Patch Release Note

Patch 86241-07
For Rapier Switches

Introduction

This patch release note lists the issues addressed and enhancements made in patch 86241-07 for Software Release 2.4.1 on existing models of Rapier L3 managed switches. Patch file details are listed in Table 1.

Table 1: Patch file details for Patch 86241-07.

Base Software Release File	86s-241.rez
Patch Release Date	23-Apr-2003
Compressed Patch File Name	86241-07.paz
Compressed Patch File Size	966631 bytes

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

- Release Note: Software Release 2.4.1 for Rapier Switches, (Document Number C613-10338-00 Rev A) available from www.alliedtelesyn.co.nz/documentation/documentation.html.
- Rapier Switch Documentation Set for Software Release 2.4.1 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 the issue that has been resolved. For details on level numbers, please contact your authorised distributor or reseller.

Features in 86241-07

Patch 86241-07 includes all issues resolved and enhancements released in previous patches for Software Release 2.4.1, and the following enhancements:

PCR: 02219 Module: SWI Level: 2

The layer 3 filter sometimes did not compare entries correctly. This may have meant that layer 3 filters did not work as expected all of the time. This issue has been resolved.

PCR: 02404 Module: IPG Network affecting: No

DVMRP multicast forwarding failed to send tagged packets to a tagged port. Packets were erroneously sent untagged to tagged ports. This issue has been resolved.

PCR: 02569 Module: IPV6 Level: 2

IPv6 was not sending some packets (such as Router Advertisements) at startup, which meant that IPv6 did not function correctly. This issue has been resolved.

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: 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: 03026 Module: IPG Network affecting: No

After setting the IGMP query timer with the SET IP IGMP command, and saving the configuration, the IGMP Other Querier timeout was not set to the correct value after a restart. 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: 03037 Module: QOS Network affecting: No

A new value is now shown in the output of the SHOW QOS POLICY command. This is the value of the port bandwidth used when the default traffic class percentage bandwidth is set on a QoS Policy.

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: 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: 03061 Module: LOAD Network affecting: No

When starting a load that failed, a flash compaction could not be started manually. 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: 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: 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: 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: 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: 03132 Module: SWITCH Level: 2

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

PCR: 03134 Module: TCP Level: 2

When using the SET TELNET LISTENPORT command, a fatal error sometimes occurred. 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: 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: 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: 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: 03154 Module: PCI Level:

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

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: 03169 Module: IPV6 Level: 2

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

PCR: 03171 Module: DVMRP, IPG Level: 3

DVMRP was erroneously forwarding packets to a VLAN with a downstream neighbour. 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: 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: 03184 Module: USER Level: 4

An extra chararcter was erroneously displayed in the output of the SHOW LOG command when Remote Security Officer was enabled from a configuration script. This issue has been resolved.

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: 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: 03202 Module: CORE Level: 3

There are two sources of time kept in the device. The real time clock, and the milliseconds since midnight (msSinceMidnight). The msSinceMidnight can reach midnight slightly before the real time clock which means that the value of the msSince Midnight is larger than the number of milliseconds in a day. This meant that at midnight, the elapsed time since the time-to-live value for the Firewall and IP-NAT TCP sessions appeared very large and Firewall and IP-NAT sessions were prematurely aged out. This issue has been resolved by pausing the msSince Midnight variable at midnight to wait for the real time clock to catch up.

PCR: 03203 Module: IPV6 Level: 3

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

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: 03217 Module: DVMRP Level: 2

If a DVMRP interface was deleted and then added again, DVMRP routes associated with this interface were not reactivated. This issue has been resolved.

PCR: 03219 Module: IPG Level: 2

The IGMP group entry timer was not decreasing when UDP data kept arriving for the group. 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: 03240 Module: OSPF Level: 2

A fatal error occurred when OSPF was under high load. This issue has 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: 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: 03268 Module: SWI Level:

When using MVR on a Rapier 48 or Rapier 48*i*, multicast packets were not forwarded correctly between ports 1-24 and 25-48. This issue has been resolved.

PCR: 03269 Module: IPG Level: 4

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

PCR: 03282 Module: FIREWALL Level: 3

The DISABLE FIREWALL POLICY PING command was stopping private ping flow through the device when ICMP Forwarding and NAT were enabled. This issue has been resolved.

PCR: 03283 Module: SWI Level: 3

The RESET SWITCH PORT COUNTER command was clearing all learned MAC addresses for the specified port. This command should only reset the switch port's counters. This issue has been resolved.

PCR: 03285 Module: IPG Level: 4

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

PCR: 03287 Module: Firewall Level: 2

When the firewall was set to ACTION=NAT, it was allowing inbound traffic, (for example FTP) even though a port was specified for a particular application, (for example Telnet). 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: 03297 Module: PIM Level: 2

The Designated Router (DR) of the PIM interface was not resetting when the RESET PIM INTERFACE command was executed. This issue has been resolved.

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: 03301 Module: IPG Level: 3

Packets processed by the firewall were not having their TTL decremented. 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: 03303 Module: PIM Level: 3

The PIM Designated Router (DR) is now elected over an entire VLAN interface, rather than on a per-port basis.

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: 03312 Module: IPG Level: 2

RIP packetw were discarded when MD5 authentication was used. 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: 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: 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: 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: 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: 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: 03360 Module: STP Level: 4

Typing "?" after SET STP=*stp-name* at the CLI to request context-sensitive Help only returned the PORT and DEFAULT options. This issue has been resolved so that all options are shown.

PCR: 03363 Module: SWI Level: 2

The MAC address table entry was not removed when a port shifted between VLANs. 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: 03385 Module: FILE, INSTALL, SCR Level:

Critical files (*prefer.ins*, *config.ins* and *enabled.sec*) are now copied from NVS to FLASH at boot time if they do not exist in FLASH, or if the NVS version of the file is different from the FLASH version.

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: 03402 Module: IPG Level:

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

PCR: 03404 Module: MLD Level: 2

When a MLD *Done* report was received, the entire MLD snooping entry was deleted, rather than just the port the MLD *Done* was received on. This issue has been resolved.

PCR: 03408 Module: PIM Level: 2

A *Prune* message was sent in reply to every multicast data packet when there was no output forwarding list for the data. This issue has been resolved.

Features in 86241-06

Patch file details are listed inTable 2:

Table 2: Patch file details for Patch 86241-06.

Base Software Release File	86s-241.rez
Patch Release Date	28-Feb-2003
Compressed Patch File Name	86241-06.paz
Compressed Patch File Size	369480 bytes

Patch 86241-06 includes all issues resolved and enhancements released in previous patches for Software Release 2.4.1, 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: 02562 Module: SWI

Dynamic Port Security allows for dynamic MAC address learning on a switch port. If a MAC address is unused for a period of time, it will be aged from the database of currently accepted MAC addresses. This allows the learning of new MAC addresses. Dynamic Port Security is useful because port security allows the number of devices that are connected to a particular switch port to be limited.

For more information on Dynamic Port Security, see “*Dynamic Port Security*” on page 38 of this patch release note.

PCR: 03042 Module: PIM Level: 3

PIM join messages were being sent by a switch connected to an upstream and a downstream switch or router in the same VLAN when a multicast group had no members. This issue has been resolved.

PCR: 03044 Module: BGP Level: 2

The switch did not always advertise its preferred routes to destinations that were affected by flapping routes. In these conditions, a BGP network does not run efficiently. This issue has been resolved.

PCR: 03048 Module: STP Level: 2

A switch port belonging to an enabled STP instance would not respond to ARP requests if the port had been disabled from STP operation. This prevented the flow of some types of traffic into affected switch ports. This issue has been resolved.

PCR: 03054 Module: TTY, TACPLUS

When a connection is made by Telnet, or directly through the ASYN port, a TTY session is created with:

- an *idle timeout* time. The default idle time is zero, which means the TTY session will not time out if there is a lack of activity. If a TACACS+ server is configured on the switch, and the idle time *attribute value pair* (AVP) is configured on the TACACS+ server and is received by the switch, the value of the idle time from the TACACS+ server is used to set the TTY session.

- a *timeout* of zero, which means that the TTY session will not time out. If a TACACS+ server is configured on the switch, and the timeout *attribute value pair* (AVP) is configured on the TACACS+ server and received by the switch, the value of the timeout from the TACACS+ server is used to set the TTY session timeout. After the timeout period has elapsed, the user will either be disconnected by termination of their TTY connection (the default setting), or have their privilege level reduced to USER (the lowest privilege level). If the user's privilege level is already at the lowest level, then the user will be disconnected by termination of their TTY connection. If the user's privilege level is reduced, the TTY session timeout count is reset to its initial value.

