Software Maintenance Release Note

Version 86273-09 for Rapier and AT-8800 series switches

Introduction

This release note lists the issues addressed and enhancements made in version 86273-09 for Software Release 2.7.3 on existing models of Rapier and AT-8800 series switches. File details are listed in Table 1.

Table 1: File details for version 86273-09.

Maintenance Release Date	10 March 2006
Compressed File Name	86273-09.rez
Compressed File Size	4127940 bytes

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

- Release Note: Software Release 2.7.3 for AT-9900, AT-8900, SwitchBlade, AT-9800, AT-8800, Rapier, Rapier i, AT-8700XL, and AT-8600 Series Switches and AR400 and AR700 Series Routers (Document Number C613-10431-00 REV A) available from www.alliedtelesyn.co.nz/documentation/relnotes/relnotes.html
- Rapier series switch or AT-8800 series switch for Software Release 2.6.4 available on the Documentation and Tools CD-ROM packaged with your switch, or from www.alliedtelesyn.co.nz/documentation/manuals.html.

Caution: Using a maintenance release for a different model 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 Inc. 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 Inc 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.

Enabling and Installing this Release

To use this maintenance release you must have a base release license for Software Release 2.7.3. Contact your distributor or reseller for more information.

To enable this release and install it as the preferred release, use the commands:

```
enable rel=86273-09.rez num=2.7.3
set install=pref rel=86273-09.rez
```

Features in 86273-09

Maintenance release 86273-09 includes the all issues resolved and enhancements released in previous maintenance releases for software release 2.7.3, and the following enhancements:

Level 1

CR00012196 Module: IPv6 Level: 1

When RIPng deleted a route from the IPv6 route table, routing for associated IPv6 flows was not updated correctly. This caused data forwarding on those flows to use invalid routes.

This issue has been resolved.

Level 2

CR00008699 Module: Switch Level: 2

Previously, when 300 MAC address filters were added to a port and the port was reset, the CPU became 100% utilised.

This issue has been resolved.

CR00008742 Module: Switch Level: 2

Previously, if a switch port's learn limit was changed to a number that was less than the currently-learned number of MAC addresses, you were unable to delete the learned MAC addresses. The switch also did not lock the port.

This issue has been resolved. The switch now deletes all learned MAC addresses and starts learning again.

CR00008993 Module: IPv6 Level: 2

IPv6 sometimes dropped a few data packets after the neighbour cache entry went to a Stale state while forwarding under heavy load.

This issue has been resolved.

CR00009216 Module: Firewall Level: 2

Previously, the TCP Setup Proxy in the firewall sometimes produced an incorrect sequence number for a TCP RST packet, or forwarded a TCP RST packet in the wrong direction.

These issues have been resolved.

CR00009242 Module: LACP Level: 2

Enhancements have been made so that:

- When any of the ports in a trunk group is disconnected, there is no momentary communication interruption.
- When the second last LACP trunk port is disconnected, there is no momentary communication interruption.

Also, an issue has been resolved in which LACP was randomly setting the switch port to STP BLOCK.

CR00010071 Module: BGP Level: 2

In the configuration file or output resulting from the commands **create config** and **show config dynamic=bgp**, BGP commands were in incorrect order.

This issue has been resolved.

CR00010137 Module: Non-classifier filtering Level: 2

When a Layer 3 filter was defined to send packets to the CPU, some of those matching packets may have been discarded. This occurred for filters created using the **add switch l3filter** command, when all of the following occurred:

- there were multiple entries per **match** clause
- the first entry had a **nomatchaction** that denied the packet
- later entries in the **match** clause should have accepted the packet

This issue has been resolved. All entries within a match clause are now checked for full matches before being checked for partial matches.

CR00010241 Module: OSPF Level: 2

In the configuration file or output resulting from the commands **create config** and **show config dynamic=ospf**, the command **set ospf type=2** occurred when **set ospf type=1** should have occurred.

This issue has been resolved.

CR00010265 Module: Switch Level: 2

When the ingress and egress port were defined in an Layer 3 filter with an action of **deny**, the filter denied the traffic to be sent out all the egress ports and not just the egress port specified in the filter.

This issue has been resolved.

CR00010318 Module: RIP Level: 2

If RIP was configured to send RIP version 2, then multiple routes to the same destination with different masks were not correctly included in the RIP response or trigger response messages. Only the best route was sent.

This issue has been resolved.

CR00010598 Module: OSPF Level: 2

When filtering OSPF routes, IP route filters did not filter out intra-area interface routes.

