditions on the network, the deny parameter may be toggled such that the RS starts passing traffic that should be blocked. Upon identifying a new source MAC address the L2 table management routine initiates an L2 table look-up for the same MAC as a destination address. It then (for L4 bridging) updates the line card/exit port information with the values for the new source MAC port. Unfortunately, if the existing table entry was a deny flow, this update overwrite of the indicator to drop this traffic, thus turning the deny entry into a permit entry. A modification has been made to check for the existence of an ACL that would insure this traffic would continue to be dropped.	33251
ACL – In version 8.0.3.7 a condition was present where the RS could crash when modifying an ACL in with the ACL editor. Upon saving an ACL modified with ACL editor the RS will crash. This problem has now been corrected.	33101
ARP – In a redundant network configuration with very high volumes of traffic, a link failure can cause all of the existing traffic to be redirected to the RS CPU while the redundant path is identified. In a VRRP environment a gratuitous ARP's is sent by the backup router to accelerate the failover process. If the gratuitous ARP is lost or it's processing is delayed the failover may be delayed. To address this type of failure in a real time network the RS can now be configured such that the failover time can be optimized by keeping the failed link in an up state, thus keeping a huge volume of traffic from going to the CPU. Therefore the CPU will receive and process the gratuitous in the minimum amount of time and the failover time is minimized. The new RS configuration command is:  port enable force-link-up wx.y.z  With this command in the RS configuration, the traffic will continue to be send traffic out a specific port even when the link is operationally "down". This will keep the traffic from being sent to the RS CPU and delaying the failover process. In addition, when a gratuitous ARP is received on a given port, the RS will now update the associated flows rather than flushing and creating new flows.	31957
BGP – Prior to version 8.0.3.0 the RS can crash after the command "bgp show neighbors" issues, this only occurs in configurations where the BGP peer is set with the max-prefix option. This issue was resolved in an earlier patch release, but was not documented. The issue has been re-verified and is documented as resolved in this release of ROS.	23522
BGP – When the RS is configured for BGP and there are Route Maps defined, the RS will crash when issuing the "route-map show all" command. BGP does not have to be started for this crash to occur. This problem has now been corrected.	32023
DNS – The RS cannot resolve hostnames that appear to be comprised of only hexadecimal characters. If DNS is configured on the RS (system set dns server ...), then an attempt is made to use a host name made up of only hex like characters (abc123), using ping, telnet ... the operation will fail because the DNS name will not be resolved. Modifications have been made to provide support for DNS names consisting of only a,b,c,d,e,f and numeric digits.	33397
HRT – In a configuration with a WAN port interconnecting two routers, after enabling HRT traffic stops. This interruption in traffic forwarding occurs when HRT entries have a WAN port as their exit port. It is necessary to do some additional processing where an exit port is a WAN port, this additional processing is require to determine the next hop MAC address. This issue has now been resolved.	31900 31895
HRT - When using the Hardware Routing Table on a port with BGP configured, bouncing the BGP session may cause the HRT table to be loaded incorrectly. The exit information for the effected routes was not set properly when this condition occurred, thus the downstream hosts were not be able to access upstream networks. If however, the CPU had to forward a packet to any of the upstream networks, this action would correct the associated HRT entry and connectivity with that network would be restored. This condition has now been corrected in this release of the ROS firmware.	32031
L4 Bridging - The CPU utilization can go as high as 100% while passing traffic through an l4-bridging enabled VLAN. When a topology change occurs in an L4 bridged network, the L3 flows created by L4 bridging functions, were not removed from the forwarding table. Thus excess traffic was sent to the CPU running up the CPU utilization. Now, when the RS receives a packet, while in L4 bridging mode, where an L3 entry corresponding to the L3 info in the packet exists, the RS will not discard the packet, it will remove the existing L3 entry and install the new one. This minimizes the load on the CPU for this type of traffic.	23953 32718
Port Mirror - L3 flows are not updated when one of the exit ports is a port mirror monitor port. When the exit port list of an L3 flow includes a port-mirroring "monitor-port", flows are not updated when an ARP update is processed.	33153
Port Stats – For ports on a 16 port line card statistics can be recorded on ports without connections. These statistics are usually "Routed packets - Switched (data)" and "IP table misses". This is not an operational problem, it an issue with the way the statistics are collected on the 16 port line card. For the 16 port line card, some of the statistics are collected for two ports at a time, the output of the command "statistics show port-stats" now identifies the "2 port" stats.	32808
Rate Limit – The output of the "ip show dos rate-limit" command does not match the default parameters. The output of this command has been improved, the display now shows correct default values. In addition, the RS now displays the default values in 'ip show dos rate-limit' command and in configs mode, the default value is displayed against the 'default' keyword.	33740



CUSTOMER RELEASE NOTES

Issues Resolved in version 8.0.3.8	ID																																				
<p>SmartTrunk – Flooding of traffic on the Primary port of a SmartTrunk stops, if it's link is disconnected. When the primary port of the SmartTrunk goes down, and a new primary port is selected, if the old primary port and the new primary port were on different line cards, the L2 entries exiting the RS on the SmartTrunk must be updated. In addition, a display issue has been fixed where a SmartTrunk as an input port, for example, with gi.3.2 and et.6.1 and a SmartTrunk as an output port, with et.4.1, et.5.5, if the command "l2-tables show port-macs verbose gi.3.2 decode-smarttrunks", the display would indicate the specified port as well as port et.6.1. This has now been corrected as well.</p>	33161																																				
<p>SmartTrunk – Hot-swapping a WAN card out, can cause the links of a SmartTrunk to transition down and then back up. This issue has been resolved in this release.</p>	32802																																				
<p>SmartTrunk - L3 Flows do not update correctly when the exit port is a SmartTrunk. This condition can be observed in a VRRP configuration when a VRRP master router recovers from a failover only a portion of the flows are transitioned back from the backup VRRP router. The proportion of flows that transition back to the Master is a function of the number of links in the SmartTrunk. For a two port SmartTrunk approximately half would revert back to the master, and a third for a three port SmartTrunk. This is an issue in the ARP processing functions where, if the exit port of an ARP entry was a SmartTrunk, instead of removing all of the flows exiting the ports in the SmartTrunk, only the flows on the designated port of the SmartTrunk were properly removed. This condition has now been corrected and now all of the traffic will reacquire the master router when a VRRP transition occurs.</p>	32027																																				
<p>STP – The command "stp set vlan-disable &lt;port-list&gt;", does not produce the desired functionality after the RS is rebooted. When this command is included in the RS configuration, all non configured VLANs for the specified ports are placed into a blocking state to reject the need to process any inbound traffic associated with these VLANs. When the RS is rebooted the STP configuration functions were executed after the STP characteristics have been set, this STP over road the state of the VLANs, at initialization time, since no loop could be detected. A modification has been made to insure the appropriate STP state is set once STP has completed its initialization.</p>	32739																																				
<p>System – On a system configured with a redundant CM, if a syslog server is define in the RS configuration:  <pre>system set syslog server 50.1.1.100 source 50.1.1.2 level info</pre> error messages may appear on the console of the backup CM:  <pre>%ERR-E-SYSLOG_Q_SEND_FAIL, SysLog Queue send failed</pre> This is the result of the Backup-CM attempting to send messages to the syslog server. Now the backup_CM is restricted from sending messages to the syslog server, only the Master CM can send messages to the syslog server.</p>	33274																																				
<p>Telnet – When a single login attempt fails, the RS reports the incident, through the syslog, as a - multiple login failure. The informational message has been modified to the singular tense since the message is displayed for each login failure. This was a display issue and had no effect on the operation of the RS.</p>	33854																																				
<p>WAN – Disabling an E1 port "port disable e1.x.y" and then re-enabling the port by removing the port disable command from the configs will render the port unusable until the RS is rebooted. The same condition occurs when the command "port disable force link down" is used. This issue has now been resolved.</p>	32003																																				
<p>WAN - Wan Port status inconsistencies between the native RS CLI and the Cisco like CLI show commands. This is a display issue, when the commands "port show port-status" and "show port-status" are issued the output differs.</p> <pre>rs# port show port-status e1.5.1:1   Flags: M - Mirroring enabled B - MLP Bundle S - SmartTRUNK port P - Configured as 802.1p</pre> <table border="1" data-bbox="243 1344 1218 1459"> <thead> <tr> <th>Port</th> <th>Port Type</th> <th>Duplex</th> <th>Speed</th> <th>iation</th> <th>Negot- Value</th> <th>IFG State</th> <th>Link State</th> <th>Admin Flags</th> </tr> </thead> <tbody> <tr> <td>e1.5.1:1</td> <td>E1</td> <td>Full</td> <td>1856000</td> <td>n/a</td> <td></td> <td>Down</td> <td>Up</td> <td>B</td> </tr> </tbody> </table> <pre>rs# show port status e1.5.1:1   Flags: M - Mirroring enabled B - MLP Bundle S - SmartTRUNK port P - Configured as 802.1p</pre> <table border="1" data-bbox="243 1543 1218 1669"> <thead> <tr> <th>Port</th> <th>Port Type</th> <th>Duplex</th> <th>Speed</th> <th>iation</th> <th>Negot- Value</th> <th>IFG State</th> <th>Link State</th> <th>Admin Flags</th> </tr> </thead> <tbody> <tr> <td>e1.5.1:1</td> <td>E1</td> <td>Full</td> <td>2048000</td> <td>n/a</td> <td></td> <td>Down</td> <td>Up</td> <td>&lt;----No Flag</td> </tr> </tbody> </table> <p style="margin-left: 40px;">^----- Speed inconsistency</p> <p>These display inconsistencies has been corrected in this release of the ROS firmware.</p>	Port	Port Type	Duplex	Speed	iation	Negot- Value	IFG State	Link State	Admin Flags	e1.5.1:1	E1	Full	1856000	n/a		Down	Up	B	Port	Port Type	Duplex	Speed	iation	Negot- Value	IFG State	Link State	Admin Flags	e1.5.1:1	E1	Full	2048000	n/a		Down	Up	<----No Flag	31933
Port	Port Type	Duplex	Speed	iation	Negot- Value	IFG State	Link State	Admin Flags																													
e1.5.1:1	E1	Full	1856000	n/a		Down	Up	B																													
Port	Port Type	Duplex	Speed	iation	Negot- Value	IFG State	Link State	Admin Flags																													
e1.5.1:1	E1	Full	2048000	n/a		Down	Up	<----No Flag																													

Issues Resolved in version 8.0.3.7	ID
------------------------------------	----



CUSTOMER RELEASE NOTES

Issues Resolved in version 8.0.3.7	ID
WAN – On the T3 / DS3 ports the Transmit-Clock-Source cannot be changed to use external clock. The port settings show as local when the port is configured for loop timing. This issue has now been corrected.	19653
IP - if the interface name starts with "lo" it is considered to be the loop back address. A modification has been made to parse beyond the first two character of the interface name when looking to for the loop-back address.	27261
HRT – There is a condition where L3 flow creation will cause HRT to exit and revert to flow mode forwarding. This condition is caused by an interaction between the L2 and L3 table managers and only exists on the older line cards. This issue has now been corrected.	27937
ATM – Large bursts of packets, smaller than 64 bytes, trigger a condition that causes the ATM OC12 port to stop transmitting traffic. Hotswapping the line card corrects the condition. This issue has now been resolved with a software modification to the image for the ATM module I/O buffers.	28852
STP / PVST - The problem is that we are forwarding multicast join v2 messages out all ports , including ports that should be in a "blocking" state according to PVST. The problem occurs when PVST is configured over a range of ports as in the following command: pvst enable port t3.7.1:1-4.35 spanning-tree vlan3 When configured over the same ports individually this condition does not occur: pvst enable port t3.7.1:1 spanning-tree vlan3 pvst enable port t3.7.1:2 spanning-tree vlan3 pvst enable port t3.7.1:3 spanning-tree vlan3 pvst enable port t3.7.1:4 spanning-tree vlan3 This problem has been corrected in this release if the ROS firmware.	28908
HRT - When a multicast ACL is applied to an HRT interface, the ports associated with the interface revert to flow mode operation. Since the ACL is related multicast and since HRT does not support IP multicast routing the ports should remain in Hardware Routing mode. This issue has been corrected in this release.	29900
WAN - Packet drops occur if an MLP T1 channel transitions to a down state and then back up again. This issue only occurs on the RS3x000 chassis. When the MLP switches to the active port being used, the ARP entries must be updated to reflect the new next hop information, and the new exit port information on the existing flows. The port and crossbar architecture for the RS3x000 chassis allow for a much larger range of ports. In the case of MLP there was a data structure that didn't account for the greater capacity, which caused the exit port to be improperly set causing both a display and forwarding problem. This problem does not exist on 9.0.0.x firmware and has now been corrected in this release.	30403
SmartTrunk – When Attempting to enable destination-based forwarding on a SmartTrunk the RS will crash. Adding the command: ip set port st.1 forwarding-mode destination-based to the RS configuration will cause the RS to repeatedly crash at boot time. This crash does not occur in the version 9.0.0.x firmware and has now been corrected in this release.	30494
ATM - When changing the ATM port MTU to 4470 AND add the framing for c-bit parity the MTU on the active configuration changes correctly, but when the RS is reboot the MTU reverts back to its default setting of 9212. This issue has now been resolved.	30496
ATM – A condition can occur where the where an ATM OC-12 port appears to hang. This condition is resolved by reinitializing the line card (hotswap out and back in). It was determined this condition was caused by a leak in the input buffer on the ATM port, eventually the port would run out of input buffers and could no longer receive traffic. This issue has now been resolved.	30538