PCR: 03056 Module: SSH Level: 3

During an SSH session between the switch and the Secure CRT client, the client did not receive a reply to its MAX-packet-size CMSG. The switch does not support this message, but will now send a negative response to satisfy the secure CRT client's requirements.

PCR: 03064 Module: SNMP Level: 4

The MIB objects *ifTestTable* and *ifRcvAddressTable* were incorrectly included in the switch's SNMP implementation. These have been removed.

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: 03070 Module: BGP Level: 2

When BGP imported other route types, it would advertise routes that had nexthops of the BGP peers themselves. The BGP peers would reject these routes and close the peering session, thus preventing the exchange of routing information between BGP peers. This issue has been resolved.

PCR: 03072 Module: BGP Level: 4

The Import parameter of the ADD, SET, DELETE and SHOW BGP commands now has an INTERFACE type. INTERFACE routes were previously grouped with STATIC routes.

PCR: 03073 Module: UTILITY Level: 2

If the CREATE QOS POLICY command was executed with a range that had a number more than four characters long, for example, CREATE QOS POLICY=123-12345, then a switch restart occured. An error message is now displayed if more than four numbers are entered for a range.

PCR: 03074 Module: USER Level:

The SET USER command now requires the PASSWORD option if a PRIVILEGE is specified. This enables privilege levels to be lowered from a higher level (MANAGER, or SECURITY OFFICER), to USER.

PCR: 03081 Module: SWI Level:

An untagged packet would occasionally be sent on a tagged port. This issue has been resolved.

PCR: 03082 Module: SWI Level:

When PIM was enabled, IGMP snooping would occasionally work incorrectly. This issue has been resolved.

PCR: 03087 Module: IPG Level:

When interfaces with IGMP proxies were deleted, a software restart could sometimes occur. This issue has been resolved.

PCR: 03100 Module: DHCP Level:

DHCP was assigning incorrect IP addresses to clients when they moved from a relayed to a non-relayed range. Gateway checks have been added to remove this issue.

PCR: 03101 Module: IPG Level: 2

Deriving the originating VLAN from incoming packets could, in some circumstances, cause a software restart. This issue has been resolved.

PCR: 03102 Module: IPG Level: 3

The PING command when executed with the LENGTH and PATTERN parameters could produce an ICMP echo packet with an incorrect ICMP checksum. This issue has been resolved.

PCR: 03104 Module: IPG Level: 3

When an IP packet with an invalid TOTAL LENGTH field was received by the CPU routing process, subsequent valid packets were dropped. This issue has been resolved.

PCR: 03107 Module: FR, PPP Level: 2

The mechanism for freeing discarded packets in Frame Relay and PPP could, in some circumstances, cause a software restart. This issue has been resolved.

PCR: 03108 Module: MLDS Level: 4

The DISABLE MLDS command appeared twice in configuration files. This issue has been resolved.

PCR: 03110 Module: IPG Level: 2

The ADD IP MVR command could cause a software restart. This issue has been resolved.

The ADD IP MVR command parameter GROUP now only accepts multicast addresses.

PCR: 03113 Module: DVMRP Level: 2

With DVMRP configured, the switch did not forward multicast data to downstream interfaces on the same VLAN. This issue has been resolved.

PCR: 03114 Module: DHCP Level: 3

DHCP clients that shifted between relayed ranges were not always recognised, and were occasionally allocated incorrect addresses. This issue has been resolved.

PCR: 03121 Module: DVMRP Level: 2

Invalid DVMRP prune messages could cause a software restart. This issue has been resolved.

PCR: 03122 Module: SWI Level: 2

Adding a static ARP entry to a trunk group could cause a software restart. This issue has been resolved.

PCR: 03123 Module: DHCP Level: 3

After sending a DHCP NAK in response to a client's DHCP REQUEST with a bad lease time, the switch would fail to age out its corresponding DHCP OFFER entry. This issue has been resolved.

PCR: 03125 Module: DS3 Level: 3

The switch would disassert the AIS, IDLE, LOF and LOS alarms if the defect conditions that had caused the alarm were disasserted, then reasserted before the alarms had been disasserted. This issue has been resolved.

PCR: 03127 Module: IPV6 Level: 2

When a static link local address was configured using the ADD IPV6 INT=xxx IP=yyy command, it was not reflected in the switch's dynamic configuration. Consequently, the command would be absent from the switch's configuration after CREATE CONFIG and switch RESTART commands were executed. This issue has been resolved.

PCR: 03136 Module: BGP Level: 2

The ADD BGP PEER command MAXPREFIX parameter now has a default of 24000, instead of OFF. Previously, with no maximum prefix checking by default, if the switch received a very large number of prefixes from a BGP peer, buffer exhaustion could result in a software restart.

PCR: 03011 Module: OSPF Level: 3

The SHOW OSPF NEIGHBOUR command did not reflect a change made to the router priority on a dynamic OSPF interface of a neighbouring router. This issue has been resolved.

PCR: 03035 Module: OSPF

Link state advertisements could incorrectly show an area as a stub area. This happened during the time when a Direct Route (DR) was removed from a configuration and before a Direct Backup Route (BDR), or an Other Direct Route (Other DR) was elected. This issue has been resolved.

PCR: 03045 Module: IPG, SWI Level: 3

The switch would flood DVMRP unicast messages to all ports in the VLAN. This issue has been resolved.

PCR: 03046 Module: IPG Level: 3

ICMP packets originating from the switch used the wrong Equal Cost Multiple Path route. This issue has been resolved. Also, improvements have been made to ensure that the ICMP packet will be transmitted over the best available route. If the best route becomes unavailable, a new route will be found, if available, so that the ICMP packet continues to reach the destination address.

PCR: 03051 Module: PCI Level: 2

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

Features in 86241-05

Patch file details are listed in Table 3:

Table 3: Patch file details for Patch 86241-05.

Base Software Release File	86s-241.rez
Patch Release Date	17-Jan-2003
Compressed Patch File Name	86241-05.paz
Compressed Patch File Size	332388 bytes

Patch 86241-05 includes all issues resolved and enhancements released in previous patches for Software Release 2.4.1, and the following enhancements:

PCR: 02315 Module: SNMP Network affecting: No

Support has been added for SNMPv2c.

SNMP responses will be sent in the same version format as the request message. Minimal configuration is required to specify a SNMP format, because this is decided on a message by message basis. The only thing you need to specify is the version of SNMP received by trap hosts.

To create an SNMP community, use the command:

```
CREATE SNMP COMMUNITY=name [ACCESS={READ|WRITE}]
    [TRAPHOST=ipadd] [MANAGER=ipadd]
    [OPEN={ON|OFF|YES|NO|TRUE|FALSE}] [V1TRAPHOST=ipadd]
    [V2CTRAPHOST=ipadd]
```

To add a trap host or management station to the previously created SNMP community, use the command:

```
ADD SNMP COMMUNITY=name [TRAPHOST=ipadd] [MANAGER=ipadd]
    [V1TRAPHOST=ipadd] [V2CTRAPHOST=ipadd]
```

PCR: 02389 Module: DS3 Network affecting: No

DS3 interface and board type support has been added. DS3 is now supported over PPP and Frame Relay. DS3 MIB support has been added.

For more information on DS3, see "*DS3 Interfaces*" on page 31 of this release note.

PCR: 02414 Module: IPv6, SWI, IPG, VLAN Network affecting: No

This patch resolves issues that arose after previous modifications made under this PCR number.

Sometimes IPv6 features did not enable correctly. Also, there were some errors in the output from configuration commands. These issues have been resolved.

PCR: 02560 Module: IPG, SWI, VLAN Network affecting: No

IP packet throughput has been improved.

PCR: 03002 Module: USER Network affecting: No

Debugging commands are now available for the RADIUS and TACACS control protocols. Raw packets, decoded packets, and errors can now be displayed.

Access control packet debugging allows the contents of the packets to be viewed. The debugging commands allow both raw (hexadecimal dumps) and/or decoded (human-readable) packet displays. Information on any errors occurring in the transactions can be displayed once the appropriate debugging command is issued.

Only users with SECURITY OFFICER privileges in system secure mode are able to enable RADIUS and TACACS debugging.

