Patch Release Note

Patch 86261-09
For Rapier and AT-8800 Series Switches

Introduction

This patch release note lists the issues addressed and enhancements made in patch 86261-09 for Software Release 2.6.1 on existing models of Rapier and AT-8800 Series switches. Patch file details are listed in Table 1.

Table 1: Patch file details for Patch 86261-09.

Base Software Release File	86-261.rez
Patch Release Date	15-Jun-2004
Compressed Patch File Name	86261-09.paz
Compressed Patch File Size	389936 bytes

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

- Release Note: Software Release 2.6.1 for Rapier and AT-8800 Series Switches (Document Number C613-10383-00 Rev A) available from *www.alliedtelesyn.co.nz/documentation/documentation.html*.
- Rapier Series Switch or AT-8800 Series Switch Documentation Set for Software Release 2.6.1 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 86261-09

Patch 86261-09 includes all issues resolved and enhancements released in previous patches for Software Release 2.6.1, and the following enhancements:

PCR: 40053 Module: PRI Level: 2

A PRI interface was sometimes incorrectly shown as *down* in the output of the **show interface** command when a PPP link was active on the interface. This issue has been resolved.

PCR: 40105 Module: SWI Level: 3

The device did not drop packets when a port was configured with an intrusion trap via the **set switch port intrustionaction=trap** command. This issue has been resolved.

PCR: 40116 Module: FIREWALL Level: 2

When the firewall was used on a NAT interface in conjunction with IP policy filters, Telnet to this interface was not possible. This issue has been resolved.

PCR: 40123 Module: OSPF Level: 2

OSPF did not refresh a network LSA when it received a LSA with errors from another vendor's device. This has now been fixed.

PCR: 40178 Module: STP Level: 3

When STP was disabled, any changes to the RSTP parameters **maxage, hellotime,** or **forwarddelay** in the **set stp** command were not shown in the **show stp** command. This issue has been resolved.

PCR: 40208 Module: IPV6 Level: 2

The IPv6 ND entry was not added to the device's forwarding database, so IPv6 packets were flooded out all ports. This issue has been resolved.

PCR: 40214 Module: TACP Level: 2

Logging in via TACACS+ sometimes caused a fatal error if the user's name and password had expired on the TACACS+ server. This issue has been resolved.

PCR: 40236 Module: SWI Level: 2

A Layer 3 filter configured to trap packets with the *RouterAlert* option did not always filter MLD packets. This was due to variations in the MLD packet fields. This issue has been resolved.

PCR: 40258 Module: SWMX Level: 3

MLD Snooping did not read an MLD report as a correct MLD packet format when PADN was placed before the Router Alert option. This issue has been resolved.

PCR: 40263 Module: TACPLUS, USER Level: 2

Occasionally a fatal error occurred if users were changed with the **login** command, and a TACACS+ server authenticated the users. This issue has been resolved.

PCR: 40271 Module: IGMP, PIM Level: 2

A static IGMP entry was not created with the **create ip igmp destination** command from a configuration script or after enabling PIM for that interface. A PIM *Join* was also not created. This issue has been resolved. Now a PIM *Join* is sent to the RP following the PIM RP election process.

PCR: 40275 Module: IPV6 Level: 2

It was possible to create two identical 6-to-4 tunnels with the same IPv4 destination. This issue has been resolved.

PCR: 40277 Module: IPG Level: 2

BGP routes were not always readvertised to peers after a next-hop route was lost and then reactivated. This issue has been resolved.

PCR: 40279 Module: IPG Level: 2

Occasionally the device suffered a fatal error if it received a large number of directed broadcast packets. This issue has been resolved.

PCR: 40285 Module: DHCP Level: 3

Existing options for DHCP policies could not be removed with the **delete dhcp** command. This issue has been resolved.

PCR: 40290 Module: IPG Level: 3

An incorrect nexthop for a RIP route was advertised in RIP messages. This issue has been resolved.

PCR: 40298 Module: TTY Level: 2

When a second device logged in, the CLI command prompt was sometimes not displayed until the user pressed a key. This issue has been resolved so that the prompt is displayed immediately.

PCR: 40299 Module: IPG Level: 2

When the most recently added VLAN was deleted, the switch did not respond correctly to subsequent DHCP *Discover* messages. This issue has been resolved.

PCR: 40305 Module: SWI Level: 2

IGMP *Query* packets sent over a non-master trunk port were incorrectly flooded out the master port of the trunk group. This issue has been resolved.

PCR: 40311 Module: IPG Level: 2

A fatal error sometimes occurred when a large number of IP flows were being deleted when an interface went down. This issue has been resolved.

PCR: 40326 Module: SWI Level: 2

If a multicasting device received multicast packets on a port in one switch instance it could not send them out a port in another switch instance. This issue has been resolved.

Features in 86261-08

Patch file details are listed in Table 2:

Table 2: Patch file details for Patch 86261-08.

Base Software Release File	86-261.rez
Patch Release Date	24-May-2004
Compressed Patch File Name	86261-08.paz
Compressed Patch File Size	374,848 bytes

Patch 86261-08 includes all issues resolved and enhancements released in previous patches for Software Release 2.6.1, and the following enhancements:

PCR: 3514 Module: SWI, GUI Level: 3

An incorrect IPSec Security Association (SA) was used to transmit packets when the SA's IP address was assigned dynamically on another VPN gateway. This issue has been resolved.

PCR: 03990 Module: OSPF Level: 2

If a route filter was added after OSPF had exported its routes to other devices in the same OSPF area, the filtered routes were not purged from the link state database. However, other devices in the same OSPF area did purge their routes. This issue has been resolved.

PCR: 31231 Module: SW56, SWI, VLAN Enhancement

This enhancement provides optional blocking between ports in a private VLAN whilst still enabling layer 2 switching to an associated uplink port.

This enhancement has been applied to the Rapier-24i, the AT-8824 and the AT-8848 switches.

PCR: 31241 Module: SWCX, SWI Level: 2

With STP enabled, the switch was removing the VLAN identifier prior to forwarding incoming frames. Untagged frames however, were forwarded correctly. This issue has been resolved.

PCR: 31248 Module: IPG Level: 2

When a packet was destined for a network address, the switch would forward the packet to that network and incorrectly create an ARP request containing the address of the network. This issue has been resolved.

PCR: 31258 Module: IPG, DHCP Level: 2

If DHCP clients do not respond to echo requests, the DHCP server can not detect an addressing conflict, so may offer in-use addresses to clients. This issue has been resolved.

This PCR introduces a new parameter, **probe**, to the **create dhcp range** and **set dhcp range** commands. This parameter allows for address probing using ARP requests and replies instead of the normal ping mechanism. This feature is limited to clients on the same subnet (broadcast domain) as the DHCP server, and therefore can not be used with the **gateway** parameter.

The new syntax is:

```
create dhcp range=name [probe={arp|icmp}]
   [other-parameters]

set dhpc range [probe={arp|icmp}] [other-parameters]
```

PCR: 40035 Module: VRRP Level: 2

When VRRP was enabled and the IP module was reset on the master device that owned the virtual router address, IP or ARP packets sent to the virtual MAC address were not accepted by the master. This issue has been resolved.

PCR: 40039 Module: OSPF Enhancement

The router has been enhanced to enable up routes to be inported from BGP to OSPF. See “Importing BGP routes into OSPF” on page 40.

PCR: 40046 Module: IPG Level: 2

The next hop advertised in a RIP *Response* must be directly reachable on the logical subnet over which the advertisement is made. The device sometimes advertised the next hop of a route that was not on this subnet. This issue has been resolved.

PCR: 40047 Module: TACP

All TACACS+ commands now require Security Officer privilege when the device is in security mode.

PCR: 40049 Module: SW56 Level: 3

Frames with errors (for example, exceeding the maximum frame length) at the MAC layer were sent to the CPU and processed despite being invalid. This issue has been resolved. Invalid frames are now discarded.

PCR: 40050 Module: STP Level: 2

Sometimes the switch erroneously transmitted STP BPDUs that contained VLAN tags. This issue has been resolved.

PCR: 40058 Module: PORTAUTH Level: 3

The **control** parameter in the **set portauth port supplicant** command was incorrectly reflected in the dynamic configuration if that command was executed when port authentication was disabled. This issue has been resolved.

PCR: 40059 Module: DVMRP Level: 2

DVMRP now interoperates with all Cisco IOS versions.

PCR: 40062 Module: SWI Level: 3

If a mirror port was configured using the **set swi port mirror** command, and then the **enable switch mirror** command was entered, the switch would issue a warning that no mirror port had been set. This issue has been resolved.

PCR: 40064 Module: SW56 Level: 2

Executing the **reset switch** command was causing the Rapier 48 switch to lockup. This issue has been resolved.

PCR: 40067 Module: MNIX Level: 2

When using PPP multilink, many frames were being incorrectly marked as lost. Depending on the number of PPP links configured, this resulted in degraded performance and an occasional a loss of connectivity. This issue has been resolved.

PCR: 40068 Module: SCR, TTY, USER Enhancement

The switch has been enhanced to enable a text message to be displayed on the user's console immediately after logging into the device. This message must be contained within an ASCII text file called *login.txt* and reside in flash memory.

PCR: 40070 Module: CORE Level: 3

On AT-8800 series switches, a warning log message was generated for the fan's status when there was more than a 20% variation in fan speed between "Actual" and "Expected". This has been changed so the log message is only generated when the fan stops.

PCR: 40071 Module: IPG Level: 2

Routing tables were not being updated correctly when better BGP routes were learnt. This issue has been resolved.

PCR: 40076 Module: USER, PPP Level: 2

The calling-station ID was not being sent to Radius when authenticating a PPPoE connection. This issue has been resolved.

PCR: 40079 Module: SWI Level: 3

When port authentication was enabled, the command **enable switch port** had no effect, when entered from the GIU, even when port authentication affecting parameters were set to default. This issue has been resolved.

PCR: 40080 Module: IPV6 Level: 3

Setting the command **set ipv6 nd** to its default value of 0 was producing an error rather than indicating an unspecified value. This problem has been resolved.

PCR: 40083 Module: IPG Level: 2

The switch failed to add multiple dynamic RIP routes for unreachable next hops on the same subnet as the sending RIP interface. This problem has been resolved.

PCR: 40084 Module: IPG Level: 2

Non-querier received IGMP *Leave* messages were incorrectly updating the Refresh time of the Group. The Refresh time is now updated only when receiving a Specific query message.

PCR: 40086 Module: OSPF Level: 2

This PCR corrects an error introduced by PCR 40011 patch 06. This PCR caused invalid commands to be created in the config file when it was written.