This issue has been resolved.

CR00010886 Module: IPv6, IP Gateway, PPP Level: 2

When a user enabled a Dial-on-Demand PPP interface, sometimes the switch did not apply the associated IP route change. This meant that routes via the Dial-on-Demand PPP interface were not available for use. When this occurred, routed traffic failed to activate the associated Dial-on-Demand PPP interface.

This issue has been resolved.

CR00011175 Module: IPv6 Level: 2

After a route's metric and/or preference changed, the route's position in the Equal Cost Multi Path chain was not always updated properly. This sometimes caused the forwarding process to select a sub-optimal route.

This issue has been resolved.

CR00011300 Module: User Level: 2

Previously, if the switch was acting as an 802.1x authenticator, and it received an illegal RADIUS packet (an Access-Reject packet with an EAP code of "successful"), the switch would reboot.

This issue has been resolved. The switch now rejects such authentication requests.

CR00011304 Module: VRRP Level: 2

VRRP did not function correctly when the switch was configured with protected VLANs.

This issue has been resolved.

CR00011490 Module: MLD, MLD Snooping Level: 2

The following issues occurred:

- an MLDv2 Report message parsing issue meant that sometimes the switch recognised only the first multicast group address in the message.
- if the **robustness**, **qinterval** or **qrinterval** were changed, groups' initial timeout period was sometimes set to 260 instead of being calculated by using the following formula from RFC 3810:
- robustness * qinterval + qrinterval
- the Other Querier Timeout—the timeout period for registration of the "All Router" group—was not calculated by using the following formula from RFC 3810:
- robustness * qinterval + qrinterval/2
- When **robustness**, **qinterval** or **qrinterval** were set to non-default values, the timeout values (or MA timers) of newly reported multicast address groups were not updated to reflect these changed values. This issue was also recorded as CR00007844.
- MLD & MLD Snooping groups were sometimes incorrectly set with a timer value that was inconsistent with the internally maintained individual port timers. Therefore, registered groups could lose port members temporarily.

These issues have been resolved. This CR also included enhancements to MLD and MLD Snooping; see "Enhancements to MLD and MLD Snooping (CR00011490)" on page 19.

CR00011907 Module: IP Gateway Level: 2

Previously, if the IP Helper attempted to redirect packets to an address that matched the network broadcast address of the egress interface, the packets were only forwarded if **directedbroadcast=yes** for the egress interface. By default, **directedbroadcast=no**, so such packets were dropped.

This issue has been resolved. IP can now distinguish between packets redirected by the IP Helper and real directed broadcast packets. If **directedbroadcast=no**, IP still redirects packets from IP Helper when necessary.

Level 3

CR00009785 Module: TTY Level: 3

If a user entered the **set tty page=off** command, and saved the configuration with the **create config** command, the resulting configuration file invalidly recorded the command as **set tty page=0**.

This issue has been resolved.

CR00010504 Module: IP gateway Level: 3

When a VRRP master was configured with VRRP adoption enabled, pings from the VRRP master to its own VR IP address failed.

This issue has been resolved.

CR00010508 Module: BGP Level: 3

When the switch received a BGP update message and created new prefix entries for the routes in the update, it reversed the order of the AS segments.

This issue has been resolved.

CR00011303 Module: VRRP Level: 3

When a VRRP master switch that was also configured with Protected VLANs received an ARP request, duplicate ARP entries were added into the ARL table.

This issue has been resolved.

Level 4

CR00008222 Module: DHCP Level: 4

Previously, ARP generated an ARP log message with an unknown port number (p0) when DHCP assigned an IP address to a client, even though the switch knew the port number.

This issue has been resolved. Whenever DHCP asks ARP to add an ARP entry, the log message now includes the actual port number.

CR00010442 Module: Utility Level: 4

Some commands that require an 8-digit hexadecimal number incorrectly allowed users to enter values larger than 0xFFFFFFFF.

This issue has been resolved.

Enhancements

CR00011271 Module: Switch, Utility

A new switch filter feature enables you to use a switch filter to make a VLAN secure without preventing access to other VLANs. For more information, see "Securing a Single VLAN through Switch Filters (CR00011271)" on page 18.

CR00011490 Module: MLD, MLD Snooping

Several enhancements have been made to MLD and MLD Snooping, in accordance with RFC 3810, *Multicast Listener Discovery Version 2 (MLDv2) for IPv6*. For details, see "Enhancements to MLD and MLD Snooping (CR00011490)" on page 19.

This CR also fixed some issues in MLD and MLD Snooping; see "CR00011490" on page 5.

