Patch Release Note

Patch 86251-05 For Rapier Switches and AR800 Series Modular Switching Routers

Introduction

This patch release note lists the issues addressed and enhancements made in patch 86251-05 for Software Release 2.5.1 on existing models of Rapier L3 managed switches and AR800 Series L3 modular switching routers. Patch file details are listed in Table 1.

Table 1: Patch file details for Patch 86251-05.

Base Software Release File	86s-251.rez
Patch Release Date	15-May-2003
Compressed Patch File Name	86251-05.paz
Compressed Patch File Size	320764 bytes

This release note should be read in conjunction with the following documents:

- Release Note: Software Release 2.5.1 for Rapier Switches, and AR800 Series Modular Switching Routers (Document Number C613-10354-00 Rev A) available from *www.alliedtelesyn.co.nz/documentation/documentation.html*.
- Rapier Switch Documentation Set for Software Release 2.5.1 available on the Documentation and Tools CD-ROM packaged with your switch, or from *www.alliedtelesyn.co.nz/documentation/documentation.html*.

WARNING: Using a patch for a different model or software release may cause unpredictable results, including disruption to the network. Information in this release note is subject to change without notice and does not represent a commitment on the part of Allied Telesyn International. While every effort has been made to ensure that the information contained within this document and the features and changes described are accurate, Allied Telesyn International can not accept any type of liability for errors in, or omissions arising from the use of this information.

Some of the issues addressed in this Release Note include a level number. This number reflects the importance of the issue that has been resolved. The levels are:

Level 1 This issue will cause significant interruption to network services, and there is no work-around.

Level 2 This issue will cause interruption to network service, however there is a work-around.

Level 3 This issue will seldom appear, and will cause minor inconvenience.

Level 4 This issue represents a cosmetic change and does not affect network operation.

Features in 86251-05

Patch 86251-05 includes all issues resolved and enhancements released in previous patches for Software Release 2.5.1, and the following enhancements:

PCR: 02583 Module: FIREWALL Level: 2

UDP packets passed through the firewall by a reverse enhanced NAT rule were getting an incorrect IP checksum. This caused IP to discard the packets. This issue has been resolved.

PCR: 03059 Module: FIREWALL Level: 2

SMTP proxy was falsely detecting third party relay under some circumstances. This issue has been resolved.

PCR: 03095 Module: DHCP Level: 2

DHCP policies are no longer stored in alphabetical order in the DYNAMIC CONFIGURATION script because this did not work when the DHCP INHERIT parameter was used.

PCR: 03148 Module: IPG Level: 3

If the Gratuitous ARP feature was enabled on an IP interface, and an ARP packet arrived, (either ARP request, or reply) that had a Target IP address that was equal to the SenderIP address, then the ARP cache was not updated with the ARP packet's source data. This issue has been resolved.

PCR: 03177 Module: IPG Level: 3

Deleting an IP MVR group range would only delete the last IP address of the range from the multicast table, not the entire range. This issue has been resolved.

PCR: 03199 Module: IPV6 Level: 3

RIPng was receiving invalid routes and packets. This issue has been resolved.

PCR: 03241 Module: FIREWALL Level: 3

When deleting a list associated with a policy, all rules were being deleted. Now only the rules associated with the policy and list are deleted.

PCR: 03270 Module: SWI Level: 3

The inter-packet gap has been reduced by 4 bytes on the Rapier 48*i* stacking link. This allows for non-blocking operation with tagged packets.

PCR: 03299 Module: IKMP Level: 2

Under some circumstances, ISAKMP suffered a fatal error if more than 8 SA proposals were presented. This issue has been resolved.

PCR: 03314 Module: SWI Level: 2

Layer 3 filters that matched TCP or UDP port numbers were being applied to the second and subsequent fragments of large fragmented packets. This issue has been resolved.

PCR: 03354 Module: FIREWALL Level: 3

The SET FIREWALL POLICY RULE command was not accepting the value 24:00 (midnight) for the BEFORE parameter. This issue has been resolved.

PCR: 03371 Module: DHCP Level: 3

A minimum lease time can no longer be specified when creating a DHCP policy. This complies with RFC 2131.

PCR: 03383 Module: IPG Level: 2

If there were a large number of routes in the route table, and the SHOW IP ROUTE command was executed, the device stopped operating. This issue has been resolved.

PCR: 03390 Module: HTTP Level: 2

Occasionally a fatal error occurred when the GUI browser started or a page was refreshed. This issue has been resolved.

PCR: 03392 Module: IPSEC, IKMP Level: 3

IPV4 is the default for the IPVERSION parameter in the CREATE IPSEC POLICY and CREATE ISAKMP POLICY commands. This default was unnecessarily displayed in the SHOW CONFIGURATION DYNAMIC command output. This issue has been resolved.

PCR: 03395 Module: BGP Level: 3

The amount of time that BGP peers 'back off' for after changing from the ESTABLISHED state to the IDLE state has been changed. Previously, this 'back off' time grew exponentially and never decayed. The 'back off' time is now always one second.

PCR: 03396 Module: ETH Level: 3

Some memory was lost on the AT-AR022 ETH PIC when hotswapping. This issue has been resolved.

PCR: 03400 Module: SSL Level: 3

Sometimes SSL did not allow its TCP session to close properly. This happened if the *Fin* packet was not piggy-backed on a data packet, or if the SSL Handshake was never completed with the far end. This meant that the closing *Alert* was not sent, so the session could not close. Also, SSL leaked memory when it received invalid SSL records. These issues have been resolved.

PCR: 03402 Module: IPG Level: 2

IP routes deleted from the route cache occasionally caused a fatal error. This issue has been resolved.

PCR: 03405 Module: STREAM Level: 2

The reconnection to the stream printing TCP port failed after a single successful connection was made. This issue has been resolved.

PCR: 03407 Module: IPG Level: 3

The default for the PROXYARP parameter in the SET IP INTERFACE command for a VLAN interface was OFF. The default is now ON.

PCR: 03410 Module: VLAN, CORE Level: 3

If a patch was running with a major software release, after a VLAN was added at the command line, the VLAN was not shown as UP. This issue has been resolved.

PCR: 03412 Module: FIREWALL Level: 3

FTP data transfers did not succeed for some types of NAT. Also, the presence of flow control TCP flags meant that some TCP control packets were not recognised. These issues have been resolved.

PCR: 03413 Module: BGP Level: 2

BGP was updated according to the most recently added route. BGP now updates to reflect the best available route, regardless of when it was added.

PCR: 03415 Module: FIREWALL Level: 2

When using a policy routing rule, the firewall did not translate the source IP address of a broadcast packet correctly. This issue has been resolved.

PCR: 03416 Module: SWI Level: 3

Previously, the ADD SWITCH L3FILTER MATCH command was accepted if the TYPE parameter was not specified. This command now requires the TYPE parameter, and an error message will be returned if the TYPE parameter is not specified.

PCR: 03424 Module: DHCP Level: 2

When static DHCP was set to the first IP address in a range, that range would stay in the *Reclaim* mode. This issue has been resolved.

PCR: 03426 Module: IPV6 Level: 3

If the valid and preferred lifetimes of an IPv6 address for a given interface were set to infinity, they were not included in the dynamic configuration. This issue has been resolved.

PCR: 03429 Module: SWI, VLAN Level: 3

The SHOW VLAN command was displaying a port that did not exist. This issue has been resolved.

PCR: 03430 Module: BGP Level: 3

BGP traps were sent incorrectly when a BGP peer became Established, or moved into a lower state. This issue has been resolved.

PCR: 03432 Module: STP Level: 2

STP settings were not retained when a port was deleted from the VLAN that the STP belongs to. This issue has been resolved.

PCR: 03436 Module: IP, DHCP Level: 2

When the device was acting as a DHCP client and the DHCP server provided a gateway address, a statically configured default route was deleted and replaced with a default route with the provided gateway address. The correct behaviour is to only delete a dynamic default route in this situation. This issue has been resolved; the correct behaviour is now applied.

PCR: 03439 Module: IPX Level: 3

The IPX traffic filter match counter was not incremented if a route was cached. This issue has been resolved.

PCR: 03441 Module: L2TP Level: 2

PPP configured on a L2TP access concentrator (LAC) should be dynamic. If PPP was incorrectly configured to be static, the static PPP was destroyed when the L2TP tunnel was formed so that only the first connection succeeded. This issue has been resolved so that an L2TP tunnel is not created if the PPP is static.

PCR: 03443 Module: DHCP Level: 3

When a DHCP entry expired while other DHCP entries in the range were in *Reclaim* mode, unnecessary ARP packets were generated causing an ARP storm. This issue has been resolved.

PCR: 03444 Module: FR Level: 3

The CIR and CIRLIMITED parameter in the SET FRAMERELAY DLC command now regulates the behaviour of the transmission rate. Previously, the transmission rate did not reflect changes to the CIR setting if the new CIR was higher than the old CIR (provided that the new CIR is within the physical maximum of the network and the hardware), or changes to the CIRLIMITED setting if CIRLIMITED was turned ON then OFF. This issue has been resolved.