Issues Resolved in version 8.0.3.7	ID
<p>CM – The Control Module may become overwhelmed with informational messages from the WAN line cards, preventing normal line card configuration from taking place in a timely fashion.</p> <p>Explanation: When a router with multiple Channelized T3 line cards installed undergoes a complete configuration (as at CPU failover time), while traffic is being forwarded to the WAN cards the control module will receive a warning message for each received packet, until the rest of the configuration has taken place (i.e. configuration of VLANs/interfaces etc.) If care is not taken to filter these messages from reaching the (slow) console port, continuation of the execution of the rest of the configuration may be severely delayed.</p> <p>Solution: There are multiple solutions to alleviate this problem, which allow the user the ability to limit certain messages from reaching the console port.</p> <ol style="list-style-type: none"><li>1.) Only allow Fatal and Error messages to the console port with the following configuration command: system set console level error</li><li>2.) Only allow Fatal and Error messages to be sent from the WAN module to the control module with the following configuration command: wan set message-log level error slot X (where X is the slot number containing the WAN module)</li></ol> <p>These commands can always be disabled if the customer wishes to review all of the informational and warning messages as well, however we suggest that a syslog server be used to review the messages instead of the console port, due to the negative affects the slowness of the console port may have on the rest of the system.</p>	30575
<p>Error log – During the boot process the error message - %ERR-U-UNKNWNERR, unknown error number '-59' may appear in the bootlog file. This error message occurs during power up, a spurious interrupt is detected by the CM in relation to the PCMCIA flash handler. This issue was resolved in the RS32000 and RS8x00 platforms, since RS 1000.3000 do not have flash cards, an additional modification was necessary. This issue has now been corrected for the RS1000/3000 platforms.</p>	30636
<p>Telnet - If a command was being executed and the user killed the telnet session from the client side, the router would not sense the session was killed and it would cause the router to enter in a state where it would consume all the telnet sessions available. No user was able to connect to the router after this condition occurred and the error message "%SYS-E-BUSY, tn_serv: fopen.0: mount device busy" would be displayed. Once in this state it is not possible to kill the telnet sessions and the RS must be rebooted to restore Telnet access. This problem has been fixed in 8.0.3.7. If the user exits the telnet session before a command has finished executing, once the command finishes, the router will automatically kill the session.</p>	30666
<p>SmartTrunk - traffic stops when link on a SmartTrunk is pulled if port-mirroring is enabled. When a physical link on a SmartTrunk is disconnected, the flows with the disconnected link as an exit port will not be flushed if a port mirroring is included in the flow. The resolution is to flush the flow when the exit port has been disconnected regardless of port mirroring.</p>	30667
<p>VLAN – added support for IEEE 802.1p rewrite for L3 traffic. The problem is that RS CLI didn't allow the user to specify an interface for which the .1p value will be overwritten. This was not a bug, it was simply never implemented to this point in time. This functionality has now been added.</p>	30671
<p>ARP - Gratuitous ARPs not being handled correctly when the local-proxy-arp functionality enabled, the RS was handling a gratuitous ARP as if it were a normal ARP request. The result was that in some cases devices such as Windows workstations would not renew their IP address with the DHCP server because it would think there was a duplicate IP address on the network. This issue has now been resolved.</p>	30770
<p>BMON - When sending broadcast packets exceeding the specified rate for BMON, the RS38000 signals that the broadcast rate has been exceeded and the BMON stats indicate the port has been shutdown, but arriving packets continue to be forwarded through the RS. This issue has now been resolved and was specific to the RS38000, it did not occur on any of the following platforms: RS1000, RS3000, RS8x00.</p>	30815
<p>WAN - When a T-1 link, on a channelized T-3 port, is forced to the down state via the CLI while the PPP session is established, the output of the command "port show serial-link-info" shows the channel as "up". However the output of the command "port show port-status t3.slot.port.lgn:channel" will show the port is actually "down". This is a display only issue and has been corrected in this release of firmware.</p>	31418



CUSTOMER RELEASE NOTES

Issues Resolved in version 8.0.3.7	ID
<p>System – The RS console can become unresponsive when a poor connections is made to a fiber optic GBIC gigabit port. When the fiber isn't completely plugged in or the fiber is damaged the link LED on the receiver end of the bad or disconnected fiber will be red. This condition causes periodic interrupts to the CPU for link state change. The result will cause the SR_H task to busy thus competing for CPU resources with the console task. In some cases the following error messages may also be displayed in the console:            %SR-W-SPURIOUSINT, spurious interrupt, unknown reason 0x0            %STP-I-PORT_STATUS, Port status change detected: gi.1.2 - Port Down            %STP-I-PORT_STATUS, Port status change detected: gi.1.2 - Port Up</p> <p>a threshold has now been defined, when this condition is identified the port will be disabled for a period of 5 seconds and the following message will be displayed:            %SYS-E-UNSTABLE_LINK, Port gi.14.1 disabled due to unstable link.</p> <p>followed by the usual port-down message...            %STP-I-PORT_STATUS, Port status change detected: gi.14.1 - Port Down</p> <p>This process will repeat until the condition is corrected.</p>	<p>31431 31679</p>
<p>ISIS – With multiple ISIS routers on the same LAN, and when the DIS has more than one IP address associated with its interface to the LAN (there are at least two IP networks on the LAN). A routing loop can occur between the non-DIS routers when one of the two networks is no longer reachable by the DIS. Traffic will bounce between the two routers that have appeared to have advertised a route to the network for which they have no interface. This issue has now been resolved.</p>	<p>31456</p>
<p>Rate Limit – In some cases, negating the entire Rate Limit portion of the configuration, at the same time, can result in a core dump. This problem has now been corrected</p>	<p>31483</p>
<p>WAN T3 - When a T-1 link on T-3 line goes down (Red Alarm) and the command “port disable forced link down” is added to the configuration to hold the link down until it is time to bring it back on line. If the “forced link down” command is removed from the configuration before circuit comes back up the port will remain administratively down and no traffic will pass. With the link up reapplying and negating the “force link down” command will recover the operation of the port. This issue has now been corrected.</p>	<p>31528</p>
<p>L2 – in some cases the application of an L2 filter to limit broadcast traffic between specific ports would also limit traffic on port pairs not specified in the definition of the filter. For example the desire is to filter broadcast traffic from port 1 to port 2, the filter would also filter traffic from port 1 to port 3 ... This issue has now been corrected in this release.</p>	<p>31543</p>
<p>CLI – When changing the configuration of a WAN port, with out negating the original configuration for the port, the CLI will attempt to merge the two commands. Once done it will no longer be possible to negate the command from the configuration since it will have the speed option specified twice. This condition has now been corrected, when the second attempt is made to configure a WAN port the command will be errored out and the change to the configuration will only take place after the original configuration for the port is negated.</p>	<p>31581</p>
<p>IGMP – In an IP multicast network topology with multiple switches, servers, and clients, some of hosts incorrectly timeout of their respective IGMP groups. Modifications have been made to IGMP to allow for redundant server / switch environments so clients won't be prematurely removed from their groups.</p>	<p>31593</p>
<p>POS – In some cases, when configuring SmartTrunks over POS ports it may be necessary to stop and restart PPP in order to establish a connection. IP NCP is not being negotiated on POS links in the SmartTrunk until PPP restarts. This issue has now been corrected.</p>	<p>31613</p>
<p>STP – When an RS is configured with only WAN ports (no Ethernet ports), the error message “%stp-E-xmtgfull” is displayed on the console repeatedly when BPDU packets are received over the WAN ports. This issue has now been resolved.</p>	<p>31700</p>
<p>STP / PVST – In lab tests, it was found that the RS could crash when repeatedly negating and reconfiguring PerVLAN Spanning Tree. This problem has now been resolved.</p>	<p>31708</p>
<p>WAN - Entering port disable on physical WAN port prior to creating a data port (logical channel) causes the port state to be inconsistent. The admin state on the physical port is “down”, but is not copied to the newly created data port, therefore the data port is placed in the up state. This issue has now been corrected.</p>	<p>31755</p>
<p>WAN – The channelized T3 line card can crash when one of the T1 ports is administratively disabled. This condition occurs because although the port is placed into a disabled state PPP is still able to establish a connection. The RS now has additional checks to preclude the Data Link protocol from being able to establish a connection if the port is in a down state even if the physical connection is in an up state.</p>	<p>31862</p>

Issues Resolved in version 8.0.3.6	ID
------------------------------------	----



CUSTOMER RELEASE NOTES

Issues Resolved in version 8.0.3.6	ID
<p>WAN – When configuring Wan ports over a range of VCs, the ports will not be configured properly and the result will be a router core dump at some future point in time. The symptom of this issue is the display of the following list of error messages on the RS console following the activation of the Frame Relay configuration commands.</p> <pre>%STP-E-NOVC, Unable to access VC information %WAN-I-MSG, Loadable module 9: -NOSUPPRESS-VC_UP, VC 5 on port 1 is up %STP-E-NOVC, Unable to access VC information %WAN-I-MSG, Loadable module 9: -NOSUPPRESS-VC_UP, VC 6 on port 1 is up %STP-E-NOVC, Unable to access VC information %WAN-I-MSG, Loadable module 9: -NOSUPPRESS-VC_UP, VC 7 on port 1 is up</pre> <p>This problem has now been corrected.</p>	20238
<p>OSPF – Under some conditions, the RS may crash after clearing the OSPF database, this error condition has recently been attributed to the redistribution of static routes into OSPF. The actual source of the problem was an improperly defined pointer upon clearing the OSPF database. This problem has now been corrected.</p>	28576
<p>PVST – When enabling PVST on channel within channelized T3 port that is already in MLPPP bundle, the PVST command is not marked as an error. When PVST is enabled on an MLPPP virtual port (mp.1), and then the command - "pvst enable port t3.7.1:5" is issued, the CLI should mark the second command in error. Modifications have been made to add a check for this condition and mark the command in error.</p>	28975
<p>VRRP-Stopping VRRP does not clean up entry, route-bit still exists After negating/stopping VRRP, the virtual MAC address's entry is still installed with the Route-also bit. Because of this, when a new master is elected, the previous master still routes packets destined for the virtual MAC, instead of bridging it to the new master.</p>	29129
<p>Route Reflector – In the case where the RS receives a route it originated, due to an error in another vendor's product, the RS mistakenly installs the route. In the case where the RS is also a Route Reflector this improper route is also propagated to the reflector clients. This issue has now been corrected such that the RS will no longer install improper routes of this type.</p>	29520
<p>Port – The RS 10/100 port state remains in the up state even when the ports on each end of the link are intentionally mis-configured for speed. Even though one port is set for 100 Mb/s and the other is set for 120Mb/s the RS port status remains "up", this issue has now been corrected.</p>	29521
<p>QOS - outbound routed packets always have .1p=7 when using the command: "qos set ip &lt;name&gt; &lt;n&gt;"</p> <pre>qos set ip test8 1 1.1.1.17 qos set ip test8 3 1.1.1.19 qos set ip test8 7 1.1.1.23</pre> <p>The actual problem is that the CLI should have rejected these commands because the RS can only change the .1p value for I4-bridged packets. A check has been added, to the CLI, that will reject this command unless a port is specified.</p>	29577
<p>Policy Routing – A crash can occur when the RS is configured with the "ip-router policy export destination " when no export-source is specified. Although this is an invalid configuration, modification has been made to insure a policy will not be created without all of the required configuration components.</p>	29586
<p>ACL - When an ACL is applied to the all-ip keyword, a core dump can occur when the hotswap operation is performed. In this case the keyword "all-ip" was, during the hotswap operation' to be a valid interface name and this caused a crash since "all-ip" is not a real interface. This condition is now handled correctly.</p>	29597
<p>WAN - Unable to delete WAN port-set parameters, even after all of the port dependencies have been removed. This problem was introduced in 8.0.3.3 with the modifications made to the support for adding/negating secondary ip addresses. This problem has now been resolved.</p>	29655
<p>STP – after an 'stp filter-bpdu' command is negated from the RS configuration, PVST BPDUs are still filtered. This issue has now been corrected.</p>	29662
<p>NAT – the output of the 'nat show statistics' command, displays more globals used than the maximum specified. When using NAT with IP Overload, occasionally the statistics displays more globals used than are available. This issue has now been corrected, this was a problem with the statistics not NAT.</p>	29713
<p>Radius Accounting - Radius authentication and accounting is working fine. The issue is with accounting on Telnet and SSH sessions rather than console logins. Telnet session commands are not recorded to an accounting log file. This issue has now been corrected.</p>	29719
<p>SNMP - When a MIB walk is performed on an RS32/30000, after a Control Module failover, the observed behavior is that the RS doesn't populate the physical port information for Channelized T3 cards properly. This problem has been corrected in this release.</p>	29730



