5200 Great America Parkway
Santa Clara, CA, 95054

CUSTOMER RELEASE NOTES

Riverstone Networks Switch Router
System Firmware Version 9.1.2.1
October 2002

INTRODUCTION:

This document provides specific information for version 9.1.2.1 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 9.1.2.1 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 9.1.2.1 firmware image will not fit onto an 8 MB PC-Flash Card. If you do not have 16 MB of flash memory, do not attempt to store the 9.1.2.1 firmware image in Flash. With 16 MB of flash only a single copy of the ROS firmware will fit. It is however, possible to boot the 9.1.2.1 image from a tftp boot server.

The minimum memory requirement for this release is 128 megabytes, 256 megabytes is recommended for systems running the BGP routing protocol.
The RS2000 is not supported in this release of the ROS firmware.

Firmware Image Name	Version No.	Type	Release Date
ros9121	9.1.2.1	Patch	October 2002
ros9120	9.1.2.0	Maintenance	September 2002
ros9101	9.1.0.1	Patch	August 2002
ros9100	9.1.0.0	Minor	June 2002

Version numbers explained

Version number									**Description**
ros	9	1	2	1	-	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! This software is only supported until the first GA release containing the functionality (usually 6-8 weeks).

HARDWARE CHANGES AND ENHANCEMENTS:

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

New line cards supported in the 9.1.0.0 release

NOTE: Support for these cards was introduced in version 9.1.0.0. Since it's release, there have been several significant changes made for the operation of these cards, therefore the minimum supported version for systems with these line cards has been changed to version 9.1.2.1.

Part number	Description
G3M-GBCFM-02	2 port Gigabit Ethernet for RS 1000/3000
R38-GBCFM-04	4 Port Gigabit Ethernet for RS 38000
G8M-GBCFM-02	2 port Gigabit Ethernet for RS 8x00
R38-GBCFM-08	8 Port Gigabit Ethernet for RS 38000
G8M-S48DM-01*	1 port SRP OC-48 for RS 8x00
R38-P12MM-04*	4 port MPLS PoS OC-12c, for RS 38000
G8M-P03MM-02*	2 port MPLS PoS OC-3c, for RS 8x00
G8M-P12MM-02*	2 port MPLS PoS OC-12c for RS 8x00
SFP03-01 *	PoS OC-3 pluggable optics SR
SFP03-09 *	PoS OC-3 pluggable optics IR
SFP48-01	1310 nm SMF OC48 optic, LC, 2 Km
SFP48-09	1310 nm SMF OC48 optic, LC, 15 Km
SFP48-05	1310 nm SMF OC48 optic, LC, 40 KM
SFP48-07	1550 nm SMF OC48 optic, LC, 5 KM

* This Line Card not released at time of publication of Release Notes

FIRMWARE CHANGES AND ENHANCEMENTS AND NOTES:

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 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.

Note: Change made in the implementation of the Rapid Spanning BPDUs (Change in default behavior)

The current implementation of Rapid Spanning Tree in the Riverstone platforms is IEEE802.1wD (Draft). The current plans are to add support for the IEEE802.1w standard in version 9.4.0.0 of the ROS software. This implementation will not be backward compatible with the current implementation of RSTP, therefore is will be necessary to plan network upgrades on a per LAN bases where RSTP is employed.

In the initial implementation of Rapid Spanning Tree, the RS was sending RSTP BPDUs with type 00. The standard (IEEE 802.1w standard) now specifies the router should send RSTP BPDUs with type 02. This change however could result in lack of interoperability with the previous versions of the RS RSTP. To enable interoperability and backward compatibility a CLI command has been added to the RS configuration mode:

```
stp set rstp-type-disable-on-ports
```

This command provides a means for configuring RSTP to allow transmission of BPDUs with type 00 instead of 02. This change has been completed for Ethernet ports and SmartTrunks, but the WAN ports will be done at some later time. (32795, 31572)

Note: RIP advertises the loop back route by default … (Change in default behavior)

RS was automatically advertising the loopback interface, this was inconsistent with the behavior of the other protocols on the RS. The new behavior is to not include the Loop back (lo0) interface as a direct interface, it will be excluded by default. This is consistent with the behavior of OSPF. To include the Loopback (lo0) route, include the command: “rip add interface lo0”. Remember, RIP will not advertise routes with a variable subnet mask, therefore, use RIP v2 or a class-full network mask.

Note: Changes to the MD5 authentication support, for ISIS (Change in default functionality)
In version 9.x firmware the RS implementation of MD5 authentication has been updated to be compliant with the current specification and to will provide interoperability with other vendor’s implementation of MD5 provided they have implemented the same specification. Although, these modifications to MD5 make this implementation incompatible with the original RS implementation of MD5, therefore, when upgrading from version 8.x to 9.x it will be necessary to upgrade all systems intercommunicating with MD5 together.

I addition, since the only options for the "authentication-method" were “md5” or “none”, in version 9.x the "authentication-method" was eliminated. Now if a Key is specified “MD5” is enabled, if not, no authentication is enabled. Upgrading from version 8.x to version 9.x requires a configuration change to remove the "authentication-method" option from the configuration, otherwise the command in the configuration will be in error.

Features and Enhancements in 9.1.0.0 Firmware (see the user documentation for more details):

L2 Protocols and Features

802.1X Support

The 802.1x standard defines a methodology for authenticating and authorizing traffic from a specific MAC Source Address on a specific port. The original conceptual use of this technology was to augment 802.11 wireless access devices security. Users would move from one location in a building to another and transfer from one wireless NAP to another. To ensure that a user has access to the network, the 802.1x scheme was created. The user's computer is challenged by either the NAP or a device connecting the NAP, for the first packet received (and on a regular basis afterwards) for a user ID and password. This information is sent to a centralized RADIUS server for authentication, and if authorized, traffic from the MAC address is allowed through, otherwise it is dropped. Mircrosoft has enhanced their Windows XP offering to support the protocol, and have had a working Beta network running at Sea-Tac airport with Wayport Inc offering wireless customers with XP on their networks to connect to Wayports network. We will support this use of the function, but our primary focus will be for authenticating and authorizing access for Consumer Broadband Access customers as part of our Subscriber Management Solution.

The mode of operation is enabled on a per port basis and allows for authorization of MAC addresses only for the port it arrives upon. When enabled, traffic is dropped unless the source MAC has been authorized. The source device sends an Ethernet frame with the Authentication ether type, including the EAP protocol. The user is either authenticated using a local database or a centralized default Radius server. Once the device has been authenticated, the RS will learn the SA and allow traffic from the SA to transit through. If the SA is not authenticated, the RS must continue to drop traffic. This feature is used to support customer authentication for Ether-to-the-home environments.

Enhancements to L2 MAC Learning

Per Port MAC Limiting

Limit the number of MAC addresses that a port may learn and when the maximum is reached, drop new frames which have unknown source MAC addresses. This will resolve the issue where excessive L2 misses are sent to the CM and overwhelm the CPU. When the mac-limit is reached, new L2 traffic will be dropped until an entry is aged out allowing for a new address to be learned.

Per VLAN MAC Learning limits

This feature allows the operator to limit the number of MAC addresses that may be learned per VLAN on an RS. This is useful for Metro TLS providers who wish to limit the exposure that one customer may monopolize a large proportion of the RS resources. When the maximum number of addresses have been learned, then new frames with unknown source addresses will be dropped in software.

The following cli are provided

- Port enable mac-limit <num> ports <portlist> vlan <vlan name>
- This command sets mac limit for the port and vlan.

- Port show mac-limit <portlist| all-ports> vlan <vlan>
- This command displays the port, vlan, configured mac limit, and number of current macs counted on that port for the vlan.

ATM Multicast Support Enhancements

In the 8.0.3.3 and later release of code, support for IGMP on a routed interface on ATM was added. The release was able to discern which vc the IGMP came in on, and send the multicast traffic on the vc requesting the stream only. It did not keep track of which IP address was sending the join or leave on a vc. This causes an anomaly in a Video over DSL (VoDSL) environment where two or more set top boxes (STB) are attached. In this scenario, if one STB is receiving a specific multicast stream, and a second box cycles through "channels" with joins and leaves through the channel the first STB is viewing, then the multicast group is dropped due to the RS seeing a leave for the group coming in on the vc. The second STB sees the dropped stream and resends a join. This causes a flicker on the TV monitor as the stream is dropped and then restarted.

The 9.1 release tracks the number of joins and leaves for a specific multicast group on a vc, and does not immediately drop a vc from a multicast transmission if the number of leaves is less than the number of joins received. A query is sent down the vc to ask if any STB wishes to continue receiving the stream. The second STB responds yes, and the stream is not interrupted. If the second STB was turned off, no response is received and the stream then is stopped on the vc.

L3 Protocols and Features

ISIS Convergence Enhancements - LSP Generation and SPF Calculation Throttling

ISIS is a well thought out, reliable routing protocol. With that reliability comes latency in convergence. For most traffic, the design is appropriate. In environments which demand immediate (or close to immediate) response to network changes, the protocol needs enhancing. As an example, a network transiting Voice over IP traffic needs to maintain sub-second convergence.

The standard implementation of ISIS has interval timers for SPF Calculation and LSP Generation. Events that affect LSP generation or SPF calculation are batched, and the task is executed regularly at these interval points. This function is proper for a typical environment, but does not allow for fast convergence (immediate execution of a task when the event causing a task to executes occurs) and provide limits on excessive CPU utilization (stream of events causing tasks to execute). In order to meet the convergence needs, events need to be processed much quicker, but this processing could cause excessive CPU processing. Compromise is needed to address these conflicting issues. First, process events quickly, but throttle back if too many events are received too quickly, using an exponential back off algorithm. This new feature is to change the interval timer to become a maximum timer between events. In addition, two new values are added, an initial event delay and an inter-event delay.

These parameters are used as follows;

- If no events causing either an SPF Calculation or LSP Generation during the maximum timer interval, then operate as we currently do.
- For the first event that is seen during a maximum period wait the initial-timer delay value then perform the function (either SPF calculation or LSP Generation).
- For subsequent events wait a period of Tn=min(2*Tn-1,MaxT), where Tn=0 time interval is the incremental-timer delay configured. MaxT is either the spf-interval or lsp-interval selected.
- If no events occur during the delay period, for a length of two times the initial delay time, then the timer (Tn) reverts to the initial delay value for the next event period.

For the LSP generation throttling, the following is a suggested extension to the "isis set interface" command, with the lsp-interval value being used as the max-timer.

"lsp-throttle-enable initial-timer <milliseconds> incremental-timer <milliseconds>"

For spf calculation throttling the following is a suggested implementation of a command
isis set spf-interval <seconds> throttle-enable initial-timer <milliseconds> incremental-timer <milliseconds>"

Default Values	SPF	LSP
Interval Timer	10 sec.	5 sec.
Initial Delay Timer	5 sec	0 msec
Incremental Timer	5 sec	5 sec

If no values are entered using the CLI, then the SFP and LSP default values (shown above) will be used. These enhancements are called SPF Throttling and LSP Throttling.