PCR: 03446 Module: SWI Level: 3

After unplugging a fibre uplink cable and then plugging it back in, a short Ping timeout occurred. This issue has been resolved.

PCR: 03450 Module: PIM, PIM6 Level: 2

Receiving PIM *State Refresh* messages now creates and/or maintains PIM forwarding information.

PCR: 03453 Module: FIREWALL Level: 3

The dropped packets counter for the firewall was not incrementing correctly. This issue has been resolved.

PCR: 03454 Module: IPV6 Level: 3

Occasionally, removing the cable from an IPv6 interface caused the device to stop responding. This issue has been resolved.

PCR: 03456 Module: PIM Level: 2

A VLAN interface receiving a PIM *Prune* message on a port stopped forwarding multicast data to that port too early. This could cause multicast data to arrive after a PIM *Prune*, so an override PIM *Join* message was not sent, leading to a loss of multicast data. This issue has been resolved.

PCR: 03457 Module: OSPF Level: 2

Disabling OSPF caused a fatal error if there was a large routing table. This issue has been resolved.

PCR: 03459 Module: IPV6 Level: 2

A fatal error sometimes occurred when packets were forwarded via an IPv6 interface, and IPv6 flows were disabled. This issue has been resolved.

PCR: 03461 Module: IPG Level: 3

The ENABLE IP MVR DEBUG=ALL command was erroneously shown in the output of the SHOW CONFIG DYNAMIC=IP command. This SHOW output no longer includes the ENABLE IP MVR DEBUG=ALL entry.

PCR: 03462 Module: PIM, PIM6 Level: 3

PIM *Graft* and *Graft-Ack* counters were not incrementing. This issue has been resolved.

PCR: 03465 Module: DHCP Level: 3

The IPMTU parameter in the ADD DHCP POLICY command was accepting values in the range 0-4294967295. This parameter now accepts values in the correct range of 579-65535.

PCR: 03463 Module: PIM, PIM6 Level: 3

PIM-SM *Null* register messages did not update the register counter correctly, and did not trigger *Register* debug messages. This issue has been resolved.

PCR: 03464 Module: PIM, PIM6 Level: 3

PIM-SM *Null* register messages for non-PIM-SM domain sources did not have the *Border* bit set. This issue has been resolved.

PCR: 03467 Module: IPG Level: 3

An invalid message appeared when the PORT parameter was specified for the ADD IP ROUTE command. This issue has been resolved.

PCR: 03471 Module: IPV6 Level: 2

A fatal error sometimes occurred when forwarding traffic over an IPv6 tunnel. This issue has been resolved.

PCR: 03473 Module: PIM, PIM6 Level: 3

The SET LAPD MODE=NONAUTOMATIC command did not change the LAPD mode from automatic to non-automatic. This issue has been resolved.

PCR: 03474 Module: FIREWALL Level: 3

The SMTP proxy did not correctly allow outgoing (private to public) SMTP sessions when the DIRECTION parameter was set to OUT or BOTH in the ADD FIREWALL PROXY command. This issue has been resolved.

PCR: 03475 Module: NTP Level: 3

The PURGE NTP command did not change the UTC offset to the initialised value. This issue has been resolved.

PCR: 03476 Module: IPV6 Level: 3

RIPng was showing routes to interfaces that were DOWN as being UP. This issue has been resolved.

PCR: 03478 Module: PIM, PIM6 Level: 3

The message format for PIM-SM periodic (*,*,RP) *Join* messages was incorrect when the message contained more than one joined RP address. This issue has been resolved.

PCR: 03484 Module: FIREWALL Level: 3

The firewall was not denying an ICMP packet, even if ICMP Forwarding was disabled when using Standard NAT. This issue has been resolved.

PCR: 03492 Module: HTTP, LOAD Level: 2

Some memory loss occurred when loading a file via HTTP. This issue has been resolved.

PCR: 03494 Module: BGP, FIREWALL Level: 2

If the firewall was enabled when BGP was in use outgoing BGP data packets would have IP header errors and incorrect checksums. This problem has now been fixed.

PCR: 03497 Module: PIM, PIM6 Level: 2

In a network with an alternative path, if the link connected to the interface where a Candidate Rendezvous Point (CRP) advertised its RP candidacy was down, the CRP did not re-advertise its RP candidacy on other available interfaces (the alternative path). This meant that the CRP did not update its PIM routes, which was necessary to re-establish the PIM tree in order for multicast data to flow again. This issue has been resolved.

PCR: 03498 Module: SWI Level: 3

The SHOW SWITCH FDB command showed a number of irrelevant entries. This issue has been resolved.

PCR: 03502 Module: IPG Level: 3

The ENTRY parameter from the ADD IP FILTER command was not included in the output of the SHOW CONFIG DYNAMIC command. This issue has been resolved.

PCR: 03513 Module: IPG Level: 3

An enhancement allows for the creation of static IGMP group memberships that do not time out. For details on this feature, see "*Static IGMP*" on page 24.

PCR: 03515 Module: DHCP Level: 3

DHCP was offering network and broadcast addresses to clients. This issue has been resolved.

PCR: 03517 Module: FIREWALL Level: 3

An error was not returned if the SET FIREWALL POLICY RULE command was executed with PROTOCOL=1 when ICMP forwarding was turned on. This issue has been resolved so that an error is now displayed.

PCR: 03523 Module: FIREWALL Level: 2

In some circumstances the checksum for the TCP header was set to zero. This issue has been resolved.

PCR: 03526 Module: SWI Level: 3

The Switch MIB did not show the correct *dot1StpPriority* value. This issue has been resolved.

PCR: 03531 Module: SWI Level: 3

After creating a trunk group, the activity LEDs did not flash unless the configuration was used at reboot. This issue has been resolved so that the LEDs flash correctly whenever a trunk group is created.

PCR: 03468 Module: PIM Level: 3

The source IP address in a PIM *Register* message was not the DR interface's IP address. This issue has been resolved.

PCR: 03533 Module: PIM Level: 3

A forwarded PIM-DM state *Refresh* message did not update the metric and preference values. This issue has been resolved.

PCR: 03535 Module: IPG Level: 2

IGMP *Query* messages were not sent after IGMP was disabled and then re-enabled. This issue has been resolved.

Features in 86251-04

Patch file details are listed in Table 2:

Table 2: Patch file details for Patch 86251-04.

Base Software Release File	86s-251.rez
Patch Release Date	15-April-2003
Compressed Patch File Name	86251-04.paz
Compressed Patch File Size	240936 bytes

Patch 86251-04 includes all issues resolved and enhancements released in previous patches for Software Release 2.5.1, and the following enhancements:

PCR: 02571 Module: IP Level: 3

A fatal error occurred if the IP module was reset after the ADD IP EGP command was executed. This issue has been resolved.

PCR: 02577 Module: IPG, LOG Level: 4

The ability to log MAC addresses whenever the ARP cache changes has been added. To enable this, use the command:

```
ENABLE IP ARP LOG
```

To disable it, use the command:

```
DISABLE IP ARP LOG
```

The logging of MAC addresses is disabled by default. Use the SHOW LOG command to view the MAC addresses that have been logged when the ARP cache changes.

PCR: 03025 Module: GUI Level: 2

A buffer address was incrementing and not returning buffers for reuse when the command line interface was accessed via the GUI interface. This issue has been resolved.

PCR: 03044 Module: BGP Level: 2

During route flapping, peers were sometimes not told about routes to the same destinations as the flapping routes. This issue has been resolved.

PCR: 03048 Module: STP Level: 2

If a port belongs to an enabled STP instance, but the port has been disabled from STP operation with the DISABLE STP PORT command, the port will not respond to ARP requests. This patch implements a workaround that allows disabled STP ports to respond to ARP requests.

PCR: 03089 Module: CORE Level: 4

The SET SYSTEM NAME command was accepting character strings greater than the limit of 80 characters. This issue has been resolved.

PCR: 03094 Module: STP, VLAN Level: 3

The VLAN membership count for STP ports was incorrect in the default configuration. This issue has been resolved.

PCR: 03096 Module: VLAN Level: 2

OSPF and RIP *Hello* packets were being sent out all trunked ports. Now these *Hello* packets are only sent out the master port of the trunked group.

PCR: 03097 Module: IPV6 Level: 3

A device could not Telnet to a device outside its own subnet. This issue has been resolved.

PCR: 03098 Module: PIM, DVMRP, IPG Level: 2

When multicasting in hardware, the switch would not forward packets from a VLAN ingress interface to a non-VLAN interface downstream. This issue has been resolved.

PCR: 03105 Module: FIREWALL Level: 3

Incorrect handling of TCP sessions, and poor load balancing performance could be caused by TCP virtual balancers not selecting a new resource if required. This issue has been resolved.