CUSTOMER RELEASE NOTES

Issues Resolved in version 8.0.3.6	ID
Route-Reflector – in some cases the Route Reflector server, on the RS, does not withdraw more specific routes from its client routers. If a client has learned a route from IBGP and EBGP, and then learned a more specific route (eg /24 of a /23 network) via IBGP. When the IBGP route /23 is withdrawn before the less-specific route, the client router will not withdraw the /24 as it should. This only happens if the less-specific IBGP route is withdrawn first, before the associated EBGP route. This issue has now been corrected.	29901
DIAG – From time to time, the ATM-OC12 module may fail the SAR SDRAM Memory test. This only happens under extreme testing conditions and is a timing problem with the diagnostic test itself. The diagnostic test has now been modified to operate properly even under extreme test conditions.	30010
Multi-Path – In some cases the RS is incorrectly deleting L3 flow entries that are associated with a multi-path route. In a network configuration with "equal cost" multi-path routes to a specific destination network, if one of the port/interface to the next hop went down, the RS will delete the L3 entries that were actually going out on the other ports/interfaces. Modifications have been made to insure that only L3 entries deleted are those that were going out on the port/interface that went down.	30070
VRRP - When a SmartTrunk comes up, it selects one of its ports as the designated port for broadcast and multicast traffic. The designated port election process is repeated only in the case where the physical port (original designated port) goes down, or the entire SmartTrunk goes down. When the designated port election process occurs, the RS will update all of the flows exiting on any ports within the SmartTrunk. The flow that represents the VRRP MAC address is "special" - flagged as "filtered". Filtered flows are those for which traffic matching them needs to be sent for L3 processing. Filtered flows should not be included in the "update" process triggered by the designated port election. Including filtered flows in this process can cause traffic to be forwarded incorrectly – flooded and unknown L2 traffic. This problem has now been corrected in this release.	30189
Redundant CM – On the RS32000, when booting the router on the Control Module in slot CM/9 and then performing a failover to the Control Module in slot CM/8 and again to the Control Module in slot CM/9, the On-Line LED, on CM/8 remains green instead of yellow/amber. The output for the command "systems show hardware" shows the correct status for both CMs. This issue has now been corrected.	30382
DIAG – Modification have been mad to improve the coverage of the diagnostic tests in the ATM OC-12 module. It was discovered that the current diagnostic test for the ATM OC-12 module didn't cover the entire L2 table memory. In this release of the ROS firmware additional coverage has been added to the diagnostic test facility to insure complete coverage of this memory structure.	30402
SNMP – For the RS16000, the response when polling the MIB variable sysHwNumSlots is 16. The expectation is the value 8 for the actual number of slots in the chassis; the RS16000 has 2 channels per slot where other RS routers such the RS3000 and RS8x00 have a single channel per slot. Modifications have been made to insure the RS16000 reports the correct number of Slots the SNMP variable sysHwNumSlots is poled.	30446

Issues Resolved in version 8.0.3.5	ID
ACL - after removing and adding some QOS commands the RS crashed. The problem was that the partial completion buffer in the CLI structure was limited to 32 bytes. This has now been increased this to 256 bytes. The correct thing to do probably would be to use malloc or sprintf when printing to this buffer, but allocation 256 bytes is more than enough.	21921
ACL - when using port ACL's in a L4 bridging environment, if all ports associated with the ACL are not configured for L4 bridging, the ACL apply line will be errored out, and the permit/deny statement can never be removed unless the RS is rebooted. This issue has now been resolved in this release of the ROS firmware. This bug is related to applying the ACL to the input and output (configuring at separate times) of a specific port.	28578
ARP – An infrequent, spontaneous crash can occur from time to time, it is related to ARP cache maintenance. One of the conditions that can set up an environment for the condition to occur is adding an IP interface to a new T1 channel in a CT3 card. An other might be Multiple BGP peers accessible though the same next hop gateway. ARP Cache maintenance was being performed unnecessarily in these cases.	23815
BGP - when issuing the command "bgp clear peer-host all", the RS may crash and reboot. When the BGP peer is configured with the "shutdown" option and then attempt to clear the peer the RS will crash. This issue has now been resolved	28263
BMON - When multiple ATM ports in the same VLAN with the Ethernet port that BMON is enabled on, the BMON functionality will not operate properly. The BMON implementation has been changed so that by default it monitors broadcasts by reading hardware counters rather than the number of packets arriving at the CPU. The old behavior is still available with the cpu-broadcast option for packets limited. In addition, BMON tracing that previously required a debugger to be attached to set a variable has been given a CLI interface.	27952
CM failover – in the RS38000 a CM failover would cause the entire chassis to reinitialize, with the advent of version 8.0 of the ROS firmware "Hitless Failover was introduced". In order to support this functionality on the RS38000 it was necessary to enhance the Control Module of the RS38000, this enhancement is in the form of a new FPGA. These new control Modules are now available and supported in this release of the ROS firmware.	28334



CUSTOMER RELEASE NOTES

Issues Resolved in version 8.0.3.5	ID								
CM failover – The interface create command are executing on the backup CM, while the MPLS ports in their VLAN have not yet been discovered. This results in an interface being created on a VLAN with no ports in it, which fails due to an MTU error. Unfortunately, when the command fails it leaves some state around which makes it impossible to add the interface later. This problem has now been corrected.	25597								
Custom Forwarding – If both destination based and custom forwarding mode are configured on the same ATM oc-3 port, the destination mode should take precedence. If the card is hot-swapped out and in the forwarding mode will revert to Custom mode. Custom mode forwarding can no longer be configured in the same port with destination or host mode. This is not required as only one mode works at any given time and hence only one should be allowed to be enabled.	26538								
DHCP - DHCP Option 82 , causes DHCP request to be dropped by the Switch unless L2 table is cleared. Once the L2 relearns the I2 information the request is forwarded to the Server. The problem is that the option 82 information is not being appended into the DHCP discover and offer packets, but once we clear the L2 tables the RS now will append the appropriate Option 82 information to the Request and the packet will be acknowledged and the client then will get its IP address.	28591								
ICMP – On occasion, in L4 bridging mode, the RS would evaluate and drop the first two ICMP packets of a stream. This issue has now been addressed in this version of the ROS firmware	28580 28892								
ICMP – The RS places ICMP echo requests in the high priority queue when there is a large volume of ping traffic mixed with large amount of CPU bound traffic the RS may be observed to miss a response from time to time, in actuality an ICMP request gets dropped because the High priority queue is overrun. The command "system set buffs-in-recv-ctrl-only" can be used to increase the size of the high queue. On the ATM line card the ICMP traffic was placed in the Low queue. A modification has been made to place the ICMP traffic, inbound on an ATM port in the High queue.	28265								
ISIS - Command execution failed for "isis set system-id 0000.0000.2054" this is the Binary Coded Decimal form of the ISIS system ID. In this release the system id in BCD format is now supported.	27807								
ISIS – In a network where there is a large number of ISIS adjacency, an adjacency may be dropped periodically. In this release of the ROS firmware, there have been some modifications to improve the diagnostic capabilities for identifying the source of this type of problem.	28163								
OSPF – For some configurations, an OSPF LSA may cause the RS to crash – the LSA has an unexpected TOS value. The RS now saves the TOS information and floods it out in the LSA. This problem has now been corrected.	26970 27307								
OSPF – There is a display issue where the OSPF checksum displayed in the output of the command "ospf show statistics" does not correspond to the checksums reported on the adjacent routers, nor is it the checksum being used in the OSPF LSA. The output of the command "ospf show database" will display the correct checksum. This is the checksum that is being in the LSAs. This issue has been corrected in this release.	28117								
OSPF – There is a Minor display issue of the descriptive text for "ospf set interface strict-routers" option. The CLI states the default is OFF, but the actual default is ON. The online help has been modified to reflect the actual default.	28251 28408								
Port - Display issue with the output of the command " port show autonegotiation-capabilities gi.*" where the Received bandwidth . capability is stated to be "100 base TX FD"  <table border="0" data-bbox="243 1333 925 1407"> <thead> <tr> <th><u>Port</u></th> <th><u>Capability</u></th> <th><u>Advertised</u></th> <th><u>Received</u></th> </tr> </thead> <tbody> <tr> <td>gi.7.1</td> <td>Asym-Sym Pause 1000 baseX FD</td> <td>Asym-Sym Pause 1000 baseX FD</td> <td>100 baseTX FD Asym-Sym Pause</td> </tr> </tbody> </table> This display issue has now been resolved.	<u>Port</u>	<u>Capability</u>	<u>Advertised</u>	<u>Received</u>	gi.7.1	Asym-Sym Pause 1000 baseX FD	Asym-Sym Pause 1000 baseX FD	100 baseTX FD Asym-Sym Pause	27814
<u>Port</u>	<u>Capability</u>	<u>Advertised</u>	<u>Received</u>						
gi.7.1	Asym-Sym Pause 1000 baseX FD	Asym-Sym Pause 1000 baseX FD	100 baseTX FD Asym-Sym Pause						
Port – It is not possible to add a port description to either a SmartTrunk or ports belonging to the SmartTrunk. In this release, it is possible to specify a port description for a SmartTrunk port and/or the ports within the SmartTrunk.	27882								
Port – The Hash mode set on a port will revert to its default value if the port has been added to a SmartTrunk and then removed from the SmartTrunk. Modifications have been made to correct this issue, the hash mode will remain consistent even after the port is added to and removed from a SmartTrunk.	27015								
POS- Adding a VLAN to a POS OC3 trunk port it will cause the PPP NCP/LCP to bounce. When adding a VLAN to a POS OC3 port in trunk mode, the port's PPP NCP and LCP are brought down and back up. This behavior has now been corrected.	27595								
QOS – On the gigabit cards on the RS38000, QOS set weighted-fair queuing operates incorrectly with regard to the distribution of traffic across the control, high, medium and low priority queues. This issue has been corrected in this version of the firmware. However, it is important to remember that when setting the percentages for WFQ, any unused time by any priority gets assigned to the highest priority that needs it. Example, 50% ctl, 15% hi, 10% med and 25% low. If there is no medium traffic, the control queue will have access to 60% of the time if it needs it.	27964								
QOS – when issuing the command "qos show one-p-priority-overwrite-with-map all", to view the .1p priority mapping, the RS may crash. Modification to the way the QOS data structures are accessed have been made to connect this problem.	27421 27424								



CUSTOMER RELEASE NOTES

Issues Resolved in version 8.0.3.5	ID
SNMP – The RS implementation of SNMP, prior to version 9.0.0.0, is based on an SNMP v1 Agent. With the implementation of the high speed line cards , this implementation of SNMP was enhanced to support 64 bit counters. Recently a version check was added to insure consistence response to queries for various versions of SNMP, the RS (running pre version 9.0 firmware) will no longer respond to SNMP v2 or v3 queries.	28328
SNMP – The SNMP trap source, when configured with the command “snmp set trap-source 10.23.34.45” does not take effect until the RS is rebooted. The trap handler has now be modified dynamically reconfigure as the router configuration is changed.	28164
STP – In some configurations the STP Filter-BPDU stops filtering when the VLAN port list is changed. The result of the condition is continuous topology change events. This condition has now been corrected.	26091
WAN – In some configurations a traffic interruption can occur after an IP interface is removed from VLAN containing a WAN port. Problem occurs when the ip interface is removed, traffic totally stops. The VLAN shows both ports still on the same VLAN. When this condition occurs the following error will be displayed on the consol.  %L2TM-W-INVALID_WAN_VLAN, WAN Module in slot number 3 is receiving frames from non-member VLAN (1). Possible misconfiguration.  This problem has now been corrected	27213
WAN – The port statistics on the Serial line card, configured for MLPPP, displays the same statistics for all of the ports in the MLP bundle. The main problem found and fixed was that the MLP bundle RX & TX stats were being shown for ports that were part of an MLP bundle, but that were non operational.	28357