PCR: 40087 Module: TACP Level: 2

The following TACACS+ issues have been resolved and enhancements made:

1. The following command has been added to enable users to grant outbound telnet privileges to TACACS+ authenticated users based on thier privilege level:

   ```
   set tacplus telnet
   ```

2. The command **show tacplus telnet** has been added to enable users to view the level of TACACS+ privilege that is currently required for using telnet on the switch.
3. The mappings between TACACS+ privileges and local privileges have been modified. Levels 0-6 are defined as *user*, level 7 is defined as *manager*, levels 8-14 are defined as *user*, and level 15 is defined as *security officer*.
4. The **show tacplus user** command has been modified to display the correct login time.
5. The format of TACACS+ log messages now follow the same port naming convention as the USER module.
6. The resolution on the TACACS+ expiry and idle timers has been increased.
7. The issue of TACACS+ users being inappriately logged out has been resolved
8. The **set tacplus key** command was not extracting the information entered by the **create config** command, or displayed using the **show config** command. This issue has been resolved.

PCR: 40097 Module: FW Level: 2

Changing the time on the router by using the **set time** command was causing any temporary firewall rules configured, i.e. those rules specified with a TTL parameter, to timeout. This issue has been resolved.

PCR: 40099 Module: VLAN Level: ?

If a mirror port was configured using the command, **set switch mirror=*port x***, then another port was configured to be *tagged* using the command, **set vlan=*default* port=*y* frame=*tag***, the tagging configured for *port x* would be removed. This issue has been resolved.

PCR: 40100 Module: FIREWALL Level: 2

When a firewall rule was added using the commands,
add firewall policy rule action=nat list=*text file name*
(where the text file contained a list of IP addresses), the device dropped packets that matched the rule parameters in the list, instead of translating them.

This issue has been resolved by ensuring that the device translates the addresses of packets that match the rule parameters and whose addresses exist in the list file, but drops packets whose addresses do not exist in the list file.

For outbound packets that match the rule parameters, but not the list, the rule matching process continues until a matching rule is found. If no matching rule is found, the default rule *allow all* is applied. For inbound packets that match the rule parameters, but not the list, the rule matching process is terminated and the packets will be dropped as they are when **action=allow** is specified.

PCR: 40101 Module: VRRP Level: 2

When proxy ARP was enabled on an interface that was set up as a VRRP virtual router, the switch was sending proxy ARP response messages using its own switch's MAC address rather than that assigned to the Virtual Router. This issue has been resolved, by ensuring that Proxy ARP responses now use the MAC address assigned to the virtual Router.

PCR: 40103 Module: NVS Level:3

The NVS read and write routines were not displaying the correct number for the permanent log entries when the default was changed. This issue has been resolved.

PCR: 40106 Module: FIREWALL Level: 3

The command **add firewall policy=policy1 dynamic=remote file=*filename.txt*** was not accepted when the filename exceeded eight characters (excluding the three suffix characters). This issue has been resolved by enabling the device to shorten these file names before writing them to the config file.

PCR: 40107 Module: SWI Level:3

When a switch port is set with a learn limit, and the packet source address is a broadcast or multicast address. Then, rather than ignoring these addresses the switch was learning them and entering them into its forward database. This issue has been resolved.

PCR: 40110 Module: SWI Level: 3

The output from the **show log output=permanent** command was displaying the default number rather than the number configured by the **create log output** command.

PCR: 40112 Module: PIM6 Level: 2

PIM Dense Mode *Graft* and *GraftAck* messages were not being sent. This issue has been resolved.

PCR: 40113 Module: TTY Level: 3

As a result of PCR 31133 introduced in patch release 04, the **delete alias** command was not operating. This issue has been resolved.

PCR: 40114 Module: TTY Level: 3

If the keys Ctrl+C were depressed following a restart and login, the text displayed when the port history list was empty has been improved. The text displayed is now:

```
Info (1036278): The history list is empty.
```

PCR: 40115 Module: IPv6 Level: 3

The *Fail* counter of the **show ipv6 filter** command was not incrementing beyond one. This issue has been resolved.

PCR: 40118 Module: IPG Level: 2

Patch 05 introduced the possibility of fatal errors occuring when using Equal-Cost Multi-Path Routing for CPU bound data. This issue has been resolved

PCR: 40119 Module: IPG Level: 2

If a port was added to a VLAN as *tagged* by using the command **set vlan=vlan*x* port=y frame=*tagged*,** and then a mirror port was configured, the frames transmitted to the mirror port were correctly transmitted as *untagged*. However, if the configuration was saved and the switch rebooted, then the mirrored frames contained a VLAN tag. This issue has been resolved to ensure that the mirrored data is always transmitted as *untagged* frames.

PCR: 40121 Module: IPG Level: 3

The **create ip mvr vlan, add ip mvr vlan,** and **destroy ip mvr vlan**, commands were not accepting VLAN IDs greater than 255. This issue has been resolved by enable these commands to accept VLAN IDs up to 4094.

PCR: 40124 Module: IPG, SWI Level: 2

When a tagged port was deleted from a VLAN on a Rapier *i* or AT-8800, all MAC addresses, L3 entries and ARPs learned from the port were removed regardless of VLAN membership. This issue has been resolved by ensuring that only entries learned for the specified VLAN are removed.

PCR: 40129 Module: DHCP Level: 2

When a DHCP client entry was detected as being in use on a VLAN interface, the 'Client ID was not being correctly stored. For example, the Client ID was appearing blank in the **show dhcp client** output. This issue has been resolved.

PCR: 40131 Module: SWMX Level: 2

In rapid STP mode, if a port was disabled, then the command **set stp default** was executed, the port could not be re-enabled. This issue has been resolved.

PCR: 40134 Module: SWI Level: ?

When a classifier-based hardware filter was added, certain classifier numbers, such as 1023, 1024, 2047, and 2048, would cause the switch to reboot. This issue has been resolved.

PCR: 40132 Module: STP Level: 2

In rapid STP mode, the **set stp default** command would not reset the STP default values for Max Age, Hello Time, and Forward Delay. This issue has been resolved.

PCR: 40137 Module: OSPF Level: 3

OSPF would reject IP packets that, after being reassembled, were larger than the standard buffer size of 1800 bytes. This has been resolved by enabling OSPF to process IP fragments whose reassembled size is up to 64 K bytes long.

PCR: 40138 Module: SWCX Level: 2

The GUI was not recognising an AT-G8SX-01 GBIC. This issue has been resolved.

PCR: 40142 Module: OSPF Level: 2

When an interface that was a designated router (DR) went to the down state, the Network LSA was not being flushed from the routing domain. For compliance with RFC 2328 12.4 , the Network LSA will now be flushed out.

PCR: 40143 Module: SWI Level: 2

Previously when 10/100 copper ports were disabled, the link state was automatically taken down. Users are now able to select whether ports are disabled or enabled. The option is applied using the command:

```
disable switch port={port-list|all} [flow=pause]
[link={enable/disable}]
```

When **link** is set to **disable**, the port is electrically disabled (the link is taken down). When the link is set to **enable** the port is disabled, but the link remains up.

PCR: 40150 Module: PPP Level: 2

When a router uses OSPF over PPP and one of its PPP links was lost, the LS updates were not alerting the router's neighbours (via links on its other interfaces) of the PPP outage. This issue has been resolved.

PCR: 40158 Module: FIREWALL Level: 3

Notifications and triggers for some Firewall events were generated only when its threshold levels were exceeded. They are now generated whenever the threshold levels are reached. The affected events are:

SMURFATTACK, TCPTINY, FRAGMENT, LANDATTACK, IPSPOOFATTACK, PINGOFDEATHATTACK, SPAMATTACK, RELAYATTACK, SMURFAMPATTACK, OTHERATTACK, RELAYATTACK

PCR: 40162 Module: SWI Level: 2

When the **set switch mirror** command was used to configure a port belonging to more than the default VLAN, the command would fail and an error message would be produced. However, the port would maintain its incorrectly mirrored condition, rather than return to its previous unmirrored condition. This issue has been resolved.

PCR: 40172 Module: QOS Level: 2

Although all changes to the **maxbandwidth** parameter of the **create qos policy** command were previously accepted, the Rapier's implementation of this parameter was inconsistently applied for values that were not exact multiples of 1 Mbps. This issue has been resolved by ensuring that this parameter's value is always rounded up to the nearest 1 Mbps, and a warning advising the user is displayed.

PCR: 40174 Module: INSTALL Level: 2

When the command **delete install=preferred** was executed, if file *nvs:gui.ins* did not exist, the command would incorrectly create it. To resolve this issue the command will no longer create this file, and will only write to it if it exists already.

PCR: 40177 Module: IPv6 Level: 3

The behaviour of the set **set ipv6 nd interface retrans** command was inconsistent. This resulted in the commands **show config dynamic=ipv6** and **show ipv6 ndconfig** not displaying their output. This issue has been resolved.

PCR: 40226 Module: DHCP Level: 2

If the **create dhcp range** command was used to try and create an invalid IP address range that contained an invalid IP address, then the **delete dhcp range** command was used to delete the invalid IP address, a fatal exception error would result. This issue has been resolved.

PCR: 40228 Module: VLAN, SW56 Level: 2

PCR 40119 introduced an error that prevented tagged VLANs from operating correctly. Communication between untagged was prevented if one of the ports was also configured as a tagged port. this issue has been resolved.

PCR: 40244 Module: IPG Level: 2

The switch was unable to correctly filter IGMP messages using the L3 filter. This issue has been resolved.

Features in 86261-07

Patch 86261-07 includes all issues resolved and enhancements released in previous patches for Software Release 2.6.1, and the following enhancements:

PCR: 40197 Module: SWI, GUI Level: 3

The presence of cards inserted into NSM bay on the NEBS Rapier24i switches was not being detected. This issue has been resolved.

Features in 86261-06

Patch 86261-06 includes all issues resolved and enhancements released in previous patches for Software Release 2.6.1, and the following enhancements:

PCR: 40190 Module: SWI, GUI

The software has been enhanced to enable the NEBS compliant Rapier24i switch to utilise the standard Rapier24i GUI resource file.

Features in 86261-05

Patch 86261-05 includes all issues resolved and enhancements released in previous patches for Software Release 2.6.1, and the following enhancements:

PCR: 03420 Module: IPG, SWI Level: 3

It is now possible to prevent specified ports from acting as IGMP all-group ports, and specify which ports are allowed to behave as all-group entry ports. This is enabled with the ENABLE IP IGMP ALLGROUP command, and disabled with the DISABLE IP IGMP ALLGROUP command.

For details, see "*IGMP Snooping All-Group Entry*" on page 44.

PCR: 03961 Module: PIM, PIM6 Level: 2

The PIM-DM prune expiry time was not reset when a *State Refresh* message was received. This issue has been resolved.

PCR: 31104 Module: OSPF Level: 2

Occasionally when a device rebooted its OSPF routes were missing from the route table. This issue has been resolved.