Features in 86273-08

Maintenance release 86273-08 includes the all issues resolved and enhancements released in previous maintenance releases for software release 2.7.3, and the following enhancements:

Level 1

No level 1 issues.

Level 2

CR00009361 Module: IP Level: 2

If the switch received a stream of IPv4-encapsulated IPv6 packets, a memory leak could occur if no IPv6-over-IPv4 tunnel was configured.

This issue has been resolved.

CR00010166 Module: Port Authentication Level: 2

When the **supplicantmac** parameter was used in the **reset portauth=[macbased] port** command to specify the supplicant to reset, all supplicants were removed from the switch's forwarding database, instead of only the specified supplicant.

This issue has been resolved.

CR00010232 Module: STP Level: 2

STP and RSTP did not work correctly when a static MAC filter was added.

This issue has been resolved, so that control traffic is not incorrectly discarded in the presence of configured switch filters. Also, configured switch filters are now applied to locally generated control traffic.

CR00010539 Module: IP Level: 2

Sometimes the forwarding of packets occurred unnecessarily slowly. This happened if the forwarding interface was associated with an IP filter with a variable field pattern, such as TCP session or ICMP code and type.

For switches, note that this issue occurred when the switch was routing IP packets in software, and had no effect on the hardware forwarding of packets.

This issue has been resolved.

CR00010731 Module: ISAKMP Level: 2

Previously, phase 1 ISAKMP exchanges would accept unsuitable values for the SA life duration attribute. This issue has been resolved, so that ISAKMP will discard any messages it receives with an unsuitable SA life duration. The lowest acceptable values that ISAKMP will receive for the SA life duration are 60 seconds or 1 kbyte.

CR00010733 Module: ISAKMP Level: 2

If an ISAKMP packet was received that had malformed payload fields, a reboot could occur. This issue has been resolved, so that any ISAKMP packets with malformed payload fields are now discarded.

CR00010735 Module: ISAKMP Level: 2

An ISAKMP denial of service (switch reboot) vulnerability existed.

This issue has been resolved.

CR00010736 Module: ISAKMP Level: 2

It was possible for a peer acting as an ISAKMP initiator to cause the switch to reboot.

This issue has been resolved.

CR00010753 Module: ISAKMP Level: 2

If an unexpected payload was received in aggressive mode, the log message would be badly formatted and could potentially result in a reboot.

This issue has been resolved.

CR00010866 Module: ISAKMP Level: 2

In certain cases if an invalid or malformed ISAKMP message was received, the exchange would not be cleaned up correctly. If this occurred frequently, then it was a possible ISAKMP Denial of Service attack, and other valid exchanges would be ignored.

This issue has been resolved.

CR00010897 Module: ISAKMP Level: 2

Previously, a reboot occurred if the last ISAKMP HASH payload had a length of zero. This issue has been resolved by adding additional checks for processing ISAKMP payloads.

CR00010900 Module: ISAKMP Level: 2

Previously, a reboot could occur if an ISAKMP HASH payload was invalidly large.

This issue has been resolved by adding additional checks for processing ISAKMP payloads.

CR00010901 Module: ISAKMP Level: 2

Previously, a reboot could occur if an ISAKMP ID payload was invalidly large.

This issue has been resolved by adding additional checks for processing ISAKMP payloads.

CR00011111 Module: IPX Level: 2

Forwarding an 802.3 or ETHII encapsulated IPX packet over a VLAN to a remote network occasionally caused the switch to reboot.

This issue has been resolved.

CR00011219 Module: IP Level: 2

When the switch received an IP packet with invalid IP option length (a corrupted packet), a reboot might occur.

This issue has been resolved.

CR00011243 Module: ISAKMP Level: 2

Previously, if an IPsec/ISAKMP tunnel was under heavy load, an ISAKMP peer may have retransmitted messages. When the last message in an ISAKMP exchange was retransmitted, the remote peer did not expect to receive the second message after the exchange had finished and caused the switch to reboot.

This issue has been resolved.

Level 3

CR00010826 Module: ISAKMP Level: 3

Previously, the "Exchange x: Failed" log message was not recorded if an ISAKMP exchange failed.

This issue has been resolved.

Level 4

No level 4 issues.

Enhancements

No enhancements

Features in 86273-07

Maintenance release 86273-07 includes the all issues resolved and enhancements released in previous maintenance releases for software release 2.7.3, and the following enhancements:

Level 1

No level 1 issues.