OSPF Restart

As a further enhancement to our hitless protection system (HPS) we are enhancing the ability to keep our routing routines alive during a transition of state between devices. In 9.0, the BGP Restart feature was added, which allows BGP peers to let each other know they support BGP restart, and to not immediately drop the peering session, but wait a predetermined amount of time and resynchronize after the restart. We will support OSPF Hitless Restart as specified in draft-ietf-ospf-hitless-restart-01.

MPLS Enhancements

Hardware support for TLS Replication (5th Generation ASIC Dependency)

In the 9.0 release, TLS functionality on MPLS, the ability to group multiple lsp's either on the same physical link and/or on different links, and replicate packets which need to be flooded to these lsp's was implemented. The 9.0 release required packets to go to the CM so that the replication bit could be set. The 5th generation MAC chips for ingress cards have been modified to allow for setting the bit in hardware. Release 9.1 needs to modify the TLS MPLS code to take advantage of this enhancement for ingress cards which have the appropriate ASIC. If an ingress card has an earlier ASIC, then the software data path for TLS must still be used for traffic from these cards.

QoS - e-lsp

Many of the Riverstone customers have started implementing MPLS based services. One of the critical needs is the ability to offer differentiated services. This could be assigned to a customer as a whole or individual applications for a given customer have the appropriate .1p and ToS bits assigned already. These need to be honored through the MPLS network. With E-LSP, the .1p as well as ToS are mapped to the EXP bits on the MPLS header at the LER based on the selected CLI. The intermediate LSRs, based on the EXP bits, place the MPLS packets into the desired queue. At end of the MPLS LSP, the EXP bits need are mapped back to the appropriate .1p/ToS information on the packets.

Fast Reroute

MPLS Fast Reroute allows for backup lsps to be created at the time the primary lsp is established. If the primary lsp fails, then the RS will failover to the backup lsp. If the failure is due to a direct connect hardware break, the failover time is between 100 and 500 msec to an lsp on the same line card.

Traffic Grooming Enhancements

Rate shaping (5th Generation ASIC Dependency)

This feature takes advantage of the new hardware ASIC support for leaky buckets on the ingress prior to sending across the switch fabric. Settings are allowed for rates from 8 kbps to a full 1 Gbps in as fine as 1 kbps increments. In addition to the rate shaping buckets, support for dual WRED dropping mechanism is being implemented in the hardware. In this case, one WRED engine drops marked packets (non-compliant packets). The second WRED instance takes effect if there are no marked packets to drop, and the WRED thresholds are hit, then regular packets will be dropped as selected by the WRED algorithm. This extends to port, L3/L4 aggregation and VLAN rate shaping.

L2 rate limiting (5th Generation ASIC Dependency)

This feature enhances upon the existing Port based and Aggregation based rate limiting. VLAN ID’s can be assigned to rate limiting buckets. The same functionality associated with port based or aggregation rate limiting applies. This requires new ASIC functions. The limitation is 1,024 buckets per channel. Extensions to the Service QoS CLI are needed to incorporate this function.

Weighted and Strict Priority Queuing (5th Generation ASIC Dependency)

On a per port basis, on outbound traffic, allow to select a new third mode of strict priority processing of Control with weighted fair queue processing of the remaining queues. This requires new ASIC functionality to work, and this feature would be selectable only on line cards with ASICs which support this feature. By enabling this feature, control traffic will always get put to the head of the line, while remaining traffic is assigned based on the weight assigned to the specific queue.

Strict-Enforced Weighted Fair Queuing (5th Generation ASIC Dependency)

A new selection is added to implement strict enforcement of the WFQ allocation. The standard Riverstone method is to allow queues to utilize the bandwidth of other queues if no traffic is received for those queues. With this new selection, it is possible to strictly enforce the bandwidth allocation. This allows for rate limiting of traffic on outbound queues to specific rates.

NMS Enhancements

PING CLI Enhancements

CLI ping command is extended with additional usability improvement features. These include, the ability to specify higher number of probes, the inter-probe interval, setting of the DF bit, loose and strict source routing, route recording, UDP echo, TCP connection timing, ICMP echo verification, more concise output, standard deviation calculation, packet size sweeping, and the ability to set complex data patterns as the data payload of a ping packet. To make the plethora of new options more manageable, we also provide the ability to save oft used sets of options as a named set, so users can call up that option set by name. The following give relevant parameter information;

The maximum limit for ping per second:
ICMP echo: 100 echo per second (the default ping option is “ICMP echo”)
UDP echo: 1 at a time
TCP connection timing: 1 at a time.

MVST MIB

MVST MIB is support for multiple instances of RFC 1493 Bridge MIB using the logical entity support in RFC 2737 Entity MIB. This feature utilizes the SNMPV3 context feature as well.

SONET MIB

SONET MIB defines objects for managing Synchronous Optical Network/Synchronous Digital Hierarchy (SONET/SDH) interfaces. It allows monitoring of alarm on the SONET signal and gathering of performance monitoring statistics. The MIB reflects layered SONET hierarchy:
Section, Line, Path and VT. Besides of SONET MIB objects the document (rfc 2558) stipulates the way SONET layers should be represented in ifTable and ifStackTable.

SONET MIB Object groups are:

- Medium Group - This group handles the configuration information for both optical SONET/SDH interfaces and electrical SONET/SDH interfaces.
- Section/Line/Path/VT Current Groups - current table contains various statistics being collected for each layer for current 15 minute interval.
- Section/Line/Path/VT Interval Group - contains various statistics collected by each system over a configured operation time.

Since our optical cards are intended as a Path terminating equipment the VT groups are not supported.

CLI support for the MIB:

```
sonet set <port> cicuit-id <name> framing <SONET | SDH> loopback pm-intervals <num>
```

circuit-id

- Sets a circuit identifier; provided for administrative use and can be used to associate this line with a customer circuit for service level management.

framing

- Set framing to SONET or SDH.

loopback

- Exercises loopback functionality.

pm-intervals

- Sets performance monitoring (PM) for the port ON and specifies amount of 15-min monitoring intervals to be saved

The MIB shall be supported on the following Riverstone Line Cards:

POS-OC3
POS-OC12
POS-OC48
ATM-OC12
ATM-OC3

DHCP Enterprise MIB

This feature implements a mechanism for pulling a DHCP database on demand as configured. Using this MIB, operator can configure a transfer interval for the DHCP database as well as the destination TFTP Server. The business benefit of this feature is it would enable ability to periodically upload the DHCP database from the Riverstone equipments and easily restore it back if there was any catastrophic failure at the device.

Notification Log MIB – RFC 3014

This MIB module describes management objects for logging SNMP notifications. RS supports this MIB and also provides a CLI to configure and view notification logs. Named logs are supported. The maximum number of entries allowed in the log table is configurable. When configuration is done using SNMP v3, the user credentials are enforced while logging notifications.

Riverstone Config MIB

This enterprise MIB is an enhanced replacement to ctron-ssr-config-mib. The MIB also logs the changes to the device configuration with a timestamp. Note that this MIB is disabled by default in the 9.1 release.

Switching Fabric Traps

New notifications have been added for switching fabric hot swap in/out, failure and fail over. These traps are defined in Riverstone-notifications –mib.

ATM2 MIB

MIB support for per VC statistics for ATM OC3 and ATM OC12 is implemented using the atmAal5VclStatTable in ATM2 MIB draft #17

RADIUS/TACACS+ Enhancements

Multi-user access using RADIUS authorization is supported. Authentication with RADIUS/TACACS+ in the single user mode does not authenticate twice with the same credentials anymore. Authentication is done either at login or when entering the enable mode depending on the configuration.

Miscellaneous

MPLS notifications - mplsXCUp and mplsXCDown - are disabled by default in the 9.1 release. This is in conformance with the default value specified in the MIB. Use the config command - snmp enable trap mpls-lsr - to enable them.
There have been some modifications to the Service String format. SIPP and IPP chips are now distinguishable by SI and I. SOPP and OPP chips can also be differentiated by SO and O. The SOPP or OPP memory has been added after the MAC packet memory. New formats have been added for MPLS, PoS, and ATM modules. Service String can be retrieved using the MIB object RSModuleServiceString in riverstone-inventory-mib.
The MIB object entLastChangeTime does not update unless the notification entConfigChange is enabled. The notification entConfigChange is disabled by default.
The BIP counters shown by using the command, "sonet show alarms <port>" are reset every 15 minutes. Performance monitoring is not implemented for ATM OC3 interfaces.

ISSUES RESOLVED:

Issues Resolved in version 9.1.2.1	ID
Software	
ACL – When a link transitions from up-down-up the ICMP traffic passing through the RS stops. When the link goes down the hardware is programmed to drop the traffic since there is no place to send it. When the link comes back up the input port is reprogrammed to pass the traffic. In the event that an ACL is applied to the outbound interface, the traffic will not restart. This issue has now been corrected.	34024
ATM – After creating a series of ATM VCs in the RS configuration, issuing the command "atm show vcl port at.x.y.z" produces no output for the content of the VCL table. This condition occurs when the VC range specified in the "atm create vcl …" command is specified with a range beyond the max supported number of VCs. A range checking function has been added to insure the configuration command is rejected if the VC range specified is beyond the supported range.	34609
CLI - The cli will not allow the "mvst create …" instance to be negated from the RS configuration. Removing "MVST associate" commands are permitted prior to removing the port from MVST. This will cause parsing problems in the CLI. An error will now prohibit negating MVST when ports that are still enabled. Dependences in MVST commands do not allow to remove vlans, ports, ...	35725
CLI - exiting out of a search in CLIcli will cause the RS to crash SearchNDisplayTLVs. When a cntrl-Z is typed at the search prompt, it is interpreted as an escape from "config" mode. At this point the user is queried "Do you want to make your changes active?", then the RS merges the contents of the scratchpad with the active configuration and erases the scratchpad. This occurs even thought the RS was in the middle of displaying the configuration. This usually results in a crash. This behavior has been changed to treat the cntrl-Z as an escape from the "search" mode, and then continue.	35819
IP Multicast - PIM deletes an L3 flow if the packet count difference is a negative value, this may occur if the counter resets. This is noticeable in real-time streaming applications where a strict jitter tolerance exists. This issue has now been resolved.	34671
IP Multicast – The RS will crash when it received and IP multicast packet destine to the RS system MAC on it's en0 port.rec mac of itself w/ multicast dst IP causes core dump ipm_install_l3_entry This problem has now been resolved.	35079
Ping – In some cases the RS can crash when pinging a broadcast address, it may be necessary to have multiple telnet sessions doing pings to a network broadcast address. This problem has now been corrected.	34470
POS – For POS OC-12 and OC-48, pulling either tx or rx link and then rebooting the RS, the APS link does not come up. The RS with the tx link removed from does not detect that the link is down, the neighboring router does detect the link down. This only occurs when the RS boots with either tx or rx link removed. It does not occur when both tx and rx are removed. This issue has now been resolved.	34723
QOS – After repeatedly adding and deleting the WFQ configuration, a condition will develop such that it will no longer be possible Unable to negate queuing-policy command. after repeatedly adding/deleting WFQ The problem is that the CLI options were not indexed in the CLI file. This issue has now been resolved.	35870
Rate Limit – The burst-safe rate-limit B bucket counter is in not operating properly. With rate limiting set up with the burst safe feature – over a Generation 5 line card - the burst-safe rate-limiting counter were never incremented. This is strictly a display issue. These counters have now been fixed for Gen5 cards, in addition 'no support' will be printed for the counters that are not supported.	34597
SmartTrunk – In some cases where the RS is configured with a SmartTrunk with the LACP protocol, when the entire configuration is negated, the RS may crash. This problem has now been resolvedCrash in lock_vlan_set_stp_state at stpmisc.c:706;stplnkgrp.c:248	36182
SNMP – When a port's link state is changed from up to down SNMP will send a trap indicating this change. Although, if a port is manually disables with the use of the "port disable xx.y.x" command, an SNMP trap is not sent. The trap is triggered on the physical state of the port not the logical state, this behavior has been changed in this release, so that a trap will now be sent when the port's logical state changes.	28881
SNMP – The output of the command "system show capacity memory", in some cases, appears to be less than the available memory. The reason for this discrepancy is that the memory on the free list (memory that had been allocated to a task – such as RMON – and then released when the task no longer needed the memory) was not counted. This memory was available to the system and was being reused it simply wasn't being accounted for in the output of the "system show capacity memory" command. Modifications have been made to sum the "available heap" and the "free bins" as the "Bytes Free".	34275
SNMP – The SNMP variable sysHwPortSlotNumber displays only the odd numbered ports for the specified line card. This issue has now been resolved so that both the odd and even numbered ports are now displayed.	34338
SNMP – The RS can crash during an SNMP MIB walk through the sysHwPortTable, on anRS38000 with a line card in slot 16. This problem has now been resolved.	34451