The debugging commands are:

```
ENABLE RADIUS DEBUG={ALL|PKT|DECODE|ERROR} [,...]
ENABLE TACACS DEBUG={ALL|PKT|DECODE|ERROR} [,...]
DISABLE RADIUS DEBUG={ALL|PKT|DECODE|ERROR} [,...]
DISABLE TACACS DEBUG={ALL|PKT|DECODE|ERROR} [,...]
SHOW RADIUS DEBUG
SHOW TACACS DEBUG
```

PCR: 03013 Module: INSTALL Network affecting: No

The SET INSTALL command was generating an unwanted warning message on Rapier *i* series switches. This issue has been resolved.

Features in 86241-04

Patch file details are listed in Table 4:

Table 4: Patch file details for Patch 86241-04.

Base Software Release File	86s-241.rez
Patch Release Date	15-Jan-2003
Compressed Patch File Name	86241-04.paz
Compressed Patch File Size	208232 bytes

Patch 86241-04 includes all issues resolved and enhancements released in previous patches for Software Release 2.4.1, and the following enhancements:

PCR 02244 Module: UTILITY Network affecting: No

Virtual interfaces were displayed incorrectly when VLANs were multihomed. This issue has been resolved.

PCR: 02300 Module: Firewall Network affecting: No

If the command ADD FIREWALL POLICY RULE SOURCEPORT=ALL was executed, a value of “65535” was incorrectly displayed for the SOURCEPORT parameter for that rule in the SHOW FIREWALL POLICY command. This issue has been resolved.

PCR: 02340 Module: IPG Network affecting: No

PIM was disabled permanently if the RESET IP command, or the DISABLE IP command followed by the ENABLE IP commands were executed. PIM is now automatically restarted if these commands are used.

PCR: 02356 Module: FIREWALL Network affecting: No

Previously the SET FIREWALL POLICY RULE command permitted the use of the GBLIP and GBLPORT parameters in ways that were not permitted by the ADD FIREWALL POLICY RULE command. This caused problems when a configuration file was generated because some of the illegal parameters from the SET command were put into the ADD command. This resulted in a configuration that contained illegal parameter combinations. The restrictions placed on the GBLIP and GBLPORT parameters in the ADD command have now been implemented in the SET command so that these problems do not occur.

PCR: 02358 Module: IPG Network affecting: No

IP ARP packets that had invalid header values were erroneously accepted by the router. Also, IP packets with a Class E source IP address were erroneously fowarded. These issues have been resolved.

PCR: 02371 Module: FIREWALL Network affecting: No

When the system time was set to a time that was before or significantly after the current time, Firewall sessions were prematurely deleted. This issue has been resolved.

PCR: 02400 Module: CORE,FFS,FILE,INSTALL,SCR Network affecting: No

If a problem occurred with NVS, some critical files were lost. As a result, the equipment was forced to load only boot ROM software at boot time. This patch combined with the new version of the boot ROM software (pr1-1.2.0 for the AR700 series) resolves this issue.

PCR: 02491 Module: IPG Network affecting: No

The ARP cache is now updated when a gratuitous ARP request or reply packet is received.

PCR: 02506 Module: OSPF IPG Network affecting: No

The ADD IP ROUTE FILTER optional parameter INTERFACE caused the filter to not work on the OSPF external LSA’s flooding.

The SHOW IP ROUTE FILTER interface name output was truncated to 6 characters. These issues have been resolved.

PCR: 02511 Module: Ping Network affecting: No

Executing the PING command sometimes caused a memory leak. This issue has been resolved.

PCR: 02514 Module: IPG Network affecting: No

The CREATE CONFIGURATION command inserted the IMTLEAVE parameter into the configuration script when the IMTLEAVE parameter was undefined. This caused an error in the configuration script. This issue has been resolved.

PCR: 02519 **Module: IPv6** **Network affecting: No**

The DELETE IPV6 6T04 command sometimes caused an error. This issue has been resolved.

PCR: 02521 **Module: IPv6** **Network affecting: No**

The DECREMENT parameter of the ADD IPV6 INTERFACE command was not recognised in the command line. This issue has been resolved.

PCR: 02523 **Module: QOS, UTILITY** **Network affecting: No**

The SET QOS TRAFFICCLASS command now requires 7 characters to be entered for the optional EXCEEDACTION and EXCEEDREMARKVALUE parameters.

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: 02526 **Module: DVMRP** **Network affecting: No**

Under some circumstances, multiple default routes were created for DVMRP. 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: 02529 **Module: FIREWALL** **Network affecting: No**

The source IP address is now checked correctly when subnet NAT is used with standard, double, or reverse NAT. Previously, it was sometimes possible to specify an IP address outside the allowable range.

PCR: 02532 **Module: FIREWALL** **Network affecting: No**

The Firewall showed the wrong counters on Total Received Packets and Dropped Packets and displayed twice the number of received packets when discarding packets from the public side. Also, when a Deny rule was applied to the private side, the Number of Dropped Packets was always zero. These issues have been resolved.

PCR: 02534 **Module: TEST** **Network affecting: No**

The SYN test did not operate successfully when patch 52241-03 was installed. This issue has been resolved.

PCR: 02535 **Module: IPV6** **Network affecting: No**

A fatal error occurred when an IPv6 packet with an invalid payload length was received. This issue has been resolved.

PCR: 02537 **Module: L2TP** **Network affecting: No**

When PPP was used over an L2TP tunnel, a speed of zero was shown for the PPP interface on the LNS side, while the LAC side showed a non-zero PPP interface speed. This issue has been resolved so that the LNS side of the PPP interface shows the correct speed.

PCR: 02538 Module: DVMRP Network affecting: No

The source mask is now always 0xffffffff in the DVMRP forwarding table.

The temporary route in the DVMRP route table was not displaying correctly. This issue has been resolved.

An IGMP entry was erroneously added for the reserved IP address. This issue has been resolved.

PCR: 02539 Module: CLASSIFIER Network affecting: No

The TCP and UDP source and destination port parameters would accept values of more than 65535. 65535 is now the maximum value for source and destination ports. This complies with RFC768 for UDP and RFC793 for TCP.

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: 02543 Module: SWI Network affecting: No

BPDU messages are now sent to all active ports as soon as STP is enabled.

PCR: 02547 Module: IPG Network affecting: No

The ARP transmit counter total was not being incremented. This issue has been resolved.

PCR: 02550 Module: FIREWALL Network affecting: No

The standard subnet NAT rules on a private interface were not matching a packet unless its source IP address was exactly the same as the IPADDRESS value set for the rule, that is the NAT mask value was not being used. This issue has been resolved.

PCR: 02551 Module: IPG Network affecting: No

Reserved multicast data was being duplicated. 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: 02564 Module: FIREWALL Network affecting: No

Large RTSP continuation packets could cause a fatal error. This issue has been resolved.

PCR: 02565 Module: CLASSIFIER Network affecting: No

The SET CLASSIFIER and CREATE CLASSIFIER commands now display the tagged and untagged parameters correctly when the PROTOCOL parameter is set to IPX or 802.2.

PCR: 02572 Module: IPG Network affecting: No

An issue introduced in a previous patch with the SET IP ROUTE command failing 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: 02579 Module: FIREWALL Network affecting: No

The ADD FIREWALL POLICY and SET FIREWALL POLICY commands did not generate a valid port list when the optional PORT parameter was set to ALL. 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.

Features in 86241-03

Patch file details are listed in Table 5.

Table 5: Patch file details for Patch 86241-03.

Base Software Release File	86s-241.rez
Patch Release Date	26-Nov-2002
Compressed Patch File Name	86241-03.paz
Compressed Patch File Size	379165 bytes

Patch 86241-03 includes all issues resolved and enhancements released in previous patches for Software Release 2.4.1, and the following enhancements:

PCR: 02314 Module: IPG Network affecting: No

Incorrect ICMP checksums on incoming packets were not being recognised, and packets with an odd byte size were erroneously being processed. These issues have been resolved.

PCR: 02414 Module: IPv6, SWI, IPG, VLAN Network affecting: No

MLD snooping is now supported on AT-9800 Series Switches and Rapier *i* Series Switches.

PCR: 02426 Module: IPv6 Network affecting: No

The ENABLE IPV6 MTUDISCOVERY and SET IPV6 MTU INTERFACE commands were not displayed in the SHOW CONFIGURATION DYNAMIC command. This issue has been resolved.