PCR: 31125 Module: IPG Level: 3

The ADD IP ARP command returned an error message referring to the value specified for the ETHERNET parameter when that parameter was not specified or allowed. This issue has been resolved.

PCR: 31160 Module: IPG Level: 2

A memory leak occurred if DNS relay was configured, and the device kept receiving DNS *Query* packets. This issue has been resolved.

PCR: 31176 Module: PIM6 Level: 2

PIM6 was not sending unicast bootstrap messages to new neighbours. This issue has been resolved.

PCR: 31178 Module: FIREWALL Level: 4

If the SMTP Proxy detected a third party relay attack, the "`SMTP third party relay attack`" trigger message was not displayed. This issue has been resolved.

PCR: 31202 Module: QOS Level: 3

The HWQUEUE parameter in the SET QOS HWQUEUE command incorrectly accepted values from 0 to 9999. The upper limit for this parameter is 3. This issue has been resolved. The correct limit is now enforced.

PCR: 31211 Module: SWI Level: 2

On Rapier and AT-8700XL switches, duplicate forwarding switch filter entries were sometimes generated on ports defined as 802.1x authenticators. This occurred when the value of the PIGGYBACK parameter was modified using the SET PORTAUTH PORT TYPE=AUTHENTICATOR command. This issue has been resolved.

PCR: 31212 Module: GARP Level: 3

GARP packets were incorrectly transmitted out of a port when it had STP enabled but was not in the STP Forwarding state. This issue has been resolved.

PCR: 31220 Module: OSPF Level: 2

OSPF neighbours did not reach the Full state when IP route filters were applied. This issue has been resolved.

PCR: 31222 Module: SWI Level: 2

A fatal error could occur when the SET SWITCH MIRROR command was executed for the first time. This issue has been resolved.

PCR: 31223 Module: IPV6 Level: 3

The neighbour discovery timeout has been set to 3 seconds in ICMPv6 to speed up Destination Unreachable detection.

PCR: 31224 Module: IPG Level: 3

The *badQuery* and *badRouterMsg* counters in the SHOW IGMP and SHOW IGMPSNOOPING commands were not incrementing correctly. This issue has been resolved.

PCR: 31230 Module: OSPF Level: 3

When an Inter-area route went down and the only other route to the destination was an AS-External route, the AS-External route was not selected. This issue has been resolved.

PCR: 31232 Module: TTY

An enhancement allows the key sequence Ctrl-Q to delete remaining text due for output to the console when in continuous paging mode. Once the text is cleared, the command prompt is restored.

The feature will mainly be useful when a SHOW command is executed that generates a large amount of output, which could take several minutes to stream to the console. It will not be effective for any commands that cause the streaming of output to continue until another command is executed (such as ENABLE or DISABLE DEBUG commands).

PCR: 31233 Module: L3F Level: 2

A filter entry was lost when the SET SWITCH L3FILTER ENTRY command did not succeed. This issue has been resolved.

PCR: 31235 Module: BRG, VLAN, PPP

An enhancement adds partial support for PPP Bridging Control Protocol (BCP). There are 10 options to this protocol, and this patch implements option number 8. With option 8, the local or peer bridge can be enabled to receive IEEE 802 tagged frames.

To enable the receipt of IEEE 802 tagged frames, use the command:

```
enable bridge tagged
```

This command enables BCP option 8 negotiation with the peer at the other end of the bridge.

To disable the receipt of IEEE 802 tagged frames, use the command:

```
disable bridge tagged
```

This command disables BCP option 8 negotiation with the peer at the other end of the bridge.

To see whether the local or peer bridge is enabled or disabled for the receipt of IEEE 802 tagged frames, use the command:

```
show bridge
```

PCR: 31236 Module: IPV6 Level: 3

Link-local addresses can only be unicast addresses. If a link-local address was added as an anycast address, no error message was returned. This issue has been resolved. Now, an error message is returned stating that a link-local address must be a unicast address.

PCR: 31239 Module: IPV6 Level: 3

The Maximum Transmission Unit (MTU) was not always set to the MTU value in the ICMP Packet Too Big Message sent from the device. This issue has been resolved.

PCR: 31247 Module: VLAN, IPG Level: 2

After IGMP snooping was disabled, multicast data was not flooded to VLANs. This was because the multicast route forwarding port map was cleared. This issue has been resolved.

PCR: 31253 Module: SWI, SW56 Level: 2

The forwarding database table sometimes did not update correctly when multiple packets with the same MAC source address were sent to the switch via different ports. This issue has been resolved.

PCR: 31259 Module: DHCP Level: 2

When the DHCP server rejected a *DHCPRequest* message, the requested IP address was not logged correctly. This issue has been resolved.

PCR: 31264 Module: USER Level: 3

The command:

```
reset user[=login-name] [counters[={all|global|user}]]
```

did not permit the valid combination of specifying a USER login name without the optional COUNTER parameter. This issue has been resolved.

PCR: 31268 Module: IPG Level: 2

PCR 31128 introduced an issue that occasionally caused a fatal error with IP flows. This issue has been resolved.

PCR: 40003 Module: FIREWALL Level: 2

A rule that was defined to change the UDP port did not succeed when standard NAT was configured. This issue has been resolved.

PCR: 40006 Module: LOG Level: 2

Executing the SHOW DEBUG command caused a fatal error if the temporary log had been destroyed with the DESTROY LOG OUTPUT=TEMPORARY command. This issue has been resolved.

PCR: 40007 Module: FIREWALL Level: 2

When an interface-based enhanced NAT was defined in a firewall policy, and a reverse NAT rule was defined to redirect traffic to a proxy server, the reverse NAT did not work correctly. The proxy server did not receive any traffic from the device. This issue has been resolved.

PCR: 40008 Module: NTP Level: 3

When the device operated in NTP Client mode, the SHOW TIME command sometimes displayed the incorrect time. This issue has been resolved.

PCR: 40011 Module: OSPF Level: 3

The ADD OSPF INTERFACE=virt0-0 command was incorrectly written to the configuration file. The interface virt0-0 can not be added as an OSPF interface. The correct command, ADD OSPF INTERFACE=virt0, is now written to the configuration file by the CREATE CONFIG command.

PCR: 40012 Module: IPG, OSPF Level: 2

The device sometimes rebooted when OSPF on demand was enabled for PPP. This issue has been resolved.

PCR: 40020 Module: SW56 Level: 3

When a port's ingress limit was set to less than 1000 with the INGRESSLIMIT parameter in the SET SWITCH PORT command, sending packets to a tagged port caused FCS errors on transmission. This issue has been resolved.

PCR: 40023 Module: IPG Level: 2

The timeout interval for IGMP group membership now conforms to RFC 2236 for IGMPv2.

PCR: 40025 Module: Firewall

Firewall NAT ARP response enhancement

Introduction

WAN connections such as those used for connecting to the Internet, sometimes utilise Ethernet interfaces. When connected in this way, a router that is also acting as a NAT device must be able to respond to ARP requests for *any* of its global IP addresses. Failure to do this will prevent any upstream devices such as ISP servers from forwarding packets to these (global) addresses, even though the router may in other respects be correctly configured.

What does the enhancement do?

This enhancement enables the NAT router to respond to any of its configured global IP addresses, not just those addresses configured to its IP interfaces or reachable by enabling proxy ARP.

Example

If a NAT router, acting as a firewall, is translating the source address of an outgoing packet to an address other than that of its own IP interface, the firewall router needs to ARP respond for this source address in order to receive and translate returning packets.

Using commands for this enhancement

This feature is always enabled when NAT rules and interface-based NATs are created, so no configuration is required. However, it is now possible to enable and disable ARP debugging on a firewall policy. Also, a new command, SHOW FIREWALL ARP displays the addresses for which the firewall may respond to ARP requests.

To enable the display of debugging information relating to ARP requests that are processed by the firewall, use the command:

```
ENABLE FIREWALL POLICY=policy-name DEBUG=ARP
```

To disable the display of debugging information relating to ARP requests that are processed by the firewall, use the command:

```
DISABLE FIREWALL POLICY=policy-name DEBUG=ARP
```

To display the addresses for which the firewall may ARP respond, use the command:

```
SHOW FIREWALL ARP [POLICY=policy-name]
```

Example output for the SHOW FIREWALL ARP command is shown in Figure 1:

Figure 1: Example output from the SHOW FIREWALL ARP command

```
IP               ARP Interfaces  NAT Type  Int        Gbl Int    Rule
(range)          Policy
-------------------------------------------------------------------------------
172.20.8.50      Public          Int based eth0-0     eth1-0     -
                 Office
172.20.8.57      All Public      Rule      eth0-1     -          1
 -172.20.8.62    LAN
-------------------------------------------------------------------------------
```

Table 3: Parameters displayed in the output of the SHOW FIREWALL ARP command

Parameter	Meaning
IP (range)	An IP address (or range of addresses) for which the device may need to make an ARP response.
Policy	The name of the policy whose NAT configuration the IP address (range) belongs to.
ARP interfaces	The interfaces within the policy that ARP requests for the IP address (range) are permitted on; one of "Public", "All Public", "Private", or "All Private". "Public" means that ARP requests are permitted on the public interface listed in the "Gbl Int" field. "Private" means ARP requests are permitted on the private interface specified by the "Int" field. "All Public" means ARP requests are permitted on all of the policy's public interfaces. "All Private" means ARP requests are permitted on all of the policy's private intrfaces.
NAT Type	The type of NAT that the IP address (range) is associated with; one of "Int based" or "Rule". "Int based" means that the address (range) was specified by an interface-based NAT configuration with the ADD FIREWALL POLICY NAT command. "Rule" means the address (range) was specified by a NAT rule configured with the ADD FIREWALL POLICY RULE command with ACTION=NAT specified.
Int	The private interface associated with the NAT configuration. If NAT Type is "Int based" then this is the private interface specified by the INTERFACE parameter in the ADD FIREWALL POLICY NAT command. If the NAT type is "Rule" then this is the name of the interface the rule is attached to, if it is a private interface. "-" indicates the rule is attached to a public interface (see the "Gbl Int" parameter).
Gbl Int	The public interface associated with the NAT configuration. If NAT Type is "Int based" then this is the public interface specified by the GBLINTERFACE parameter in the ADD FIREWALL POLICY NAT command. If the NAT type is "Rule" then this is the name of the interface the rule is attached to, if it is a public interface. "-" indicates that the rule is attached to a private interface (see the Int parameter).
Rule	The number of the rule that this entry is associated with. If NAT type is "Int based" no value is displayed.

PCR: 40031 Module: PCI, SWI, GUI, HTTP, CORE, DIAG, FFS, INSTALL

Support has been added for NEBS compliant versions of the AC and DC models of Rapier 24i and AT-8724XL.