Issues Resolved in version 9.1.2.1	ID
Software	
SNMP – The ifIndex incramentsincrements each tine the Gigabit when MPLS Gig port isis bounced, when the MPLS port is bouncing thousands of times in a few minutes, the ifDescr will increment increments every time the link goes "down/up" with a new instance of the an L3 MPLS interface. This has caused some problems for some 3rd party network management systems. This issue has now been corrected.	35418
SNMP - When enabling SNMP authentication via the CLI, the RS will display “SNMP-I-AUTHEN_FAILURE” and send out traps when SNMP authentication fails. When enabling SNMP authentication via SNMP (snmpEnableAuthenTraps), the RS will display “SNMP-I-AUTHEN_FAILURE “, BUT will not send out traps when SNMP authentication fails. A modification has been made to make the trap behavior consistent with that of the CLI configuration. Authentication: Enabling Authentication w/ snmpEnableAuthenTraps	35985
SSH – A crash can occur when an SSH client is establishing a session with the RS, this condition was reported as the result of repeated SSH attempts using an automated script. Although this condition occurred very infrequently, it was determined to be caused in the use and reuse of the username data structure. This condition has now been corrected.	34317
SSH - - The keys generated by SSH keys are not saved to backup CM. A modification was made to make sure the SSH keys are propagated to the backup CM.	34874
STP – When nNegating part of an RSTP rstp configuration, the RS is likely to crash. lines causes crash. In the following configuration a crash will occur when negating lines 2 and 3. 1 : stp set protocol-version rstp 2 : stp set bridging ring_id 1001 priority 35000 3 : stp rer-create ring ring_id 1001 This issue has now been resolved.	35252
System – On an unstable gigabit link, that is bouncing down and up the following message may eventually be displayed: %SYS-E-UNSTABLE_LINK, Port gi.7.1 disabled due to unstable link. After repairing the fiber connection the RS does not print a port up message on the console or syslog.SYS-E-UNSTABLE_LINK: After reinsert of link, no CLI message is displayed. This issue has now been corrected.	36150
Tacacs-Plus – In version 9, the behavior of Tacacs-Plus was changed such that the password challenge for “enable” mode was suppressed, when Tacacs-Plus was configured for “login” mode. The reason for the change was because the same username/password combination used to access “login” mode was accepted for access to “enable” since authentication was tested by the same server. Therefore the redundant challenge was eliminated. In this release of the ROS, the original behavior has been reinstated through the use of the command: rs(config)# tacacs-plus authentication enable old-model Note: the “old-model” qualifier is hidden; therefore there is no command line help and no command line completion this option must be typed out completely (old-model).	31503
VLAN - When using VRRP with Aggregated VLANs, traffic may not be properly forwarded across the RS. If VRRP is removed from the configuration, everything operates normally. The L2 system MAC addresses were not being properly installed in the L2 table for VRRP to operate properly in a SuperVLAN environment. This issue has now been corrected.	34575
VLAN - Untagged traffic is not dropped on trunk port, for MPLS/TLS, exceptions were made for packets mapped to the blackhole VLAN. This issue has now been resolved.	34825
VRRP – Under certain conditions when modifying ACLs the VRRP Master changes to and stays in the initialize state. To recover the VRRP configuration must be negated and reapplied. This problem has now been corrected. when acl is changed	35021
WAN – When issuing the command “ppp show stats ports mp.x” the MIB2 stats are not shown on an MP bundle. This issue has now been resolved.	34573

Issues Resolved in version 9.1.2.0	ID
Software	
HRT – The RS crashes when negating and reconfiguring the RS for HRT. By default the RS programs an HRT entry as a route. Once an ACL is applied the RS changes all of the HRT entries to flow entries. When negating the HRT configuration; the RS was negating the HRT entries and re-enabling HRT again. To fix this it is important that the L3 forwarding table be placed into flow mode before re-enabling HRT. This problem has now been corrected	34436 34438 34440
IP Multicast - Starting IGMP/DVMRP while receiving IGMP group joins, will causes increased memory usage of the RS system memory. The memory loss only occurs when the multicast traffic is present on and ATM port. Modifications have been made to insure memory is freed when the IGMP is stopped.	34386 33720

Issues Resolved in version 9.1.2.0	ID
Software	
MPLS - negating LDP L2-FECs with QOS can cause the RS to crash. This is occurring because the MPLS data structures were not being initialized properly. This problem has now been resolved.	31339 34354
MPLS - Changing MPLS LSP preference does not take effect until the RS is reset. The RS routing task doesn't recognize a change in LSP preference until the LSP's are restarted. This problem has now been corrected.	34297
MPLS – The "detour-hold-pri" option on the "mpls set label-switched-patch" command indicates the default is 0, when it should indicate the default value of 7. This issue has now been resolved and the proper default is now displayed.	34203
HRT - When using HRT on a port with BGP configured, bouncing the BGP session may cause the HRT table to be loaded incorrectly. Downstream hosts will not be able to access upstream networks. This problem has now been corrected.	31895 32031 34176
OSPF – When OSPF changes state there is no console/syslog message displayed for change in Adjacency. An new message has been added to the console / syslog to be displayed when an OSPF adjacency goes to or from the state FULL.	31388 34151
WAN – The E1 WAN statistics are incorrect for the 1 minute average. The statistics now show the true line rate of the E1 interface. The maximum rate for this type of interface can be derived through the calculation 64000 x 31 channels = 1984000, This display issue has now been corrected.	33461
IP Multicast - IGMP with static joins has interoperability issue with some 3rd party DSLAMs. In this release of the ROS software, the problem with static joins over ATM has been resolved. When an ATM VC with its associated IP interface - for which a static join is applied for a multicast group - the exit port information is properly sent to the ATM card / port / VC. In addition, a change has been made to the forwarding algorithm for strict priority queuing. Therefore, in order to support bursty video traffic, the ATM service needs to be set with the proper buffers for each priority, for the Video traffic. Example, the video stream will be coming in on low priority by default, the follow command will adjust the priority for this type of traffic: atm define service 4MCBR srv-cat cbr pcr-kbits 4000 qos-buffering-control 5000 qos-buffering-medium 5000 qos-buffering-high 5000 qos-buffering-low 20000	32861
ATM – In some configurations an ATM OC-12 port can loop packets back to itself when received frames have an unknown address. Several modifications have been made to the L2 table manager on the ATM card to insure the proper learning and aging of Layer 2 addresses. This issue has now been resolved.	30243
SVLAN – When a Stackable Access port is configured on a port of an MPLS line card, the frames transmitted out of the port retained their stacked VLAN tag in addition to their original customer VLAN tag. This issue has now bee corrected.	33763
Rate Limit - l2 rate-limit doesn't allow a rate over 200Mbps to be specified. This issue will be resolved by allowing the time-select to be optimized. Thos issue has now been resolved.	33520
Rate Limiting – In the on-line help display for the “ip dos rate-limit” command one of the default values (Set rate for HTTP traffic in bps) was displayed incorrectly: rs# ip show dos rate-limit Summary of IP dos configuration ICMP traffic is rate limited to 100000 bps BGP traffic is not rate limited … SNMP traffic is rate limited to 100000 bps HTTP traffic is rate limited to 100000 bps ← Here rs(config)# ip dos rate-limit ? bgp - Set rate for BGP traffic in bps (Default: No rate limit) http - Set rate for HTTP traffic in bps (Default: 25000 bps) ← Here … vrrp - Set rate for VRRP traffic in bps (Default: 25000 bps) The display has now been improved to show correct default values. In addition, default values are also displayed in the “ip show dos rate-limit” command and in configs mode default value is displayed when the “default” option is specified.	33740
IP Multicast - PIM sends duplicate traffic to IGMP host in an IP multicast configuration with Static Joins. IGMP and static joins were contributing to the downstream list even though the interface was not owned by IGMP. There was no check for whether the interface was owned by the respective protocol before the interface was allowed to be added during the downstream traffic merge. This check has now been added to avoid the transmission of duplicate packets.	33642