PCR: 02428 Module: IPv6 Network affecting: No

Link-local address behaviour was incorrect. Also, the PUBLISH parameter was not updated by the SET IPV6 INTERFACE command, or displayed in the SHOW IPV6 INTERFACE command. These issues have been resolved.

PCR: 02467 Module: CORE Network affecting: No

The board descriptions have changed for some instances of AT-9800 Series Switches.

PCR: 02469 Module: TM Network affecting: No

After an ASYN port test, the port is now reset to its pre-test state if the test was started by a user connected to the same ASYN port.

PCR: 02477 Module: IPG, PIM, SWI Network affecting: No

The following issues have been resolved:

- When equal paths exist to a source, a PIM DM downstream switch/ router could not correctly collect information from AssertSelection between the upstream devices.
- If the Assert winner was another vendor's device, The Allied Telesyn device did not respond to the *Prune* message.
- Sometimes a receiver could not get a multicast data stream.
- If unicast routes were changed, multicast data streams sometimes failed to reach receivers or flowed incorrectly.

PCR: 02481 Module: IPv6 Network affecting: No

A fatal error occurred with IPv6 ping when an interface was plugged in and unplugged repeatedly. This issue has been resolved. Also, the *TrueMTU* value on a VLAN interface was incorrect. This value has been corrected to 1500.

PCR: 02482 Module: IPG Network affecting: No

When pinging an unreachable host via a switch, there was a delay before the switch sent a *DestinationUnreachable* message. This issue has been resolved.

PCR: 02489 Module: SWI Network affecting: No

When the switch was under heavy learning load, some MAC address were lost. This issue has been resolved.

PCR: 02494 Module: IPv6 Network affecting: No

It was possible to add the same IPv6 prefix to different IPv6 interfaces. This issue has been resolved.

PCR: 02495 Module: VLAN Network affecting: No

The ADD VLANRELAY and DELETE VLANRELAY commands returned the wrong message if the command could not be processed. This issue has been resolved.

PCR: 02498 Module: VLAN Network affecting: No

The correct protocol number is now returned by VLAN Relay.

PCR: 02499 Module: IPG Network affecting: No

Some parameters in the SET IP IGMP command had incorrect ranges. This issue has been resolved. The correct ranges are:

```
SET IP IGMP [LMQI=1..255] [LMQC=1..5] [QUERYINTERVAL=1..65535]
[QUERYRESPONSEINTERVAL=1..255] [ROBUSTNESS=1..5]
[TIMEOUT=1..65535]
```

PCR: 02502 **Module: Ping, IPv6** **Network affecting: No**

If multiple IPv6 interfaces shared the same link-local address, pings to the link-local address sometimes failed. This issue has been resolved.

PCR: 02509 **Module: DVMRP** **Network affecting: No**

The source net mask has been removed from DVMRP *prune*, *graft* and *graft-ack* messages.

Features in 86241-02

Patch file details are listed in Table 6:

Table 6: Patch file details for Patch 86241-02.

Base Software Release File	86s-241.rez
Patch Release Date	25-Oct-2002
Compressed Patch File Name	86241-02.paz
Compressed Patch File Size	132368 bytes

Patch 86241-02 includes all issues resolved and enhancements released in previous patches for Software Release 2.4.1, and the following enhancements:

PCR: 02103 **Module: SWI** **Network affecting: No**

IPX traffic passing between two switch instances using VLAN for Rapier48 now operates correctly.

PCR: 02210 **Module: DNS Relay** **Network affecting: No**

Buffer leaks occurred when DNS relay was enabled. This issue has been resolved.

PCR: 02214 **Module: IPG** **Network affecting: No**

A buffer leak occurred when a large number of flows (over 4000) were in use and needed to be recycled. This issue has been resolved.

PCR: 02220 **Module: SWI** **Network affecting: No**

The EPORT parameter in the ADD SWITCH L3FILTER ENTRY and SET SWITCH L3FILTER ENTRY commands was matching multicast and broadcast packets with software filtering. This issue has been resolved.

PCR: 02236 **Module: FIREWALL** **Network affecting: No**

Sometimes the retransmission of an FTP packet was not permitted through the Firewall. This issue has been resolved.

PCR: 02245 **Module: VRRP** **Network affecting: No**

VRRP returned an incorrect MAC address for an ARP request. This issue has been resolved.

PCR: 02263 Module: VRRP Network affecting: No

The virtual MAC address was used as the source MAC for all packets forwarded on an interface associated with a Virtual Router (VR). This was confusing when multiple VRs were defined over the same interface because only one virtual MAC address was ever used. The other virtual MAC addresses (for the other VR's) were only used if the source IP address matched the VR’s IP address. To avoid this confusion, the system MAC address is now always used unless the source IP address of the packet is the same as the VR’s IP address.

PCR: 02267 Module: BGP Network affecting: No

When route aggregation was enabled, the atomic aggregate was not being set. This issue has been resolved.

PCR: 02268 Module: FIREWALL Network affecting: No

HTTP requests from a fixed IP address were erroneously reported as a host scan attack in the Firewall deny queue. This issue has been resolved.

PCR: 02272 Module: IPG, PIM, SWI Network affecting: No

The following issues have been resolved:

- The RESET PIM INTERFACE=VLAN command was not working correctly.
- Packets with Time to Live (TTL) set to less than 4 were not being forwarded.
- VLAN tags were not being inserted into IP multicast packets on multi-tagged ports.
- A fatal error occurred when PIM and RIP were both running.

PCR: 02274 Module: TPAD Network affecting: No

ARL message interrupts have been re-enabled after a software table rebuild to fix synchronisation of the software forwarding database with the hardware table.

PCR: 02276 Module: FIREWALL Network affecting: No

The CREATE CONFIG command did not save the SOURCEPORT parameter to the configuration file when the low value of the source port range was set to zero. This issue has been resolved.

PCR: 02277 Module: DVMRP Network affecting: No

Report sending and default routes were not working correctly. Also, the SHOW CONFIGURATION DYNAMIC and SHOW CONFIGURATION=DVMRP commands were not working correctly. These issues have been resolved.

PCR: 02280 Module: TELNET, TTY Network affecting: No

TELNET sessions are now closed with “^D” only when the session is in the login state.

PCR: 02291 Module: DHCP Network affecting: No

DHCP now processes *Discover* messages smaller than 300 bytes.

PCR: 02292 Module: IPSEC Network affecting: No

IPSec no longer logs packets that match an ACTION=ALLOW policy. The overhead of this logging was affecting non-IPSec traffic.

PCR: 02294 Module: IKMP Network affecting: No

The LOCALRSAKEY parameter in the CREATE ISAKMP POLICY and SET ISAKMP POLICY commands was not accepting the value zero. This issue has been resolved.

PCR: 02298 Module: IPSEC Network affecting: No

The PURGE IPSEC command caused a fatal error. This issue has been resolved.

PCR: 02299 Module: VRRP Network affecting: No

If a packet with a destination IP address equal to a VRRP IP address was received when the router didn't own the IP address, (because it didn't have an interface with that IP address) the router incorrectly tried to forward the packet and send an ICMP "redirect" message to the source. Now, if such a packet is received, it will be discarded and an ICMP "host unreachable" message will be sent to the source.

PCR: 02301 Module: IPG Network affecting: No

If a DNS relay agent was configured with overlapping subnets, sometimes the DNS server response was returned to the client with a source IP address of an interface on the relay agent that was different from the interface the request was received on. This issue has been resolved.

PCR: 02302 Module: IPv6 Network affecting: No

The default router lifetime value has been corrected. Also, the SET IPV6 INTERFACE command now updates valid and preferred lifetimes correctly.

PCR: 02303 Module: INSTALL Network affecting: No

When enabling or disabling feature licences, a message will now be generated with a warning that changes to feature licences may not take effect until after a reboot.

PCR: 02304 Module: VRRP Network affecting: No

VRRP used the wrong source IP address in ICMP redirects. RFC 2338 states that the source IP address of ICMP redirects should be the IP address that the end host used when making its next hop routing decision. In the case of a packet sent to a VRRP virtual MAC address, this is the primary VRRP IP address associated with the MAC address, provided such a VR exists and is in the master state. This issue has been resolved.

PCR: 02309 Module: STP Network affecting: No

On models except Rapier *i* Series Switches, the ENABLE STP DEBUG PORT command did not work correctly. This issue has been resolved.