PCR: 40038 Module: OSPF Level: 2

After a Summary LSA for the default route in a stub area had been refreshed by an Area Border Router, and the Area Border Router was restarted, the Summary LSA was not advertised into the stub area again. This issue has been resolved.

PCR: 40070 Module: CORE Level: 3

On AT-8800 series switches, a warning log message was generated for the fan's status when there was more than a 20% variation in fan speed between "Actual" and "Expected". This has been changed so the log message is only generated when the fan stops.

PCR: 40091 Module: IPG Level: 2

When there were multiple routes to the same destination, the wrong port number occasionally appeared in a Layer 3 switch hardware table entry. This could lead to incorrect traffic flow. This issue has been resolved.

Features in 86261-04

Patch file details are listed in Table 4:

Table 4: Patch file details for Patch 86261-04.

Base Software Release File	86-261.rez
Patch Release Date	19-Nov-2003
Compressed Patch File Name	86261-04.paz
Compressed Patch File Size	261628 bytes

Patch 86261-04 includes all issues resolved and enhancements released in previous patches for Software Release 2.6.1, and the following enhancements:

PCR: 03910 Module: IPG Level: 3

When RIP demand mode was enabled, and one interface changed to a reachable state, the triggered *Request* packet was not sent from that interface, and triggered *Response* packets were not sent from all other RIP interfaces. This resulted in slow convergence of routing tables across the network. This issue has been resolved.

PCR: 03927 Module: BRI

Support has been added for the AT-AR021 (S) BRI-S/T PIC (Port Interface Card) with basic rate ISDN.

PCR: 03967 Module: IPG Level: 2

RIP did not send the correct next hop address if the route originated from a different subnet to that of the egress interface. This issue has been resolved.

PCR: 03970 Module: IPV6 Level: 3

If an IPv6 filter that blocked traffic on a VLAN interface was removed, the traffic was still blocked. This issue has been resolved.

PCR: 03978 Module: OSPF Level: 3

Occasionally an error occurred with OSPF's route table calculation, so all routes in the network were not discovered. The error only happened with a network topology that involved connections between routers via both a Point to Point link and a transit network link. This issue has been resolved. A new command has been added that forces a route table recalculation by rerunning the Shortest Path First calculation. The command is:

```
RESET OSPF SPF [DEBUG]
```

If DEBUG is specified, debugging information for the route table calculation is output to the port from which the command was executed. SPF debugging can be turned on for every route table calculation using the ENABLE OSPF DEBUG=SPF command, but this will be overridden if DEBUG is specified with the RESET OSPF SPF command.

PCR: 31009 Module: HTTP Level: 3

The server string was not copied correctly into an HTTP file request when loading information from the configuration script. This issue has been resolved.

PCR: 31064 Module: SWI Level: 2

When 10/100 copper ports were disabled with the DISABLE SWITCH PORT command, their link state was still UP. This issue has been resolved.

PCR: 31072 Module: SWI Level: 3

If the DISABLE SWITCH PORT command appeared in the configuration script, an interface could come up even though *ifAdminStatus* was set to 'down'. This issue has been resolved.

PCR: 31084 Module: IPV6 Level: 2

A fatal error sometimes occurred because of incorrect responses to Neighbour Solicitation messages. This issue has been resolved.

PCR: 31093 Module: SWI Level: 1

If a switch port was disabled on a switch running STP, traffic was sometimes not passed through that port after it was re-enabled. This issue has been resolved.

PCR: 31096 Module: FFS Level: 3

The SHOW FILE command caused an error when the displayed file had a duplicate entry due to file size mismatch. This issue has been resolved. An error message is now logged when the SHOW FILE command detects a duplicate file. The first FFS file will be deleted when a duplicate exists.

PCR: 31098 Module: DHCP Level: 3

Static DHCP address ranges were not reclaimed if the *Reclaim* operation was interrupted by the interface going down. This issue has been resolved.

PCR: 31100 Module: L2TP Level: 3

An error occurred in L2TP when call names consisted of numeric characters only. This issue has been resolved. The ADD L2TP CALL command now only accepts call names that contain at least one alphabetic character.

PCR: 31119 Module: LOG Level: 2

The maximum value that the MESSAGES parameter accepted for the CREATE LOG OUTPUT command was different from the value that could be set with the SET LOG OUTPUT command. The DESTROY LOG OUTPUT command did not release the NVS memory that was reserved for the output. These issues have been resolved.

PCR: 31132 Module: DHCP Level: 2

The DHCP server did not take any action when it received a DHCP *decline* packet. This was because the device only checked the *ciaddr* field in the packet, and not the *RequestedIPAddress* option. This issue has been resolved.

PCR: 31133 Module: IPG

This PCR introduces an enhancement that extends an issue that was resolved in PCR 03890, in which switch port entries are only created for special router multicast addresses. It is now possible to specify reserved multicast addresses that will be treated as multicast packets from routers. Use the following commands to configure this feature.

ADD IGMPSNOOPING ROUTERADDRESS

Syntax

```
ADD IGMPSNOOPING ROUTERADDRESS=ipaddr[,...]
```

Description

where:

- *ipaddr* is a reserved IP multicast address in dotted decimal notation.

This command adds reserved IP multicast addresses to the list of router multicast addresses. The IP address specified must be within the range 224.0.0.1 to 224.0.0.255. This command is only valid if the IGMP snooping router mode is set to IP with the SET IGMPSNOOPING ROUTERMODE command.

SET IGMPSNOOPING ROUTERMODE

Syntax

```
SET IGMPSNOOPING ROUTERMODE=
   {ALL|DEFAULT|IP|MULTICASTROUTER|NONE}
```

Description

This command sets the mode of operation for IGMP Snooping.

If ALL is specified, all reserved multicast addresses (i.e. 2240.0.1 to 224.0.0.255) are treated as router multicast addresses.

If DEFAULT is specified, the following addresses are treated as router multicast addresses:

- IGMP Query: 224.0.0.1
- All routers on this subnet: 224.0.0.2
- DVMRP Routers: 224.0.0.4
- OSPFIGP all routers: 224.0.0.5
- OSPFIGP designated routers: 224.0.0.6
- RIP2 routers: 224.0.0.9

- All PIM routers: 224.0.0.13
- All CBT routers: 224.0.0.15

If IP is specified, addresses that are treated as router multicast addresses are specified with the ADD/DELETE IGMPSNOOPING ROUTERADDRESS command. In this mode, the switch will retain previous addresses that have already been specified.

If MULTICAST is specified, the following addresses are treated as router multicast addresses:

- DVMRP Routers: 224.0.0.4
- All PIM routers: 224.0.0.13

If NONE is specified, no router ports are created.

DELETE IGMPSNOOPING ROUTERADDRESS

Syntax `DELETE IGMPSNOOPING ROUTERADDRESS=ipaddr[,...]`

where

- *ipaddr* is a reserved IP multicast address in dotted decimal notation.

Description This command deletes reserved IP multicast addresses from the list of router multicast addresses. The IP address specified must be within the range 224.0.0.1 to 224.0.0.255. This command is only valid if the IGMP snooping router mode is set to IP with the SET IGMPSNOOPING ROUTERMODE command.

SHOW IGMPSNOOPING ROUTERADDRESS

Syntax `SHOW IGMPSNOOPING ROUTERADDRESS`

Description This command displays information about the list of configured IP multicast router addresses currently configured on the switch (Figure 2).

Figure 2: Example output for SHOW IGMPSNOOPING ROUTERADDRESS

```
IGMP Snooping Router Address
------------------------------------------------------------------------
IGMP Snooping Router Mode ..... IP

Router Address List
-------------------------------
224.0.0.4
224.0.0.6
224.0.0.80
224.0.0.43
224.0.0.23
224.0.0.15
224.0.0.60
------------------------------------------------------------------------
```

PCR: 31134 Module: RSTP Level: 2

Bridges transmitted BPDUs at the rate specified by the local *helloTime* value when they were not the root bridge. This is the behaviour specified in 802.1w-2001. This behaviour can cause instability in the spanning tree when bridges are configured with different *helloTime* values, especially when the root bridge's *helloTime* is significantly less than other bridges in the tree. This issue has been resolved. Non-root bridges now adopt the root bridge's *helloTime* value propagated in BPDUs.

PCR: 31135 Module: IPV6 Level: 3

The ADD IPV6 HOST command accepted an invalid IPv6 address. This issue has been resolved.

PCR: 31140 Module: FIREWALL Level: 4

The firewall sent an erroneous IPSPOOF attack message when processing large packets. This issue has been resolved.

PCR: 31145 Module: SWI Level: 3

The port counters were not incremented:

- *ifInDiscards*
- *ifinErrors*
- *ifOutDiscards*
- *ifOutErrors*

This issue has been resolved.

PCR: 31146 Module: SWI Level: 3

The following SNMP MIB objects could not be set:

- *Dot1dStpPriority*
- *Dot1dStpBridgeMaxAge*
- *Dot1dStpBridgeHelloTime*
- *Dot1dStpBridgeForwardDelay*

This issue has been resolved.

PCR: 31147 Module: DHCP Level: 3

DHCP was incorrectly using the directly connected network interface source IP address as the source IP address of packets it generates. This issue has been resolved. DHCP now uses the local IP address as the source address for the packets it generates when a local IP interface address is set. If a local IP interface address is not set, then it uses the IP address of the interface where packets are sent from as the source address.

PCR: 31148 Module: PIM, PIM6 Level: 2

When the device rebooted with PIM or PIM6 enabled, it sometimes did not send a *Hello* packet quickly enough. This issue has been resolved.

PCR: 31152 Module: DHCP Level: 2

When a DHCP client was in the renewing state, and it sent a DHCP *Request*, the device did not add the ARP entry to the ARP table. Instead, the device generated an ARP *Request* in order to transmit the DHCP *Ack*. This caused a broadcast storm in the network when the client kept sending DHCP *Request*s. This issue occurred because the *ciaddr* field, not the *giaddr* field, was checked in the *Request* packet when the device determined whether to add the ARP entry. This issue has been resolved.

PCR: 31153 Module: IPG Level: 4

In the output of the SHOW IP DNS CACHE command, "TTL" was displayed as seconds. This has been changed to minutes because the TTL is updated every minute.

PCR: 31154 Module: STP Level: 4

The current implementation of RSTP conforms to the IEEE standard 802.1w-2001. However, several minor deviations from the standard are possible without having a functional impact on the behaviour of RSTP. These changes are useful for debugging RSTP, and tidy up aspects of RSTP that sometimes have no purpose. The following three variations have been implemented:

- The *Learning* and *Forwarding* flags are set in BPDUs to indicate the state of the Port State Transition state machine.
- The *Agreement* flag is set in BPDUs only when a Root Port is explicitly agreeing to a proposal from a designated port. Do not set the *Agreement* flag in BPDUs transmitted by Designated Ports.
- The *Proposal* flag is not set in a BPDU sent by a designated port once the port has reached the forwarding state.