PCR: 03109 Module: LOG Level: 3

A log was only partially created if there was insufficient NVS memory for log creation on the router. A change has been made so that a log is not created if there is insufficient memory, and a warning message is displayed.

PCR: 03110 Module: IPG Level: 3

An error occurred with the ADD IP MVR command. This issue has been resolved. Also, this command accepted any IP addresses for the GROUP parameter, but now only accepts multicast addresses.

PCR: 03111 Module: FIREWALL Level: 1

TCP sessions could fail if the public side of the firewall was using Kerberos and the private side had a very slow connection to the firewall. This issue has been resolved.

PCR: 03115 Module: PING Level: 3

The SHOW CONFIG DYNAMIC=PING command was giving an incorrect port number. This issue has been resolved.

PCR: 03116 Module: FIREWALL Level: 2

An error sometimes occurred in the firewall module under heavy FTP or RTSP traffic loads. This issue has been resolved.

PCR: 03117 Module: FIREWALL Level: 1

The TCP sequence numbers are no longer altered through the firewall when TCPSETUP is disabled with the DISABLE FIREWALL POLICY command.

PCR: 03119 Module: CLASSIFIER Level: 4

TCP source and TCP destination ports were swapped when viewed in the GUI. This issue has been resolved.

PCR: 03120 Module: ETH, IPG Level: 4

The SHOW IP INTERFACE command was showing ETH interfaces as up at startup, when SHOW INTERFACE and SHOW ETH STATE had them as down. This issue has been resolved.

PCR: 03124 Module: IPV6 Level: 4

The SHOW IPv6 COUNTER command now shows the *outAdvert* messages in the Total Out Messages counter field.

PCR: 03132 Module: SWITCH Level: 2

Classifiers that were added to hardware filters were not applied to the hardware. This issue has been resolved.

PCR: 03139 Module: IPV6 Level: 3

The SHOW IPV6 INTERFACE command was not displaying the link layer address and EUI when the interface was down. This issue has been resolved.

PCR: 03140 Module: IPG, SWI Level: 2

Static ARPs were deleted when a port went down. This issue has been resolved.

PCR: 03144 Module: CURE Level: 4

Users with either USER or MANAGER level privilege can now execute the STOP PING and STOP TRACE commands. Previously, MANAGER privilege was needed to execute these commands.

PCR: 03145 Module: IPG Level: 4

The SET IP ROUTE FILTER command was not processing some parameters. This issue has been resolved.

PCR: 03146 Module: PORT Level: 4

The PAGE parameter in the SET ASYN command now only accepts numeric values between 0 and 99, ON or OFF, and TRUE or FALSE.

PCR: 03147 Module: BGP Level: 4

When the DISABLE BGP DEBUG command was used, debugging messages were still being displayed by the BGP module. This issue has been resolved.

PCR: 03149 Module: SWITCH Level: 3

When the Layer 3 Filter Match entry IMPORT was created, EPORT could be set on the filter entry. If the Layer 3 Filter Match entry EMPORT was created, then IPORT could be set on the filter entry. Setting parameters that did not match could cause undesirable results. This issue has been resolved.

PCR: 03150 Module: FIREWALL Level: 3

The CREATE FIREWALL POLICY command was not checking for valid name entries, so invalid printing characters could be used for policy names. This issue has been resolved.

PCR: 03152 Module: IPG Level: 3

An additional check has been added to validate the MASK specified in an ADD IP ROUTE command. The check tests that the mask is contiguous.

PCR: 03153 Module: ACC Level: 4

The SHOW CONFIG=ACC command was not showing the *rscript* file. This issue has been resolved.

PCR: 03154 Module: PCI Level:

The SHOW IP MVR command output was showing dynamic members in the incorrect column. This issue has been resolved.

PCR: 03155 Module: FFS Level: 4

The SHOW FFILE command output has changed. The first column that listed where the file was stored has been removed. The title of the original second column (now the first column) has been changed from “creator” to “module”. The file format specifier has been altered from:

DDDD:MMMM\NNNNNNNN.TTT

to:

MMMM\NNNNNNNN.TTT

PCR: 03157 Module: IPV6 Level: 3

When changing the ACTION parameter between INCLUDE and EXCLUDE on IPV6 filters the interface information was not preserved between changes. The interface information is now preserved.

PCR: 03159 Module: SWI Level: 2

Switch trunk speed checks only checked for gigabit settings, not speed capabilities. It is now possible for uplink modules which support 10, 000 and gigabit speed to attach to trunks where speeds are 10Mb/s or 100Mb/s.

PCR: 03162 Module: IPV6 Level: 3

The performance of IPv6 has been improved by introducing IPv6 flows.

PCR: 03163 Module: IPG Level: 3

IGMP Snooping did not use DVMRP messages to identify a port. This issue has been resolved.

PCR: 03166 Module: IPG Level: 4

The output of the SHOW IP IGMP COUNTER and SHOW IGMPSNOOPING COUNTER commands was incorrect. This issue has been resolved.

PCR: 03167 Module: DVMRP Level: 2

When multicasting to a VLAN interface, if more than 2 DVMRP neighbours existed on a single port, and any one of those neighbours was pruned, the multicast data would stop flowing to the port. This happened even though it was still required for the remaining DVMRP neighbours. This issue has been resolved.

PCR: 03169 Module: IPV6 Level: 2

Duplicate Address Detection (DAD) was not sent on VLAN interfaces. This issue has been resolved.

PCR: 03180 Module: IPG Level: 3

If all 32 VLAN interfaces had IP addresses attached, only 31 VLANs could be multihomed. Now all 32 VLAN interfaces with IP addresses can be multihomed.

PCR: 03186 Module: CORE, FFS, TTY Level: 3

When the QUIT option was chosen after the SHOW DEBUG command was executed, the output did not immediately stop. This issue has been resolved, but there may be a short delay before the command prompt reappears.

PCR: 03187 Module: IPG Level: 3

SNMP *linkup* traps were not all appearing due to too many outstanding ARP requests. This issue has been resolved. IP now does not limit the number of outstanding ARP requests.

PCR: 03189 Module: FIREWALL, LB Level: 3

A fatal error occurred for the load balancer when there were no UP resources in a resource pool. This issue has been resolved. Load balanced TCP connections will now only retry SYNs once after 5 seconds. The round robin selection algorithm will now select an UP resource in a resource pool with only one UP resource, even if it was used for the last successful connection.

PCR: 03194 Module: LB Level: 3

Sometimes healthcheck pings were not sent to the load balancer resources. This issue has been resolved.

PCR: 03195 Module: USER Level: 3

When a user was logged in as MANAGER, and Telnet was set to OFF, and the CREATE CONFIGURATION command was executed, Telnet would be reset to ON on startup. This issue has been resolved.

PCR: 03196 Module: IPV6 Level: 3

The system became unstable if the ADD IPV6 TUNNEL command failed. This instability was caused by the partially created tunnel entry not being properly removed from the tunnel database. The tunnel entry is now completely removed.

PCR: 03198 Module: PRI Level: 3

The PRI interface would occasionally take a long time for the ifOperStatus of the interface to become UP. This issue has been resolved.

PCR: 03203 Module: IPV6 Level: 3

RIPng was not sending a response back to a RIP request message. This issue has been resolved.

PCR: 03205 Module: DHCP Level: 2

The following issues with DHCP have been resolved:

- DHCP assigned an incorrect IP address to clients shifting from a relayed to a non-relayed range. Gateway checks have been added to resolve this issue.
- DHCP clients shifting between relayed ranges were not always recognised, and were occasionally allocated incorrect addresses.
- DHCP offered entries did not time out after a NAK on a bad lease time request.

PCR: 03206 Module: IPG Level: 3

IPv4 filters now behave like IPv6 filters.

PCR: 03208 Module: FIREWALL Level: 2

When the configuration script was created using the CREATE CONFIG command, the GBLIP parameter in the ADD FIREWALL POLICY command was listed twice. This caused the command to fail when the device was restarted. This issue has been resolved.

PCR: 03211 Module: SWI Level: 2

When the MARL table had been fully populated, the addition of another multicast group caused an entry to be deleted, and the new entry was not added. This issue has been resolved so that no more groups can be added when the table is full.

PCR: 03212 Module: IPV6 Level: 3

The TRACE command was not working when using an ipv6 link-local address. This issue has been resolved.

PCR: 03213 Module: IPSEC Level: 3

A memory leak occurred when some IPSEC processes failed. This issue has been resolved.

PCR: 03216 Module: PIM, PIM6 Level: 2

PIM4 and PIM6 were not sending Hello packets if the HELLOINTERVAL was not a multiple of 10. This is set with the ADD PIM INTERFACE, ADD PIM6 INTERFACE, SET PIM INTERFACE, and SET PIM6 INTERFACE commands. This issue has been resolved.