Level 2

CR00008281 Module: PORT AUTH Level: 2

When the switch was in the Port Authentication multi mode, PORTAUTH did not adequately handle WindowsXP as a supplicant.

This issue has been resolved.

CR00008391 Module: NAT Level: 2

An issue existed in IP NAT when creating a new session for a packet destined for an IP address that had been dynamically allocated to a private IP address. The session created would NAT the destination address to the source address of the packet instead of the private IP address.

This issue has been resolved.

CR00009169 Module: LOAD BALANCER Level: 2

Previously when particular combinations of load balancer trigger parameters were configured, the resulting command created by `create config` or `show config dynamic` were missing spaces between words.

This issue has been resolved.

CR00009201 Module: ARP Level: 2

An ARP timeout caused the removal of the ARP entry resulting in packet loss until the entry was re-added.

This issue has been resolved.

CR00009247 Module: GUI AGENT Level: 2

If the switch was configured with a large number of VLANs, then attempting to view STP-related pages on the GUI could cause a reboot.

This issue has been resolved.

CR00009313 Module: PORT AUTH Level: 2

When a switch port was disabled using the `disable switch port` command, the MAC address of the authorised supplicant on the port remained in the FDB table. The supplicant's MAC address is now removed when the port is disabled. This has been resolved on both single- and multi-supplicant mode.

When portauth was disabled by using the `disable portauth` command, the supplicant MAC address in the switch filter was not removed. This has

been resolved and all MAC addresses added by portauth internally are deleted when the supplicant is removed or unauthorised. Also the same behaviour in `purge portauth port, set portauth port default, disable portauth port` and `reset portauth portmultimib` commands has been fixed in both 802.1x and MAC-based port authentication.

CR00009387 Module: SW56 Level: 2

Previously, entries in the FDB table of multi-instance switches were being removed by incorrect MAC address aging.

This issue has been resolved.

CR00009641 Module: IPv6 Level: 2

When many IPv6 instances were created on one vlan interface and then one IPv6 peer changed its address, the switch could experience an unexpected reboot when its peering IPv6 interfaces changed their addresses.

This issue has been resolved.

CR00009677 Module: QoS Level: 2

Previously the user could not configure a maximum bandwidth on creation of a traffic class.

This issue has been resolved.

CR00009963 Module: STP Level: 2

When multiple STP instances were configured on a switch with multiple VLANs and a topology change happened on one STP instance, the learned IP table entries on ports that did not belong to the STP instance in question were being unnecessarily deleted.

This issue has been resolved.

CR00010030 Module: PORT AUTH Level: 2

In Multi-Supplicant mode, the `set portauth port` command cleared the FDB entries even though there was no configuration resulting from the command. This has been resolved now, and the MAC address of the authorised supplicant will not be removed from the FDB table by the `set portauth port` command.

CR00010168 Module: BGPv4 Level: 2

When BGP damping was enabled, withdrawn routes were not correctly having their damping history maintained until they either returned or the damping history timed out and they were deleted.

This issue has been resolved.

CR00010169 Module: BGPv4 Level: 2

When a route's attribute was updated in the BGP route table, a damping record was not created in the history.

This issue has been resolved.

CR00010226 Module: QoS Level: 2

When creating or setting QoS traffic classes, the parameters `exceedaction` and `exceedremarkvalue` parameters were erroneously rejected.

This issue has been resolved.

Level 3

CR00006256 Module: GUI Level: 3

A fatal exception could occur when trying to view Classifier configuration information via the GUI.

This issue has been resolved.

CR00009309 Module: PPP Level: 3

After adding a PPP access concentrator service, it was not possible to delete this service using the `del ppp acservice=<name> vlan=<number>` command.

This issue has been resolved.

Level 4

CR00007424 Module: IPv4 Level: 4

When using the `add ip route filter` command, the filter ID must be within the range 1 to 100. However if the filter ID is not specified or it is specified (within range) more than once, then more then 100 IP route filters can be added.

This issue has been resolved.

Features in 86273-06

Maintenance release 86273-06 includes the all issues resolved and enhancements released in previous maintenance releases for software release 2.7.3, and the following enhancements:

Level 1

No level 1 issues.

Level 2

CR00008281 Module: PORTAUTH Level: 2

When the switch was acting as an authenticator, in multi-mode, it had an issue when interoperating with a WindowsXP supplicant.

This issue has been resolved.

CR00009387 Module: SW56 Level: 2

Previously, entries in the FDB table of multi-instance switches were being removed by incorrect MAC address aging.

This issue has been resolved.