PCR: 31158 Module: CORE Level: 3

On AT-8800 series switches, when the fan status changed, the device did not send a SNMP trap and log. When the temperature was above the allowable threshold, the device sent the wrong SNMP trap. This issue has been resolved. Also, the temperature thresholds of the AT-8824 and AT-8848 have been set to different values of 62º C and 67º C respectively.

PCR: 31159 Module: FW, VLAN Level: 2

Static ARP entries sometimes prevented the firewall from working correctly. This is because when an VLAN interface is added to the firewall, the CPU takes over the routing from the switch silicon in order to inspect the packet. Hence all the Layer 3 route entries must be deleted. However, static ARP Layer 3 entries were not being deleted from the silicon. This issue has been resolved. When interface is added to the firewall, all hardware layer 3 routing is now turned off to allow the firewall to inspect packets.

PCR: 31161 Module: LOG Level: 3

If the number of messages to be stored in the TEMPORARY log output was changed with the SET LOG OUTPUT MESSAGE command, the SHOW LOG command output did not return any matching log messages. This issue has been resolved. Existing messages are now displayed.

PCR: 31162 Module: SWI Level: 2

A STP topology change incorrectly deleted static ARP entries. This issue has been resolved.

PCR: 31167 Module: IPG Level: 2

IP MVR member ports were not timing out. MVR member ports now timeout in the same way as IP IGMP ports. The timeout values are configured by IGMP. Also, IGMP interfaces were incorrectly being enabled and disabled by MVR. This issue has been resolved.

PCR: 31170 Module: SWI Level: 2

After an AT-8800 series switch was powered down or rebooted, non-auto negotiating copper GBICs were not handled correctly. This issue has been resolved.

PCR: 31171 Module: PORTAUTH, USER,STP Level: 2

This PCR enhances the robustness of the 802.1x port authentication protocol.

PCR: 31174 Module: IPG Level: 2

If a device had IPSec and firewall enabled, it could not handle long ICMP packets even when enhanced fragment handling was enabled on the firewall. If a long packet is passed to the firewall for processing, the firewall chains the fragmented packets. The firewall can process chained packets, but IPSec could not process these packets, and dropped them. This was only an issue for packets between 1723 and 1799 bytes long. This issue has been resolved. The way IP processes fragmented packets has been changed so that IPsec no longer drops chained packets.

PCR: 31179 Module: SWI Level: 3

Addresses learned with static port security were not added to the configuration when the CREATE CONFIG command was executed. This issue has been resolved.

PCR: 31180 Module: USER Level: 2

The following commands did not require security officer privilege when the device was in security mode, but this privilege should have been required:

- ADD USER
- SET USER
- DELETE USER
- PURGE USER
- ENABLE USER
- DISABLE USER
- RESET USER

This issue has been resolved. Security officer privilege is now required for these commands when security mode is enabled with the ENABLE SYSTEM SECURITY_MODE command.

PCR: 31184 Module: SW56 Level: 2

Some issues occurred on 48 port Rapier series switches when MAC addresses were learned and then relearned on a different port. These issues have been resolved.

PCR: 31185 Module: SWI Level: 2

Tagged ports did not tag packets received from the bridge before transmitting them. This issue has been resolved.

PCR: 31190 Module: SWI, SW56 Level: 2

When static port security was enabled with the RELEARN parameter in the SET SWITCH PORT command, and a switch port was reset or unplugged, the MAC entries were removed (unlearned) from the forwarding database table. The MAC entries should only be removed when dynamic port security is in use. This issue has been resolved.

PCR: 31191 Module: PORTAUTH, USER Level: 2

A device in a supplicant role failed to authenticate if it used EAP-MD5 encryption with Windows 2000 or 2003 Server as the RADIUS server. Also, a fatal error occurred if the device received EAPOL packets containing a very large value in the packet length field. These issues have been resolved.

PCR: 31192 Module: LOG Level: 3

Syslog entries did not contain the date, time and unique identifier of the message source. This issue has been resolved. The CREATE LOG OUTPUT and SET LOG OUTPUT commands have been modified to control whether or not this information is included.

The following parameter has been added to the CREATE LOG OUTPUT and SET LOG OUTPUT commands:

```
[SYSLOGFORMAT=NORMAL|EXTENDED]
```

If the SYSLOGFORMAT parameter is set to EXTENDED the date, time and unique identifier of message source are included in the syslog message. If the parameter is set to NORMAL, this information is not included in the syslog message. The default is NORMAL.

PCR: 31193 Module: IPG Level: 2

When IP multicasting was not enabled, all IP multicast packets were passed to the CPU, causing overloading. This issue has been resolved. Now, if IP multicasting is not enabled, these packets are not sent to the CPU.

PCR: 31194 Module: BGP, IP Level: 3

When executing the command:

```
ADD IP ROUTEMAP ENTRY SET ASPATH
```

followed by the command:

```
ADD IP ROUTEMAP ENTRY COMMUNITY ADD=YES
```

where the values for ROUTEMAP and ENTRY were the same in both commands, the second command failed and returned a "`ROUTEMAP clause already exists`" error message. This issue has been resolved.

PCR: 31201 Module: SW56, SWI Level: 2

Fibre GBICs on Rapier and AT-8800 series switches sometimes did not establish a link when powered on for the first time. This issue has been resolved.

PCR: 31205 Module: VRRP Level: 3

Two VRRP log messages were displayed when they should not have been. The log messages were:

```
Vrrp 1: Vlan vlan2 10 Port Failed decrementing priority by 20
Vrrp 1: Vlan vlan2 1 Port up incrementing priority by 2
```

This issue has been resolved. These messages are now displayed at the correct time.

PCR: 31215 Module: SNMP Level: 4

The entry for the *FanAndPs* group in the private MIB did not return valid information. This issue has been resolved.

PCR: 31221 Module: SW56 Level: 1

On AT-8848 switches, a STP loop occurred if the Gigabit uplink port 49 was in the blocking state. This issue has been resolved.

PCR: 31237 Module: CORE Level: 3

Sometimes the initialisation of fan and temperature monitoring was delayed, and this was reported as a failure. This issue has been resolved. The delay was temporary and is no longer reported as a failure.

Features in 86261-03

Patch file details are listed in Table 5:

Table 5: Patch file details for Patch 86261-03.

Base Software Release File	86-261.rez
Patch Release Date	7-Nov-2003
Compressed Patch File Name	86261-03.paz
Compressed Patch File Size	176500 bytes

Patch 86261-03 includes all issues resolved and enhancements released in previous patches for Software Release 2.6.1, and the following enhancements:

PCR: 31164 Module: SWI Level: 2

On AT-8800 Series switches, fibre GBICs were treated like copper GBICs if the switch had been powered off for more than one minute. This issue has been resolved.

Features in 86261-02

Patch file details are listed in Table 6:

Table 6: Patch file details for Patch 86261-02.

Base Software Release File	86-261.rez
Patch Release Date	3-Nov-2003
Compressed Patch File Name	86261-02.paz
Compressed Patch File Size	384839 bytes

Patch 86261-02 includes all issues resolved and enhancements released in previous patches for Software Release 2.6.1, and the following enhancements:

PCR: 03726 Module: TTY, USER Level: 3

The time recorded when a user logged in was overwritten when the same user logged in a second time while the original connection was still active. This meant the SHOW USER command displayed the same time for both connections. This issue has been resolved.

PCR: 03781 Module: STP Level: 2

A buffer leak occurred when rapid STP was specified with the SET STP MODE=RAPID command, but STP had not been enabled with the ENABLE STP command. This issue has been resolved.

PCR: 03855 Module: IPG Level: 2

Previously, an IP multicast stream destined for an IP multicast group was forwarded out ports in the All Groups IGMP snooping entry even after this entry had timed out. This issue has been resolved.

PCR: 03861 Module: IPV6 Level: 2

When a connector was plugged into one physical interface, the RIPng request packet was erroneously transmitted from all interfaces on the switch. This issue has been resolved.

PCR: 03873 Module: IPG Level: 4

The STATIC and INTERFACE options have been removed from the PROTOCOL parameter in the ADD IP ROUTE FILTER and SET IP ROUTE FILTER commands. These parameters were redundant because received static and interface routes are always added to the route table.

PCR: 03890 Module: IGMP, SWI Level: 2

The switch was adding a router port for multicast packets to destinations with an address in the range 224.0.0.x. Switch port entries are now only created for special router multicast addresses.

PCR: 03905 Module: TTY Level: 3

A fatal error occurred in the text editor while selecting blocks and scrolling up. This issue has been resolved.

PCR: 03926 Module: PIM Level: 2

Repeated *Assert* messages were sent after the prune limit expired. This issue has been resolved. The default dense mode prune hold time has been changed from 60 seconds to 210 seconds.

PCR: 03932 Module: PING Level: 3

The ADD PING POLL command had a duplicate entry for the LENGTH parameter in the dynamic PING configuration if LENGTH was not the default value. This generated an incorrect configuration file when the CREATE CONFIG command was executed. This issue has been resolved.

PCR: 03935 Module: ISAKMP Level: 3

ISAKMP debug messages now correctly output IPv6 addresses when using IPv6, and IPv4 addresses when using IPv4.

PCR: 03937 Module: IPSEC Level: 2

The IP version of packets was not being checked, so an IPv4 packet could match an IPv6 IPSec policy. This issue has been resolved.

PCR: 03940 Module: PKI Level: 1

The following two issues have been resolved:

- Large CRL files were not decoded correctly.
- The certificate database was not validated immediately after the CRL file was updated.

PCR: 03941 Module: FIREWALL Level: 2

TCP *Keepalive* packets for FTP sessions were passing through the firewall during the TCP setup stage with TCP Setup Proxy enabled. *Keepalive* packets include sequence numbers that have already been acknowledged. Such packets now fail stateful inspections and are dropped by the FTP application-level gateway.

PCR: 03954 Module: IPV6 Level: 2

An anycast address could not be assigned when the prefix for the anycast address had previously been assigned on that interface. This issue has been resolved.

PCR: 03958 Module: FIREWALL Level: 2

The ADD FIREWALL POLICY RULE and SET FIREWALL POLICY RULE commands no longer accept the GBLREMOTEIP parameter with standard NAT, or enhanced NAT for a private interface.

PCR: 03965 Module: IPSEC Level: 3

IPv6 used the same SA soft expiry timer at both ends of a link, which used memory unnecessarily. This issue has been resolved.

PCR: 03973 Module: IPG Level: 3

When equal cost multipath routes were used, the IP option field for trace route was not applied correctly. This issue has been resolved.