PCR: 03222 Module: PIM, PIM6 Level: 2

If the RP candidate advertising time was set to a non-default value with the ADVINTERVAL parameter in the SET PIM command, the hold time in the message was not being updated correctly. This issue has been resolved.

PCR: 03229 Module: LOAD Level: 3

Zmodem was not naming some loaded files. This issue has been resolved.

PCR: 03232 Module: BGP Level: 3

Values for the KEEPALIVE and HOLDTIME parameters in the ADD BGP PEER and SET BGP PEER commands were not interacting correctly. This issue has been resolved.

PCR: 03234 Module: IPG Level: 3

The PURGE IP command did not remove ENABLE IP IGMP from the configuration. This issue has been resolved.

PCR: 03236 Module: IPG Level: 3

IGMP queries were being sent after IGMP was disabled. This issue has been resolved.

PCR: 03237 Module: IPG Level: 2

RIP *Request* packets for IPv4 were not being transmitted when the link came up or when the switch restarted. This issue has been resolved.

PCR: 03238 Module: SWI Level: 2

When RIP interfaces were deleted, the IP routes learned through those interfaces were not timing out correctly. Now, all IP routes learned though a RIP interface are removed when the RIP interface is deleted, and no timeouts occur.

PCR: 03239 Module: QOS Level: 2

QoS Traffic Class maximum bandwidth limiting was being overwritten by the port or trunk maximum bandwidth value. This should only happen when the Traffic Class maximum bandwidth has *not* been set manually with the CREATE QOS TRAFFICCLASS MAXBANDWIDTH parameter. This issue has been resolved.

PCR: 03240 Module: OSPF Level: 2

A fatal error occurred when OSPF was under high load. This issue has been resolved.

PCR: 03245 Module: SWI, IPG, PIM Level: 2

Multicast streams would not commence forwarding immediately due to IGMP packets initiated but not sent while a VLAN was changing from the DOWN to UP state. Also, multicast streams could be received while the VLAN was changing from DOWN to UP, causing a PIM Reverse Path Forwarding unicast route lookup failure. This was due to the unicast route being unusable as the VLAN was still considered down. These issues have been resolved.

PCR: 03247 Module: MVR Level: 4

The *Joins* and *Leaves* counters in the SHOW IP MVR COUNTER command output did not count subsequent join or leave requests after the first join or leave. This issue has been resolved.

PCR: 03250 Module: SWI Level: 4

The DELETE SWITCH FILTER command did not work properly when the ENTRY parameter was assigned a range with hyphen ("-"). This issue has been resolved.

PCR: 03252 Module: PIM Level: 3

An assert storm sometimes occurred with PIM-DM. This issue has been resolved.

PCR: 03255 Module: FIREWALL Level: 3

The firewall doubled the IPSPOOF event timeout from 2 minutes to 4 minutes. This issue has been resolved.

PCR: 03256 Module: MLD Level: 3

MLD did not respond correctly when it was in *exclude* mode and it received a request block. This issue has been resolved.

PCR: 03259 Module: SWI Level: 4

On a Rapier 24*i*, when large ping packets were forwarded through a port with ingress limiting, the ping packets were dropped. This issue has been resolved.

PCR: 03261 Module: VLAN, IPG Level: 4

VLAN and IPG packet debugging has been restored.

PCR: 03262 Module: PPP Level: 3

The CREATE CONFIGUATION command adds the PPP TEMPLATE LQR parameter when LQR is enabled. But the configuration script always used "LQR=ON" even when the LQR value was not the default. This meant that if a user entered LQR=40, the configuration would represent LQR=ON. This issue has been resolved.

PCR: 03266 Module: PIM Level: 2

The handling of the upstream neighbour for a *GraftACK* message has been corrected.

PCR: 03269 Module: IPG Level: 4

IGMP reports sometimes contained errors because of MVR. This issue has been resolved.

PCR: 03276 Module: IPG Level: 3

ECMP routing was incorrectly selecting the first route of equal cost found when retrieving routes that were not cached. This issue has been resolved.

PCR: 03277 Module: IPG Level: 3

IGMP Proxy can now forward IGMP Reports.

PCR: 03285 Module: IPG Level: 4

RIP packets can now contain up to 25 routes per packet instead of 24.

PCR: 03288 Module: L2TP Level: 2

When a radius lookup performed by the L2TP Access Concentrator (LAC) failed, the LAC attempted to disconnect the call from its tunnel. If the tunnel had not been created, the device restarted. This issue has been resolved.

PCR: 03291 Module: PPP Level: 2

A PAP authentication failure with PPPoE could cause a fatal error. This issue has been resolved.

PCR: 03292 Module: IP Level: 3

When adding static routes with the ADD IP ROUTE command, the order of the route in the route table was the reverse of the order entered. This issue has been resolved.

PCR: 03293 Module: PPP Level: 3

The MAXSESSION parameter of the SET PPP ACSERVICE command could not be changed when the service was defined over a VLAN. This issue has been resolved.

PCR: 03296 Module: IPG Level: 2

Broadcast TCP packets were being processed by the device, causing fatal errors when firewall SMTP Proxy was configured. Non-unicast TCP packets are now dropped by IP.

PCR: 03298 Module: FIREWALL Level: 3

The SHOW FIREWALL POLICY was not showing the correct debugging items, as set with the ENABLE FIREWALL POLICY DEBUG command. This issue has been resolved.

PCR: 03300 Module: FIREWALL Level: 3

Firewall rules were not being applied to broadcast packets received on a public interface. This issue has been resolved.

PCR: 03302 Module: SWI Level: 3

Following a period of high traffic load, the CPU utilisation would occasionally fail to drop below 40%. This issue has been resolved.

PCR: 03306 Module: IPG Level: 3

IGMP Proxy was setting a delay timer of 1-100 seconds when replying to an IGMP query with a requested maximum delay of 10 seconds. This issue has been resolved.

PCR: 03307 Module: IPG Level: 3

IGMP Proxy did not disable the DR status of an existing IGMP interface when that interface became the IGMP Proxy Upstream. IGMP Proxy also did not enable the DR status of an interface when it became anything other than the IGMP Proxy Upstream. These issues have been resolved.

PCR: 03308 Module: IPG Level: 3

IGMP Proxy now sends an IGMP *Leave* message once all members have left an IGMP group.

PCR: 03317 Module: OSPF Level: 2

Enabling OSPF via the GUI sometimes caused a fatal error. This issue has been resolved.

PCR: 03321 Module: DHCP, Q931, TELNET Level: 4

Debugging for DHCP and Q931 was not being disabled when a Telnet session finished. This issue has been resolved.

PCR: 03332 Module: TTY Level: 2

A log message is now created when a user is forced to logout from an asynchronous port when another user (i.e. someone connected via Telnet) resets the asynchronous connection with the RESET ASYN command.

PCR: 03333 Module: IPG Level: 3

After VRRP was enabled, the link status of the switch ports was shown as UP, even if there was no connection to the ports. This issue has been resolved.

PCR: 03334 Module: MVR Level: 3

The SET IP MVR command now has extra error checking. This is to ensure that if the IMTLEAVE parameter is not specified, the original range of ports set by the CREATE IP MVR command are still contained within the newly specified port range.

PCR: 03336 Module: CORE Level: 4

"AT-A42" was being incorrectly displayed as "AT-A42X-00" in the output of the SHOW SYSTEM command. This issue has been resolved.

PCR: 03341 Module: STP Level: 3

STP ignored some BPDU packets coming in on tagged ports. This issue has been resolved. Now the VLAN tag is ignored on all devices except Rapier *i* Series Switches with multiple STPs on the receiving port.

PCR: 03345 Module: IPG Level: 4

The RESET IP COUNTER=ALL command was not working correctly when issued from the command line. This issue has been resolved.

PCR: 03346 Module: SNMP Level: 4

Sometimes the *Agent Address* field in SNMP traps was not the same as the IP source address. This meant that sometimes the NMS did not send an alarm to the network manager when traps were received from switches. This issue has been resolved.

PCR: 03348 Module: SWI Level: 3

The Uplink card sometimes unnecessarily changed its status from UP to DOWN. This issue has been resolved.

PCR: 03349 Module: BGP Level: 3

When there were a large number of BGP routes, the SHOW BGP ROUTE command sometimes caused an error. This issue has been resolved.

PCR: 03350 Module: IP, SWI Level: 3

A fatal error occurred if an IP ARP route entry was deleted after an IP route filter was added while the IP route was equal to zero. This issue has been resolved.

PCR: 03351 Module: DHCP Level:

Several issues with the DHCP Server have been resolved.

PCR: 03352 Module: PPP Level: 3

The MRU parameter in the SET PPP command was incorrectly handled as an interface parameter when the configuration script was generated. This meant that the OVER parameter was omitted. The MRU parameter is now correctly handled as a link parameter.

PCR: 03353 Module: PPP Level: 3

Dynamic interface details were added through the SET INTERFACE command when the CREATE CONFIGURATION command was executed. This caused errors on startup. This issue has been resolved.