PCR: 02311 Module: SWI Network affecting: No

It was possible to set the trunk speed to 10/100M, even if the port within the trunk was not capable of this speed. This issue has been resolved.

PCR: 02313 Module: IPV6 Network affecting: No

The SHOW IPV6 INTERFACE command now shows the address lifetime aging status that is determined by the DECREMENT parameter in the ADD IPV6 INTERFACE command. The default valid and preferred address lifetimes have been changed to 30 days and 7 days respectively.

PCR: 02320 Module: IPV6 Network affecting: No

The interface address preferred lifetime was not operating correctly. This issue has been resolved.

PCR: 02321 Module: FR Network affecting: No

A fatal error occurred when the command SET FR=0 LMI= was executed if the LMI was already set to ANNEXA, ANNEXB or ANNEXD. This issue has been resolved.

PCR: 02326 Module: IPv6 Network affecting: No

A fatal error occurred when a PING was executed over an IPV6 tunnel that had previously been deleted. Also, packet forwarding with link-local addresses was not working correctly. These issues have been resolved.

PCR: 02327 Module: IPG/FIREWALL Network affecting: No

In some situations, multihomed interfaces caused the Firewall to apply NAT and rules incorrectly when packets were received from a subnet that was not attached to the receiving interface. This issue has been resolved.

PCR: 02328 Module: BGP Network affecting: No

BGP was not sending a withdraw message to a peer for a withdrawn or replaced route when the new best route came from that peer. This issue has been resolved.

PCR: 02330 Module: IPv6 Network affecting: No

A buffer leak was occurring in IPv6 fragmentation. This issue has been resolved.

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: 02332 Module: IPSEC Network affecting: No

The sequence number extracted from the AH and ESP header was in the wrong endian mode, which caused an FTP error with IPSEC anti-replay. This issue has been resolved.

PCR: 02334 Module: FIREWALL Network affecting: No

It is now possible to set the domain name of the SMTP server to none (0.0.0.0) with the SET FIREWALL POLICY SMTPDOMAIN command, even if a server name has not previously been specified.

PCR: 02335 Module: CLASSIFIER Network affecting: No

The SHOW CLASSIFIER command was not displaying Layer 3 information if the classifier had been created with the parameters ETHFORMAT=SNAP and PROTOCOL={IP|0000000800}. This issue has been resolved.

PCR: 02343 Module: PPP Network affecting: No

When acting as a PPPoE Access Concentrator (AC), if a PPPoE client sent discovery packets without the "host-unique" tag, the discovery packets sent by the AC were corrupted. This issue has been resolved.

PCR: 02346 Module: BGP, IPG Network affecting: No

It is now possible to set a preference value for dynamically learned routes based on their protocol using the command:

```
SET IP ROUTE PREFERENCE={DEFAULT|1..65535}
    PROTOCOL={BGP-EXT|BGP-INT|OSPF-EXT1|OSPF-EXT2|OSPF-INTER|
    OSPF-INTRA|OSPF-OTHER|RIP}
```

PCR: 02347 Module: SWI Network affecting: No

The CREATE CONFIGURATION command was not correctly generating the DISABLE SWITCH HWFILTER and DISABLE SWITCH L3FILTER commands. This issue has been resolved.

PCR: 02348 Module: ENCO Network affecting: No

When the PAC card was under severe load, the related driver occasionally did not fully transfer all result data from the chip. This caused an *actCmdFail* error. This issue has been resolved.

PCR: 02354 Module: SCC, SYN, PPP Network affecting: No

In a previous patch, a fatal error occurred after a RESTART ROUTER command was executed when using PPP over SYN. Also, on AR745 models, PPP was using an 8 MB boundary instead of a 16 MB boundary. These issues have been resolved.

PCR: 02357 Module: FR Network affecting: No

The following issues have been resolved:

- PIM was not sending Hello messages over a Frame Relay (FR) interface.
- A fatal error occurred if 64 was entered as the interface value in the DESTROY FRAMERELAY command. The command now only accepts 0-63 for this parameter.
- The ADD FRAMERELAY DLC command incorrectly accepted a TYPE parameter. Also, this command was not accepting the ENCAPSULATION parameter.
- The CREATE CONFIGURATION command incorrectly generated the CIR and CIRLIMITED parameters for the ADD FRAMERELAY DLC command.
- FR interfaces with static DLCs were always shown as DOWN. The status of the interface was not being updated when a circuit was added to the interface.

PCR: 02359 Module: IPG Network affecting: No

When an IP Multihomed interface was used as an OSPF interface, neighbour relationships were only established if the IP interface for OSPF was added first in the configuration. Now, OSPF establishes neighbour relationships regardless of the IP Multihomed interface configuration order.

PCR: 02363 Module: FFS, FILE, TTY Network affecting: No

The FLASH compaction process is now transparent to the file edition process. The FLASH system is now more stable.

PCR: 02365 Module: SWI Network affecting: No

Address learning on the mirror port is now correctly re-enabled when it is no longer the mirror port.

PCR: 02367 Module: SWI Network affecting: No

New commands have been added to enable the addition and deletion of static multicast addresses to and from the multicast forwarding table. The new commands are:

```
ADD SWITCH MULTICASTADDRESS IP=ipadd VLAN=vlan-id
   PORT=port-list
```

```
DELETE SWITCH MULTICASTADDRESS IP=ipadd VLAN=vlan-id
```

PCR: 02369 Module: IPG Network affecting: No

When the SET IP ROUTE command was executed to change any parameter other than METRIC1, which is the RIP metric, the RIP metric was reset to 1. This metric is now only updated if a value for the parameter is specified.

PCR: 02371 Module: FIREWALL Network affecting: No

When the system time was set to a time that was before or significantly after the current time, Firewall sessions were prematurely deleted. This issue has been resolved.

PCR: 02376 Module: PPP Network affecting: No

When the PPP ONLINELIMIT was exceeded for PPP over TDM, the PPP link stayed open, allowing Link Quality Report (LQR) packets to be transmitted. This caused the *ifOutOctets* counter to increment. Now, if the ONLINELIMIT is exceeded, the link will close.

PCR: 02378 Module: SWI Network affecting: No

Entering 63 for the EPORT parameter in the ADD SWITCH L3FILTER command caused a fatal error. This parameter now accepts the values 63 and 64.

PCR: 02395 Module: VRRP, TRG Network affecting: No

The SHOW VRRP command now shows the number of trigger activations for the Upmaster and Downmaster triggers.

PCR: 02397 Module: DVMRP Network affecting: No

After a prune lifetime had expired, the interface was not joined back to the DVMRP multicast delivery tree. This issue has been resolved.

PCR: 02398 **Module: IPV6** **Network affecting: No**

The following issues have been resolved:

- It was possible to assign the same network on different IPV6 interfaces
- The loopback address was being added to other interfaces
- The tunnel configuration was not showing correctly in IPV6 configuration commands

RIPv6 now sets the metric of routes for interfaces that are DOWN to 16, and immediately sends responses when the link status of VLAN interfaces changes.

PCR: 02399 **Module: TRACE** **Network affecting: No**

The Trace utility has been modified. Previously, Trace sent a group of packets at once and waited for multiple responses in order to assess the minimum, maximum and average time to cover a certain "hop distance" towards the target host. Now Trace sends each packet in each group individually, and waits either for a response or a time-out before sending the next packet in the group.

PCR: 02401 **Module: IPV6** **Network affecting: No**

Neighbour discovery and PIM6 caused a fatal error when IPv6 was not enabled, or when the IPv6 feature license was not present. This issue has been resolved.

PCR: 02402 **Module: SNMP, CORE, SHOW, FILE** **Network affecting: No**

SNMP MIB support has been enhanced for CPU utilisation and file statistics. MIB support has been added for Allied Telesyn contact details and fast buffers.

PCR: 02403 **Module: STP** **Network affecting: No**

A watchdog timeout occurred when the command ENABLE STP PORT was executed. This issue has been resolved.

PCR: 02406 **Module: IPV6** **Network affecting: No**

A Router-Alert option has been added. Also, the SHOW IPV6 MLD INTERFACE command now works correctly.

PCR: 02409 **Module: IPG** **Network affecting: No**

A warning now appears when the DELETE IP INTERFACE command is executed before the DELETE DVMRP INTERFACE command.

PCR: 02410 **Module: VRRP** **Network affecting: No**

VRRP pre-empt mode was not working with advertisement updates of 1 second or more because this did not allow for interface start time on startup. Now a check is made to verify that interfaces are UP before timers are started.