Issues Resolved in version 9.1.2.0	**ID**
Software	
IP Multicast - When an IGMP host is statically joined into a multicast group, the host does not properly join the multicast group if the RS has been rebooted. A modification has been made to check for the upstream information during the static downstream interface additions.	33635
Rate Limit - system set rate-limit-range allows multiple ranges to be defined on the same slot. The CLI lets you keep adding selections for rate-limit range on the same slot, it becomes confusing since all are seemingly active in the RS configuration, only the last entry is active. For example: 24 : system set rate-limit-range middle slot 3 25 : system set rate-limit-range high slot 3 26 : system set rate-limit-range low slot 3 ← this command is the active command the RS should only allow one range to be defined at a time. The CLI will now reject the additional commands.	33631
IP Multicast – A memory leak has been identified in RS configurations where IP multicast is configured over ATM virtual circuits. Modifications have been made to insure memory is properly freed for ATM Virtual circuits.	33381
IP Multicast – using the multicast trace facility (mtrace) can cause the RS to crash. This problem has been resolved in this release of the ROS software.	32946
ATM - Excessive packet loss can be detected when routed and bridged VC's are configured on same ATM port. When the ATM port gets a multicast or unknown DA packet it must replicate the packet out each VC on the VLAN. The algorithm used to perform the replication was too slow and in some cases the FPGA could not run at line rate doing packet replication. This problem was fixed by improving the performance of the packet replication algorithm.	32860
IP Multicast - Multicast traffic does not forward correctly when using PIM over an ATM link. When configured for PIM, the ATM port's implementation of "split horizon" was overly aggressive in blocking traffic that needed to be multicast out the ATM port on VC other than the VC it arrived on. This issue has now been corrected.	31264
RIP – The loop back interface (lo0) is being advertised by RIP even when it is not added to any routing protocol. RIP was not keeping track if it had been enabled on the loopback interface or not. Hence, by default it would advertise all loopback routes. This has now been fixed. RS was automatically advertising the loopback interface, this was inconsistent with the behavior of the other protocols on the RS. The new behavior is to not include the Loop back (lo0) interface as a direct interface, it will be excluded by default. This is consistent with the behavior of OSPF. To include the Loopback (lo0) route, include the command: "rip add interface lo0". Remember, RIP will not advertise routes with a variable subnet mask, therefore, use RIP v2 or a class-full network mask.	30629
Layer 2 MAC - Invalid source MAC addresses causes issues with the Layer 2 tables. If the RS receives multiple frames with a multicast MAC in the Source addresses field, the L2 learning is negatively affected. The L2 tables have been modified to quickly age the these invalid MAC address entries. These modifications have resolved this problem.	30230
ATM - After creating an interface on an ATM VC / port and making it type point to point. The wrong warning message is displayed every 15 minutes, the message is: %ARP-W-HOSTUNREACH, 192.1.1.2: no route to host. ARP entry will be added when the route becomes available. There is a route to the destination host, 192.1.1.2, is in the FIB and it can be pinged successfully.	19713
SNMP - Anomalies in entity MIB for the RS 38000, the cards which are visible in the Entity table are not shown in the sysHwModuleEntry, but it is seen in sysHwModuleTable. In some cases, even though there is no card present, the sysHwModuleStatus shows that it is offline (there should not have been an entry at all). Sometimes the CLI shows a card as online but in SNMP it shows as offline. Because of this when the user tries to make it online from EMS, it gives an error indicating that card already occupied. In 9.1 the switching fabrics does not show up in the Entity table. These issues have now been resolved.	34016
IP Multicast - excessive latency between the time a multicast group join is issued to the actual join is achieved. The latency can be as long as 2 seconds between the time a join is issued and the time the actual join occurs. The latency occurs when attempting to leave and join a series of multicast groups and then reverse direction. This issue has now been resolved.	34012
IP Multicast – A crash can occur when running PIM/RP over ATM, while running the capacity test using 400 sources and 10 groups and then disconnecting the link and then re-connecting it. This issue has now been corrected.	33931
ATM – In recent releases of the ROS the ATM cross-connect functionality is not operation as expected, this problem has now been corrected.	33789
System - Secondary CM3 hangs when both primary and secondary are booted together. In a configuration with redundant CM3's, each time both the CMs are booted together the backup CM3 hangs for a while and then it gives the following message: %CPU_TASK-I-ATTEMPT_CONN, Attempting to establish connection %CPU_TASK-I-CONNECT_DONE, Connection established SNMP Research SNMP Agent Resident Module Version 15.2.1.4 %HBT-I-HBTTIMEOUT, Failed to receive heartbeat from active CPU (HBT_STATE_SYNC) %HBT-I-MASTERCPUFAIL, active 'Control Module (CM3)'in slot CM has failed %SYS-I-SANITY_CHECK, Failover Sanity Check on modules: 0x0. Then, both the primary and backup CMs, reboot successfully, provided they-re booted separately.	33470

Issues Resolved in version 9.1.2.0	ID
Software	
MPLS – A crash can occur when hotswapping a line card into an RS configured for OSPF, MPLS, RSVP and LDP. In the MPLS hotswap function, if the profile is a vlan-vlan type, the RS now insures that all of the ports belonging to the VLAN(s) are enabled for their appropriate VLAN functionality. This issue has now been resolved.	33179
IP Multicast / ATM – In an IP multicast configuration, where the multicast traffic is time sensitive the QOS priority queueing dose not produce the desired results when the traffic is transmitted over an ATM link. The default QOS method has now been changed to be strict priority, this will correct the problem.	32912
STP/RSTP - "RSTP interoperability with previous versions on WAN" - The BPDU type for RSTP BPDUs has been changed from 00 to 02 according to the recent IEEE 802.1w standard. This change however could result in lack of interoperability with the previous versions of the RS RSTP. To enable interoperability and backward compatibility a CLI command has been added to the RS configuration mode: stp set rstp-type-disable-on-ports This command provides a means for configuring RSTP to allow transmission of BPDUs with type 00 instead of 02. This change has been completed for Ethernet ports and SmartTrunks, but the WAN ports will be done at some later time. (32795, 31572)	32859
IP Multicast - IGMP static joins do not work on an ingress interface of the RS. No multicast traffic flows into the RS when a static join is applied to the ingress port. The workaround is to have another Interface - tied to a VLAN "looped" with the IGMP static join applied to it. This will provide the S,G state needed for rapid channel changes for VODSL. This problem has now been resolved.	32849
MPLS – changing an MPLS port from trunk to access and then back to trunk again, the LDP session won't transition to the up state. This issue has now been resolved.	23405

Issues Resolved in version 9.1.0.1	ID
Software	
ARP - A system crash may occur when two redundant ATM VCL's are configured and connected in a back-to-back configuration. The reason for the crash is that two ARP related data structures are out of sync with regard to a specific entry. Once this is state is determined all further processing of this entry should cease. This condition can occur when an ARP route entry is being changed. This problem has now been corrected such that, once notification has been made that and ARP route entry has been changed all current processing of this information will stop and the record will be re-read.	31810
ATM - In earlier versions of code the RS did not correctly support two set top boxes connected via a DSLAM to a single ATM VC. This issue is seen when one of the Set Top Boxes changes to the same channel that the other is currently a member of (i.e. sends a request to join the same multicast group). In this instance the "picture" will be seen to jump between one STB and the other. This release of code now correctly tracks leaves and joins on the VC.	30439
ATM – RS crash when configuring an ATM port in VLAN based L2 Martini tunnel. When configuring an ATM-OC12 port on the customer facing side of an L2-FEC, a system crash may occur. This issue has now been fixed.	31612
ATM – The L2 hash mode cannot be changed on an ATM port. When the hash mode is changed, via the CLI ("port set at.x.y hash-mode"), it does not take effect in the RS. This functionality is used the tune the RS L2 tables for their most efficient use. It turns out, for ATM ports, the Set Hash Function was not getting executed when the hash algorithm was changed in the RS configuration. This issue has now been corrected and the L2 hash variants, for ATM ports, can be changed via the CLI.	32851
ATM – VLAN frames being transmitted out an ATM port are not carrying the 802.1p bit in the 802.1q header. This problem has been corrected.	32944
ATM - When a priority map is created to map all traffic to either low, medium or high queues, the mapping does not properly work when applied to an ATM OC-3 port. This issue has now been corrected.	32346
BGP - RS receives IBGP route with the originator ID as it's own and accepts the routes. In earlier versions of firmware the RS was incorrectly accepting BGP routes from a Cisco route reflector server which it had originated. RS1 is a route reflector client of RR1. RS1 advertises the prefix 192.168/16 to RR1. Under normal circumstances RR1 should only advertise this prefix to other route reflector clients. However in some versions of Cisco IOS the route reflector RR will actually advertise the 192.168/16 prefix back to RS1. RS1 will then place the prefix in its RIB. This behavior is now corrected in the RS firmware.	29520
IP - When an interface on the RS, belonging to a non-backbone area is brought down, the router brings the whole area down, even thought there is a stub-host configured (loopback address). This issue has now been resolved.	31740
IP Multicast – PIM configured over a Gigabit Ethernet port has slow response to IGMP Client joins and leaves. When configuring IP Multicast with PIM/IGMP over a Gigabit Ethernet connection, changing multicast groups will experience delay of 3 seconds or more before receiving the new multicast stream. Enhancements have been made to reduce the delay to under 3 seconds.	31735

Issues Resolved in version 9.1.0.1	**ID**
Software	
IP Multicast - PIM Sparse Mode is not currently supported with RIP. An new configuration command is needed, "rip set rib multicast".	26833 22296
MPLS – In an MPLS network, with a primary LSP and a backup LSP, primary LSP may not recover if the failover was causes by disabling a port. If a port on the LSR has been disabled for a long period of time, causing the primary LSP to failover, the primary LSP may never recover after the port is re-enabled. This issue has now been resolved, ports can be disabled for any period of time and when re-enabled the Primary LSP will recover.	33057
MPLS - In some cases, sending L2 or L3 traffic over a Martini Tunnel, on a PoS OC-12 link, may cause the RS to crash. When traffic arriving on this port has MAC addresses in the same subnet the “local flow” processing should take effect. To resolve this issue, the MPLS code was moved to avoid the crash, into a section following “local flow” processing.	31241
MPLS – LSP failing with "state: Null status: UserConfig", this issue has now been resolved. Label-Switched-Path: "tunnel-rs1-to-rs2" state: Up uptime: 0d, 0h, 5m, 20s to: 2.2.2.2 from: 1.1.1.1 lsp-id: 5 reroute-lsp-id: 1 . . . Protection-Path "rs1-rs3-rs2": state: Null status: UserConfig lsp-id: 16386 reroute-lsp-id: 3 . . .	32756
MPLS - When a PE port, facing a CE, is on an MPLS enabled line card, IEEE802.1q packets are double tagged. This problem has been fixed In the routine for executing "mpls set customer-profile ...", the RS now turns off the IEEE802.1q encapsulation in the TMAC if the customer facing port is a MPLS port.	31544
MPLS – When an MPLS port transitions down and up, on a transit router, causes the ILM table to fill up. When LER’s MPLS primary path is failed over to backup a few times and then an LSR port is bounced down and up the ILM Table fills up. RS# mpls show ilm-table Interface LDP-label-range RSVP-label-range Labels ------------ ---------------------- ------------------------ --------- lo 17-4096 4097-8192 3 16 IF-1 17-4096 4097-8192 4097 4098 4099 3 4100 4101 4102 4103 . . . 4112 16 The following error messages may be seen: mpls show label-switched-path ingress verbose the router shows "PolControlFailure" state: Down status: PolControlFailure %MPLS-I-PATHREQUESTREJECT, Path "IF-1-XERTIX-IF-1_IF-1-XERTIX-IF-1-PRIMERA": label request is rejected. MPLS Error = (0x18, 0x87). This problem has now been resolved.	33022
MPLS – When configuring the LDP FEC to map 1p priority to exp, the mapping is not properly set. When adding the command: ldp set l2-fec vlan 2008 copy-1p-to-exp to the RS configuration, the parameter representing the copy-1p-to-exp for VLAN 2008 is not set. The issue has now been corrected.	33146
MPLS - With Transparent LAN Services, When creating a TLS customer facing port that receives SNAP packets, for example Cisco's PVST BPDUs, the LDP session will not stay up for more than 1 minute. This problem has been resolved.	31958
POS APS – pulling and reinserting the transmit fiber on a PoS APS port with an IP interface, interrupts traffic. L2 traffic is unaffected by this type of failure but is an IP interface is present the traffic does not recover. This problem has now been corrected.	32942