PCR: 03358 Module: SWI Level: 2

Port numbers on a Rapier16f*i* were incorrect. This issue has been resolved. For details on checking the port numbers on a Rapier16 f*i*, see "Checking the Port Map on Rapier16fi Switches" on page 32.

PCR: 03364 Module: PIM Level: 4

PIM will no longer accept obsolete commands.

PCR: 03369 Module: FIREWALL Level: 2

TCP checksums in TCP packets passing through the firewall were being recalculated incorrectly when the TCP setup proxy was disabled, and enhanced NAT was in use. This issue has been resolved.

PCR: 03370 Module: MVR Level: 4

The output of the SHOW IP MVR COUNTER command has been corrected. Also, the output of the SHOW IP MVR command has been modified. The new output is shown in Figure 1:

Figure 1: Example output from the modified SHOW IP MVR command

```
Multicast VLAN
-------------------------------------------------------------------------------
VLAN   Mode         Imtleave   Source Ports   Receiver Ports
                                                 Current Members  Group Address
-------------------------------------------------------------------------------
22     compatible   3          9,10           1-3, 6-7
                                                 1,6              235.1.1.1
                                                 2,7              234.1.1.1
3      compatible   8          12,13          4,5,8,9
                                                 4,8              255.1.1.1
-------------------------------------------------------------------------------
```

PCR: 03372 Module: IPG Level: 3

When a Rapier*i* Series Switch was using layer 3 multicast protocols, IGMP group members on the upstream interface for the multicast stream would always be forwarded to, even if they left the group. This issue has been resolved.

PCR: 03373 Module: HTTP Level: 3

The HTTP proxy server terminated a session when uploading a large file. This issue has been resolved.

PCR: 03375 Module: IPG Level: 2

The following issues with IPv6 have been resolved:

- Incorrect default values were set for the PREFERRED and VALID parameters in the ADD IPV6 PPFEFIX command. The correct default for PREFERRED is 604800 seconds (7 days), and the correct default for VALID is 2592000 seconds (30 days).
- The PREFERRED and VALID parameters in the ADD IPV6 PPFEFIX and SET IPV6 PREFIX commands were accepting values that could make the preferred life time longer than the valid life time.
- The POISONREVERSE parameter in the ADD IPV6 RIP command was not added to the automatic configuration.

PCR: 03379 Module: IPSEC Level: 3

If IPsec was using PPPoE, the initiator continued to keep the IPsec SA even if the PPPoE session failed and the ISAKMP Heartbeat timer expired. This issue has been resolved.

PCR: 03387 Module: PIM, PIM6 Level: 2

A memory leak occurred in IP or IPV6 if PIM-SM received IGMP or MLD reports, and there was no Rendezvous Point for the reported group.

PCR: 03388 Module: DHCP Level: 3

The DHCP lease *Expiry* time showed incorrectly in the SHOW DHCP CLIENT command when the lease straddled across multiple months and years. This issue has been resolved.

PCR: 03393 Module: ISAKMP Level: 3

The allowable UDPPORT range has been changed from 1-5000 to 1-65535 in the ENABLE ISAKMP command.

PCR: 03397 Module: SWI Level: 3

The SHOW SWITCH FDB command output was incorrect when using the Protected VLAN feature. This issue has been resolved.

Features in 86251-03

Patch file details are listed in Table 3:

Table 3: Patch file details for Patch 86251-03.

Base Software Release File	86s-251.rez
Patch Release Date	18-Feb-2003
Compressed Patch File Name	86251-03.paz
Compressed Patch File Size	80884 bytes

Patch 86251-03 includes all issues resolved and enhancements released in previous patches for Software Release 2.5.1, and the following enhancements:

PCR: 02429 Module: IPG Level: 2

When more than two firewall policies were configured, an unexpected switch restart sometimes occurred. This issue has been resolved.

PCR: 03041 Module: PPP Level: 1

PPPoE can now be configured on VLAN interfaces in both Client Mode and Access Concentrator (AC) mode. To configure PPPoE in Client Mode, the physical-interface parameter VLAN*n-servicename* has been added, where *servicename* is 1 to 18 characters in length, and for a PPPoE client is usually supplied by the ISP providing the service. To specify that any service name is acceptable, you can use the special service name ANY.

The modified commands using the *VLANn-servicename* parameter are:

- ADD PPP
- CREATE PPP
- DELETE PPP
- SET PPP
- SHOW PPP

The modified commands and parameters are described at the end of this patch release note in "*PPPoE Client on VLAN Interfaces*" on page 35 For all other unmodified parameters and commands refer to the PPP Chapter in your software reference manual.

PCR: 03050 Module: ETH Level: 3

When an Ethernet port received a MAC Control PAUSE frame it did not stop transmitting packets for a short period of time, as specified in the IEEE 802.3 Ethernet standard. This issue has been resolved.

PCR: 03058 Module: SWI Level: 4

The state of a port not participating in STP was displayed as *disabled*, instead of *broken*. This issue has been resolved.

PCR: 03063 Module: HTTP Level: 1

When HTTP proxy was configured and HTTP requests were sent in quick succession, a fatal error could occur. This issue has been resolved.

PCR: 03065 Module: SWI Level: 2

When the TX cable was unplugged from a fibre port the operating status was incorrectly reported as *UP*. This issue has been resolved.

PCR: 03067 Module: DHCP Level: 1

When replying to a DHCP REQUEST that had passed through a DHCP relay, the broadcast bit of DHCP NAK messages was not being set. This issue has been resolved in accordance with RFC2131.

PCR: 03068 Module: SWI, QOS Level: 2

The SET QOS HWPRIORITY and SET QOS HWQUEUE commands were not accepting all parameters correctly. This meant that the HWPRIORITY and HWQUEUE commands could not be modified with the associated SET command, but had to be made in the configuration script. This issue has been resolved.

PCR: 03069 Module: SWI Level: 1

An issue with Secure Shell clients not being able to connect to a Secure Shell server unless 3DES was installed on both the client and the server has been resolved.

PCR: 03077 Module: CORE Level: 4

The fault LED incorrectly reported a power supply fault (three flashes) on the 48V DC switch versions. This issue has been resolved.

Features in 86251-02

Patch file details are listed in Table 4.

Table 4: Patch file details for Patch 86251-02.

Base Software Release File	86s-251.rez
Patch Release Date	29-January-2003
Compressed Patch File Name	86251-02.paz
Compressed Patch File Size	28756 bytes

PCR: 02542 Module: IPV6 Network affecting: No

The SHOW IPV6 commands were incorrectly including RIPng down routes, and routes on the sending interface. The IPv6 routing table now recognises down routes.

PCR: 02574 Module: DVMRP Network affecting: No

Some change actions, and the resending of prune messages were not operating correctly. This issue has been resolved.

PCR: 02587 Module: OSPF Network affecting: No

When OSPF was enabled on startup, an OSPF interface would sometimes stay in the DOWN state. This issue has been resolved.

PCR: 03015 Module: SWI Network affecting: No

When ports were added to a trunk group on a Rapier 16, the ports operated in the wrong duplex mode. This issue has been resolved.

PCR: 03029 Module: SWI Network affecting: No

Layer 3 filtering was not correctly modifying a packet's IPDSCP field. This issue has been resolved.

PCR: 03031 Module: FIREWALL Network affecting: No

The ADD FIREWALL POLICY RULE command included an erroneous check on port ranges for non-NAT rules. This check is now restricted to NAT rules.

PCR: 03032 Module: SWI Network affecting: No

If the ENABLE IP IGMP command was executed before the ENABLE SWITCH L3FILTER command, Layer 3 filtering did not discard packets destined for the CPU. This issue has been resolved.

PCR: 03040 Module: IPG Network affecting: No

Sometimes IP flows were not deleted correctly when both directions of the flow were in use. This issue has been resolved.

PCR: 03051 Module: PCI Network affecting: No

The ECPAC card was not working correctly. This issue has been resolved.

Features in 86251-01

Patch file details are listed in Table 5:

Table 5: Patch file details for Patch 86251-01.

Base Software Release File	86s-251.rez
Patch Release Date	23-December-2002
Compressed Patch File Name	86251-01.paz
Compressed Patch File Size	11884 bytes

Patch 86251-01 includes the following enhancements:

PCR: 02331 Module: IPG, ETH Network affecting: No

IP is now informed when an Ethernet interface goes up or down, after a 2.5 second delay.

PCR: 02525 Module: TELNET, PING, IPV6, TCP Network affecting: No

The ADD IPV6 HOST command was not accepting the INTERFACE parameter when adding a host with a link-local address. This issue has been resolved.

PCR: 02527 Module: TCP Network affecting: No

TCP did not send a *TCP Reset* message under some circumstances, for example when the Telnet server was disabled. This issue has been resolved.