PCR: 03974 Module: IPG Level: 3

The IP filter blocked ping packets when the ACTION for these was set to INCLUDE with the ADD IP FILTER command. This issue was caused by the default SMASK value of 255.255.255.255, which blocked all incoming packets. This issue has been resolved.

PCR: 03982 Module: FIREWALL Level: 3

The SMTP proxy did not correctly filter sessions where messages were fragmented. This had the potential to prevent the detection of third-party relay attacks. This issue has been resolved.

PCR: 03986 Module: BGP, IPG Level: 2

Route flapping occurred if an interface went down and there was another route to that interface's next hop. This issue has been resolved.

PCR: 03993 Module: FIREWALL Level: 4

The AUTHENTICATION parameter has been removed from the "?" CLI help for firewall commands. This was not a valid parameter.

PCR: 03994 Module: SWI Level: 2

Port speed and duplex values set with the SET SWITCH PORT SPEED command were sometimes not applied correctly. This issue has been resolved.

PCR: 03996 Module: FIREWALL Level: 2

Occasionally some firewall timers stopped early, resulting in sessions being removed prematurely. Because of this, TCP *Reset* packets could be sent by the firewall before TCP sessions were finished. This issue has been resolved.

PCR: 31001 Module: DHCP Level: 2

When executing the SET DHCP POLICY, DELETE DHCP POLICY and DESTROY DHCP POLICY commands, memory was not de-allocated correctly. This issue has been resolved.

PCR: 31002 Module: UTILITY Level: 2

Sometimes the device rebooted when a severe multicast storm occurred due to a loop in the network. This issue has been resolved.

PCR: 31012 Module: PIM Level: 2

The *prune* time limit was not being cancelled when an IGMP join was received by the switch. This was forcing the switch to send a *Graft* message in the upstream direction. This issue has been resolved by cancelling the prune time limit whenever an IGMP *Join* is received.

PCR: 31013 Module: SWI Level: 2

If ports were set to a speed of 100m when creating a switch trunk, the speed could not subsequently be set to 1000m, even if the ports were capable of that speed. This issue has been resolved.

PCR: 31015 Module: STP Level: 2

The PORT and PORTPRIORITY parameters of the STP PORT command were not always updating switch instances on ports that are members of multiple STP instances. This issue has been resolved.

PCR: 31017 Module: NTP Level: 3

The *RootDispersion* value in NTP packets was negative. RFC 1305 states that only positive values greater than zero are valid. This issue has been resolved.

PCR: 31019 Module: PIM6 Level: 2

The checksum for the PIMv2 *Register* message for IPv6 was not being calculated correctly. This issue has been resolved.

PCR: 031020 Module: PIM Level: 2

When the switch received a generation ID change message, it was not responding by sending a PIM HELLO message. This issue has been resolved.

PCR: 31028 Module: BGP Level: 2

BGP did not always send *Withdrawn* advertisements when a route went down. This issue has been resolved.

PCR: 31036 Module: CORE Level: 4

The output of the SHOW SYSTEM command has been changed on AT-8800 Series switches. The output now includes the status of the temperature and fan. See Figure 3 on page 31 and Table 7 on page 32.

Figure 3: Example output from the SHOW SYSTEM command.

```
Switch System Status                              Time 08:32:23 Date 06-Nov-2003.
Board      ID  Bay Board Name                          Rev    Serial number
-------------------------------------------------------------------------------
Base      148      8848                               P3-7   58476578
-------------------------------------------------------------------------------
Memory -   DRAM : 65536 kB    FLASH : 32768 kB
-------------------------------------------------------------------------------
SysDescription
AT-8848 version 2.6.1-02 30-Oct-2003
SysContact

SysLocation

SysName

SysDistName

SysUpTime
3608 ( 00:00:36 )
Boot Image      : rmb106.fbr size 496544 06-Nov-2003
Software Version: 2.6.1-02 30-Oct-2003
Release Version : 2.6.1-00 20-Aug-2003
Patch Installed : Release patch
Territory       : japan
Help File       : help.hlp

Main PSU        : On
RPS Monitor     : Off

Current Temperature : Normal

Fan     Status
---------------
1       Normal
2       Normal
3       Normal
4       Normal
---------------

Configuration

Boot configuration file: Not set
Current configuration: None

Security Mode   : Disabled

Patch files
Name            Device     Size      Version
-----------------------------------------
86261-02.paz    flash      170996    2.6.1-2
-----------------------------------------
```

Table 7: New parameters displayed in the output of the SHOW SYSTEM command for AT-8800 series switches.

Parameter	Meaning
Current Temperature	The status of the switch's temperature. "Normal" means the switch is operating in the required temperature range. "Warning" means there has been a temperature-related error requiring attention. "Failed" means there was an internal error while reading the temperature.
Fan Status	The status of each of the switch's four fans. "Normal" means the fan is operating as expected. "Warning" means a fan is operating outside the desired range. "Failed" means there was an internal error while reading the fan status.

PCR: 31040 Module: PIM Level: 2

When two devices are BSR candidates, and have the same preference set with the SET PIM BSRCANDIDATE PREFERENCE command, the device with the higher IP address was not elected as the candidate. This issue has been resolved.

PCR: 31041 Module: PIM Level: 3

A *Prune* message sent to an old RP neighbour was ignored when a new unicast route was learned. This issue has been resolved.

PCR: 31042 Module: PIM Level: 3

On Rapier series switches, an *Assert* message was not sent after the prune limit expired. This issue has been resolved.

PCR: 31044 Module: SWI Level: 4

The log message "`IGMP Snooping is active, L3FILT is activated`" has been changed to "`IGMP packet trapping is active, L3FILT is activated`". The revised message is clearer when IGMP is enabled and IGMP snooping is disabled.

PCR: 31052 Module: FIREWALL Level: 3

The following changes have been made to the ADD FIREWALL POLICY RULE and SET FIREWALL POLICY RULE commands:

- An IP address range for the IP parameter is now only accepted when enhanced NAT is configured.
- An IP address range for GBLREMOTE parameter is now only accepted when reverse or reverse-enhanced NAT is configured.
- The GBLIP parameter is not accepted for a public interface when enhanced NAT is configured.

PCR: 31057 Module: SW56 Level: 4

Port link status LEDs on disabled ports were not always operating correctly on AT-8800 Series switches. This issue has been resolved.

PCR: 31058 Module: NTP Level: 3

When the interval between the NTP server and client exceeded 34 years 9 days and 10 hours, the time set on the client was incorrect. This issue has been resolved.

PCR: 31063 Module: IPG Level: 2

MVR was not operating if IGMP had not been enabled. This issue has been resolved.

PCR: 31068 Module: STP Level: 2

A fatal error occurred when the PURGE STP command was executed when STP instances were defined with VLAN members. This issue has been resolved.

PCR: 31071 Module: SWI Level: 4

The warning given when a QoS policy is active on a port operating at reduced speed has been changed to reflect the problem more accurately. The old message was:

```
Warning (2087343): Port <Port num> is currently used in QoS
policy <QoS policy num>, this policy may become incorrect
due to the port bandwidth.
```

The new message is:

```
Warning (2087350): Port <Port num> is operating at less than
its maximum speed: this may affect QoS policy <QoS policy
num>.
```

PCR: 31074 Module: PPP Level: 2

The PPP idle timer was not being updated correctly. This issue has been resolved.

PCR: 31079 Module: SW56 Level: 2

Ports sometimes stopped operating if the port speed was changed while packets still occupied the switching fabric. This issue has been resolved. All packets are now released before changes can be made to port configurations.

PCR: 31080 Module: IPv6 Level: 2

When a ping was sent to the device's link-local address, the device flooded the ICMP *Reply* packet over the VLAN. This issue has been resolved.

PCR: 31082 Module: STP Level: 2

The root bridge did not transmit BPDU messages with changed *hellotime*, *forwarddelay* and *maxage* values. This issue has been resolved.

PCR: 31085 Module: LDAP Level: 3

LDAP could not receive large messages spanning multiple packets. This issue has been resolved.

PCR: 31094 Module: FILE Level: 3

Files with lines over 132 characters in length could not be transferred using TFTP. This limit has now been raised to 1000 characters to match the maximum command line length.

PCR: 31097 Module: SW56 Level: 2

When broadcast packets were transmitted to one of two VLAN interfaces, and a ping was sent to the other interface, 10% of the pings timed out. This issue has been resolved.

PCR: 31099 Module: FIREWALL Level: 4

In the output of SHOW FIREWALL EVENT command, the DIRECTION of denied multicast packets was shown as “out”, not “in”. This issue has been resolved.

PCR: 31102 Module: DHCP Level: 2

When a boot file for DHCP was specified with the ADD DHCP POLICY FILE command, a blank space was added after the filename in the configuration. This meant the file could not be found. This issue has been resolved.

PCR: 31106 Module: MLD Level: 2

When the device received a version 1 *Query* packet, it become a non-querier on that interface, even if it should have remained as the querier. This issue has been resolved.

PCR: 31110 Module: IPV6 Level: 2

When the preference value for RIPng was changed with the SET IPV6 ROUTE PREFERENCE command, the new value was not updated in the IPV6 routing table. This issue has been resolved.

PCR: 31118 Module: SWI Level: 2

When the TYPE parameter was specified for the ADD SWITCH L3FILTER command, the type was sometimes a different value in the device’s hardware table. This issue has been resolved.

PCR: 31122 Module: RMON Level: 3

The *etherHistoryIntervalStart* node in the *etherHistoryTable* showed incorrect values for the first and last 30 second interval periods. This issue has been resolved.

PCR: 31129 Module: IPX2 Level: 2

A fatal error occurred if IPX was disabled and then re-enabled when there was a high rate of incoming IPX traffic on the device. This issue has been resolved.

PCR: 31130 Module: FFS Level: 2

In some circumstances FlashROM was corrupted. This issue has been resolved. FlashROM is now write protected.

PCR: 31137 Module: CORE Level: 4

Rapier Series switches with a DC power supply did not recognise the DC power supply. This issue has been resolved.

Features in 86261-01

Patch file details are listed in Table 8:

Table 8: Patch file details for Patch 86261-01.

Base Software Release File	86-261.rez
Patch Release Date	2-Oct-2003
Compressed Patch File Name	86261-01.paz
Compressed Patch File Size	94120 bytes

Patch 86261-01 includes the following enhancements and resolved issues:

PCR: 03268 Module: SWI Level: 1

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: 03524 Module: OSPF, IPG Level: 2

OSPF disabled RIP unless RIP was activated using the SET OSPF RIP command. This issue has been resolved.

PCR: 03798 Module: IKMP Level: 3

ISAKMP did not support the IPSec message option *ID_IPV6_ADDR_SUBNET* (RFC 2407, 4.6.2.7). ISAKMP was using the *ID_IPV6_ADDR* (RFC 2407, 4.6.2.6) option instead. This issue has been resolved.