PCR: 02411 **Module: IPV6** **Network affecting: No**

The SHOW TCP command was not showing the listening status for IPv6.

PCR: 02412 Module: IPV6 Network affecting: No

An ISDN call was activated by IPv6 Router Advertisements over IPv6 tunnel interfaces. This issue has been resolved.

PCR: 02415 Module: IPG Network affecting: No

Packets with a RIP source address and next hop address that are not on the same subnet as the interface will now be processed. If the received next hop is not on the same subnet, it is treated as 0.0.0.0.

PCR: 02418 Module: IPV6 Network affecting: No

ICMPv6 was returning an error for non-zero fragment offsets. This issue has been resolved.

PCR: 02421 Module: PIM Network affecting: No

The GUI was incorrectly accepting multiple entries for VLANs. This issue has been resolved.

PCR: 02422 Module: GARP Network affecting: No

The GUI was returning incorrect GARP counters. This issue has been resolved.

PCR: 02428 Module: IPV6 Network affecting: No

Link-local address behaviour was incorrect. Also, the PUBLISH parameter was not updated by the SET IPV6 INTERFACE command, or displayed in the SHOW IPV6 INTERFACE command. These issues have been resolved.

PCR: 02450 Module: IPV6 Network affecting: No

Large local packets were not being fragmented. Also, the More Fragment flag in the IPv6 fragment header was not being set correctly. These issues have been resolved.

PCR: 02452 Module: IPv6 Network affecting: No

Received Router Advertisements (RAs) were discarded when the interface was enabled to send RAs. This issue has been resolved.

PCR: 02457 Module: IPV6 Network affecting: No

The IPv6 priority filter was not matching correctly when TCP was specified as the protocol type. This issue has been resolved.

PCR: 02463 Module: DVMRP, IPG Network affecting: No

Multicast multi-homing was not working correctly. This issue has been resolved.

Features in 86241-01

Patch file details are listed in Table 7:

Table 7: Patch file details for Patch 86241-01.

Base Software Release File	86s-241.rez
Patch Release Date	26-July-2002
Compressed Patch File Name	86241-01.paz
Compressed Patch File Size	27732 bytes

Patch 86241-01 includes the following enhancements:

PCR: 02036 Module: SWITCH Network affecting: No

A new command allows the Layer 3 aging timer to be changed:

```
SET SWITCH L3AGEINGTIMER=<seconds>
```

where seconds can be 30 - 43200. After each cycle of the ageing timer, all existing Layer 3 entries with the hit bit set will have the hit bit reset to zero, and all existing Layer 3 entries with the hit bit set to zero will be deleted.

The SHOW SWITCH command output now displays the Layer 3 ageing timer value.

PCR 02138 Module: SWI Network affecting: No

The built in Self Test Code for all Rapiers, except G6, has been improved to enhance the detection of faults in switch chip external packet memory.

PCR: 02158 Module: FIREWALL Network affecting: No

When a TCP RST/ACK was received by a firewall interface, the packet that was passed to the other side of the firewall lost the ACK flag, and had an incorrect ACK number. This issue has been resolved.

PCR: 02185 Module: VRRP Network affecting: No

The SHOW CONFIG DYNAMIC=VRRP command was not showing port monitoring and step values correctly. This issue has been resolved.

PCR: 02229 Module: IPG Network affecting: No

The PURGE IP command now resets the IP route cache counters to zero.

PCR: 02240 Module: SWI Network affecting: No

The SENDCOS filter action did not operate correctly across switch instances. This was because the stacklink port on the Rapier 48 did not correctly compensate for the stack tag on frames received via the filter. This issue has been resolved.

PCR: 02241 Module: FIREWALL Network affecting: No

Firewall subnet NAT rules were not working correctly from the private to the public side of the firewall. Traffic from the public to private side (destined for subnet NAT) was discarded. These issues have been resolved. ICMP traffic no longer causes a RADIUS lookup for access authentication, but is now checked by ICMP handlers for attacks and eligibility. If the ICMP traffic matches a NAT rule, NAT will occur on inbound and outbound traffic. HTTP 1.0 requests sometimes caused the firewall HTTP proxy to close prematurely. Cached TCP sessions were sometimes not hit correctly. These issues have been resolved.

PCR: 02242 **Module: IPG** **Network affecting: No**

On a Rapier 24, adding an IP interface over a FR interface caused an ASSERT debug fatal error. This issue has been resolved.

PCR: 02250 **Module: FIREWALL** **Network affecting: No**

Sometimes the Firewall erroneously used NAT. This issue has been resolved.

PCR: 02259 **Module: DHCP, IPG** **Network affecting: No**

A dual Ethernet router was incorrectly accepting an IP address from a DHCP server when the offered address was on the same network as the other Ethernet interface. An error is now recorded when DHCP offers an address that is in the same subnet as another interface.

DS3 Interfaces

The AT-RP24i/DS3 provides one standards-based unchannelised DS3 interface. The interface has the following features:

- 44.736 Mbit/s interface rate, 44.210 Mbit/s payload data rate
- Separate transmit (Tx) and receive (Rx) BNC connectors
- 75-ohm impedance
- B3ZS line encoding
- Automatic compensation for lines up to 135m (450ft)
- Loop or internal timing
- C-bit framing
- Support for PPP and Frame Relay encapsulation

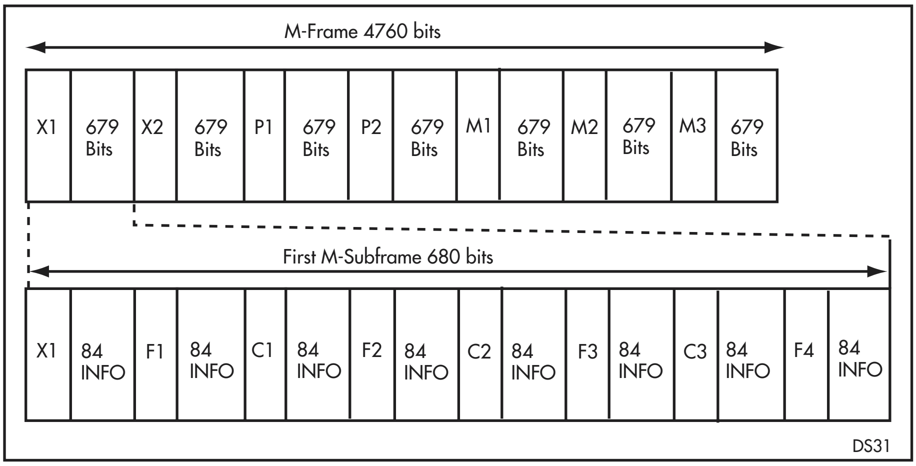
The interface meets the following specifications:

- ANSI T1.103, Digital Hierarchy - Synchronous DS3 Format
- ANSI T1.107, Digital Hierarchy - Formats
- ANSI T1.231, Digital Hierarchy - Layer 1 In-Service Digital
- RFC 2496 (DS3 MIB)

Digital Signal 3 (DS3) is a classification of digital signals, and sits at Layer One of the OSI model. The purpose of Layer One is to provide a transmission link between two entities and to monitor the quality of the link. In DS3 the link monitoring is achieved by adding overhead information alongside the data payload.

The DS3 interface rate is 44.736 Mbit/s with a payload rate of 44.210 Mbit/s. The signal is partitioned into *Multi-frames* (M-frames), and the M-frames are partitioned into seven M-subframes. Each M-subframe is further subdivided into 8 blocks of 85 bits with 84 bits available for payload, and one bit for framing overhead. The frame structure is shown in Figure 2 on page 32.

Figure 2: DS3 Framing Structure.



The switch with the DS3 interface is called the *near end*. The entity the switch connects to is called the *far end*. X1 and X2 are set to 1 if the near end is receiving an *Alarm Indication Signal* (AIS), a *Loss Of Frame* (LOF), or a *Loss Of Signal* (LOS). This allows the near end to indicate to the far end that it is experiencing a problem and is known as *Far End Receive Failure* (FERF).

P1 and P2 form the *P-bit channel*. They provide parity information for the preceding M-frame.

M1, M2, and M3 form a *frame alignment channel* used by the hardware to locate all seven M-subframes.

F1, F2, F3, and F4 form an *M-subframe alignment channel* which is used by the hardware to identify all frame overhead bit positions.