PCR: 02552 Module: SWI Network affecting: No

If ingress filtering was supported within trunk groups, ports with ingress filtering enabled were erroneously added to the trunk group. This issue has been resolved.

PCR: 02574 Module: DVMRP Network affecting: No

Some change actions, and the resending of prune messages were not operating correctly. This issue has been resolved.

PCR: 02581 Module: TM Network affecting: No

The test facility was not testing switch ports. This issue has been resolved.

Availability

Patches can be downloaded from the Software Updates area of the Allied Telesyn web site at *www.alliedtelesyn.co.nz/support/updates/patches.html*. A licence or password is not required to use a patch.

Static IGMP

This section describes an enhancement to the *Internet Group Management Protocol* (IGMP), which is supplied as a patch on Software Releases 2.5.1 for Rapier *i* Series switches.

It is possible to have a network segment that either has no multicast group members, or has a host that is unable to report its group membership with IGMP. In such cases, no multicast traffic is sent to the network segment. This enhancement provides a mechanism for the user to pull down multicast traffic to the segment.

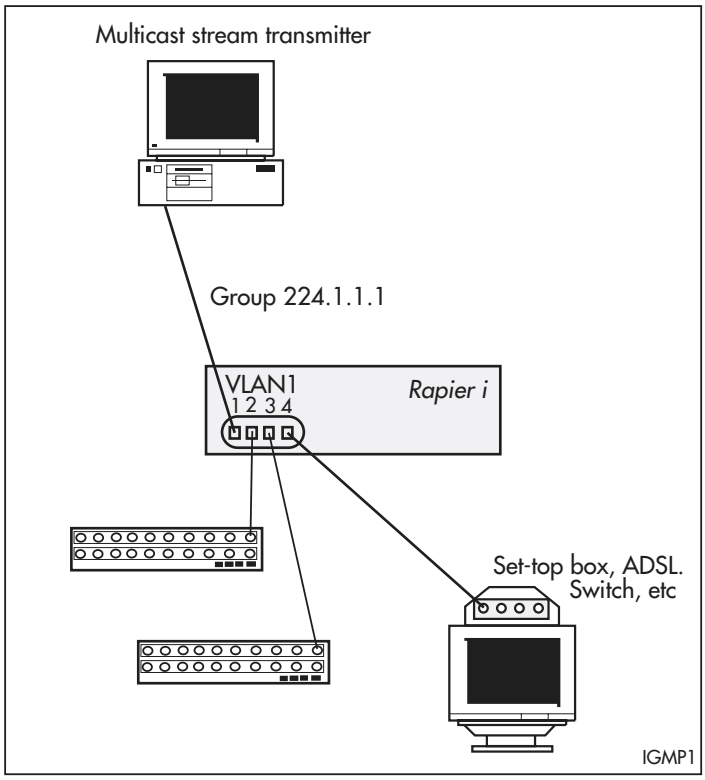
Currently the switch forwards multicast data on a dynamic basis to hosts who have joined the multicast group. This enhancement allows the user to instruct the switch to forward multicast data over a specified interface and port, as shown in Figure 2 on page 25. This capability is essential for sending multicast traffic to hosts that cannot report their group membership with IGMP. It plays an important role in video over ADSL applications.

Figure 2 on page 25 illustrates a switch forwarding the multicast stream to a set-top box after a user specifies that group 224.1.1.1 multicast data should be forwarded out of port 4 of VLAN1.

Unlike conventional IGMP membership, this user-specified static membership never times out.

The user will also be able to filter some IGMP debug messages by source IP address and group destination address.

Figure 2: Forwarding multicast data over a specified interface and port.



Configuration Example

The following configuration example illustrates the steps required to create a static IGMP association. It assumes that *vlan1* has already been configured as an IP interface on the switch.

1. **Enable IGMP on the switch.**

   ```
   ENABLE IP IGMP
   ```

2. **Enable IGMP on vlan1.**

   This must be done before the static IGMP association is created.

   ```
   ENABLE IP IGMP INTERFACE=VLAN1
   ```

3. **Create the static IGMP association.**

   The multicast data for the group specified by the DESTINATION parameter will be forwarded over the ports specified by the PORT parameter. If the PORT parameter is not entered, the association will default to all ports belonging to the interface.

   ```
   CREATE IP IGMP DESTINATION=224.1.2.3 INTERFACE=VLAN1
      PORT=1-4
   ```

4. **Check the configuration.**

   Check that the static IGMP association has been created and IGMP is enabled.

   ```
   SHOW IP IGMP DESTINATION=224.1.2.3 INTERFACE=VLAN1
   ```

Commands

This enhancement modifies one command:

- SHOW IP IGMP
  This command now includes a DESTINATION parameter. Only the modified parts of the command text are shown below.

and has seven new commands:

- ADD IP IGMP DESTINATION
- CREATE IP IGMP DESTINATION
- DELETE IP IGMP DESTINATION
- DESTROY IP IGMP DESTINATION
- DISABLE IP IGMP DEBUG
- ENABLE IP IGMP DEBUG
- SHOW IP IGMP DEBUG

Modified Command

SHOW IP IGMP

Syntax

```
SHOW IP IGMP [COUNTER] [INTERFACE=interface]
    [DESTINATION=ipaddress]
```

where:

- *ipaddress* is an existing IGMP group destination address, or a pattern matching one or more IGMP group destination addresses.

Description

The enhancement to this command is the addition of a new parameter, DESTINATION.

The DESTINATION parameter allows the user to screen out all IGMP information not related to the specified group destination address, i.e. only information relating to the multicast group destination address is displayed. Any of the four octets of the IP address may be replaced by '*' to enable wildcard matches, e.g. 224.*.*.*.

If both the COUNTER and DESTINATION parameters are specified, counters will only be displayed for the interfaces that have a group destination address matching that of the DESTINATION parameter.

Static groups will have their refresh time displayed as "Infinity".

All other parameters for this command remain the same. See the IP chapter in your switch's software reference for more information.

Examples

To display information about all group destination addresses starting with "224" on *vlan1*, use the command:

```
SHOW IP IGMP INTERFACE=VLAN1 DESTINATION=224.*.*.*
```

Figure 3: Example output from the SHOW IP IGMP DESTINATION command showing Static Groups.

```
IGMP Protocol
-------------------------------------------------------------------------------
Status ........................... Enabled
Default Query Interval ........... 125 secs
Default Timeout Interval ......... 270 secs

Last Member Query Interval ....... 10 (1/10secs)
Last Member Query Count .......... 2
Robustness Variable .............. 2
Query Response Interval .......... 100 (1/10secs)

Interface Name .......... vlan1               (DR)
IGMP Proxy .............. Off
Group List ..............

  Group. 224.0.1.22         Static association          Refresh time Infinity
  Ports  1,3
  Static Ports 3
```

Table 6: Parameters in the output of the SHOW IP IGMP DESTINATION command.

Parameter	Meaning
Static Ports	A list of the static ports; a subset of the ports listed in the Ports field. The Static Ports field is only displayed for static groups on a VLAN.

See Also SHOW IP IGMP DEBUG

New Commands

ADD IP IGMP DESTINATION

Syntax

```
ADD IP IGMP DESTINATION=ipaddress INTERFACE=interface
   PORT={ALL|port-list}
```

where:

- *ipaddress* is an existing IGMP group destination address.
- *interface* is the name of the interface over which multicast data is forwarded. This must be a VLAN interface.
- *port-list* is a port number, a range of port numbers (specified as a-b), or a comma separated list of port numbers and/or ranges. Port numbers start at 1 and end at m, where m is the highest numbered Ethernet port, including uplink ports.

Description

This command adds additional ports, through which multicast data is forwarded.

The DESTINATION parameter specifies the IP address from where multicast data is forwarded.

The INTERFACE parameter specifies the interface over which multicast data is forwarded. This must be a VLAN interface, e.g. VLAN1.

The static IGMP association identified by the DESTINATION and INTERFACE parameters must already exist.

The PORT parameter specifies the ports through which multicast data is forwarded. If any of the ports specified in the port list are already part of the association, or are not valid ports for the specified interface, an error message is displayed.

A port may belong to several associations if it belongs to several interfaces (i.e. if there are overlapping VLANs). If one of the ports specified in the port list already has a dynamic IGMP host, it will be replaced by the new static entry. If ALL is specified, all ports belonging to that interface will forward multicast data.

Examples

To add port 5 to the list of ports through which multicast data for 224.1.2.3 will be forwarded over *vlan1*, use the command:

```
ADD IP IGMP DESTINATION=224.1.2.3 INTERFACE=VLAN1 PORT=5
```

See Also

DELETE IP IGMP DESTINATION
SHOW IP IGMP

CREATE IP IGMP DESTINATION

Syntax

```
CREATE IP IGMP DESTINATION=ipaddress INTERFACE=interface
   [PORT={ALL|port-list}]
```

where:

- *ipaddress* is an existing IGMP group destination address.
- *interface* is the name of the interface over which multicast data is forwarded.
- *port-list* is a port number, a range of port numbers (specified as a-b), or a comma separated list of port numbers and/or ranges. Port numbers start at 1 and end at m, where m is the highest numbered Ethernet port, including uplink ports.