Issues Resolved in version 8.0.3.4	ID
ARP – Gateway ARP packets are sent every 30 seconds, modifications in this version of the ROS firmware have been made to restrict the transmission of Gateway ARP messages to within 30 seconds of its expiration.	27881
ARP – The ATM static ARP entry is deleted if an ATM port is removed from a VLAN. This issue has now been corrected.	27294 27364
ATM - Cross-connect is not operating in this release - generating error: %L2TM-W-INVALID_VLAN. This problem has now been corrected.	27105
ATM – Modifications have been made to provide support for bridging IPX 802.3 raw packets.	25623
ATM – The ATM OC12 connection is not coming up over a trunk port, this problem happens intermittently and has now been corrected.	27853
ATM – The ATM static ARP entrees are removed when an Ethernet line card is hotswap out. This issue has now been corrected.	27608
ATM – When a VC is removed from a VLAN, the Layer 2 table information may become corrupt interrupting the transmission of traffic. This issue has now been corrected.	27297
ATM OC12 – In some cases the ATM OC12 port will corrupt IEEE802.3 formatted frames, this is the type of encapsulation used on IPX raw packet format. The corruption problem has now been corrected.	25126
ATM OC12 -when a VC is negated from a VLAN, it should only remove the one ARP entry associated with it and it's peer address. The problem has now been corrected so when a VC is negated the static ARP entries for the other ARP entries will no longer be removed.	27434
ATM OC3- Traffic through an ATM OC3 port may fail, after closing greater than 64 VCs. This problem has now been resolved.	27946
CLI – Comment commands with overlapping ranges of line numbers can result in a crash. The RS will no longer allow overlapping or descending comment ranges.	27571
CLI/Telnet - When DHCP debug and terminal monitoring are turned on DHCP file output is showing up in the monitoring telnet session. Modifications have been made to insure the DHCP file output does not show up in terminal monitoring session.	27900
CLI/WAN – Changes have been made to the order of execution of certain of the configuration commands. These commands have to do with the logging and display of various categories of syslog messages.	27665
DHCP – Support for large numbers of clients and short lease times -Make sure we do not fill up the virtual file system with the DHCP lease database when there is a large number of DHCP clients and a relatively small lease time.	27171



CUSTOMER RELEASE NOTES

Issues Resolved in version 8.0.3.4	ID
Hotswap – After hot swapping out an ATM line card, a series of the following error messages may be displayed on the console: ERROR: channel_SOPP_Get_EPT16 called by slave CPU during hotswap This had no effect on the operation of the router and has now been resolved.	27889
HRT - HRT is not functioning properly after it has been disabled and then re-enabled, due to lack of memory. The following error may be displayed - %HRT-E-NOMEMFORINTNODE. HRT will now re-start when it is re-enabled.	27658
HRT – The Backup-CM takes over after disabling and the re-enabling HRT. This issue has now been corrected.	27808
ISIS – Setting the ISIS system ID to and invalid value can result in a system crash. This issue has now been corrected.	27563
MPLS - When attempting to configure a VLAN based FEC, after the FEC is connected to the remote peer, when adding another port to the VLAN the static filters are not properly updated. The result is that communication with the remote peer through the new port is not successful.	27557
Port Mirroring - Port-mirroring on T1 interface will inhibit OSPF adjacencies from being formed; this issue has now been corrected.	26570
QOS - The QOS does not appear to work when used at L2 with L4-bridging and the QOS specified on the IP header. A warning message has been added that warns user to specify port(s) if the rule is to be applied to l4-bridged traffic.	27101
Redundant CM – After CM failover, perform a hotswap-in of a gigabit line card, line card and ports do not show up in system show hardware. This issue has now been corrected.	26005 27759
Redundant CM – During the boot process a CM failover can occur if the router is configured with a large number of WAN modules. Modifications have been made to the heartbeat task to insure this premature take-over by the Backup CM does not occur any longer.	27681
Redundant CM – During the period of time where the Backup CM is booting and the Master CM identifies it presents, if a hotswap operation is initiated on the Master CM the Backup will crash. Modifications have been made to minimize the possibility of this event.	27485
Redundant CM – The Backup CM can appear to hang if during the boot process the Active configuration is modified (save active) or the Startup configuration is modified (save startup). A protection mechanism has been added to keep the synchronization process from executing if the Backup CM hasn't completed the boot process.	27158
Redundant CM – The Backup CM can crash when attempting to access some functions reserved for access by the Master CM. Therefore a check has been added "I Am Master" before attempting to access these structures.	27300
Redundant CM – The configuration on the Backup CM is not the same as that on the Master CM. Modifications have been made to insure that the two active configurations get out of sync.	27614
Redundant CM – When attempting to hotswap out a line card during a Control Module failover can cause the RS to crash. Modifications have been made to complete the hotswap out operation prior to allowing the failover operation to initiate. Now when attempting to force a CM failover when a hotswap operation is in progress the following informational message will appear: %HBT-I-FAILOVER_DURING_HOTSWAP_OUT, CPU failover - waiting for Hotswap Out to complete	26673
SNMP - Added support to display default bucket in CICS0-BGP-ACCOUNTING-MIB.txt. Modified traffic index ranges in the MIB to include 0. Note: a new MIB which is part of the 9001 branch contains support for these latest changes.	27613
SNMP - ifInOctets for individual T1's showing the same statistics as mlp bundle, not the statistics for the individual T1. This issue has now been corrected.	25560
SNMP – The output of the snmp show trap authentication has a display problem. The CLI output of "snmp show trap" has been fixed to reflect the correct setting of authentication trap enable/disable. This is the behavior of authentication trap after the modification: 1. The SNMP authentication traps are disabled by default (on startup) 2. In order to enable them, one has to do the following: - add the command "snmp disable trap authentication" to the configuration. - save active - negate the command - save active ← This will enable authentication traps 3. After this, adding the command "snmp disable trap authentication" to the config will disable authentication traps again.	27379
SNMP – the RMON Utilization History MIB reporting incorrect value, the RS is displaying 10 * 1% instead of 100 * 1% which is specified by the MIB. The value of etherHistoryUtilization is still significant up to a percent instead of hundredth of a percent.	27262
SNMP / OSPF – Under some cases doing a MIB walk through the OSPF MIB the RS may crash; this problem has now been corrected.	27175
STP – In a Stackable VLAN environment with STP enabled –a tunneled BPDU is forwarded out a port blocked by STP, this should not be the case. This problem has now been corrected.	27458



CUSTOMER RELEASE NOTES

Issues Resolved in version 8.0.3.4	ID
System - Removed a potentially dangerous situation where a Ctrl-S can suspend indefinitely tasks other than the console that require write access to the serial port.	27775
Telnet – Killing a telnet session that is in the process of some action such as a ping may result in a system crash. Protection has now been added to insure this type of action will not crash the system.	26233
WAN – On WAN ports the CLI allows configuration commands to be negated from the configuration in such a way that the WAN related configuration is no longer valid. In the event this happens the following type of error messages might be seen depending on the type of traffic arriving at the RS. %L2TM-W-INVALID_WAN_VLAN, WAN Module in slot number 3 is receiving frames from non-member VLAN (1). Possible misconfiguration Now this problem has been corrected, the RS will now display the message: %SYS-E-PORT_NEGATE, port can't be negated before all the other commands related to the port are negated	27213
WAN - Unable to delete a wan port set parameters - if an interface has been created over that port and the interface has been deleted. This issue has now been resolved.	27568
WAN - when the RS is rebooted, the CPU can get over loaded with warning messages sent from the WAN card. This condition occurs when there are a very large number of connections defined over the high capacity WAN cards and a lot of traffic is present at boot time. This issue has now been resolved.	27386

Issues Resolved in version 8.0.3.3	ID
ATM – In some cases, after a CM fail over, ARPs, over WAN interfaces, get resolved for the wrong exit port. This turned out to be a synchronization issue between the primary and backup CM.	24830
CM – under some circumstances the error message %CPU_TASK-W-NOBACKUP, There is no Backup CM is printed repeatedly on the console of the Control Module in a router configuration where no backup Control module exists. This message is not necessary and has been removed.	26344
CT3 – Traffic on the primary interface can be interrupted, when negating a secondary IP address from the primary interface. This problem has now been corrected.	26303
GateD – in some configurations of a large number of interfaces, a port changing state can result in the gated task consuming CPU cycles when checking for duplicate interfaces. Performance improvements have been implemented in this release of the ROS firmware.	26425
Hot swap - Under certain circumstances, with custom mode forwarding enabled, the following message may be observed following a hotswap out: %IP-E-BADMEM, SIPP_delete_ip_addr_for_channel level0_of	26501 27099
Hotswap – In some cases when hotswapping in an MPLS will be unsuccessful and the result will be the following message in the system console. %SYS-I-HOTSWAP_INQUEUED, hotswap busy, request for hotswap-in slot 1  This condition can occur if the CM fails over from Master to Backup between the time the card was hot swapped out and back in.	26617
Hot-Swap – The message "%SYS-I-HOTSWAP_NOT_ALLOWED, Hotswap not allowed while Backup CM is processing config" may be displayed inappropriately, the operation of the router is OK.	23393
Hotswap – Under some cases, when a Ethernet card, with a large number (approximately 200 or greater) of IP interfaces and OSPF adjacencies, is hotswapped out and back in, a core dump can occur. This issue has now been corrected.	26785
HRT – Under some circumstances, after removing output ACL's, HRT enabled ports are not reverting to HRT mode. This issue has now been resolved.	27052
HRT -after changing from Custom mode forwarding (cust-forward-mode) to Hardware Routing Table (hrt) the RS crashed at %HRT-F-BADFREE, Freeing Invalid Address. This problem has now been corrected	26412
ICMP – Performance improvement has been made by changing the default behavior for ICMP redirects, by default the RS will not send ICMP redirects. The RS can be configured to send ICMP redirects.	26249
L3-TM – There is a condition that can occur where an layer 3 table entry can become corrupt and when it is deleted from the L3 table the RS will crash. Prior to the router crashing it was reported that the router hung for a short period of time. The L3 table maintenance function has now been modified to protected against this event.	26644
LFAP – In L4-Bridging configurations LFAP was unable to account for all of the traffic forwarded through the router.	26343



CUSTOMER RELEASE NOTES

Issues Resolved in version 8.0.3.3	ID
LFAP – Recently is has been identified that LFAP is not accounting for packet fragments, this issue has now been corrected.	26076
MPLS/LDP - After hotswaping an mpls module, the interfaces are removed from ldp. The config "ldp add interface xxx" will be marked as an error "E". To recover, it is necessary to restart ldp so the interface will be added back to the LDP configuration. This problem has now been corrected.	26609
MPLS/LDP – Under some circumstances, issuing the command "ldp clear all" or "ip age all" will result in a system crash. This issue has now been corrected.	18811
Multicast – repeatedly changing multicast groups can cause video quality to degrade on the new channel and sometimes 'freezes'. It was determined that traffic is being sent through the CPU unnecessarily. This issue has now been resolved.	24649
OSPF – In some cases a crash can occur after executing the command 'ospf monitor neighbors'.	25216
Port Mirror - Enabling Port mirroring on an ACL, regardless of the interface associated with the ACL, will stop all of the traffic over ATM interfaces. This issue has now been resolved.	21491
Port Mirroring - When port-mirroring is applied to an Ethernet port in the same configuration as an ATM, traffic on the ATM port stops. The symptom of this situations is that the dropped packet counter for the ATM port increment. The ATM OC-12 card will also display an error message ATM_OC12-E-MSG, ATM module 1: -ATM-INGRESSVCDOWN, VCL is down: ingress packet is discarded. Functionality has now been added to allow port mirroring to be configured in routers containing ATM cards.	15824
Port Statistics – In some cases using the command "statistics clear port-stats" does not clear statistics the statistics associated with the specified port, this issue has now been corrected.	27089
QOS - If a QOS configuration is set up such that the QOS commands are not fully specified, such as: qos set ip MED medium 224.0.0.0/8 any as opposed to: qos set ip MED medium 224.0.0.0/8 any any any any any any any any any any any any qos set ip MED medium any 224.0.0.0/8 any any any any any any any any any any any any Not specifying the full command. When you enter the command it is fine. But when you reboot the box with the command saved to startup, the priority is changed, and the volume of traffic may overrun the QOS queue to which it is now mapped.	26482
Rate Limit – It was identified the IP DOS rate Limit function was not accepting a rate lower than 128K for the " ICMP, OSPF, modifications have been made to allow finer resolution when configuring this function.	27028
Rate limiting – when applying rate-limiting on a 16 port line card, the RS stops forwarding traffic for 2 seconds. The larger the number of ports on which rate-limiting is configured, the longer the RS stops working. This issue has now been resolved.	26215
RS16000 - The Backup CPU on 16K system, which should have the advanced ASIC features such as HRT enabled, doesn't. Hence, as long as the original master CM is operational, the HRT mode is set, but the moment the Backup CM takes over HRT is disabled and will remain disabled through subsequent fail-overs. The router must be power cycled to recover. This Problem has now been corrected.	25641
SmartTrunk - Under some circumstances, SmartTrunk flows do not recover when ports, of same line card, go down/up. When one of the links within a SmartTrunk goes down and then back up, in bound traffic on that port does not get forwarded. This issue has now been corrected.	26995
SNMP – In testing this version of the of ROS against the "CERT Advisory CA-2002-03 Multiple Vulnerabilities in Many Implementations SNMP" a small memory leak was detected and has now been corrected.	26834
SRT – Currently, SRT is initialized to wildcard all the fields and the route lookup mode is "flow-route". If a flow already exists in the hash location where the initialized SRT flow would be located, the already existing flow can be used to forward the inbound traffic, as opposed to the SRT flow. SRT is now initialized with no wildcarding.	27074
Stackable VLANs – When Stackable VLANs are configured over ATM, L2 flood ports for Stackable VLAN over ATM do not get entered into the L2 table upon reboot, this issue has now been corrected.	26994
Statistics – There is an issue with the Physical Error Statistics, in that under certain circumstances the "RX frames Okay" counter displays a negative value, this issue has now been corrected.	25792
Telnet – There is a DOS vulnerability where telnet Password Guessing temporally consumes memory. The message "Out of Memory" would be displayed on the RS console. Mechanisms have now been put in place to protect against this type of attack.	26936
Time Zone - setting the time-zone to a numeric value instead uct+X does not function properly. This issue has now been resolved.	25924