C1, C2, and C3 form the *C-bit channel*.

C-bit Parity Mode

In C-bit parity mode the C-bits are described as follows:

- The first C-bit in M-subframe 1 is set to 1 to identify the format as C-bit parity. If this is zero the format is assumed to be M23.
- The second C-bit in M-subframe 1 is designated Nr and is set to 1.
- The third C-bit in M-subframe 1 provides the *Far End Alarm and Control signal* (FEAC) which is used to:
  - Send alarm or status information from the far end back to the near end.
  - Initiate DS3 loopbacks.

The three C-bits in M-subframe 3 are designated as CP-bits and are used to implement CP-bit parity. At the near end the CP-bits are set to the same value as the P-bits. The parity of the CP-bits of frame N are compared with the parity of the CP-bits of frame N+1. A difference in parity between N and N+1 is deemed a CP-bit parity error.

The three C-bits in M-subframe 4 are designated as FEBE bits. The FEBE bits are returned to the far end to indicate the occurrence of a framing error or CP-bit parity error. If none occur, the FEBE bits are set to all ones. One or all of the FEBE bits are set to zero if a CP-bit parity error or an error in the F or M bits is found.

The three C-bits in M-subframe 5 are assigned as a 28.2kbits/s terminal-to-terminal-path maintenance data link. This data link can be switched off at the command interface, If it is switched off, the C-bits in M-subframe 5 are set to all ones. If switched on, the maintenance channel can convey the following information:

- Path Identification Signal.
  A set of ASCII text strings that can be used to uniquely identify this particular DS3 path. This can be useful if the DS3 signal is, at some point in its path, multiplexed into a higher order signal such as DS4 or OC-3. It is common for lower-order signals to be switched within a cross-connect. If this happens it is possible that the wrong DS3 signal is switched through to the switch. When this happens the overhead bits are all correct, so there is no indication that the wrong signal has been applied. The Path Identification Signal can be agreed by the two parties at either end of the network and tested to ensure that it is the right DS3 signal that has been received.
- Idle Signal.
  A set of ASCII text strings that can be used to provide the location of the source of an idle signal.
- Test Signal.
  A set of ASCII text strings that can be used to provide the location of the source of a test signal.

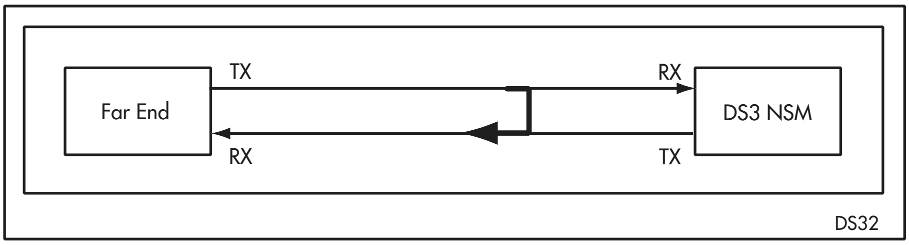
These signals are sent once every second. All other C-bits are for future use.

Loopbacks

The DS3 interface provides four types of loopback; line, payload, diagnostic, and remote. These loopbacks are activated by the ENABLE DS3 TEST command.

Line loopback is shown in Figure 3 on page 33. In this loopback mode the receive signal is looped straight to the transmit signal.

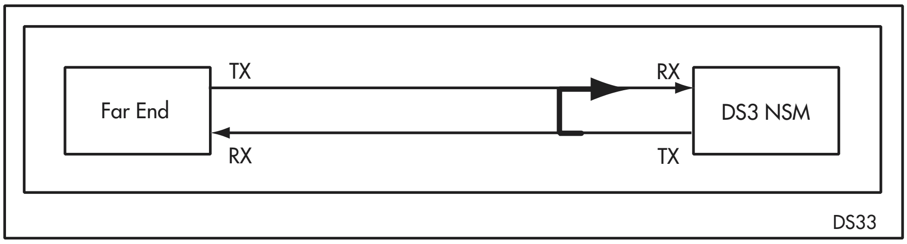
Figure 3: Line Loopback.



Payload loopback is similar to line loopback. The difference is that only the payload load is looped back from receive to transmit. The overhead is sourced from the DS3 NSM.

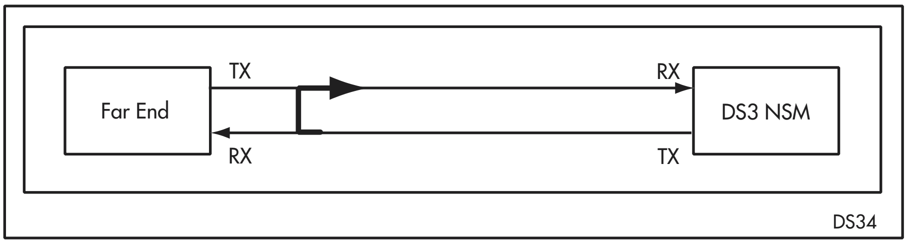
Diagnostic loopback is shown in Figure 4 on page 34. In this loopback mode the transmit signal is connected straight to the receive signal.

Figure 4: Diagnostic Loopback.



In C-bit parity mode it is also possible for the switch to request a loopback at the far end. This is shown in Figure 5 on page 34. This is achieved using the FEAC channel. The switch can also respond to remote loopback requests via the FEAC channel from the far end. This results in a near end Line Loopback (see above).

Figure 5: Remote Loopback.



Note that it is possible to configure near end local and remote loopbacks at the same time.

DS3 Configuration

The DS3 interface on the switch is automatically configured by the software modules when the switch sets up. Certain aspects of the DS3 signal can be altered to allow the switch to connect to another vendor's equipment via the DS3 interface.

The configuration of the DS3 interface can be changed with the command:

```
SET DS3=instance [CLOCK={LOOP|INTERNAL}] [CMTCE={ON|OFF}]
    [DIRECTION={TRANSMIT|RECEIVE}] [EIC=equipment-id]
    [FAC=facility-id] [FDET={ON|OFF}] [FIC=frame-id]
    [GENNO=generator-id][LIC=location-id] [PARAM15=threshold]
    [PARAM24=threshold] [PORT=port-id] [PRIM15=threshold]
    [PRIM24=threshold] [UNIT=unit-id] [TYPE=[{PID|ISID|TSID}]
```

The CLOCK parameter specifies the clock source for the DS3 interface. The default is LOOP timing where the clock is derived from the received DS3 signal. If INTERNAL is selected the DS3 transmit signal is timed using an internal clock.

The CMTCE parameter specifies whether the terminal-to-terminal path-maintenance link is switched on. When CMTCE is set to OFF the maintenance link is switched off and the C-bits in M-subframe 5 are all set to one. If CMTCE is set to ON the maintenance link is switched on. The path maintenance link allows a number of identification messages to be inserted in to the path overhead of the DS3 signal. These messages are in the form of text characters and allow the users at either end of the DS3 path to ensure that the correct DS3 signal has reached their equipment.

The DIRECTION parameter is used with the EIC, FAC, FIC, LIC or UNIT parameters to specify whether the text string is the text to transmit, or the text to expect in the received signal. If TRANSMIT is specified, the user is specifying a text to be transmitted out on the path. If RECEIVE is specified, the user is specifying the ASCII characters expected on the incoming path. If the DIRECTION parameter is present the TYPE parameter must also be present.

The EIC parameter specifies the Equipment Identification Code. This is 0 to 10 characters in length and describes the equipment at the near end, e.g. “RAPIER SW”. This parameter is only meaningful with the CMTCE parameter set to ON. With CMTCE set to OFF this parameter is ignored. The default pattern is “ignore”.

The FAC parameter specifies the FACility identification code. This is 0 to 38 characters in length and describes the DS3 path.

This data element is called FI in the ANSI specification, it is named FAC in this document to avoid confusion with the FIC parameter.

The FAC parameter is only valid if the TYPE parameter is set to PID. This parameter is only meaningful with the CMTCE parameter set to ON. With CMTCE set to OFF this parameter is ignored. The default pattern is “ignore”.

The FDET parameter specifies whether fast detection of AIS is enabled. If ON is specified, the AIS detection time is 2.23ms. If OFF is specified, the AIS detection time is 13.5ms. The default is ON.

The FIC parameter specifies the Frame Identification Code. This is 0 to 10 characters in length and describes where the equipment is located within a building, e.g. “FRAME 255”. This parameter is only meaningful with the CMTCE parameter set to ON. With CMTCE set to OFF this parameter is ignored. The default pattern is “ignore”.