Issues Resolved in version 9.1.0.1	ID
Software	
QOS – The command “qos over-write tos-byte”, is not functioning. This issue has now been resolved, there were multiple issues, in the routing mode, the precedence wasn’t working properly. In addition, the existing entries were not getting updated as policies were added. Also a new CLI error message - to reject the command if a user attempted to apply TOS rewrite on an l4-bridged port since this is not supported.	31101
QOS – The command “qos show ip” gives incorrect information when QOS is applied to a SmartTrunk. The problem was that the command didn't recognize SmartTrunks; this problem has now been corrected.	32707
QOS – The Weighted Fare Queuing (WFQ) is not distributing traffic correctly on .1q Trunk ports. In earlier versions of code when an ATM service profile was created an incorrect percentage of traffic would be apportioned to each of the internal queues on egress from the ATM port. For example a service profile may be created such as: atm define service test srv-cat cbr pcr-kbits 10000 qos-control 10 qos-high 20 qos-medium 30 qos-low 40 atm apply service test port at.1.1.0.100 When testing this scenario on a network tester such as an Ixia or Adtech the percentage of each type of traffic was seen to be incorrect. This was due to a software error on the way that bytes were being counted. This issue has now been resolved.	32947
QOS - When the router is configured with the command "qos set weighted-fair idle 100" on a Gigabit card using 5th Gen Input Packet Processor, the router crashes. Since the crash only occurs when the Idle value is 100% and since it makes no sense to set idle to 100%, the range has been changed to be from 1% to 99%.	31770
RADIUS - accounting has problems using global key, authentication works, but when the RS tries to process a radius accounting packet, it doesn't use the global key. The workaround is to set a server key to get radius accounting to work. This issue has now been resolved and RADIUS accounting will now operate with the specified global key.	33116
RADIUS – In version 9.1.0.0 the Radius implementation has been updated. In the process, a correction was made from the implementation in 9.0 such that the default value for Acct-Status-Type was changed from 7 (Accounting-On) to 3 (Interim-Update) to meet the spec. In the process some accounting attributes were lost in the transition to new RADIUS implementation. In 9.1.0.0 the missing three fields have been restored: Acct-Session-Id, Acct-Authentic and User-Name (Acct-Session-Id is a “MUST” field in the RFC).	31703
RADIUS - Setting the global radius parameters for retries and timeouts, in the RS configuration, does change the default values for the Radius server setting. This issue has now been corrected.	31677
RADIUS – The Radius authentication is not working correctly when using Radius set source lo0. The global radius command to set the source address for radius packets from the switch (radius set source lo0) does not work in version 9.1.0.0. The RADIUS session processing was ignoring the global RADIUS source address. This problem has now been resolved.	31499
RMON - The RMON II MIB, sysUpTime, was less than the TimeMark for some tables such as the al-host table. This is now fixed so the sysUpTime will always be greater than the TimeMark.	32748
SmartTrunk – The RS can crash when SmartTrunk set to destination based forwarding mode. With the command 'ip set port st.1 forwarding-mode destination-based', the RS crashes. As long as the command 'ip set port st.1 forwarding-mode destination-based' is part of the RS configuration the router will crash at boot time. . If that command is removed from the config, the router successfully boots. This issue has now been resolved.	31736
SNMP – Additional VLAN statistics have been exposed for customer use. There is now SNMP MIB Support for per-VLAN bytes statistics on trunk ports. The CLI commands for accessing these statistics are: Configuration mode; rs(config)# port enable per-vlan-stats Enable mode; rs# port show per-vlan-stats This information has been placed in the dot1qPortVlanStatisticsTable in Q-Bridge-MIB, there are counters for in/out/discard frames only.	32698
SNMP – After SNMP executes a get on the mplsOutSegmentTable, when the MPLS network re-converges the RS can crash. The data is fetched as part of MPLS Control Task, there was a bug in which additional orphan entries are created, these orphan entries are causing the crash accessing an invalid memory location. The issue has now been corrected.	31877
STP / MVST - When using MVST over TLS, a port in blocking mode in one VLAN affects another VLAN that was not configured for MVST. This issue has now been resolved in this release.	31335

Issues Resolved in version 9.1.0.1	ID
Software	
TACACS+ - When TACACS+ is configured for "login mode" authentication, "enable and diag mode" password authentication is suppressed so it is not necessary to issue the "login mode" password a second time to gain access to enable mode. A request has been made to be able to use the locally defined enable password when TACACS+ is set for login mode authentication. In this release of the ROS firmware there is a change in the behavior of TACACS+ authentication. Changes in 9.1.0.0 to avoid redundant authentication under RADIUS and TACACS+ did not take into account the case where Authentication is used on login mode, but a system password is set on enable or diag modes.	31973
VLAN - When adding a new port to a Martini based VLAN, the L2 FEC losses connectivity. This occurred because the RS was updating the l2 entries of MPLS customer facing ports. This is not the correct behavior, Now the RS will not update these ports. if the port is added to or removed from a VLAN.	31929
MPLS – L2 filters are not programmed correctly when a Fast Reroute LSP goes through a state transition. The state transition sequence can either be from Up to Detour or from Detour to Up. This issue has now been corrected in this release of the ROS firmware.	32320
VLAN – The LDP L2 FEC connectivity can be lost after changes are made to the L2 network configuration such as commenting out and in VLAN related commands.	31575
MPLS – L2 Filters not recreated properly after configuration changes for a multi-site martini customer network.	31909
HRT – In a configuration with a WAN port interconnecting two routers, after enabling HRT traffic stops. This interruption in traffic forwarding occur where 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

Issues Resolved in version 9.1.0.0	ID
Hardware	
RS16000 – The Power Supply Status/ID bits are incorrect resulting in the wrong status or the wrong type of power supply being reported	24192
Control Module - Hotswap of flash cards is not supported during run-time	
Non MPLS Gigabit line cards configured for Software MPLS: Cannot ping with a packet size 1500 from a router upstream of ingress router.	20189
The 16 port Fast Ethernet line card stops transmitting after receiving a packet greater 1998 bytes in length.	26230
Software	**ID**
ACL - when an ACL is commented out of a configuration and then commented back in, the ACL will no longer take effect.	25703
ARP - After creating multiple interfaces over trunk port, it may not be possible to create multiple static ARP entries. If this occurs the router will return the following error: %CLI-E-FAILED, Execution failed for "arp add 221.1.1.2 mac-addr 000000:000062 exit-port gi.4.6" %SYS-E-BADPORT, ARP entry cannot be added as the port gi.4.6 is not part of the interface to which 221.1.1.2 belongs. %SYS-I-ACTIVECFGTOBACKUP, active configuration updated on Backup CM	26374
ATM - After hot-swapping an ATM line card, the trunk/stackable port/VC do not get added back to their appropriate VLAN.	21560
ATM - Cross-connect is not operating in this release - generating error: %L2TM-W-INVALID_VLAN	27105
ATM – If the four port ATM line card is hot-swapped out and in the following error message may be displayed. %SYS-E-PORTBUSWRITE, Port bus write error at address 0xc2b4000c	26261
ATM – OC12: The force-bridge option will not take effect until the RS is rebooted.	22976
ATM – OC-12: When applying PPP on 65K VCs, the SYS-HEAP95FULL warning message may be displayed. However once the Apply operation is complete the memory required to perform this activity will be returned to the system.	15451
ATM – OC12: when negating an interface and it's VC, the VC will appear to remain a member of the Default VLAN	18593
ATM – OC-3 : negating a VC service definition, may cause the traffic over the affected VC to follow port definition not VP definition.	15789
ATM – OC-3: After removing an ATM VCL from an interface, it's associated ARP entry sill exists.	25691

Issues Resolved in version 9.1.0.0	ID
ATM – OC-3: In a redundant CM configuration - negating the VLAN configuration information, for an ATM OC3 port, on the Primary CM, will not remover the associated lines from the configuration on the Backup.	26031
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
ATM – VC aware IGMP multicast is not currently supported	
ATM – When adding and removing and re adding VCLs, the VCL create operation 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
ATM OC-12: Removing an interface and the VC itself will show VC in the default VLAN	18593
POS – A system hang can occur if a POS OC-12 card configured as APS is hot-swapped out and back in.	26265
POS - Hotswap of POS line card is not supported in an APS configuration. The result of this action can be a system crash the hotswap in operation is attempted on the protection card	26911
POS - Jumbo frame greater than the 9000 byte MTU cannot be forwarded as either Layer-2 or Layer-3 traffic.	17426
POS OC48 – HRT is not currently supported in the POS OC48 line card. Attempting to enable HRT may result in the following error: %SYS-E-PORTBUSWRITE, Port bus write error.	26593
POS OC48 - PPP is not negotiated on the protection port once APS is removed	26315
POS OC48 - The layer 2 exit port information is not being displayed in some specific configurations of the POS OC48 port	27177
POS OC48 – The POS OC48 port can be made a trunk port without being placed in force-bridging mode.	26322
POS OC48 – When L2 aging is performed on the Layer-2 table of the OC48 line card, the aged entries are not removed.	26658
POS OC48 – Hardware load balancing (hlwb), of l3 traffic only operates if the OC48 link is not over subscribed. If the OC48 link is oversubscribed, there will be an abrupt decline in the usable bandwidth.	25673
POS OC48 – It may not be possible to negate the PPP configuration after hot-swapping out an OC48 module	24188
POS OC48 - throughput numbers for OC48 is not wire speed. This condition exists for Small size packets 64 bytes through 256 bytes, as the size of the packet increases the throughput approaches 100%. The loss at 64 bytes is approximately 5% - 7%.	26006
CM Failover - "%SYS-W-CLI_CHANNELIZED_ERROR_CONVERSION_FAIL" on config save after Failover.	26722
CM Failover – When the RS is configured for MPLS, after a CM failover the CPU may receive packets with the wrong VLAN ID.	26662
CLI – Using the "q" (quit) pagination option during the "vlan show" output, may causes system to appear to hang for approximately 50 seconds.	27219
Comment – A crash may occur, if there is an attempt to remove an entire configuration with the “negate all” command and that configuration contains commands that are commented out.	27200
CM Failover - DVMRP is only supported on Ethernet and Gigabit Ethernet cards, during failover multicast traffic will stop.	24371
CM Failover – When the RS is configured for RIP, after CM Failover, RIP routes turn to kernel routes and remote route disappear.	26203
DHCP - With L4-Briding enabled, DHCP clients cannot renewal after release	24340
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
Hotswap – The RS may hang when at 16 port Fast Ethernet card is Hotswap out. This is most likely to occur when some of its ports are configured as Trunks and added to 500 or more VLANs.	15246
IGMP – The T1 and T3 line cards don’t currently support IGMP. These cards do not forward IGMP traffic when an end device receives multicast traffic via DVMRP.	25817
Multicast – A Crash can occur when the DVMRP is negated and PIM-SM is started.	26806
Multicast – in a multicast configuration, after negating the command “port disable force-link-down” it is not possible to ping directly connected routers.	26048
Multicast: forwarding cache is not being cleaned up properly	24323