CUSTOMER RELEASE NOTES

Issues Resolved in version 8.0.3.3	ID
Web-Cache - When a web-cache policy is applied on an interface, all the packets that traverse the interface and are forwarded by the CPU will cause a debug message to be printed on the console. The result can be high CPU utilization and an un-useable console port, this issue has now been resolved.	26300

Issues Resolved in version 8.0.3.2	ID
ACL / L2 Filters – blocking RIP traffic with an ACL and a l2 filter in a LAN environment is not completely successful, it does result in the RIP packets being sent to the CPU for TTL expired. These packets should be dropped as well, this issue has now been resolved.	25279
ARP - removing the trunk port from VLAN will not age out the ARP entries associated with the port and traffic continues to flows. This problem has now been corrected.	25015
ARP – The system would send ARP requests for addresses which have static ARP entries. This behavior has now been corrected.	26007
ARP - When setting the arp keep-time, 'arp set interface all keep-time 60', the arp entry is still in the arp table after 60 seconds. This was due to the resolution of the ARP aging timer. The resolution of the timer has been increased to improve the accuracy of the aging.	22300
ATM – in some cases creating a large number of ATM VCs, with the create range command (atm create vcl port at.7.1.0.1-250), will error out after the router is rebooted. This issue has been corrected in this release.	25158
ATM – Interfaces created with VLAN option produces warnings about wrong subnet. 2001-12-18 13:45:19 %ATM_OC12-W-MSG, ATM module 3: -ATM-L3_ERROR_INARP_DSTADDR, could not find any l3 entry which is on the same subnet as the given peer address(10.10.1.1). This issue has now been corrected.	24966
ATM – On a router configured with an ATM OC-3 card, a core dump may occur after CM fail-over, and an IP multicast client leaves an IGMP group.	24617
ATM – On the ATM OC-3 line card, IGMP leaves are not processed correctly over the ATM OC-3's PVCs.	24736
ATM - Removing peer address removes VC from VLAN. This case only occurs when the IP interface is created with the vlan option rather than the port option. Removing the peer address removes the VC from VLAN. This inhibits any bridge operations on the VC. This problem has now been corrected.	24869
ATM – The 4 Port ATM line card, when not fully populated with PHYs, may not be recognized by the backup CM when it is hot-swapped in. The workaround is to insert all four ATM PHYs.	24781 24751
ATM – When the ATM OC-3 port is configured with a large number of VCs in a large number of VLANs (~600) the console can appear to hang and the boot time can increase by 4 to 5 minutes.	24222
ATM - When the system polls the inventory for port state, if a bad port is encountered, the system may core dump. A missing PHY on an ATM card can cause a core dump after CM Fail-over occurs because the missing PHY is considered to be a bad port under this circumstance.	24751
Backup CM –making configuration changes while the backup CM is booting can cause the backup CM to not properly initialize the hardware of the system. The primary CM will no longer send updates to the Backup CM until it's boot process has completed.	24657
BGP - When the syslog server is unreachable, the BGP may log-up-down messages causing the console to be unusable for several minutes. Make sure syslog server is reachable to avoid this problem.	24672
BMON - When BMON is enabled the following ERR_errlog message is printed to the console continuously. This problem has now been corrected. %SYS-E-GET_PORT_SEM, getting system active port semaphore failed -24	25312
CLI – A core dump can occur when telnetting into the RS and then entering characters in Hanja (Korean Hanja 2byte mode). This problem has now been corrected.	24287
CM Fail-over – under some circumstances, the RS38000 backup CM crashes on boot-up when rebooting master from slot 9.	24678
CT3 –Testing for the bit error rate (BERT) on a Channelized T3 card would always result in no sync.	26483



CUSTOMER RELEASE NOTES

Issues Resolved in version 8.0.3.2	ID
DHCP - In some cases the output to the command "dhcp show binding" contains what appear to be invalid hardware addresses. This us usually followed by a spurious DB-EMPTY message is being displayed. The error message was in error and corrected in this release of firmware. The address format is due to the dhcp spec allowing up to 16 bytes for the address. The output of the "dhcp show binding" is based on a 6 byte MAC address since it is the form of address in the greatest use.	25165
Hot-swap – Hot-swapping a card in and out of one slot and then into different slot may cause the backup CM to crash.	24718 24768
Hotswap - Hotswapping in an unpopulated atm OC-3 line card ina system with a redundant CM will fail to recognize the existing ModPHYS. The self diagnostic check reports errors when the cardis inserted. The message for the port without a PHY should be "port not detected" but "port not operational" is reported and the ATM card is unusable after failover to the Backup CM. 2001-12-13 16:31:19 %SYS-I-HOTSWAPIN, module in slot 1 is hotswapped in 2001-12-13 16:31:19 %SYS-E-PORTNOTOPER, Port at.1.3 is not operational. 2001-12-13 16:31:19 %SYS-E-PORTNOTOPER, Port at.1.4 is not operational.	24781
Hot-swap – In some cases hot-swapping a out POS card can causes the "INTERFACE-E-ZEROPORTSINIF" message to be displayed on the system console repeatedly. During this period the console may become inaccessible.	24329
HRT – If the Hardware Routing Table (HRT) is enabled on an RS16000 with Control Module (CM) redundancy, a crash can occur immediatly following the failover.	24651
HRT - pings to the Backup CM on a 16000 fail after change-mastership. This problem has now been corrected.	25177
IP Stack – The crash due to a null pointer reference for an IP interface, seen at Macon Georgia, has been resolved in this release.	25964
IP-HELPER – If the IP helper (DHCP relay) server is not reachable, an error message would be printed indicating this condition for each DHCP packet. This message is now limited from being printed more than 5 times per 10 seconds.	26067
Load Balance – A crash can occur after commenting out the load-balance configuration commands and then issuing the command "show virtual-hosts". This issue has now been corrected.	25368
MPLS – Changing an MPLS associated port from trunk mode to access mode could result in a crash.	25906
MPLS – The "input vlan drop frame" counter does not work on MPLS line cards when they are not configured for MPLS mode.	22390
MPLS -The in some cases the ILM table can contain the wrong ILM entry and the traffic is hitting the empty ILM entry, the result is that the traffic is dropped. After the execution of the "mpls clear all" command the condition is resolved. The problem has been observed under certain dynamic condition, and has been quite difficult to reproduce.	24637
OSPF – OSPF trap issue, the symptoms of this problem are there are many OSPF traps generated by the RS and the spf task is running a relatively high rate in the CPU. This issue has now been resolved in this release.	25909
OSPF MIB: router crashed while doing "get" on certain portions of the OSPF MIB may resulting a core dump. One area where this behavior has been observed is while doing get on one of the following two variables: getone -v1 10.51.50.123 ospfAreaStatus.0.0.0.1 getone -v1 10.51.50.123 ospfLsdbAreald.0.0.0.0.1.11.11.11.11.11.11.11.11.11	24835
Port duplex – repeatedly changing a port from full-duplex to auto-negotiation will eventually result in the port generating collisions and deferred transmissions. This issue has now been corrected.	25344
Port Mirror - when negating port-mirror command from the RS configuration the router can crash. This condition will only occur when port mirroring an ACL. This issue has now been corrected.	22805
Port Mirror – When port mirroring is enabled the out bound traffic destine for the target port can be interrupted. Do not enable port mirroring with 8.0.3.0 firmware, this problem will be corrected with 8.0.2.1 and 8.0.3.1 patch releases.	24890
Port Mirror - With port mirroring is configured, it may not be possible to ping or telnet through the target port.	24128
Port Mirroring – traffic inbound on a SmartTrunk port may not be mirrored when the configuration of the SmartTrunk changes. This issue has now been corrected	25496
Port mirroring – under certain conditions, traffic is blocked on the target port when port mirroring is enabled. This issue has now been corrected.	25041
POST - Power on Self Test has %DDT-E-XBAR_FABRIC errors when ATM OC-12 card exists. This diagnostic test has now been corrected.	25221



CUSTOMER RELEASE NOTES

Issues Resolved in version 8.0.3.2	ID
SMARTTRUNK – If a smarttrunk includes ports from multiple cards, flooded traffic (traffic for which the destination is unknown) will not fail over to the backup ports when the flooded port is disabled.	25422
Smarttrunk – The port state is shown as UP even when the physical link is down. This is a display issue in the output of the SmartTrunk status and has now been corrected.	24571
SmartTrunk – When a SmartTrunk is configured across multiple line cards and the primary link is removed, any layer-2 flooded traffic does not get redistributed to the remaining links.	25422
SNMP – The ifInOctets and ifOutOctets OIDs were reported incorrectly for ATM-OC12 ports.	26107
SNMP – The ifSpeed and ifHighSpeed OIDs were reported incorrectly for GigE, ATM-OC3, and ATM-OC12 ports.	26095
SNMP - When setting the ifMauDefaultType to anything other than the default 100Mbps HD, the ifMauType is not set to default when ifAutoNegAdminStatus is changed to disabled. This issue has now been corrected.	23664
SSH – A crash could occur when logged into the system via SSH and using the “cli terminal monitor” facility.	26080 26234
SSH – control C (^C) is not being recognized when connecting to the router using SSH. This issue has now been corrected.	25292
SSH - SSH CRC attack detection has been added to ros8030-s3 build. This function is to protect the RS from an attempt to gain access to the system. The intention of this attack is to gain privileged access to a system, This would probably never be successful on a router, the reported results is that more often than not the target of the attack crashes before allowing unauthorized access to the system.	25996 25514
SSH – The non-interactive mode of SSH is not supported, receipt of specific non-interactive commands can cause the RS to core dump. The SSH server is now protected from these non-interactive SSH commands it might receive.	24885
STP - STP message age is incorrect immediately following a port status change. The message is usually 2 seconds, but for the first BPDU transmitted after a port transition the message was 3 seconds. This issue has now been corrected.	25414
Syslog – In version 8.0.3.0 the option for a local copy of the syslog was added. The intended implementation was a Local (active) copy, with a maximum size specified. In addition, it was intended to have a prev_syslog file to preserve the information logged through the next reboot. Each successive reboot should then over write the previous perv_syslog file, but multiple copies of prev_syslog, were being created until the boot-flash was exhausted. This problem has been corrected, now there will be just one previous copy of the syslog at any point in time.	25931
SYSTEM – If the “local_copy” option for “system set syslog” is used, older copies of the syslog were not properly deleted during a reboot causing the number of files to increase on the flash card until full.	25960
SYSTEM – Under some situations, the switching fabric may arbitrarily reset itself, this will induce a very short delay on the transmission of a few packets when the reset occurs. The frequency between resets may be as short as 40 minutes and the duration of the reset is less than 1.5 seconds. The Switch Fabric Reset interrupt handler has been modified to identify and filter out “spurious” interrupts if the Fabric heartbeat packets are still being received correctly. This problem has now been resolved.	25905
SYSTEM – When receiving an IP packet which cannot be routed or handled, a blocking flow is ordinarily installed. This process did not occur correctly for packets which contained a well known destination/service (TELNET, HTTP, SNMP, SSH). A blocking flow is now created and/or rate limited for packets with these well known destination ports.	26062 26241 26243 26422 26507
SYSTEM – When routing, receiving an IP packet with invalid options could cause the system to crash.	25053
VLAN Aggregation – Under some conditions when VLANs have been aggregated into a super VLAN, communications between the subVLANs can be interrupted. If the layer 2 table entries for the aggregated VLAN are aged out, then traffic will again flow between the subVLANs. The workaround, to minimize the duration of this condition, should it occur, would be to reduce Layer-2 aging time to 15 seconds.	24802
VRRP - The vrrp operational state of the router is not consistent with the vrrp walk of the MIB vrrpOperState. When the vrrp state of the router is 'master' the mib shows 'backup' and vice versa. This inconsistency has now been corrected.	24775
WEB-CACHE – The counter showing the number of flows being cached would not increment. Additionally, a debug message would be printed to the console if a packet is received while there is no web-cache server available.	24888 26536
Web-cache – under some circumstances the web cache used counter is not properly incremented, this has now been corrected.	24888