Description

This command creates a static multicast association to forward multicast data from a multicast group to one or more ports.

The DESTINATION parameter specifies the IP address from where multicast data is forwarded.

The INTERFACE parameter specifies the interface over which multicast data is forwarded.

The static IGMP association identified by the DESTINATION and INTERFACE parameters must not already exist.

The PORT parameter specifies the ports through which multicast data is forwarded. If any of the ports specified in the port list are not valid ports for the specified interface, an error message is displayed. An empty port list can be specified by giving no value to the PORT parameter. Ports may be added later using the ADD IP IGMP DESTINATION command. If ALL is specified, or if the PORT parameter is not entered, all ports belonging to that interface will forward multicast data.

Since static IGMP associations are identified by the combination of destination and interface, one destination or interface may belong to several different associations. Also, ports may belong to several associations if there are overlapping VLANs. There is no conflict with existing standard (dynamic) IGMP hosts: if a new static association's port already has a dynamic IGMP host, the new static entry will replace it.

IGMP destinations added with this command will never time out. They are removed with the DESTROY IP IGMP DESTINATION command.

Examples

To forward multicast data to 224.1.2.3 out ports 1 to 4 using *vlan1*, use the command:

```
CREATE IP IGMP DESTINATION=224.1.2.3 INTERFACE=VLAN1 PORT=1-4
```

See Also

ADD IP IGMP DESTINATION
DESTROY IP IGMP DESTINATION

DELETE IP IGMP DESTINATION

Syntax `DELETE IP IGMP DESTINATION=`*`ipaddress`* `INTERFACE=`*`interface`*
`PORT={ALL|`*`port-list`*`}`

where:

- *ipaddress* is an existing IGMP group destination address.
- *interface* is the name of the interface over which multicast data is forwarded. This must be a VLAN interface.
- *port-list* is a port number, a range of port numbers (specified as a-b), or a comma separated list of port numbers and/or ranges. Port numbers start at 1 and end at m, where m is the highest numbered Ethernet port, including uplink ports.

Description This command deletes ports from a static multicast group. Multicast data from the multicast group will no longer be forwarded out the port(s). The static association identified by the DESTINATION and INTERFACE parameters must exist for this command to succeed.

If any of the ports specified in the port list are not assigned to this static association, an error message is displayed. When the last port is removed, the static association will still exist, although it will have no functionality until ports are added again. To destroy the entire static association, use the DESTROY IP IGMP DESTINATION command.

Examples To remove ports 1-4 from the list of ports through which multicast data for 224.1.2.3 will be forwarded over *vlan1*, use the command:

```
DELETE IP IGMP DESTINATION=224.1.2.3 INTERFACE=VLAN1 PORT=1-4
```

See Also CREATE IP IGMP DESTINATION
SHOW IP IGMP

DESTROY IP IGMP DESTINATION

Syntax `DESTROY IP IGMP DESTINATION=`*`ipaddress`* `INTERFACE=`*`interface`*

where:

- *ipaddress* is an existing IGMP group destination address.
- *interface* is the name of the interface over which multicast data is forwarded.

Description This command destroys a static IGMP association. It is not necessary to delete the ports first. The static IGMP association identified by the DESTINATION and INTERFACE parameters must already exist for this command to succeed.

Examples To stop the switch forwarding all multicast data for 224.1.2.3 over *vlan1*, use the command:

```
DESTROY IP IGMP DESTINATION=224.1.2.3 INTERFACE=VLAN1
```

See Also CREATE IP IGMP DESTINATION

DISABLE IP IGMP DEBUG

Syntax `DISABLE IP IGMP DEBUG`

Description This command disables all IGMP debugging messages and resets the DESTINATION and SOURCEIPADDRESS parameters set in the ENABLE IP IGMP DEBUG command to ALL. Debugging is disabled by default.

Examples To disable all IGMP debugging messages and reset the IGMP debug message filters to ALL, use the command:

```
DISABLE IP IGMP DEBUG
```

See Also SHOW IP IGMP DEBUG

ENABLE IP IGMP DEBUG

Syntax

```
ENABLE IP IGMP DEBUG [DESTINATION={ALL|ipaddress}]
   [SOURCEIPADDRESS={ALL|ipaddress2}]
```

where:

- *ipaddress* is an IGMP group destination address.
- *ipaddress2* is the IP address of a host that responds to IGMP queries.

Description This command enables IGMP debugging of destination and source IP addresses. Debugging is disabled by default.

The DESTINATION parameter specifies the destination multicast group address for debugging. The default is ALL.

The SOURCEIPADDRESS specifies the host IP address responding to IGMP queries. The default is ALL.

If DESTINATION and SOURCEIPADDRESS are both specified, only debug messages that match both parameters are displayed. Some debug messages are displayed before the packet is fully decoded, and are unable to be filtered.

Examples To enable debugging information relating to IGMP host 10.41.0.22, use the command:

```
ENABLE IP IGMP DEBUG SOURCEIPADDRESS=10.41.0.22
```

To show all IGMP debug messages, use the command:

```
ENABLE IP IGMP DEBUG
```

See Also SHOW IP IGMP DEBUG

SHOW IP IGMP DEBUG

Syntax `SHOW IP IGMP DEBUG`

Description This command shows the IGMP debugging options that have been set.

Figure 4: Example output from SHOW IP IGMP DEBUG.

```
IGMP Debugging Information
--------------------------------------------------------------------------------
IGMP Debugging                  Enabled
Filter by group destination     224.1.2.3
Filter by source IP             10.10.1.123
--------------------------------------------------------------------------------
```

Table 7: Parameters displayed in the output of the SHOW IP IGMP DEBUG command.

Parameter	Meaning
IGMP Debugging	Whether or not IGMP debugging is enabled; one of "Enabled" or "Disabled".
Filter by group destination	The Group Destination Address specified by the DESTINATION parameter in the ENABLE IP IGMP DEBUG command. If the parameter was not given, "No" is displayed instead of the IP address.
Filter by source IP	The source IP address specified by the SOURCEIPADDRESS parameter in the ENABLE IP IGMP DEBUG command. If the parameter was not given, "No" is displayed instead of the IP address.

Examples To display IGMP debugging information, use the command:

```
SHOW IP IGMP DEBUG
```

See Also DISABLE IP IGMP DEBUG
ENABLE IP IGMP DEBUG

Checking the Port Map on Rapier16f*i* Switches

This section explains how to check that the port map on your Rapier16f*i* is correct. If the port map on your Rapier16f*i* is incorrect, this Note explains how to restore the correct settings.

This information is for Rapier16fi switches only.

The port map on your Rapier16f*i* will be incorrect if:

- it has software release 86s-251, but the 86251-04 patch is *not* loaded, or

- software release 86s-251 and patch 86251-04 are loaded, but the patch was corrupted after a restart or reboot.

The Rapier16*fi* requires the 86251-04 patch to operate correctly. Without this patch the port map is incorrect. An incorrect port map will cause problems if the configuration file refers to a port number.

The 2.5.3 software release for Rapier16fi switches will resolve this port map issue.

This section should be read in conjunction with the following document:

- Rapier Switch Documentation Set for Software Release 2.5.1 available on the Documentation and Tools CD-ROM packaged with your switch, or from *www.alliedtelesyn.co.nz/documentation/documentation.html*.

How to check that the port map is correct

The *ifIndex* and *Interface* fields in the SHOW INTERFACE command show the port map settings. *ifIndex* shows the index of the interface in the interface table, and *Interface* shows the physical or logical interface that maps to the index entry.

A correct port map

If the 86251-04 patch is successfully installed, and the port map is correct, the output from the SHOW INTERFACE command will be similar to that in Figure 1 on page 33.

Figure 1: Example output from the SHOW INTERFACE command *with* 86251-04.paz installed

```
Interfaces                                  sysUpTime:          00:00:09

DynamicLinkTraps.....Disabled
TrapLimit............20

Number of unencrypted PPP/FR links.....0

ifIndex Interface     ifAdminStatus   ifOperStatus     ifLastChange
--------------------------------------------------------------------------
 1      port9         Up              Down                  00:00:00
 2      port10        Up              Down                  00:00:00
 3      port11        Up              Down                  00:00:00
 4      port12        Up              Down                  00:00:00
 5      port13        Up              Down                  00:00:00
 6      port14        Up              Down                  00:00:00
 7      port15        Up              Down                  00:00:00
 8      port16        Up              Down                  00:00:00
 9      port1         Up              Down                  00:00:00
 10     port2         Up              Down                  00:00:00
 11     port3         Up              Down                  00:00:00
 12     port4         Up              Down                  00:00:00
 13     port5         Up              Down                  00:00:00
 14     port6         Up              Down                  00:00:00
 15     port7         Up              Down                  00:00:00
 16     port8         Up              Down                  00:00:00
 17     vlan1         Up              Down                  00:00:00
--------------------------------------------------------------------------
```

Although the *ifIndex* and *Interface* numbers do not match, *this is the correct port map*.