PCR: 03826 Module: BGP Level: 2

When BGP imported routes from IP with the ADD BGP IMPORT command, and there were multiple import choices, the best IP route was not always imported. This issue has been resolved.

PCR: 03828 Module: IPV6 Level: 2

The MTU value for IPv6 PPP interfaces was always set to 1280 bytes. This MTU value is now correctly set to 1500 bytes, and 1492 bytes for PPP over Ethernet (PPPoE).

PCR: 03836 Module: OSPF Level: 2

OSPF sometimes chose routes with an infinite metric over routes with a finite metric when selecting the best local route. This issue has been resolved.

PCR: 03861 Module: IPV6 Level: 2

When a connector was plugged into one physical interface, the RIPng request packet was erroneously transmitted from all interfaces on the switch. This issue has been resolved.

PCR: 03864 Module: BGP Level: 2

BGP sent *Update* packets when the local host route table changed but did not affect BGP. Also, BGP did not send *Withdrawn* packets when there was a change in the best route. These issues have been resolved.

PCR: 03865 Module: FIREWALL Level: 2

When dual firewall policies were defined, public to private passive mode FTP transfers sometimes failed. This issue has been resolved.

PCR: 03867 Module: BGP Level: 2

BGP sometimes chose routes with an infinite metric over routes with a finite metric when selecting the best local route. This issue has been resolved.

PCR: 03875 Module: IPG Level: 2

Sometimes OSPF routes were not entered in the IP route table. This issue has been resolved.

PCR: 03876 Module: PING Level: 2

A fatal error occurred if the TRACE command was executed when a trace was already in progress. This issue has been resolved.

PCR: 03881 Module: SW56 Level: 2

On AT-8800 series switches, if a port was not set to autonegotiate, and the cable was unplugged and then plugged back in, the port stopped sending packets. This issue has been resolved.

PCR: 03882 Module: SW56 Level: 2

When port had a learn limit configured, MAC addresses were not added to the forwarding database. Also, when a MAC address was learned on a port, and then the same address was learned on another port, the forwarding database did not change to the more recently learned port. These issues have been resolved.

PCR: 03883 Module: IPG Level: 3

Some IP addresses were not displayed correctly in log messages. This issue has been resolved.

PCR: 03884 Module: IPG Level: 2

The IGMP MVR membership timeout was not operating correctly. Membership of a multicast group is now eliminated when it times out. Also, *Leave* messages were not being processed correctly, which sometimes delayed the membership timeout. These issues have been resolved.

PCR: 03885 Module: CORE Level: 3

The operation of the FAULT LED on AT-8800 series switches has been modified. Now, if there are multiple faults, resolving one fault will not turn off the LED.

PCR: 03886 Module: SW56 Level: 3

AT-8800 series switches received frames when the physical link was not established. This issue has been resolved.

PCR: 03888 Module: DHCP, TELNET Level: 2

When the device was configured as a DHCP server, a fatal error sometimes occurred when a telnet session to the device was closed while DHCP was reclaiming IP addresses. Also, a telnet error message displayed an incorrect value when a telnet command line parameter was repeated (for example, SHOW TELNET TELNET). These issues have been resolved.

PCR: 03895 Module: DHCP Level: 2

If the DHCP server had a policy name greater than 5 characters long, and a very long MERITDUMP or ROOTPATH value, the device could not correctly create the configuration. This issue has been resolved.

PCR: 03896 Module: TTY Level: 3

A fatal error occurred when a long string of text was pasted over an existing long string of text at the CLI. This issue has been resolved.

PCR: 03898 Module: ETH Level: 3

An ETH interface was sometimes shown as *Up* in the output of the SHOW INTERFACE command when it was actually *Down*. This issue has been resolved.

PCR: 03902 Module: FIREWALL Level: 3

Under some circumstances traffic did not have NAT applied if a standard subnet NAT rule was added to a public interface. Such rules did not correctly match incoming traffic when the REMOTEIP parameter in the ADD FIREWALL POLICY RULE command was not specified, and the destination IP address was not the interface's actual IP address. If this situation occurred, traffic was redirected back out the public interface. This issue has been resolved.

PCR: 03903 Module: SWI Level: 2

Filtering was not working correctly on AT-8848 switches between port groups 1-24, 25-48, and the two GBIC ports. This issue has been resolved.

PCR: 03904 Module: SWI Level: 3

Port mirroring was not working correctly on AT-8848 switches where the source, destination and mirror ports were spread between two or more of the port groups 1-24, 25-48, and the two GBIC ports. This issue has been resolved.

PCR: 03906 Module: SWITCH Level: 2

Software emulation of layer 3 hardware filtering was not operating correctly. Packets that the switch had no routing information for were filtered incorrectly. The first packet of a flow that should have been dropped was not dropped, and a flow that should have been allowed was being dropped. This issue has been resolved.

PCR: 03907 Module: IPV6 Level: 2

The CREATE CONFIG command did not generate the TYPE parameter for ADD IPV6 INTERFACE commands. This issue has been resolved.

PCR: 03909 Module: SCC Level: 2

A fatal error sometimes occurred when encryption is enabled with Frame Relay over a synchronous link. This was due to errors in the synchronous transmit queue when then the transmission of a synchronous frame timed out (because the device started up). This issue has been resolved.

PCR: 03911 Module: SWI Level: 3

The ADD SWITCH FILTER command returned an incorrect error message if a broadcast address was specified for the DESTINATION parameter. This issue has been resolved.

PCR: 03914 Module: IPG, VLAN Level: 3

When IGMP snooping was disabled with the DISABLE IGMPSNOOPING command, IGMP packets were not flooded. This issue has been resolved.

PCR: 03915 Module: CORE, SW56 Level: 2

Installing GBICs in AT-8800 series switches caused an error with the I2C bus. This issue has been resolved.

PCR: 03918 Module: DHCP6 Level: 2

DHCP6 server suffered a fatal error if it received more than 689 requests for temporary addresses. This issue has been resolved.

PCR: 03919 Module: IPV6 Level: 2

A fatal error could occur if pinging a deleted IPv6 interface. This issue has been resolved.

PCR: 03920 Module: L2TP Level: 3

If the LNS was configured without associating a PPP template to an IP address range, the device restarted when the dynamic PPP was created. This issue has been resolved.

PCR: 03921 Module: IP ARP Level: 3

ARP requests with invalid source MAC and IP addresses were being processed, but should have been dropped. This issue has been resolved.

PCR: 03924 Module: IPG Level: 2

The CPU can no longer receive multicast traffic when there are no Layer 3 interfaces configured as static multicast senders.

PCR: 03925 Module: IPV6 Level: 3

Incorrect debug information was returned when an ICMPv6 *PacketTooBig* message was received. This issue has been resolved.

PCR: 03928 Module: IKMP Level: 2

ISAKMP in *aggressive* mode did not establish a connection when the peer client sent 10 or more payloads. This issue has been resolved.

PCR: 03930 Module: FIREWALL Level: 2

A fatal error sometimes occurred when certain types of traffic travelled over a WAN interface connected to the Internet. This issue has been resolved.

PCR: 03931 Module: IPSEC Level: 3

The IPSec configuration was not created correctly when the RADDRESS and LNAME parameters in the CREATE IPSEC POLICY command were used together. This issue has been resolved.

PCR: 03933 Module: SW56, SWI Level: 2

When a Rapier rebooted while a GBIC port was receiving broadcast packets, some copper GBICs did not send packets after the switch booted up. Also, when a copper GBIC received pause frames on a Rapier, it did not stop sending packets. These issues have been resolved.

PCR: 03934 Module: IPSEC Level: 2

The CREATE IPSEC POLICY command failed if the interface specified with the INTERFACE parameter did not have a global IPv6 interface defined. This PCR implements a workaround by using the interface's link-local IPv6 address if no other IPv6 address can be found.

PCR: 03936 Module: IKMP Level: 3

When ISAKMP was used with IPv6, an incorrect IP address was displayed in the output of the SHOW ISAKMP EXCHANGE command. This issue has been resolved.

PCR: 03938 Module: IKMP Level: 3

DHEXPONENTLENGTH parameter in the CREATE ISAKMP POLICY command was not accepted when creating ISAKMP policies that used IPv6. This issue has been resolved.

PCR: 03939 Module: IPV6 Level: 2

When a *NeighbourAdvert* message containing an anycast target address was received, the device incorrectly performed Duplicate Address Detection. This issue has been resolved.

PCR: 03942 Module: SW56 Level: 2

IP multicasting was not operating correctly across all ports on an AT-8848 switch. This issue has been resolved.

PCR: 03946 Module: IPSEC Level: 3

When IPSec was used with IPv6, an incorrect IP address was displayed in the output of the SHOW IPSEC SA command. This issue has been resolved.

PCR: 03949 Module: IPSEC Level: 3

If a local IP address and remote IP address were not specified in the CREATE IPSEC POLICY command for IPv6 IPSec, the SET IPSEC POLICY configuration was shown unnecessarily in the output of the SHOW CONFIG DYNAMIC=IPSEC command. This issue has been resolved.

PCR: 03952 Module: SWI Level: 3

MAC address are now deleted from the all the internal tables for ports where the learn limit has been exceeded.

PCR: 03953 Module: SW56 Level: 3

On AT-8800 series switches, strict QoS scheduling is now enforced for ports where egress rate limiting is applied. On Rapier *i* series switches, the same QoS setup is now applied to all of the appropriate ports when setting up egress rate limiting.

PCR: 03969 Module: IPG Level: 2

When saving the IP filter configuration, non-default values for the source IP address mask were not always saved correctly. This issue has been resolved.

PCR: 03976 Module: SW56 Level: 3

On AT-8800 series switches, if a port was set to use 10 Mbps full duplex with the SET SWITCH PORT SPEED=10MBFULL command, there was a delay before the port was set. This delay has been minimised.

PCR: 03979 Module: CORE Level: 3

On AT-8800 series switches, the temperature at which a temperature alarm is generated has been increased.

PCR: 31037 Module: SW56 Level: 2

Uplink modules on Rapier series switches sometimes did not enable a link correctly. This issue has been resolved.

Importing BGP routes into OSPF

Introduction

With this enhancement you can import routes from BGP into OSPF. OSPF will then redistribute these routes. This enhancement adds three parameters to the **set ospf** command, and modifies the output of the **show ospf** command. The new parameters are **bgpimport**, **bgpfilter** and **bgplimit**.

BGP can learn thousands of routes, so it's important to consider the network impact of importing these routes. Routing devices in the OSPF domain may become overloaded if they store too many routes. You can prevent this by limiting the number of routes that will be imported.

Do not enable the importing of BGP routes into OSPF unless you are sure about the consequences for the OSPF domain.