Issues Resolved in version 8.0.3.1	ID
ATM – If an IP interface is created over a VLAN and the ports with in the VLAN are changed, traffic across the interface will be disrupted indefinitely. This problem has now been corrected.	25144
ATM OC12 – A memory leak can occur when receiving specific types of unsupported traffic on the ATP VC. It was recently determined that a memory leak can occur when the ATM LANE packets such as EGRESS_LANE_ECHO, EGRESS_LANE2_LLC, EGRESS_FORCED_CPU_XMIT, EGRESS_FORCED_BDG_DROP or EGRESS_RERR arrive at the ATM oc12 port of the RS. The RS has no support for ATM LAN Emulation. This issue has now been corrected.	25237
ATM OC3 – For IEEE802 formatted frames the ATM OC3 card tends to drop the length information and shift all subsequent bytes by two when transmitting the frame. This issue only shows up in a bridges Atm environment with non IP traffic. This problem has now been resolved.	25382
ATM-OC12 - -ATM-INGRESSVCDOWN are displayed repeatedly on the main console. It was determined that in a bridged and routed environment the presents of invalid layer 2 multicast packets would result in the above messages being displayed on the RS console. In addition to the above messages some IEEE802 encapsulated frames were corrupted. This problem is limited to bridged traffic and does not effect Ethernet V2 formatted frames, This problem has been resolved in this release.	25186 25188
ATM-OC12 – under some conditions the inbound traffic path, to the RS, enters a locked state. This condition is seen when incoming bridged frames are IEEE802 encapsulated and is more likely when the inbound traffic must be flooded to a series of outbound ports. This problem has now been resolved.	09468 25233
Hot Swap - When hotswapping out a line card, that is configured with an IP custom forwarding mode, the router crash. This is by the order of a couple of operations in the hotswap sequence. Part of the configuration clean up process was executed after the hotswap operation had completed. Thos issue has now been resolved.	25252
HRT / MPLS – when configuring Hardware Routing is configured on an MPLS line card running in gigabit mode, if may be seen that ping traffic doesn't go thru the RS. When HRT is disabled on an MPLS port, the traffic passes successfully. This problem has now been resolved.	25168
PoS / PPP - When PoS OC-3 link is brought down and up, IPCP does not always come back up. This problem has been resolved by ensuring that PPP negotiations to bring the port up are invoked *immediately* after STP indicates the port is up.  Note: the RS by default always initiates BCP (bridging) negotiations and if the peer (Cisco GSR or Juniper) does not support bridging it'll reject it and the negotiations fails. This is normal behavior and should not cause any concern.	25527
Telnet – Under some circumstances, when a ping flood is in progress through a telnet session and the telnet session is killed, the result is the RS may crash.	24785 21238

Issues Resolved in version 8.0.3.0	ID
ATM – If the ATM line card not fully populated with Mod-PHYs it will not be recognized by the slave CPU when hot-swapped in. When hot-swapping in unpopulated ATM line card after boot-up the slave fails to recognize even the existing phy's. Instead of the ports “port not detected”, but the message generated is “port not operational”. After a CM failover the ATM card is not operational. These are messages displayed on the backup CM console after a hotswap In for module 1: 2001-12-13 16:31:07 %SYS-I-HOTSWAP_INRXD, received hotswapped-in request for slot 1, detecting, please wait 2001-12-13 16:31:18 %SYS-I-PORTNOTDETECTED, Port at.1.3 not detected. 2001-12-13 16:31:18 %SYS-I-PORTNOTDETECTED, Port at.1.4 not detected. 2001-12-13 16:31:18 %SYS-I-DSCVMOD, discovered '4-ATM "T" module in slot 1 2001-12-13 16:31:18 %SYS-I-INITPORT, initialized slot 1, port 1 2001-12-13 16:31:18 %SYS-I-INITPORT, initialized slot 1, port 2 2001-12-13 16:31:18 %SYS-E-PORTNOTOPER, Port at.1.1 is not operational. 2001-12-13 16:31:18 %SYS-E-PORTNOTOPER, Port at.1.2 is not operational. 2001-12-13 16:31:19 %SYS-I-HOTSWAPIN, module in slot 1 is hotswapped in 2001-12-13 16:31:19 %SYS-E-PORTNOTOPER, Port at.1.3 is not operational. 2001-12-13 16:31:19 %SYS-E-PORTNOTOPER, Port at.1.4 is not operational. This issue has now been resolved in this release of the ROS firmware.	24750
ATM – Improved performance scalability for OAM packets.	23537
FLOW-BRIDGING – GVRP could stop functioning after a few minutes if running in flow bridging mode.	24009 22830
ML-PPP – Defining the MTU for an ip interface on an MLP port (eg. port mp.1) would cause an invalid option error.	23995



CUSTOMER RELEASE NOTES

Issues Resolved in version 8.0.3.0	ID
ML-PPP – If running multilink PPP and your configuration file includes “stp set vlan-disable” (used to eliminate messages warning that an interface is receiving packets for a VLAN it isn’t a member of), then when a T1 in the multilink bundle is taken out of service, traffic may not redistribute properly across the remaining ports which are in service.	19521
MPLS – LDP sessions could bounce when the ROSRD is busy processing routes.	23763
MPLS – under some conditions, when deleting an MPLS neighbor from the RS configuration a core dump could occur. This issue has now been corrected	24640
MULTICAST – When performing IGMP snooping, if multiple clients in the same VLAN join the same multicast group, then only one client leaves, the RS will improperly remove itself from the group.	24499
POS – When configuring an FCS of 16, an FCS of 32 would be displayed instead.	23103
RATE-LIMIT – Setting the rate limit to be equal to the port speed will cause the “Time Interval” field to be Null, as reported by “rate-limit show all” command.	23914
ROSRD – “lo0” now behaves the same as a physical port; a route associated with lo0 will now propagate even if no physical ports for that route are up.	23916
ROSRD – If the routing process is busy processing routes, commands that call this facility could take up to 2 minutes to complete. A change has been made to eliminate this delay.	23764
ROSRD – Redistributing multiple equal cost routes from OSPF to BGP would cause the route to be displayed as having multiple same Next Hop gateways instead of only being displayed once.	24356
SMARTTRUNK – Running LACP over a SmartTrunk could result in the error message “%STRNK-E-XMTQFULL”.	23378
SNMP – The MTU value for a gigabit ethernet port is now returned correctly.	23934
SNMP – The result of an SNMP query for the GBIC type, on the MPLS module, is “unknown”. The CLI output for the same information is OK, the result is the appropriate media type and manufacture. This issue has now been resolved.	24620
SNMP - When a fail over to a backup CM occurs, the MPLS and Multi-Rate WAN cards may not have entries in the ifTable.	23434
SSH – In some cases, when a non-interactive mode SSH command is directed to the RS, the RS will core dump. This occurs because the SSH server is being stopped in response to a “close” message from the client. Even though non-interactive SSH is not currently supported, some modifications have been made for handling a session kill received form a client, to allow a safe exit when a disconnect occurs.	24885
SSH – The SSH identity key files were not being copied from the primary CM to the backup CM resulting in SSH being disabled after a failover.	23797
STP - With Rapid Spanning Tree configured, Topology Change Notification (TCN) is not sent when topology change occurs. This issue has now been corrected.	21735
SYSTEM – If a route is defined to go through the lo0 interface, high amounts of traffic to this route could cause the system to run out of network buffers.	24092
SYSTEM/ARP – If a less specific route exists in the FIB that overlays a more specific directly connected interface route, then when the less specific route is removed the interface route can also be removed. In some situations, this resulted in the interface no longer being reachable causing the loss of connectivity.	24156
WAN – Clearing the port-stats on a channelized T1 would also not clear the member channels’ statistics.	23692
WAN – The use of some DS3 muxes could cause the RS to crash on bootup if both ports on a Multi-Rate Wan Card are DS3 WICs and are connected to the mux.	24305

Issues Resolved in version 8.0.3.0	ID
<p>The current release does not support the traffic coming in on one switch and the reverse traffic going out another port even if the 'dest mac' has been learned as a source on the first link.</p>  <p>For example, this release doesn't support traffic coming in on gi.1.1 and going out gi.2.1, with reverse traffic coming in on gi.2.1 and going out gi.3.1. When the L2 filter is established with input ports gi.2.1, it cannot filter with output ports of gi.3.1.</p>	<p>19243 19571</p>

**KNOWN RESTRICTIONS AND LIMITATIONS:**

**Known Restrictions in this Release**

Hardware	ID
RS16000 – The Power Supply Status/ID bits are incorrect resulting in the wrong status or the wrong type of power supply being reported	24192
The 8.0.3.0 release will not fit onto a single 8 MB flash. Customers need to upgrade to 16 MB of flash memory for this release. Two ROS 8.0.X.X images will not fit on one 16MB flash card.	
Power Supply - When one power supply is powered down, some power fluctuation may occur. Although this fluctuation is not a problem, it may result in the triggering of multiple traps.	

Software	ID
<b>ACL</b>	
Although configuration mode comments are not officially supported in this release, there is an issue of substantial importance. The comment facility is currently capable of commenting out and in any line in the configuration. The rules within an ACL must be in a specific order to achieve the desired behavior. If a rule is commented out, it is essentially removed from the configuration. As rules are configured into an ACL they either have to be added to the configuration in their desired order or the ACL editor must be employed to place the rules in the desired order. When commenting in a rule within an ACL the rule will logically be placed at the bottom of the rule base, even though its physical location in the configuration will remain unchanged. This behavior can be confirmed by comparing the active configuration to the output of the "acl show all" command. The recovery from this condition is to use the ACL editor to save the ACL, this action will restore the logical order of the rules. By the way, the rule order must change for the save operation to execute.	
<b>ATM / POS</b>	
ATM Module - IS-IS not supported on ATM-OC3	
ATM Module - It is recommended to specify the peer-address of an ATM interface. This may be necessary for applications where Inverse ARP does not function, resulting in untimely address discovery during heavy traffic situations.	
ATM - Statistics are not correct on the 4 port ATM card on the RS 38000	
ATM – When adding and removing and re adding VCLs, VCL create may not fully clean up after negating a VCL from the active configuration. The result will be that the VCL create fails due to the vcl already being open.	27112
PoS - NOTE: Using the Port Disable command does not cause APS switching to occur. APS occurs only when the link is lost, or if the cable is physically removed. This is how APS is designed to function. The port disable command cannot be used to simulate a failure; you must physically break the link for APS to occur.	
PoS - When configuring a POS port for connection to a POS port on a Juniper product, configure the peer address of the Juniper port while configuring the RS POS port.	
PoS - To route packets over a bridge encapsulation ppp link use the following command; ppp set ppp-encaps-bdg ports so.x.x	
ATM OC-3 Module - ATM PHYs do not support hot swap in this release.	08503