You do not need to take any more action if you have the correct port map.

An incorrect port map

If the 86251-04 patch is not installed, or has become corrupt, the output from the SHOW INTERFACE command will be similar to that in Figure 2 on page 34.

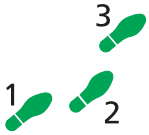
Figure 2: Example output from the SHOW INTERFACE command *without* 86251-04.paz installed

```
 Interfaces                                  sysUpTime:          00:01:22

DynamicLinkTraps.....Disabled
TrapLimit............20

Number of unencrypted PPP/FR links.....0

ifIndex Interface     ifAdminStatus   ifOperStatus     ifLastChange
--------------------------------------------------------------------------------
 1      port1         Up              Down                    00:00:00
 2      port2         Up              Down                    00:00:00
 3      port3         Up              Down                    00:00:00
 4      port4         Up              Down                    00:00:00
 5      port5         Up              Down                    00:00:00
 6      port6         Up              Down                    00:00:00
 7      port7         Up              Down                    00:00:00
 8      port8         Up              Down                    00:00:00
 9      port9         Up              Down                    00:00:00
 10     port10        Up              Down                    00:00:00
 11     port11        Up              Down                    00:00:00
 12     port12        Up              Down                    00:00:00
 13     port13        Up              Down                    00:00:00
 14     port14        Up              Down                    00:00:00
 15     port15        Up              Down                    00:00:00
 16     port16        Up              Down                    00:00:00
 17     vlan1         Up              Down                    00:00:00
--------------------------------------------------------------------------------
```

Although the *ifIndex* and *Interface* numbers match, *this port map is incorrect*.

You must restore the correct port map if your Rapier16f*i* shows this output.

How to restore the correct port map



The correct port map is restored with the following steps:

5. **Force an EPROM download to restore the bootrom.**

   To force an EPROM download, you have to restart the switch. To restart the switch, use the command:

   ```
   RESTART REBOOT
   ```

   When the switch starts up, you will see the messages in Figure 3 on page 35.

Figure 3: Router startup messages

```
INFO: Self tests beginning.
INFO: RAM test beginning.
PASS: RAM test, 4096k bytes found.
INFO: BBR tests beginning.
PASS: BBR test, 128k bytes found.
PASS: BBR test. Battery OK.
INFO: Self tests complete
INFO: Downloading router software.
Force EPROM download (Y) ?
INFO: Initial download succeeded
INFO: Executing configuration script <boot.cfg>
INFO: Router startup complete
```

Enter [Y] when the `Force EPROM download (Y)?` option appears.

6. Load the 86251-04.paz patch file, and set it as the preferred patch.

To load the 86251-04.paz file, use the command:

```
LOAD FILE=86251-04.paz
```

To make this the preferred patch, use the command:

```
SET INSTALL=PREFERRED PATCH=86251-04.paz
```

7. Reboot the switch using the RESTART REBOOT command.

Once the switch has restarted, check that the patch has restored the correct port map settings using the SHOW INTERFACE command.

PPPoE Client on VLAN Interfaces

PPP over Ethernet (PPPoE) has two modes of operation: Client Mode and Access Concentrator (AC) mode. PPPoE can now be configured on Ethernet and VLAN interfaces in both modes.

To configure PPPoE in Client Mode, the physical-interface parameter VLAN*n-servicename* has been added, where *servicename* is 1 to 18 characters in length, and for a PPPoE client is usually supplied by the ISP providing the service. To specify that any service name is acceptable, you can use the special service name ANY.

The modified commands using the *VLANn-servicename* parameter are:

- ADD PPP
- CREATE PPP
- DELETE PPP
- SET PPP
- SHOW PPP

The modified commands and parameters are described below. For all other unmodified parameters and commands refer to the PPP Chapter in your software reference manual.

ADD PPP

Syntax

```
ADD PPP=ppp-interface OVER=physical-interface
   [other parameters]
```

where:

- *ppp-interface* is the PPP interface number, from 0 to 511.
- *physical-interface* is:
  - SYN*n*
  - DS3*n*
  - ISDN-*callname*
  - ACC-*callname*
  - MIOX*n-circuitname*
  - TDM-*groupname*
  - TNL-*callname*
  - VLAN*n-servicename*

Description

This command adds a lower layer interface or link to an existing PPP interface. This configures PPP multilink, which groups links together for increased bandwidth. The following may be added:

- a synchronous port
- a DS3 port
- an ISDN call
- an ACC call
- a MIOX circuit
- TDM group
- an L2TP call
- a PPP over Ethernet service over a VLAN interface

The OVER parameter specifies the physical interface over which the PPP interface will run. For PPP over Ethernet and PPP over VLAN links, use the service name provided by your ISP, or the special service name ANY to specify that any service is acceptable.

Examples

To add a PPPoE interface on VLAN2, using the service name ANY, as an additional physical interface to PPP interface 1, and enable STAC LZS compression on the synchronous link with a check mode of LCB, use the command:

```
ADD PPP=1 OVER=vlan2-any COMP=LINK STACCHECK=LCB
```

CREATE PPP

Syntax `CREATE PPP=`*`ppp-interface`* `OVER=`*`physical-interface`*
`[other parameters]`

where:

- *ppp-interface* is the PPP interface number, from 0 to 511.
- *physical-interface* is:
  - SYN*n*
  - DS3*n*
  - ISDN-*callname*
  - ACC-*callname*
  - MIOX*n-circuitname*
  - TDM-*groupname*
  - TNL-*callname* (L2TP tunnel)
  - VLAN*n-servicename*

Description This command creates the specified PPP interface running over:

- a synchronous port
- a DS3 port
- an ISDN call
- an ACC call
- a MIOX circuit
- TDM group
- an L2TP call
- a PPP over Ethernet service
- a PPP over Ethernet service over a VLAN interface

For PPP over Ethernet and PPP over VLAN links, use the service name provided by your ISP, or the special service name ANY to specify that any service is acceptable.

The OVER parameter specifies the physical interface over which the PPP interface will run. Additional physical interfaces can be added to the PPP interface using the ADD PPP command.

Examples To create PPP interface 0 `CREATE PPP=0 OVER=vlan2-access`

DELETE PPP

Syntax

```
DELETE PPP=ppp-interface OVER=physical-interface
   [other parameters]
```

where:

- *ppp-interface* is the PPP interface number, from 0 to 511.
- *physical-interface* is:
  - SYN*n*
  - DS3*n*
  - ISDN-*callname*
  - ACC-*callname*
  - MIOX*n-circuitname*
  - TDM-*groupname*
  - TNL-*callname*
  - VLAN*n-servicename*

Description This command deletes the specified lower layer interface from an existing PPP multilink bundle. The interface may be left with no lower layer interfaces.

The OVER parameter specifies the interface to be deleted.

Examples To delete the PPoE service "*ANY*" on vlan2 as a physical interface from PPP interface 1, use the command:

```
DELETE PPP=1 OVER=vlan2-any
```

SET PPP

Syntax

```
SET PPP=ppp-interface [OVER=physical-interface]
   [other parameters]
```

where:

- *ppp-interface* is the PPP interface number, from 0 to 511.
- *physical-interface* is:
  - SYN*n*
  - DS3*n*
  - ISDN-*callname*
  - ACC-*callname*
  - MIOX*n-circuitname*
  - TDM-*groupname*
  - TNL-*callname*
  - VLAN*n-servicename*

Description This command is used to change the configuration parameters of a PPP interface running over:

- a synchronous port
- a DS3 port
- an ISDN call
- an ACC call
- a MIOX circuit
- TDM group
- an L2TP calla PPP over Ethernet service
- a PPP over Ethernet service over a VLAN interface

For PPP over Ethernet and PPP over VLAN links, use the service name provided by your ISP, or the special service name ANY to specify that any service is acceptable.

SHOW PPP

Syntax `SHOW PPP[=`*`ppp-interface`*`]`

where:

- *ppp-interface* is the PPP interface number, from 0 to 511.

Description This command displays a list of each PPP interface, users of the interface, physical interfaces that the interface is running over, and the current state of the interface.

There have not been any changes to the descriptive text or SHOW output in this command. The only change is in the Table. Table 1 shows the row which has changed, with the changed text in **bold**.

Table 8: Parameters displayed in the output of the SHOW PPP command (showing the changed row only).

Parameter	Meaning
Over	The lower layer(s) used by the PPP interface; SYN*n*, DS3*n*, ISDN-*callname*, ACC-*callname*, MIOX*n-circuitname*, TDM-*groupname,* **VLAN*n-servicename,*** TNL-*callname*.