Issues Resolved in version 9.1.0.0	ID
PIM - When a RS is connected to a Cisco, The RS may crash when a “PIM Join-Prune trace is enabled”, and the command “show ip pim joiners gigabitEthernet 4/1 224.0.2.1" or "show ip pim pruners gigabitEthernet 4/1 224.0.2.1" is executed on the Cisco.	27187
PIM - The mtrace (multicast Traceroute utility), is not supported in version 9.0.0.0	22510
PIM - The RS will drop one multicast data packet while switching from RPT to SPT mode	24521
PIM – there is a display error in the output of the command “pim show current-defaults”. RS will have the wrong value for “Elected BSR Rpset period” and “Elected BSR Holdtime”,	27223
PIM - to inter-operate with Cisco, insure BSR is configures with the hash mask length set to 4. 1. On the RS use the option, 'hashmask-len' with cbsr command, e.g. “pim sparse cbsr address <ifname or address> hashmask-len 4” 2. On Cisco use the following options "ip pim bsr-candidate GigabitEthernet4/0 4" 3. On all Riverstone routers turn on the cisco-hash option. i.e. use "pim sparse global cisco-hash"	26665 26196
PIM - Under some test conditions, with a large number of multicast groups and a high volume of multicast traffic, CPU utilization will increase to 100%, when this condition occurs the CPU utilization may stay at 100% even after the traffic is stopped.	26284
MPLS - After hot-swapping in an MPLS card, the LAP add interface commands are errored out (marked with an “E”) in the configuration. The workaround it to stop and restart LDP.	26609
MPLS - Backup without "standby" will automatically be activated at boot-up and does not shutdown. Secondary paths associated with a label switched path, without the "standby" command are automatically started if the LSP is not up on the primary path. This means at bootup all secondary paths, whether hot (with "standby") or cold (without "standby") will automatically establish.	26859
MPLS – if the MPLS interface is brought down and back up, its specified bandwidth will revert back to the default value.	20193
MPLS - if the transit RS bandwidth is over subscribed, the remote LDP session can transition down and up frequently.	25584
MPLS - The function to inhibit TTL decrementing (no-decr-ttl) is not operating in this release.	27134 26570
MPLS – The Gigabit Ethernet ports of the MPLS line card don’t support jumbo frames over 2000 bytes.	20610
MPLS – The hold & setup priority do not operate properly. An LSP with higher priority fails to tear down an old LSP with a lower priority.	17578
MPLS - The performance of the router is impacted when sending 70,000 BGP routes through the MPLS cloud. • The RS console becomes very slow. CLI commands such as ‘bgp show summary’ take a long time to complete (+ 30sec). • OSPF connection with the RS may experiences state transitions from up to down and back up. • Task Gated takes most of the CPU time when ‘debug task top’ is entered. • It takes more than 10 minutes to install all 70000 routes. 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.	19631 22231
MPLS - when creating large numbers of LSP, greater than 2000, the following error message may be displayed and instability with routing protocols. MPLS-E-SOFTLBL, No support for soft-label.."	26903
MPLS – When large numbers (~4000) of LSPs are configured the error "L2TM-W-ADD_L2_ENTRY, add L2 entry failed" may be displayed.	26486
MPLS/SVLAN: doubly tagged traffic may leak on to the wrong VLANs, when a stacked VLAN tunnel exit port is configured with a VLAN ID in the same range as the user VLANs.	26047
MPLS - Loss of LER in VPN Causes connectivity interruption to all sites in the VPN	28788 29122
MPLS/POSOC12:port disable does not make APS to switch to protecting port	29079
MPLS/POS - The MPLSCP protocol is negotiated when the MPLS-POS line card is in non-MPLS mode.	27757
MPLS – In an MPLS configuration, after removing a port from a VLAN, the error message "MPLS-W-L2FLTDEL, Unable to remove MPLS L2 filter" may be displayed/	23444
MPLS - Under certain configurations involving multiple VLANs, the following happens: 1. When traffic is sent to an LER1 on vlan1, it floods it to LSPs corresponding to vlan1 and vlan2. 2. When reverse traffic is sent to LER2 on vlan2, the L2 code finds that the source MAC has been learnt on the LSP corresponding to vlan2. As a result, LER2 installs a unicast L2 entry. However, LER1 still floods, but LER2 has a unicast l2 entry at the customer ports. This can be solved if LER1 floods only on those LSPs meant for vlan1	30377

Issues Resolved in version 9.1.0.0	ID
MPLS - If a port is part of a PORT-VLAN FEC (TLS customer profile), the L2 code currently allows packets arriving with a different VLAN (other than what is specified in the FEC) to be processed and sent into the MPLS cloud. These packets are dropped at the egress LER's backbone (MPLS) port. This behavior is aslso exhibited by L2-martini tunnels.	30511
MPLS - The RS currently does not support traffic containing customer profiles with single source and destination addresses across multiple VLANs.	29473
Port Mirror – port mirroring of an Ethernet port may causes traffic problems over ATM connections.	15932
QoS – QoS weighted-fair queue does not work properly, control traffic exceeds the specified rate.	11632
QoS - TOS precedence and TOS rewrite is not currently supported when L4 bridging is enabled.	15952
Rate Limit - aggregate rate limiting in not working if more than 1040 policy are in use.	14601
Rate Limit – The source MAC address can be corrupted when burst-safe rate limiting is applied.	15952
Rate Limit – TOS precedence and TOS is not supported when L4 bridging is enabled.	15952
Rate Limit - Applying rate limiting on 1 port of VLAN, L2 traffic for other port is not learn.	28997
BGP – in some cases where the router has learned in excess of a 150K routes, the following error may be displayed on the console; %ROSRD-E-ASSERTFAIL, Assertion failed pid[0xe10562f0], file sockaddr.c, line 191: s2	26856
HRT - If the outgoing interface is on SmartTrunk for the given route, then HRT is disabled for that route. HRT is not disabled for the whole incoming port but only just for the routes with outgoing interface on SmartTrunk.	25349
HRT – A core dump can occur, when one slot is in hrt mode and the "install lsp-route" command is commented out.	26778
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 occurs after a CM failover and the problem can be corrected by a reboot.	27036
ISIS – Route maps defined for IS-IS routes don't support the metric option.	
IS-IS – The IS-IS MD5 implementation, for version 9.0.0.0, is bases on the new draft standard HMAC-MD5. Because of this change, IS-IS with MD5 authentication is not backward compatible with previous versions of the ROS firmware. But it will be interoperable with other vendors as they update their implementations of MD5 for IS-IS.	
ISIS – The ISIS routing protocol is not supported on ATM OC-3 cards.	
Rip – RIP does not get updated properly over Wan links.	16132
RIP - RIP routes will not traverse unnumbered WAN interfaces	27026
SmartTrunk - Changing the MTU/MRU on a SmartTrunk is not currently a supported feature for any type of port. Change the MTU/MRU prior to adding the port to the SmartTrunk.	27257
SmartTrunk - A SmartTrunk configured with the Huntgroup protocol, may transition down and up, when the RS receives a large burst un-learned packets.	20481
SmartTrunk – The huntgroup protocol is not supported on SmartTrunks with POS ports	25554 26283
SNMP – The index in the rsAtmMib for rsAtmFdbVpi and rsAtmFdbVci are currently incorrect.	26882
SNMP – The ipCidrRouteNumber gives erroneous number of routes, the number of routes returned by ipCidrRouteNumber is typically lower than the number of routes actually present in the tables. However, the count of entries in the CIDR table matches the total number of routes.	23016
SNMP – For OSPF interfaces, the SNMP function “getone” fails to return the appropriate information, but “getnext” does succeed.	26457
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
The “stp force” command cannot be used in conjunction with MAC address limits.	29268
PVST – The RS may crash when more than a certain number when a moderate to large number (>30) of PVSTs are created.	20869
Forwarding mode - It is not recommended to enable both custom mode forwarding and dest-based forwarding policies on the same port. Reason being is that re-configuration can cause different policies to take effect.	26431 26538

Issues Resolved in version 9.1.0.0	ID
System – In some configurations containing Custom Forwarding mode the CPU utilization can be elevated to 100%.	26832
Telnet – A telnet session may be terminated if too much output was to be displayed. This can occur if the "terminal monitor" is enabled and there are a high number of console messages.	25917
Telnet – In some cases, after a port scan is performed against the RS, telnet access will be disabled.	20220 23904
Telnet - killing a telnet session from serial console may result in a crash if the telnet session is in the process of some action such as a packet or protocol trace.	20974
Telnet - killing a telnet session from serial console may result in a crash if the telnet session is running a ping flood.	21238
SSH – A system crash may occur when killing an SSH session, from the serial console, while a large amount of data is being displayed.	19686
SVLAN - If you hotswap out the ATM port on which stackable VLANs is enabled, and then hotswap it back in, sVLANs will no longer be enabled on the ATM port.	20699
MLP – When an MLP port transitions Up/Down the following messages may be displayed on the console constantly after alarming CHT3: %WAN-I-MSG, Loadable module 11: -NOSUPPRESS-PPP_MP_PROTOCOL_UP, IPX on mp.1 is up %WAN-I-MSG, Loadable module 11: -NOSUPPRESS-PPP_MP_PROTOCOL_UP, OSI on mp.1 is up %WAN-I-MSG, Loadable module 11: -NOSUPPRESS-PPP_MP_PROTOCOL_UP, IP on mp.1 is up %WAN-I-MSG, Loadable module 11: -NOSUPPRESS-PPP_MP_PROTOCOL_DOWN, IP on mp.1 is down %WAN-I-MSG, Loadable module 11: -NOSUPPRESS-PPP_MP_PROTOCOL_UP, IP on mp.1 is up %WAN-I-MSG, Loadable module 11: -NOSUPPRESS-PPP_MP_PROTOCOL_DOWN, IP on mp.1 is down %WAN-I-MSG, Loadable module 11: -NOSUPPRESS-PPP_MP_PROTOCOL_UP, IP on mp.1 is up %WAN-I-MSG, Loadable module 11: -NOSUPPRESS-PPP_MP_PROTOCOL_DOWN, IP on mp.1 is down %WAN-I-MSG, Loadable module 11: -NOSUPPRESS-PPP_MP_PROTOCOL_UP, IP on mp.1 is up	26726
MLP – If an MPL link is brought down by a link failure the RS may print the following message on the console repeatedly. %INTERFACE-E-ZEROPORTSINIF, Interface ipmp1 is not associated with any operational ports.	26066

KNOWN RESTRICTIONS AND LIMITATIONS:

Known Restrictions in this Release

Hardware	ID
RS2000 – The RS2000 is no longer supported.	
The 9.0 and later releases will not fit onto a single 8 MB flash. Customers need to upgrade to 16 MB of flash memory for this release. Two ROS 9.0.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.	
Power supply - When a fan tray is removed from the RS, two console messages may be generated. The first message states that power supply “x” has failed, the second message states that power supply “x” has recovered. These messages are generated by a power monitoring sensor, which detects a power change rather than a true failure. When performing an RS fan tray hot swap in a production environment, ensure that the operations staff is aware of the activity so that they know what the possible messages indicate.	
Power supply – When a chassis is configured with a single power supply and a large number of line cards, inserting the fan tray may cause the router to crash.	
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. If it is necessary to remove the Master Control module, first failover to the Backup CM and then hotswap the old Master.	
Control Module - If secondary control module is installed, ensure both primary and secondary control module's PCMCIA flash card contain the same software version.	
2 port MPLS PoS OC-3c for RS 8x00 and 2 port MPLS PoS OC-12c for RS 8x00 – If a link is physically broken from an OC-3 or OC-12 port one of these line cards after they have passed MPLS traffic, the receive LED will turn RED and stay lit until the cable is reconnected.	