**CUSTOMER RELEASE NOTES**

<b>Software</b>	<b>ID</b>
ATM OC-12: Removing an interface and the VC itself will show VC in the default vlan	18593
ATM OC-12: Lose all applied service definitions for VC groups upon hotswap	18785
POS-Under certain circumstances, If forced bridging is applied and ppp is re-negotiated, (after the initial negotiation), then an interface down -> interface up must be performed.	18829
ATM OC-12: Combination of vcmux/lc and ppp traffic is not supported	18891
ATM OC-3: It's necessary to open a VC before you can apply a service definition on the VPL	19462
POS-APS is not supported on trunk ports	19489
Stackable VLAN Over ATM: After a hotswap of the ATM line card trunk/stackable port/vc do not get added back to their appropriate VLAN.	21560
OAM - F4 OAM is not supporting the AIS/RDI services - When creating a VCL for segment OAM or a VCL for end to end OAM and enable the AIS/RDI processing, the AIS/RDI cells are not sent..	22985
ATM - ATM OC-3 Disabling force-bridging doesn't work	23191
ATM - Service definition l2-ip priority of low does not get displayed or applied properly	24248
ATM – power on diagnostics and the self test for the ATM OC3 line card may fail on reboot intermittently, even though the card is ok.	24263
<b>CLI</b>	
Comments - A facility to add comments to the router configuration was added in version 7.0 of the RapidOS firmware. In version 8.0 new features were added to provide greater functionality and faster failover to the backup Control Module, in redundant CM configurations. Currently a restriction exists - config mode comments are not supported on routers with redundant Control Modules. This restriction is expected to be removed in version 9.0 of the RapidOS firmware.	20861
<b>Control Module</b>	
Control Module - Hotswap of flash cards is not supported during run-time	
Control Module - Master CM cannot be hot-swapped out while active. The Backup CM can be hot-swapped out at anytime by pressing the hotswap button or using the "system hotswap out" command from the console.	
Control Module - If secondary control module is installed, please ensure both primary and secondary control module's PCMCIA flash card contain the same software version.	
Control Module – The RS configurations with either LACP or the Hunt-group protocol on SmartTrunks are not supported with Control Module failover. SmartTrunk with the LACP or Huntgroup protocol should not be used in redundant Control module configurations.	
<b>MPLS</b>	
<p>When the RS box is doing Martini tunnels with Cisco (GSR) as the LSR and running IS-IS as the IGP, a problem is encountered with MTU size. The default MTU for Cisco and Juniper is 1500, so when a 1518 byte packet is sent through the customer port (VLAN based or port based Martini), the packets will be dropped by the Cisco LSRs. When the MTU is changed to be bigger than 1540 on the Cisco router, the Cisco router will send IS-IS packets bigger than 1536. Then IS-IS will go down. So the IS-IS MTU must be kept at 1497. The suggested solution is:</p> <ol style="list-style-type: none"> <li>1) Under the Cisco MPLS interface configuration, do 'mtu 2000.' Then it can pass Martini traffic.</li> <li>2) Under the same interface, do 'clns mtu 1497.' Then IS-IS will keep working.</li> </ol> <p>The same problem can be encountered on Juniper's boxes. Juniper supports setting port MTU and protocol MTU as well.</p>	
NAT and LS-NAT are not supported in the MPLS line cards.	18761 18763
L4 bridging is not supported through the Martini tunnel.	19794



CUSTOMER RELEASE NOTES

Software	ID
<p>Secondary IP addresses are not supported in RSVP and LDP.</p> <p>For example:</p> <pre> 12.1.1.2      17.1.1.1      17.1.1.2    RS2 ----- RS3 ----- RS4 </pre> <p>In RS3, there are 2 ports in one VLAN, and then an interface (IP 17.1.1.1) is created over the VLAN. If a secondary IP address 12.1.1.1 is added to the interface, the LDP session between RS2 and RS3 will not come up. In other words, the secondary interface will not be recognized by LDP at all. Users that have such configurations need to remove the secondary interface and include all ports to one subnet, such as:</p> <pre> 17.1.1.3/16   17.1.1.1/16   17.1.1.2/16    RS2 ----- RS3 ----- RS4 </pre>	19824
<p>Bandwidth cannot be dynamically changed when an LSP exists. <i>When the interface bandwidth is set, it will not take effect if the interface involved is being used by an LSP.</i></p>	19902
<p>The primary path configuration is not negated if multiple options are set. If the primary path configuration has multiple options configured in separate configuration lines, the command 'negate all' won't negate the entire primary path configuration.</p>	20024
<p>MPLS/LDP: The performance of the router is impacted when sending 70,000 BGP routes through the MPLS cloud.</p> <ul style="list-style-type: none"> <li>The RS console becomes very slow. CLI commands such as 'bgp show summary' take a long time to complete (+ 30sec).</li> <li>OSPF connection with RS experiences up and down behavior.</li> <li>Task Gated takes most of the CPU time when 'debug task top' is entered.</li> <li>It takes more than 10 minutes to get all 70000 routes.</li> </ul> <p>If LDP is negated on RS, then the RS gets all 70000 BGP routes very quickly (less than 40 seconds). A workaround for this problem is to use the MPLS/RSVP cloud to propagate full BGP routes.</p>	19631 22231
<p>MPLS - Currently, the RS implementation doesn't support the configuration of the same customer-id but different VLAN IDs for different customers. Workaround: After you add new ports to the VLAN, comment out and comment in the corresponding "l2p add l2-fec ..." command.</p>	23887
<p>MPLS - LDP with BGP may require as long as 15 minutes to load a complete Internet routing table to the egress LDP node. The performance of BGP full routes with LDP is improved but still slower than we would like. Additional performance improvements are scheduled for the ROS 9.0 release</p>	24285
<p>MPLS Gigabit Ethernet ports don't support jumbo frames over 2000 bytes.</p>	20610
<p>MPLS – the option no-decr-ttl is currently broken and is scheduled to be fixed in 9.0.1.0</p>	27134
<b>Multicast</b>	
<p>IGMP - Hotswap out while doing IGMP group memberships can cause a crash.</p>	27162
<p>IGMP-Snooping - If IGMP Snooping is enabled on an RS doing only L2 bridging. Even though the "Joins" and "Queries" are snooped, the Expiry timer is not updated. When the "Expiry Time" is exceeded the hosts are deleted from the multicast group and they stop receiving the multicast traffic from the Server. This problem has now been corrected.</p>	29588
<p>IGMP - L4-bridging is not currently supported when IGMP is enabled. The objective of L4 bridging is to provide the ability to apply ACLs/QOS functionality for bridged traffic. ACLs and QOS require L3 information from the IP packet header. L4 bridging makes this information available even though the packet is bridged and not routed. Since L2 filters are not at all applied or even evaluated when L4 bridging is enabled, and since IGMP relies on L2 filters, IGMP can not be supported in an L4 bridging environment. If an attempt is made to configure IGMP and L4 bridging concurrently, an increase in the CPU utilization can result. When in l4-bridging mode the RS does not create the associated L3 table entry if IGMP were to be enabled. Therefore, all traffic destined to the multicast MAC will be sent to the CPU since the complete L4 bridging information does not exist, thus causing an increase in the CPU utilization.</p>	
<b>Network Management</b>	
<p>RMON - rising and falling trap using alarm and event does not work</p>	14043
<p>RMON - statistics in host and matrix tables will keep on increasing on a port because the port stats are not being cleared.</p>	04307 16582
<p>SNMP – Under certain circumstances after Control Module fail-over, SNMP DOS packets are no longer rate limited.</p>	26439
<b>Port Mirror</b>	



CUSTOMER RELEASE NOTES

Software	ID
ATM - Port Mirroring with ACL only takes affect after reboot	21305
Port Mirroring – In some cases when an attempt is made to mirror a port with an OSPF interface configured, OSPF multicast messages can be sent out all of the ports in the VLAN containing the monitor port. After disabling Port Mirroring, this behavior is corrected by either restarting OSPF, disconnecting and reconnecting the target port or rebooting the RS.	26309
<b>Rate Limit</b>	
Rate limit - DOS rate limiting is enabled 1 min after Hotswap in of line card	26217
Rate Limit - TOS precedence and TOS rewrite does not work when L4 bridging is enabled.	15952
<b>Routing</b>	
BGP - It is possible to restrict the length of the prefix from a particular peer. Any route received with a prefix more specific than the restricted length will not be added to the routing table.	
BGP - Mpath will select four best equal cost routes instead of one when there are multiple EBGP peers	
BGP - Nested Route-maps: It is possible to nest route-maps within another route-map. This can be used to build a route-map using existing route-map without creating one from scratch. However, if multiple route-maps have been set, the last "set routemap" with the set option will be used.	
BGP – Searching for an invalid route in a large route table can cause BGP to lose its peering session.	24220
BGP - Specify the peer address while creating interface on the RS POS line card, and set interface FCS to 32 on the Juniper POS cards for proper interoperability.	
BGP - The following IOS commands are not supported: - show ip bgp reg - show ip bgp neighbor x.x.x.x advertised-routes - show ip bgp neighbor x.x.x.x received-routes - show ip bgp neighbor x.x.x.x routes - show ip bgp community	11387
BGP/OSPF - Routing loops can be seen sometimes while bringing down certain interfaces in non-backbone area with multiple ABRs. If the network has the same destination network available via inter area route and "AS-external," there will be routing loop issues if the inter-area route is lost to that network.	10945
DVMRP - Negating "dvmrp start" will cause a very small amount of memory leakage. This will be corrected in a future release.	08249
HRT – Hardware Routing enabled on an Ethernet port which is forwarding packets to WAN port is not supported configuration in this release. Workaround: Disable HRT on Ethernet port	31895
HRT – In load testing, after transitioning an interface down, from peer router, the router under test core dumped. This router was configures for HRT and Custom mode forwarding along with BGP and full Internet routes.	27118
ISIS – In some test conditions, ISIS over T1-FR dose not establish an adjacency due to the reception of packets with the wrong etype. This only occur after a CM failover and the problem can be corrected by a reboot.	27036
ISIS - IGP shortcuts for ISIS at level 2 is not supported.	26565
ISIS – In some cases an IS-IS adjacency may not come up on a PPP interface after hot-swapping out a WAN, POS or ATM modules.	
ISIS – In some rare occasions ISIS filters are not removed after negating the IS-IS commands from the Active configuration	23071
ISIS - The ISIS routing protocol is not supported on ATM OC-3 cards.	10410
Multicast replications for all VLANs in the replication group will stop for up to two minutes after one of the VLANs leaves the group.	20878
Multicast Replications may be lower for one VLAN versus another	20740
Multicast Traffic is not supported on unnumbered interface links.	19837
Occasionally, a multicast replication may not be deleted from the table after the source has stopped sending data.	20793
OSPF may require more time to establish an adjacency in case of point to multi-point connections.	19288 15655



CUSTOMER RELEASE NOTES

Software	ID
Routing - Assigning more than one secondary IP addresses on the same subnet to the "en0" interface is not currently supported.	10519
<b>System</b>	
When upgrading the system image on the RS flash, using the command "system image add ...", it is normal for the CPU to run at 100% utilization. The task used to down load the new image and write it to the Flash memory runs at a relatively low priority; therefore it consumes all available CPU time that is not required for any other router operations.	
<b>SmartTrunk</b>	
SmartTrunk – Adding a disabled port to a SmartTrunk is not supported. The workaround is to remove the "port disable" command, add the port to the SmartTrunk and then reissue the "port disable" command, for the specified port.	42630
SmartTrunk - Huntgroup protocol supports only up to 256 ports. In the RS 32000, huntgroup protocol is not supported for modules in slot 1 to 7. SmartTrunk with LACP protocol selected is supported only on Ethernet ports. SmartTrunk with no protocol selected is supported for all modules.	09256
SmartTrunk – The "port disable force-link-down" command issued on a SmartTrunk, will disable the SmartTrunk, but will not force the links on the physical ports into a down state.	24675
L2 Table Mgr. - After doing a software Control Module failover, the RS may core dump after displaying the following messages: L2TM-W-ST_PORT_SYNC, Error while updating L2 table of new SmartTrunk port L2TM-W-BAD_PORT, request to perform an action on an invalid port L2TM-W-TBL_MISMATCH, L2 table inconsistency	37670
This issue is the result of configuring a SmartTrunk for the LACP protocol and then doing a CM failover. The LACP functionality is not supported in a redundant CM configuration – Use the "no-protocol" option on the SmartTrunks.	
<b>Spanning Tree</b>	
PVST - Per-VLAN Spanning Tree – The "port show stp-info all-ports", shows "no-port" for per vlan spanning tree. This output was misleading and has been modified.	09336
STP - Ports need to be added to the VLAN before enabling STP on those ports when configuring Per VLAN Spanning Tree (PVST).	07445
PVST – under some circumstances, when per VLAN Spanning Tree is configured on a port based VLAN, the RS38000 will not advertise the correct root bridge.	26074
STP – On an RS that is not the Root bridge of a spanning tree, only the bridge priority will be changed when issuing the following command: stp set bridging priority 28672 hello-time 3 max-age 21 forward-delay 16	31799
<b>VLANs</b>	
802.1q - If a trunk port is created, the port is changed from access to trunk, but it is not automatically added to any VLAN other than the VLAN's to which the port already belongs. Use the <i>vlan add port</i> command to add the trunk port to the required VLANs.	
VLAN translation - The tunneling of L2 control protocol packets ( i.e. stp, pvst, gvrp, etc) is not supported in a translated environment. In this release it is not possible to, *tunnel* or transparently "translate", customer BPDU's/PDU's from one customer's edge switch to the other. This support is targeted for a future release. (Please note these protocols are supported within the core).	
VLAN Translation - an input port cannot belong to a VLAN which is equal to that of the translated VLAN." Suppose we have a VT policy with the input port gi.1.1 (VLAN 20 ), mapped to output port gi.2.1 (VLAN 420). gi.1.1 can NOT belong to VLAN 420. The CLI will disallow this from succeeding. This is true for a reverse mapping relationship as well.	
Boot - Smartboot feature does not support "en0" as the bootup interface. Use "set cfgport xxx" to configure the Smartboot bootup interface.	09218
Boldface characterization only works for ip based VLAN with the nativeVLAN	20925
Do not negate VLAN add ports commands without first negating nativeVLAN commands	20933
Do not negate trunk port without first negating nativeVLAN commands for that trunk port	20937
Multicast replication will stop after a .1Q SmartTrunk port disable/enable command is given for a port	20997