Enabling BGP route import

To enable importing BGP routes into OSPF, use the command:

```
set ospf bgpimport=on
```

Limiting the number of routes

There are two ways to limit the number of BGP routes imported into OSPF. One way is to specify a maximum number of routes with the command:

```
set ospf bgplimit=1...300
```

When the limit is reached, the importing of routes will stop until existing routes are removed. Because they are BGP routes, actions of BGP control when the routes disappear.

The other way to limit the imported routes is to configure a routing filter. This filter is used in conjunction with the **bgpfilter** parameter in the **set ospf** command to control the passing of routing information in and out of the device. To configure a filter, use the **add ip filter** command:

```
add ip filter=filter-number {action=include|exclude}
   source=ipadd [smask=ipadd] [entry=entry-number]
```

Use this filter to limit imported BGP routes with the command:

```
set ospf bgpfilter=300...399
```

where the filter number is the previously configured filter.

Take care when configuring the IP filter. If the number of imported routes reaches the **bgplimit** parameter, you may not have imported all the routes specified with the **bgpfilter** parameter.

Advertising desired routes

The order in which routes are added is arbitrary. This means that to have desired BGP routes advertised by OSPF, you must take care setting the **entry** number for the route filter with the **add ip route** command. Assign a low entry number to a filter used to import preferred BGP routes. Alternatively, set the **bgplimit** parameter above the total number of routes that BGP will ever add to the routing table.

Configuration example

This example supposes that you want to import the route 192.168.72.0 into the OSPF routing domain, but no other routes. This route is received on the gateway router as a BGP route. The following steps show the sequence of commands to use in this scenario.

1. Set up the IP filter:

   ```
   add ip filter=300 source=192.168.72.0 smask=255.255.255.255
      action=include
   ```

2. Set up OSPF BGP import parameters:

   ```
   set ospf bgpimport=on bgpfilter=300 bgplimit=1
   ```

3. Check that BGP has added the route to the IP route table:

   ```
   show ip route=192.168.72.0
   ```

   The route should be visible in the output of the command.

4. Check that OSPF has imported the route:

   ```
   show ospf lsa=192.168.72.0
   ```

   The output should show that there is an AS external LSA with this ID.

set ospf

Syntax

```
SET OSPF [BGPFilter={NOne|300...399}]
   [BGPImport={ON|OFF|True|False|YES|NO}]
   [BGPLimit=1...300] [other-parameters]
```

Description This command sets general OSPF routing configuration parameters. Use this command to configure the importing of BGP routes into OSPF. See Table 4 on page 42 for details about each parameter.

Table 4: Parameters for the BGP route import feature in the **set ospf** command

Parameter	Option/Range	Description
BGPFilter	NOne	No filters are defined so all routes from BGP will be imported into OSPF. The default is **none**.
	300...399	The route filter that will be used when importing BGP routes into OSPF. Route filters are created with the **add ip filter** command. If a route filter is defined, the entries for the filter will include or exclude routes for importation. If routes have not been included by a previous entry, they will be excluded from the import.
BGPImport	ON|True|YES	Importing BGP routes into OSPF is enabled.
	OFF|False|NO	Importing BGP routes into OSPF is disabled. The default is **off**.
BGPLimit	1...300	The maximum number of BGP routes that can be imported into OSPF at a time. Once this limit is reached, importing stops until existing routes are removed. The default is **300**.

*Caps denote command shortcuts

show ospf

Syntax `SHow OSPF`

Description This command displays information about the general configuration of OSPF routing (Figure 5 on page 43, Table 6 on page 43). New entries for the BGP route import feature are in bold.

Figure 5: Example output from the **show ospf** command

```
Router ID ..................... 123.234.143.231
OSPF module status ............. Enabled
Area border router status ...... Yes
AS border router status ........ Disabled
PTP stub network generation ..... Enabled
External LSA count ............. 10234
External LSA sum of checksums ... 1002345623
New LSAs originated ............ 10345
New LSAs received .............. 34500
RIP ............................ Off
BGP importing:
  Enabled ...................... Yes
  Import filter ................ 301
  Routes imported/limit ........ 214 / 300
Export static routes ........... Yes
Dynamic interface support ...... None
Number of active areas ......... 10
Logging ........................ Disabled
Debugging ...................... Disabled
AS external default route:
  Status ....................... Disabled
  Type ......................... 1
  Metric ....................... 1
```

Table 6: parameters for the BGP route import feature in the output of the **show ospf** command

Parameter	Meaning
BGP importing	Information about the importing of BGP routes into OSPF.
Enabled	Whether or not the importing of BGP routes into OSPF is enabled; one of "Yes" or "No".
Import filter	The IP filter number used to filter routes before they are imported into OSPF, or "None" if no filters are used.
Routes imported/limit	The number of BGP routes imported into OSPF, and the maximum number of routes that can be imported at a time.

add ip filter

Syntax `ADD IP FILter=`*`filter-number`* `{ACTion=INCLude|EXCLude} SOurce=`*`ipadd`* `[SMask=`*`ipadd`*`] [ENTry=`*`entry-number`*`] [`*`other-parameters`*`]`

Description This command adds a pattern to a routing filter. For details about the command parameters, see Table on page 44

Parameters for the BGP route import feature in the **add ip f**

Parameter	Option/Range	Description
filter-number	300...399	Filters in the range 300 to 399 are treated as routing filters, and use the **action** parameter to specify the action to take with a route that matches the pattern.
ACTion		The action to take when the filter pattern is matched.
	INCLude	Route information matching the filter will be included.
	EXCLude	Route information matching the filter will be excluded.
SOurce		The source IP address, in dotted decimal notation, for the filter pattern.
SMask		The mask, in dotted decimal notation, to apply to source addresses for this pattern. The mask is used to determine the portion of the source IP address in the IP packet that is significant for comparison with this pattern. The values of **source** and **smask** must be compatible. For each bit in **smask** which is set to zero (0) the equivalent bit in **source** must also be zero (0). If **source** is not 0.0.0.0, then **smask** can not be 0.0.0.0. The default is 255.255.255.255, unless **source** is 0.0.0.0.
ENTry	entry-number	The **entry** parameter specifies the entry number in the filter which this new pattern occupy. Existing patterns with the same or higher entry numbers are pushed down the filter. The default is to add the new pattern to the end of the filter.

*Caps denote command shortcuts

IGMP Snooping All-Group Entry

Because IGMP is an IP-based protocol, multicast group membership for VLAN aware devices is on a per-VLAN basis. If at least one port in the VLAN is a member of a multicast group, multicast packets will be flooded onto all ports in the VLAN by default.

IGMP snooping enables the switch to forward multicast traffic intelligently on the switch. The switch listens to IGMP membership reports, queries and leaves messages to identify the switch ports that are members of multicast groups. Multicast traffic will only be forwarded to ports identified as members of the specific multicast group.

This enhancement allows network managers to prevent specified ports from acting as IGMP all-group ports, and specify which ports are allowed to behave as all-group entry ports, by using the ENABLE IP IGMP ALLGROUP command.

For example, consider a video streaming service which has 15 channels. When the switch receives IGMP membership reports destined for the address 239.0.0.2 from an unauthorised user, all 15 channels of multicast data floods to that port, which may affect the service of the network. In order to avoid this, the network manager decides whether or not to allow a particular port to behave as an IGMP all-group port, e.g. port 8. Then, whenever the above IGMP

membership report is sent, the switch will not automatically add port 8 as one of the egress ports for any IGMP membership report group, so video streaming will not get forwarded to disabled all-group ports selected by the network manager.

Commands

This enhancement modifies one command:

- SHOW IP IGMP

and has two new commands:

- ENABLE IP IGMP ALLGROUP
- DISABLE IP IGMP ALLGROUP

Modified Command

show ip igmp

Syntax `SHOW IP IGMP [COUNTER] [INTERFACE=`*`interface`*`]`

Description This command displays information about IGMP, and multicast group membership for each IP interface.

This enhancement includes the line "**Disabled All-groups ports**" on the output of this command, as show in Figure 7 on page 46. Ports that are disabled have a "#" symbol next to the port number.

Figure 7: Example output from the SHOW IP IGMP command.

```
IGMP Protocol
--------------------------------------------------------------------------------
Status ........................... Enabled
Default Query Interval ........... 125 secs
Default Timeout Interval ......... 270 secs
Disabled All-groups ports ........ 1,5,7

Interface Name .......... vlan2 (DR)
IGMP Proxy .............. Off
Group List ..............

  Group. 238.0.1.2          Last Adv. 172.50.2.1         Refresh time 34 secs
  Ports 3,11,23

  Group. 224.1.1.2          Last Adv. 172.50.2.1         Refresh time 130 secs
  Ports 2,11,23

  All Groups                Last Adv. 172.50.1.1         Refresh time 45 secs
  Ports 1#,11,23


Interface Name .......... vlan4             (DR)
IGMP Proxy .............. Off
Group List ..............
  No group memberships.

--------------------------------------------------------------------------------
```

Table 1: New parameter in the output of the SHOW IP IGMP command.

Parameter	Meaning
Disabled All-groups ports	A list of ports that are prevented from behaving as IGMP all-group ports.

Examples To show information about IGMP, use the command:

```
SHOW IP IGMP
```

See Also ENABLE IP IGMP ALLGROUP
DISABLE IP IGMP ALLGROUP

New Commands

This enhancement request introduces two new commands from enabling/ disabling all-group entries on switch ports.

enable ip igmp allgroup

Syntax `ENABLE IP IGMP ALLGROUP=[{`*`port-list`*`|ALL}]`

where:

- *port-list* is a port number, a range of port numbers (specified as n-m), or a comma separated list of port numbers and/or ranges. Port numbers start at 1 ad end at m, where m is the highest numbered Ethernet switch port, including uplink ports.

Description This command enables the specified port(s) to behave as a multicast all-group ports.

The ALLGROUP parameter specifies the list of ports able to behave as all-group entry ports. If ALL is specified, all ports are able to behave as all-group entry ports. The default is ALL.

Examples To enable ports 1, 5 and 7 to behave as all-group entry ports, use the command:

```
ENABLE IP IGMP ALLGROUP=1,5,7
```

See Also DISABLE IP IGMP ALLGROUP
SHOW IP IGMP

disable ip igmp allgroup

Syntax `DISABLE IP IGMP ALLGROUP=[{`*`port-list`*`|ALL}]`

where:

- *port-list* is a port number, a range of port numbers (specified as n-m), 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 switch port, including uplink ports.

Description This command disables the specified port(s) from acting as a multicast all-group entry ports. Ports that are disabled have a "#" symbol next to the port number in the output of the SHOW IP IGMP command.

Examples To prevent ports 1, 5 and 7 from behaving as all-group entry ports, use the command:

```
DISABLE IP IGMP ALLGROUP=1,5,7
```

See Also ENABLE IP IGMP ALLGROUP
SHOW IP IGMP

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.