Software	ID
Access Control Lists	
ACL - when an ACL is commented out of a configuration and then commented back in, the ACL will no longer take effect.	25703
ATM / POS	
ATM - IS-IS not supported on the ATM ports	
ATM - 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 – OC12: The IP statistics are incorrect for the vcgroup	24109
ATM – OC-3: If DHCP is enabled, remove & restore over an ATM-OC3 link, the result will be ARP entries without exit port information. This will cause outbound traffic to be flooded to all of the ports in the VLAN to which this port is a member.	24431
ATM – Port level statistics are not correct on the 4 port ATM card on the RS38000. Most Summary statistics counters are always 0 with exception of Transmit traffic.	21420
ATM – Stackable VLANs is currently supported over ATM OC-3 only; support for OC-12 will be in a later release.	
ATM – The command “statistics show ip-interface” does not currently work for interfaces associated with ATM OC-3 or OC-12 ports.	26082
ATM OC-3 Module - Hot swap or live-incretion of the ATM Mod-PHYs are not currently supported.	
OAM - F4 OAM is not supported with the AIS/RDI services - When creating a VCL for segment OAM or a VCL for end-to-end OAM and enabling the AIS/RDI processing, the AIS/RDI cells are not sent.	22985
POS – On a SmartTrunk containing POS APS ports; after disabling the APS protection link from the far end, if the RS id rebooted, the VLANs containing the POS SmartTrunk will not transition to an UP state.	35540

Software	ID
POS – Configuring the “port disable force-link down” on the protection port of a POS OC3 APS configuration, will cause ppp to go down on APS primary connection.	35532
POS - LCP Echo is by default disabled in ROS 9.0. Even Though there are a few issues with LCP Echo - it is recommended that it be enabled to interoperate with Cisco/Juniper.	26622
POS – MVST is not currently supported over POS ports	25854
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 – Spanning Tree (STP), Ring STP (RSTP) and PerVLAN Spanning Tree (PVST_ are not currently supported over POS ports.	18448 25855 25856 26308
POS - To route packets over a bridge encapsulation PPP link use the following command – “ppp set ppp-encaps-bdg ports so.x.x”	
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 OC48 – After a CM failover the POS APS will no longer function properly.	27361
POS OC48 – In some configurations, Layer 3 flows are dropped when HRT is enabled.	26594
POS OC48 – It is recommend that in a POS APS configuration, the port with the lowest numbered be the working port, otherwise PPP may not negotiate upon reboot..	26992
POS OC48 - STP port cost, on the OC48 ports, must be set to a value lower than that of a gigabit.	26317
CM-Failover	
CM Failover – CM Hitless failover is not supported for MPLS configurations. The MPLS card will reinitialize and then become operational.	
CM Failover – CM Hitless failover is not supported for PPP configurations, PPP session will reinitialize after the backup CM has assumed mastership.	26034
CM Failover - tcp-redundancy is not supported, therefore, after a CM failover it will be necessary to restart tcp, ftp and ssh sessions.	
CM Failover – The backup CM can crash, when GVRP is started.	26394
CLI	
CLI – The COS-CLI BGP command "Neighbor <peer-group-name> send-community" is not currently supported.	18984
MAC Address	
Under certain circumstances, when ports are added/removed from LACP SmartTRUNKs, the following error message may be displayed: %STP-E-FAILREGMGMTADDR. Please remove and re-add the SmartTRUNK to the VLAN on which the error was generated.	31214
Having a large number of VLANs in a single MVST instance may lock the console for extended periods of time and not give control to the CPU. It is recommended that you increase the number of MVST instances and have less VLANs associated with each MVST instance.	30969
If a MAC limit policy is configured on a port that was added to the VLAN via the "vlan add-to-range" command, the port can be removed from the VLAN range, even though there is a MAC limit policy associated with that VLAN and port. This prevents the user from negating the MAC limit command. Please add the port back to the VLAN, then negate both commands.	30303
MAC limiting is only supported on 10/100 and Gig.	
Multicast	
Multicast – PIM, IGMP and DVMRP are not supported on channelized WAN cards (ATM, CT1, CT3, CCT3)	
Multicast - Replication of multicast packets across a VLAN trunk port with multiple will reduce the available bandwidth and the per VLAN throughput will not necessarily be an even distribution across the VLANs.	20740
Multicast – when the interconnecting link is configured for multicast, the RS may crash when negating VLAN and SmartTrunk commands.	25242
Multicast - IGMP port-awareness does not apply to the last set of clients leaving group, IGMP and DVMRP are applied to the interface. Using wsend and wlisten, when the last client(s) left the group (no more IGMP members), the multicast traffic is still sent to the port(s) of last client(s).	33478

Software	ID
MPLS / TLS	
MPLS - Loss of LER in VPN Causes connectivity interruption to all sites in the VPN	28788 29122
In this release,MPLS - when a large number of customer profiles (> 1280) are entered into the RS' configuration file, the RS may become unstable.	30709
MPLS – After a CM failover the "port flow-bridging all" is not reapplied to MPLS cards. A workaround is to apply port flow-bridging to individual ports including MPLS.	26370
MPLS – changing an MPLS port from trunk to access and then back to trunk again, the LDP session won't transition to the up state	23405
MPLS - CPU utilization increases if an Entity MIB walk is executed on MPLS card.	29151
MPLS - Customer profiles cannot be changed on the fly. To make changes to a customer profile, the customer profile must first be deleted from all the configuration files of all LERs. Once this is done the changed customer profile is entered into the configuration files of all LERs.	28853 30738
MPLS – In an MPLS configuration the POS-OC12 port disable does not make APS to switch to protecting port.	29079
MPLS – In an MPLS configuration, after removing a port from a VLAN, the error message "MPLS-W-L2FLTDEL, Unable to remove MPLS L2 filter" may be displayed/	23444
MPLS - In this release, all limitations on stackable VLAN entry ports also apply to TLS customer-facing ports.	
MPLS - In this release, MPLS diff-serv does not support LSPs that use fast-reroute mode. Furthermore, MPLS diff-serv does not support MPLS based L2-VPN TLS.	30304
MPLS -– In this release, SmartTRUNKsSmartTrunks are not supported in the customer-side TLS environment.	30251
MPLS - In this release, STP cannot resolve loops across an MPLS core in a TLS environment.	30921
MPLS – Layer 4 bridging is not supported through Martini tunnels.	19794
MPLS - LDP cannot process any session with very large numbers of L2 FECs in the LER.	26537
MPLS - Multiple customer profiles on the same port, with the same source and destination addresses, but with different VLANs is not supported in this release.	
MPLS - OSPF Traffic Engineering Database, displays remote and local IP address as the local IP address of this RS. When viewing the OSPF TED, each router reports its local interface as both its local address and the remote address on each of its links. The expected behavior is that the remote address on each link would correspond to the local interface of the remote router. This is a display issue and does not affect the operation of the RS.	33719
MPLS - Secondary IP addresses are not supported in RSVP and LDP interfaces. For example: 17.1.1.1 17.1.1.2 12.1.1.2 (12.1.1.1) RS2 ---------------- RS3 --------------- RS4 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 transition to an up state. In other words, the secondary interface will not be recognized by LDP at all. The recommended configuration is to include all ports to one subnet, such as: 17.1.1.3/16 17.1.1.1/16 17.1.1.2/16 RS2 ---------------- RS3 ------------------ RS4	19824
MPLS - The command, " ldp set l2-fec" is designed to work with l2-martini tunnels only. The command does not work with TLS.	
MPLS – The interface bandwidth/subscription cannot be dynamically changed when an LSP exists. When the interface bandwidth is set, it will not take effect if the interface involved is being used by an LSP.	19902
MPLS - The maximum number of VLANs a profile can have is 32 .The formulae is: (number of remote peers * number of VLAN)/customer profile =32. However, in this release there are issues when using multiple VLANs and profiles. It is recommended to use only one VLAN per profile.	
MPLS - The MPLS gigabit line card can support either MPLS or NAT or LS-NAT or BGP Accounting or Rate Limiting with the "burst safe" option. No more than one of these functions can be supported in this line card at any point in time	

Software	ID
MPLS - The MPLS-CP protocol is negotiated when the MPLS-POS line card is in non-MPLS mode.	27757
MPLS - The RS currently does not support traffic containing customer profiles with single source and destination addresses across multiple VLANs.	29473
MPLS - This release does not allow the mixing and matching of access-ports and trunk-ports in a customer profile.	30158
MPLS - This release does not support Internet-bound traffic on TLS ports.	28747
MPLS - this release, IGMP snooping is not supported for TLS.	
MPLS – Traffic through a Martini will be impeded when - hop-count-loop-detection-enable is configured	20588
MPLS - Unable to remove MPLS L2 filters while clearing ldp sessions.	28633
MPLS - Under certain configurations involving multiple VLANs, the following happens: 1. When traffic is sent to an LER1 on vlan1, it floods it to LSPs corresponding to vlan1 and vlan2. 2. When reverse traffic is sent to LER2 on vlan2, the L2 code finds that the source MAC has been learnt on the LSP corresponding to vlan2. As a result, LER2 installs a unicast L2 entry. However, LER1 still floods, but LER2 has a unicast l2 entry at the customer ports. This can be solved if LER1 floods only on those LSPs meant for vlan1	30377
MPLS - When changing the MTU of MPLS port, the LSP's mtu in the ott table is not changed until the RS is rebooted or the MPLS card is hot-swapped out and back in.	19388
MPLS – When configuring large numbers of LSPs (several thousand) with no-cspf, the following error messages may be displayed. %SYS-E-INVALID_ILM_INDEX, ILM label 7784 is out of range %SYS-E-INVALID_ILM_INDEX, ILM label 7785 is out of range	26324
MPLS - When the RS is configured for Martini tunnels to interoperate with the 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: 1) Under the Cisco MPLS interface configuration, do 'mtu 2000.' Then it can pass Martini traffic. 2) Under the same interface, do 'clns mtu 1497.' Then IS-IS will keep working. The same problem can be encountered on Juniper routers. Juniper supports setting port MTU and protocol MTU as well.	
MPLS - When there are 2 customer profiles on the same customer port, if one of the profiles changes, the l2 entries in that port are cleared, causing a momentary break in traffic.	30420
MPLS/POS:PPP negotiation issues after bootup on 38K POS OC12	27387
MPLS/POSOC12: The ipcp protocol does not come up after hot swap out & in when aps is configured	28297
MPLS/POSOC12:lcp echo's dropped at wire rate traffic	27702
MPLS/POSOC12:ppp doesnot negotiate when mtu is changed using port set	27581
MPLS/POSOC12:PPP not negotiated after bootup if port configured as trunk	28151
TLS - If a port is part of a PORT-VLAN FEC (TLS customer profile), the L2 code currently allows packets arriving with a different VLAN (other than what is specified in the FEC) to be processed and sent into the MPLS cloud. These packets are dropped at the egress LER's backbone (MPLS) port. This behavior is aslso exhibited by L2-martini tunnels.	30511
TLS - Local bridging among a bunch of customer facing TLS ports is possible, however, the limitation exists that none of those ports in that bunch can belong to more than one customer.	
TLS - Local bridging is allowed only between ports belonging to the same customer. Local bridging is not supported between a TLS port and a non-TLS port.	
TLS - This release does not support jumbo-frames on TLS customer ports.	29857