CUSTOMER RELEASE NOTES

Software	ID
L4 Bridging - L4-bridging is not currently supported when IGMP is enabled. The objective of L4 bridging is to provide the ability to apply ACLs/QOS functionality for bridged traffic. ACLs and QOS require L3 information from the IP packet header. L4 bridging makes this information available even though the packet is bridged and not routed. Since L2 filters are not at all applied or even evaluated when L4 bridging is enabled, and since IGMP relies on L2 filters, IGMP can not be supported in an L4 bridging environment. If an attempt is made to configure IGMP and L4 bridging concurrently, an increase in the CPU utilization can result. When in L4-bridging mode the RS does not create the associated L3 table entry if IGMP were to be enabled. Therefore, all traffic destined to the multicast MAC will be sent to the CPU since the complete L4 bridging information does not exist, thus causing an increase in the CPU utilization.	
<b>WAN</b>	
PPP - When creating an IP interface on a VLAN with a single PPP port configured, the interface should be set to "type point-to-point".	07757
WAN – the T1 WIC does not register physical layer alarms when running un-framed data.	22699
WAN - Bert testing with all 0s or all 1s for a pattern will not show "no sync" without connection.	31885
WAN - NIU won't come out of loop-back if NIU is first disconnected and then reconnected. Workaround: is to reset the loop-back to "NIU-remote-line-inband" and then retry the "loop-back none".	31889
<b>System</b>	
RADIUS/TACACS+ - The username of an authenticated user on the console port is overwritten by the username from the next successful authenticated telnet session.	14174
System - Under certain circumstance, attempting too many telnet sessions to an RS Switch Router may cause the console to freeze up. It is recommend that you limit the number of telnet sessions to 4.	10608
<b>Telnet and SSH</b>	
SSH - If a user generates an SSH key on a router on which a key is already present the SSH server will not flush out its existing key from memory and load the newly generated key, but will continue to use the old one. The new key will first be read when the router, and hence the SSH server, reboots, or when a fail over to a backup CM occurs and the new SSH server launched on the backup Control Module reads the new key (they are copied to the backup when generated) from its flash. This behavior can be avoided by first eliminating (using the ssh server eliminate_key command) the original key before generating a new one. The key elimination causes the server to eliminate its in memory key, and the generation will cause it to load the new one as it doesn't currently have one"	
Telnet – In some cases, after a port scan is performed against the RS, telnet access will be disabled.	20220 23904
<b>Miscellaneous</b>	
QoS - TOS precedence and TOS rewrite does not work when L4 bridging is enabled.	15952
VRRP - In some cases when stopping VRRP the L2 entry for the virtual MAC address is not properly modified and the original VRRP master will continue to route traffic that should be bridged to the new VRRP master. This issue is planed to be resolved in the next patch release.	24508
Port – The Gigabit Ethernet port may not indicate an operational state after a CM failover. If a gigabit port is a disabled with the "force link down" option, and this command is negated from the RS configuration, the RS will indicate that the port-status is down, even if the link is up and operational. This condition only occurs after a CM failover, event. Workaround is to hotswap the line card out and back in again.	30479

Any problems other than those listed above should be reported to our Riverstone Technical Support Staff.



**COMPLIANCE SUPPORT:**

Compliance Level	Compliant
Year 2000	Yes

Known Anomalies: None.

**IEEE STANDARDS SUPPORT:**

Standard	Title
IEEE 802.1D	Spanning Tree, GARP and GVRP
IEEE 802.1p	Traffic Prioritization
IEEE 802.1Q	VLAN Trunking
IEEE 802.1w	Rapid Spanning Tree Protocol
IEEE 802.3	10 Mbps Ethernet
IEEE 802.3u	100Base-T Ethernet
IEEE 802.3x	Full Duplex Ethernet
IEEE 802.3z	1000 Mbps Ethernet
IEEE 802.3ac	Frame extension for VLAN tags
IEEE 802.3ad	Link Aggregation Control Protocol

**IETF STANDARDS SUPPORT:**

RFC No.	Title
RFC 768	UDP
RFC 783	TFTP v2
RFC 791	IP
RFC 792	ICMP
RFC 793	TCP
RFC 862	ARP
RFC 854	Telnet
RFC 951	Bootp
RFC 1058	RIP v1
RFC 1075	DVMRP
RFC 1105	BGP
RFC 1112	Host Extensions for IP Multicasting
RFC 1157	SNMPv1
RFC 1163	BGP-2
RFC 1195	Use of OSI IS-IS for Routing in TCP/IP and Dual Environments
RFC 1213	MIB-2
RFC 1245	OSPF Protocol Analysis
RFC 1253	OSPF v2 MIB
RFC 1256	ICMP Router Discover Message
RFC 1265	BGP Protocol Analysis
RFC 1266	Experience with the BGP Protocol
RFC 1267	BGP-3
RFC 1269	Definitions of Managed Objects for BGP-3
RFC 1293	Inverse ARP
RFC 1332	PPP Internet Protocol Control Protocol (IPCP)
RFC 1349	Type of Service in the Internet Protocol Suite
RFC 1397	BGP Default Route Advertisement
RFC 1403	BGP OSPF Interaction
RFC 1483	Multiprotocol Encapsulation over ATM Adaptation Layer 5



**CUSTOMER RELEASE NOTES**

<b>RFC No.</b>	<b>Title</b>
RFC 1490	Multiprotocol Interconnect over Frame Relay
RFC 1519	CIDR
RFC 1542	Clarifications and Extensions for the Bootstrap Protocol
RFC 1548	The Point-to-Point Protocol (PPP)
RFC 1552	The PPP Internetwork Packet Exchange Control Protocol (IPXCP)
RFC 1570	PPP LCP Extensions
RFC 1583	OSPF v2
RFC 1586	Guidelines for Running OSPF over Frame Relay Networks
RFC 1587	OSPF NSSA Option
RFC 1631	IP Network Address Translator
RFC 1638	PPP Bridging Control Protocol (BCP)
RFC 1656	BGP-4 Implementation
RFC 1657	BGP-4 Definitions of Managed Objects
RFC 1661	PPP (Point-to-Point Protocol)
RFC 1662	PPP in HDLC-like Framing
RFC 1723	RIP v2
RFC 1745	BGP-r/IDRP for IP and OSPF Interactions
RFC 1771	BGP-4
RFC 1772	Application of BGP in the Internet
RFC 1773	Experience with the BGP-4 Protocol
RFC 1774	BGP-4 Protocol Analysis
RFC 1812	Router Requirements
RFC 1923	RIPv1 Applicability Statement for Historic Status
RFC 1965	Autonomous System Confederation for BGP
RFC 1966	BGP Route Reflection
RFC 1990	PPP Multi-Link Protocol
RFC 1997	BGP Communities Attribute
RFC 1998	BGP Community Attribute in Multi-home Routing
RFC 2096	IP Forwarding MIB
RFC 2131	Dynamic Host Configuration Protocol
RFC 2138	RADIUS
RFC 2139	RADIUS Accounting
RFC 2178	OSPF
RFC 2225	Classical IP and ARP over ATM
RFC 2236	Internet Group Management Protocol, Version 2
RFC 2328	OSPFv2
RFC 2338	VRRP
RFC 2370	OSPF Opaque LSA Option
RFC 2385	Protection of BGP Sessions via the TCP MD5 Signature Option
RFC 2391	Load Sharing using IP Network Address Translation (Load Balance)
RFC 2439	BGP Flap Dampening
RFC 2796	BGP Route Reflection Alternative to full mesh IBGP

**IETF STANDARDS MIB SUPPORT:**

<b>RFC No.</b>	<b>Title</b>
RFC 1471	PPP LCP (Link Control Protocol)
RFC 1472	PPP Security Protocol
RFC 1473	PPP IP NCP (Network Control Protocol)
RFC 1474	PPP Bridge NCP
RFC 1493	Definitions of Managed Objects for Bridges



**CUSTOMER RELEASE NOTES**

RFC 1595	SONET / SDH MIB
RFC 1657	BGP4 MIB
RFC 1695	ATM MIB
RFC 1724	RIPv2 MIB
RFC 1757	Remote Network Monitoring (RMON) Management Information Base
RFC 1850	OSPF and OSPF Trap MIB
RFC 1907	SNMP v2 MIB
RFC 2011	Internet Protocol (IP) MIB using SMIv2
RFC 2012	Transmission Control Protocol (TCP) MIB using SMIv2
RFC 2013	User Datagram Protocol (UDP) MIB using SMIv2
RFC 2021	Remote Network Monitoring Version 2 (RMON 2)
RFC 2096	IP Forwarding MIB
RFC 2115	Frame Relay DTE using SMIv2
RFC 2233	Interfaces Group using SMIv2
RFC 2495	E1 / DS1 MIB
RFC 2496	E3 / DS3 MIB
RFC 2618	Radius Authentication Client
RFC 2665	Ethernet-like Interface Types MIB
RFC 2668	IEEE 802.3 Medium Attachment Units (MAUs) MIB
RFC 2670	MCNS/DOCSIS compliant RF interfaces MIB
RFC 2674	MIB for Bridge with Traffic Classes, Multicast Filtering and VLAN Extension
RFC 2494	DS0, DS0 Bundle MIB

**IEEE MIB SUPPORT:**

Function	
LAG MIB	Support for 802.3ad functionality

**IETF EXPERIMENTAL MIBS SUPPORT:**

Function	Draft
DVMRP	Draft 4
802.1Q VLAN	IEEE Draft Standard P802.1Q/D9
IGMP	Draft 5
VRRP	Draft 9
DOCS-BPI	Draft 0

**IETF STANDARDS SNMP TRAP SUPPORT:**

RFC No.	Title
RFC 1157	linkDown, linkUp, authenticationFailure Traps
RFC 1493	newRoot, topologyChange Traps

**FRAME RELAY STANDARD SUPPORT:**

Standard	Title
Frame Relay Forum FRF.1.1	User-to-Network (UNI) Implementation Agreement
Frame Relay Forum FRF.3.1	Multiprotocol Encapsulation Implementation Agreement
ITU-T Q.922/ANSI T1.618	ISDN Core Aspects of Frame Relay Protocol
ITU-T Q.933	Access Signaling Annex A
ITU-T I.122/ANSI T1S1	Standards-Based Frame Relay Specification



**CUSTOMER RELEASE NOTES**

Standard	Title
ITU-T Annex D/ANSI T1.617	Additional Procedures for PVCs Using Unnumbered Information Frames

**Riverstone PRIVATE ENTERPRISE MIB SUPPORT:**

Title	Description
Novell-ixp-mib	Novell Netware
Ctron-ssr-hardware	Device specific hardware objects
Ctron-ssr-policy	L2 filters, I3 acs set/get ability
Ctron-ssr-service-status	Status of major subsystems
Ctron-ssr-capacity	New with 3.0 use for performance/capacity
Ctron-ssr-config	Retrieve/send configuration file via tftp
Ctron-Ifap-mib	Lightweigh Flow Admission Protocol MIB
Novel-rip-sap-mib	Novell Netware RIP SAP
Cisco-bgp-accounting	Tracks AS path information per flow
Riverstone-stp	STP MIB

Cabletron Private Enterprise MIBs are available in SMI v1/v2 format from the Riverstone Web Site at:

<http://www.riverstonenet.com/support/> Indexed MIB documentation is also available.

**GLOBAL SUPPORT:**

- By Phone: (408) 878-6500
- By Web: <http://www.riverstonenet.com/support>
- By Fax: (408) 878-6501
- By Mail: Riverstone Networks  
5200 Great America Parkway  
Santa Clara, CA 95054

For information regarding the latest firmware available, recent release note revisions, or if you require additional assistance, please visit the Riverstone Support Web Site.

**End of Release Notes**