The GENNO parameter specifies the test signal identification message. It is 0 to 38 characters in length and describes the signal generator that initiates a test message. This parameter is only valid if the TYPE parameter is set to ISIS. This parameter is only meaningful with the CMTCE parameter set to ON. With CMTCE set to OFF this parameter is ignored. The default pattern is “ignore”.

The LIC parameter specifies the Location Identifier Code. This is 0 to 11 characters in length and describes the specific location of the equipment, e.g. “BUILDING 1”. This parameter is only meaningful with the CMTCE parameter set to ON. With CMTCE set to OFF this parameter is ignored. The default pattern is “ignore”.

The PARAM15 parameter specifies the 15-minute counter threshold for all performance monitoring parameters (PES, PSES, SEF, UAS, LES, CES, CSES) between 1 and 900 seconds inclusive. If a trigger has been created, it will assert if the 24-hour count exceeds the value specified in PARAM15. The default is 900 seconds.

The PARAM24 parameter specifies the 24-hour counter threshold for all performance monitoring parameters (PES, PSES, SEF, UAS, LES, CES, CSES) between 1 and 65535 seconds inclusive. If a trigger has been created, it will assert if the 24-hour count exceeds the value specified in PARAM24. The default is 65535 seconds.

The PORT parameter specifies from which port a test signal is generated, and is 0 to 38 characters in length. This parameter is only valid if the TYPE parameter is set to TSID. This parameter is only meaningful with the CMTCE parameter set to ON. With CMTCE set to OFF this parameter is ignored. The default pattern is "ignore".

The PRIM15 parameter specifies the 15-minute counter threshold for all performance monitoring primitives (LCV, PCV, CCV) between 1 and 16383 seconds inclusive. If a trigger has been created, it will assert if the 15-minute count exceeds the value specified in PRIM15. The default is 16383.

The PRIM24 parameter specifies the 24-hour counter threshold for all performance monitoring primitives (LCV, PCV, CCV) between 1 and 1048575 seconds inclusive. If a trigger has been created, it will assert if the 24-hour count exceeds the value specified in PRIM24. The default is 1048575.

The PRIM24 parameter specifies the 24-hour counter threshold for all performance monitoring primitives (LCV, PCV, CCV) between 0 and 1048575 seconds. If a trigger has been created, it will assert if the 24-hour count exceeds the value specified in PRIM24. The default is 1048575.

The TYPE parameter is used with the EIC, FAC, FIC, LIC, or UNIT parameters to specify whether the text string is used to describes a path signal, an idle signal, or a test signal.

The UNIT parameter specifies where the equipment is located within a bay e.g. "SHELF6", and is 0 to 6 characters in length. This parameter is only meaningful with the CMTCE parameter set to ON. With CMTCE set to OFF this parameter is ignored. The default pattern is "ignore".

To see the current configuration use the command:

```
SHOW DS3=n STATE
```

The DS3 counters can be displayed by using the command:

```
SHOW DS3=n COUNTERS [HISTORY[=interval]] {NEAR|FAR|BOTH}
```

The counters can be reset by using the command

```
RESET DS3[=instance]
    COUNTERS[={HDLC|INTERFACE|LINK|DIAGNOSTIC|STATE|ALL}]
```

where:

- *instance* is the number of the DS3 interface.

A further description of DS3 can be found in the DS3 Interfaces section of *Chapter 3, Interfaces* in your switch's software reference.

The commands used to set up and configure the DS3 interface are:

- DISABLE DS3 DEBUG
- DISABLE DS3 TEST
- ENABLE DS3 DEBUG

- ENABLE DS3 TEST
- RESET DS3
- RESET DS3 COUNTERS
- SET DS3
- SHOW DS3 CMTCE
- SHOW DS3 CONFIGURATION
- SHOW DS3 COUNTERS
- SHOW DS3 DEBUG
- SHOW DS3 STATE
- SHOW DS3 TEST

Once the interface is set up and configured, it can be used in conjunction with Frame Relay, using the following commands:

- CREATE FRAMERELAY
- SHOW FRAMERELAY

See *Chapter 5, Frame Relay* in your switch's Software Reference.

DS3 interfaces can be tested with the test facility, using the following commands:

- DISABLE TEST INTERFACE
- ENABLE TEST INTERFACE
- SHOW TEST

See *Chapter 10, Test Facility* in your switch's Software Reference.

Dynamic Port Security

Dynamic Port Security allows for dynamic MAC address learning on a switch port. If a MAC address is unused for a period of time, it will be aged from the database of currently accepted MAC addresses. This allows the learning of new MAC addresses, which is useful because port security allows the number of devices that are connected to a particular switch port to be limited.

MAC address learning can be set to static or dynamic by using the RELEARN parameter in the following command:

```
SET SWITCH PORT={port-list|ALL} [ACCEPTABLE={ALL|VLAN}]
   [BCLIMIT={NONE|limit}] [DESCRIPTION=description]
   [DLFLIMIT={NONE|limit}]
   [EGRESSLIMIT={NONE|DEFAULT|0|1000..127000|8..1016}]
   [INFILTERING={OFF|ON}]
   [INGRESSLIMIT={NONE|DEFAULT|0|64..127000|8..1016}]
   [LEARN={NONE|0|1..256]
   [INTRUSIONACTION={DISABLE|DISCARD|TRAP}]
   [MCLIMIT={NONE|limit}] [MIRROR={BOTH|NONE|RX|TX}]
   [MODE={AUTONEGOTIATE|MASTER|SLAVE}]
   [MULTICASTMODE={A|B|C}] [RELEARN={OFF|ON}]
   [SPEED={AUTONEGOTIATE|10MHALF|10MFULL|10MHAUTO|10MFAUTO
   |100MHALF|100MFULL|100MHAUTO|100MFAUTO|1000MHALF|1000MF
   ULL|1000MHAUTO|1000MFAUTO}]
```

The RELEARN parameter determines whether dynamic or static MAC address learning will be used on this port. This parameter has no effect if the security feature limiting the number of MAC addresses is disabled (i.e. when LEARN=0 or NONE).

If the RELEARN parameter is set to OFF, static MAC address learning is used. Once a MAC address has been learned it will remain permanently in the learning database. IF the RELEARN parameter is set to ON, dynamic MAC address learning is used. If a MAC address is unused for a period of time, it will be removed from the learning database. Another (or the same) MAC address can then be learned and stored in the vacant position in the learning database. When RELEARN is enabled on a port, all existing entries in the learning database are removed. The elapsed time before a MAC address entry is removed can be set using the SET SWITCH AGEINGTIMER command (See the Switch Chapter for more information). The default is OFF.

To see whether the switch is using static or dynamic port security, use the command:

```
SHOW SWITCH PORT[={port-list|ALL}]
```

This command displays general information about the specified switch ports or all switch ports.

Figure 1-8: Example output from the SHOW SWITCH PORT command showing the RELEARN parameter.

```
Switch Port Information
---------------------------------------------------------------------------
 Port ......................... 1
   Description .................. To intranet hub, port 4
   Status ....................... ENABLED
   Link State ................... Up
   UpTime ....................... 00:10:49
   Port Media Type .............. ISO8802-3 CSMACD
   Configured speed/duplex ...... Autonegotiate
   Actual speed/duplex .......... 1000 Mbps, full duplex
   Configured master/slave mode .. Autonegotiate
   Actual master/slave mode ..... Master
   Acceptable Frame Types ....... Admit All Frames
   Broadcast rate limit ......... 1000/s
   Multicast rate limit ......... -
   DLF rate limit ............... -
   Learn limit .................. -
   Relearn ...................... OFF
   Intrusion action ............. Discard
   Current learned, lock state ... 15, not locked
   Mirroring .................... Tx, to port 22
   Is this port mirror port ..... No
   Enabled flow control ......... Pause
   Send tagged pkts for VLAN(s) .. marketing (87)
                                  sales (321)
   Port-based VLAN .............. accounting (42)
   Ingress Filtering ............ OFF
   Trunk Group .................. -
   STP .......................... company
   Multicast filtering mode ..... (B) Forward all unregister groups
---------------------------------------------------------------------------
```

Table 1-1: New parameter in the output of the SHOW SWITCH PORT command.

Parameter	Meaning
Relearn	Whether or not MAC address learning is used, one of “ON or OFF”.

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.