Software	ID
TLS - Using an atm port as ingress port for MPLS TLS does not work properly	28962 27965
TLS does not currently support flow-based bridging. Ports used with TLS must be in access-bridging mode.	29867
TLS does not currently support the use of ATM line cards.	28962 27965
Port Mirroring	
Port Mirror - after negating a port mirroring command, the MPLS ott table is no longer accessed.	19429
Port Mirror – in some cases after negating port mirroring, monitor port link state will remain in a down state.	26633
Port Mirror – When the port mirror commands are comment out or the monitor port is hot-swapped, the following message may be displayed: %L2TM-W-BAD_PORT, request to perform an action on an invalid port (Port 17; L2TM).	25757 31037
Port Mirror – with port mirror enabled, OSPF may not form and adjacency across CT1 and CT3 interfaces.	26570
Port Mirror: when port mirroring is enabled, RIP V2 may nit operate over HSSI / PPP connections.	26886
QOS	
QOS - When commenting out a QOS profile that has been applied top both a port and an interface and then negating the QOS applied command on the port, the RS will crash.	36373
QOS - qos set is not changing the 1p and internal priority for multicast packets	28954 28884
QOS - qos overwrite one-p-priority does not work	28906
QOS - after negating qos set IP command, flows are not flushed and priority not change	28884
QOS - Setting IP QoS does not take effect immediately in L4 bridging mode, existing flows must first age and be recreated.	16027
Rewriting the ToS byte for L4 bridging mode is supported only on line cards with 5th generation ASICS.	
ToS rewrites are supported only on line cards equipped with 5th generation ASICs.	
The qos set l2 ignore-ingress-802.1q command works only on line cards with 5th generation ASICS.	
The ingress priority takes precedence over values set using the qos set l2 ignore-ingress-802.1q priority command, except if the command specifies the value as “control.”	
Rate Limiting	
Rate Limit - All CLI rate limiting commands have been moved under the “Service” facility.	
Burst Safe Rate-Limiting: throughput rate changes as packet size changes.	28325
Rate Limit - aggregate rate limiting is not working on the RS38000, For multicast traffic.	14396
Rate Limit – input rate limiting does not work on RS38000, for multicast traffic	14392
Rate Limit - per flow rate limiting is not working on RS38000 for broadcast traffic	14383
Routing	
BGP – The “bgp show community all” command can get stuck in a loop when there is no community information. rs8600# bgp show community all Bad community string Bad community string Bad community string … Bad community string Bad community string The workaround is to press Control-C to stop the message from printing on the screen.	14383

Software	ID
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 - Some BGP show output will not reflect the private-AS stripping even though the feature is operating correctly.	23827
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 like 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	
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.	
HRT - after disabling a Custom forwarding mode configuration, the hardware routing table is no longer operational.	26830
HRT - If the RS receives a large number of BGP routes (160,000), it would cause hrt "No memory for internal node at level '1'". If the bgp routers are cleared, the result is gated delete all the routes. In the process, It might display the message: sipp_mem_free_bcast: addr = 8751a6c8, ** DUPLICATE FREE ** alloc type = 1	15989
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
HRT – Under certain conditions the Hardware Routing Table can run out of terminal nodes. This only occurs under test conditions where routes are being populated by a traffic generators. Real routes have a more random distribution than those generated by a Smartbits or an Ixia.	15948
HRT - with Multicast is not supported	
ISIS – When ISIS is configured with an illegal area name the routing task will stop operating.	34802
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 – Route maps defined for IS-IS routes don't support the metric option.	
IS-IS – The IS-IS MD5 implementation, for version 9.0.0.0, is bases on the new draft standard HMAC-MD5. Because of this change, IS-IS with MD5 authentication is not backward compatible with previous versions of the ROS firmware. But it will be interoperable with other vendors as they update their implementations of MD5 for IS-IS.	
ISIS - The ISIS routing protocol is not supported on ATM OC-3 cards.	
OSPF - OSPF restart is not supported over POS OC3 in this release, this functionality is expected top be available in version 9.3.0.0	34426
OSPF - if an OSPF neighbor interface transitions to the down state, the "adjacency down reason" is not available. The reason nothing is printed is when the interface goes down the neighbor structure is freed. It is in the neighbor structure that we store the adjacency down reason, because we need to keep track of per neighbor adjacency down info. So when the interface goes down all information about the neighbor is freed.	33851
Routing - Assigning more than one secondary IP addresses on the same subnet to the "en0" interface is not currently supported.	
SmartTrunk	

Software	ID
SmartTrunk – Changing STP port cost on a SmartTrunk with LACP configured, may result in the network not re-spanning if the cost is removed.	19362
SmartTrunk – Changing the configuration of a SmartTrunk with the LACP protocol option, may result in SmartTrunk state transitions from up to down and up again.	27394
SmartTrunk – The LACP protocol based SmartTrunks are not supported in RS configurations with redundant Control Modules. Currently the RS doesn't maintain protocol state information across the two CMs. SmartTrunks with the "no-protocol" option are supported in redundant CM configurations.	
SmartTrunk – On a SmartTrunk with the LACP protocol option, if wan card is hot-swapped out and in, the SmartTrunk can transition down and up. The LACP timeout can be increased to prevent this behavior, but there is no option for SmartTrunks with the huntgroup protocol.	
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.	
SNMP	
SNMP – The value in the counter udpInDatagrams increments for bad ports (a bad port is defined as a port where the udpTable does not show a listener).	24456
Spanning Tree	
RSTP – The current implementation of Rapid Spanning Tree in the Riverstone platforms is IEEE802.1wD (Draft). The current plans are to add support for the IEEE802.1w standard in version 9.4.0.0 of the ROS software. This implementation will not be backward compatible with the current implementation of RSTP, therefore is will be necessary to plan network upgrades on a per LAN bases where RSTP is employed.	
STP - "STP Tunnel mpls , commands get merged even if on diff ports", with the configuration containing the command: stp tunnel mpls ports et.1.1. Then, after configuring an STP tunnel on et.1.2 , The tunnel command for port et.1.1 is no longer displayed in the output of the config-mode show command. The tunnel for port et.1.1 is however still configured and active, but since the command is not listed in the configuration, it will not be possible to negate it from the configuration.	33218
STP - Ports need to be added to the VLAN before enabling STP on those ports when configuring Per VLAN Spanning Tree (PVST).	
STP – Spanning Tree stops operating properly after enable/disable on ports within a SmartTrunk. System does not support port disable of ports that are a part of a SmartTrunk.	33047
System	
DHCP – Using the RS as a DHCP server, DHCP binding are not carried over to the backup CM after a CM failover.	34497
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.	
Memory capacity guidelines - 1. A system with 256 megabytes of memory, has a capacity for a maximum of 150K routes in the FIB, provided each route has only one gateway. 2. A system with 512 megabytes of memory, has a capacity for a maximum of 500K routes in the FIB, provided each route has only one gateway. 3. If each route has more than one gateway, the above maximum routes will decrease, each gateway will require more memory. 4. The theoretical maximum of BGP peer hosts is 175, this doesn't mean 175 groups can be created, each with one host. The maximum number of groups is a function of the number of routes that will be redistributed to the group. 5. Creating multihop group/host will reduce the maximum number of multihop groups. A multihop group requires one host per group, therefore it will take double the space than that of a non-multihop group. Thus, the maximum number of peer host will be reduced to ~84.	
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.	
TACACS-Plus	
TACACS+ - When TACACS+ is configured with the deadtime option, the deadtime interval is set on all of the servers. So after configuring TACACS+ with deadtime, TACACS+ will skip all the servers. User cannot log in using TACACS+ within the deadtime period. For example, if we set deadtime to 3 minutes, user cannot log in during the first 3 minutes after the RS is rebooted or a Tacacs+ configuration change has been made active.	36287
Telnet and SSH	

Software	ID
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"	
VLANs	
NativeVLAN – Currently the CLI allows a trunk port to be negated even though the port has been set as a native VLAN.	20933
NativeVLAN - Do not negate trunk port without first negating nativeVLAN commands for that trunk port	20937
NativeVLAN – When hot-swapping out one line containing a native-VLAN port, it's associated native VLAN commands are marked in error "E", this is the normal behavior. In addition all other Native-VLAN configuration lines are marked as partially executed "P", this is not the appropriate behavior.	20936
SVLAN - An error may be returned when an attempt to add a Stackable VLAN access port to another VLAN, the CLI may returns the following message: %CLI-E-FAILED, Execution failed for "vlan add ports gi.7.2 to vlanx" %VLAN-E-SVLAN_ACCESS, Stackable Vlans has been enabled on access ports: gi.7.2. Please negate the vlan enable stackable-vlan command first before adding the port(s) to a vlan.	14902
SVLAN - When trying to comment out line 4, I receive the following error message: %CLI-E-FAILED, Execution failed for "comment-out vlan add ports st.25 to super" %VLAN-E-SVLAN_NEG_ACCESS, Stackable Vlans has been enabled on access port: gi.6.1. Please negate the VLAN enable stackable-vlan command first before removing this port from the vlan.	26623
VLAN - in some cases issuing the command "vlan add-to-vlan-range" will produce the error %CLI-E-FAILED, Execution failed.	26516
VLAN – When a VLAN range is not defined issuing the command "vlan add-to-vlan-range" will produce the error "%VLAN-E-NOSUCHVLAN" even though VLAN exists.	23312
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.	
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).	
VLANAGG - Need to age all applicable flows when VLAN is un-bound from super VLAN. Note: when a sub-vlan is un-binded from the super VLAN, no new flows are created, however, if a host has an existing connection at the time, that connection is still valid.	22644
WAN	
PPP – Greater than 276 total PPP interfaces defined on channelized T3 linecards may result in PPP state transitions on some ports.	
PPP – Running LCP magic numbers over PPP may cause LCP to renegotiate.	
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".	
WAN – In certain configurations, after negating l4 bridging, l2 flow are not flushed out for T3 ports.	15118

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
RFC 1490	Multiprotocol Interconnect over Frame Relay

RFC No.	Title
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:

RFC No.	Title
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
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
RFC 2925	SLA support SLA 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
ITU-T Annex D/ANSI T1.617	Additional Procedures for PVCs Using Unnumbered Information Frames

Riverstone PRIVATE ENTERPRISE MIB SUPPORT:

Title	Description
Novell-ipx-mib	Novell Netware
Ctron-ssr-hardware	Device specific hardware objects
Ctron-ssr-policy	L2 filters, l3 acls 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-lfap-mib	Lightweigth 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

http://rstone.riverstonenet.com/Mibs/

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