CR00009641 Module: IPv6 Level: 2

Previously the switch would reboot when there was a large number of IPv6 instances created on one VLAN, and one of the IPv6 peers changed its address.

This issue has been resolved.

Level 3

No level 3 issues.

Level 4

No level 4 issues.

Enhancements

No enhancements

Features in 86273-02

Maintenance release 86273-02 includes the all issues resolved and enhancements released in previous patches for software release 2.7.3, and the following enhancements:

Level 1

CR00007695 Module: PPP Level: 1

When either the Firewall was enabled or multiple L2TP tunnels were configured, and a default route existed over an L2TP tunnel, it was possible for an infinite internal packet loop to be created when a packet was sent over the L2TP tunnel after the underlying interface route to the remote IP had gone down. This caused a reboot to occur.

This issue has been resolved. (No PCR number.)

Level 2

CR00002290 Module: STP, SWI Level: 2

Previously, the forwarding database was flushed instead of being aged out when an STP topology change notification was received.

This issue has been resolved. (PCR number: 40185)

CR00002662 Module: STP Level: 2

Previously, when a port or ports was moved from one VLAN to another, the switch would reset both STP/RSTP instances that control the VLANs. This behaviour is now changed to only reset the STP process on the STP instance that the port(s) is joining. The switch will now also retain the port(s) edge-port setting during the moving process.

This issue has been resolved.

CR00006554 Module: PPP Level: 2

PPP TCP mss clamping was always fixing the mss to 1372. This issue is now fixed, so that if the MTU or MRU is less than 1472, then mss clamping clamps the mss to the correct size.

This issue has been resolved.

CR00006769 Module: PPP Level: 2

PPPoE has been modified so that a single host can be attached to multiple access concentrators without a conflict of session IDs.

CR00007005 Module: PPP Level: 2

A change was made in the 2.6.1 software release to reset the PPP idle timer for received traffic as well as transmitted traffic to avoid a PPP link idling out when receiving unidirectional traffic. However, this has undesirable side effects as it is not possible to control the received traffic. This change has been removed. Users can avoid a PPP link idling out for received unidirectional traffic by setting the value of the IDLE parameter to OFF, or in the case of received multicast traffic, setting the IDLE parameter to a value greater than the multicast hello timer.

CR00007078 Module: PPP Level: 2

When PPP was configured over L2TP over PPPoE, and the firewall was enabled, a restart could occur in some circumstances.

This issue has been resolved.

CR00007291 Module: IPG Level: 2

If RIP was configured to explicitly exchange packets with a neighbour in another subnet, the RIP packets from that neighbour were dropped.

This issue has been resolved.

CR00007341 Module: IPG Level: 2

When switches were using CIDR addressing, with a unicast address coinciding with a network broadcast address of class A, B, or C, then they could incorrectly forward traffic as directed broadcasts, even though the traffic was unicast (only).

This issue has been resolved. (PCR number: 50069)

CR00007358 Module: BRG, FR Level: 2

When Cisco encapsulation was used on a frame relay interface, the switch was not recognising bridged packets. This issue has been resolved.

Also, specifying a logical frame relay interface when adding a bridge port has been explicitly disallowed.

This issue has been resolved

No PCR number.

CR00007530 Module: CORE, FFS Level: 2

Restarts could occur when an AR202 PIC card was present in an AR040 NSM.This issue has been resolved.

CR00007888 Module: OSPF Level: 2

NSSA areas were not able to form adjacencies with some other vendors' equipment.

This has been resolved.

CR00007948 Module: SSH Level: 2

Some SSH Clients do not limit the length of the SSH username. Under some special circumstances, when the AlliedWare ™ SSH server received a username of 186 characters, the device would restart unexpectedly. This was fixed to limit a SSH username to be less than 64 characters and returning a failure message if the username was 64 or more characters.

CR00007992 Module: SSH Level: 2

Under some circumstances the SSH listen port would be closed.

This issue has been resolved.

CR00008068 Module: HTTP Level: 2

When a URL contains an IP address instead of a Domain name and the inverse DNS lookup for resolving the domain name failed, the proxy server could block the cookies incorrectly. Also the Proxy server could parse an HTTP message incorrectly if the URL field of the HTTP message contained non-ASCII characters.

These issues have been resolved

CR00008080 Module: TRG Level: 2

Triggers based on memory resource were not activated when the specified memory level was reached.

This issue has been resolved.

CR00008101 Module: FILE Level: 2

The COPY command returned an error message saying the input filename was invalid, even if a valid filename was given.

This issue has been resolved.

CR00008117 Module: IPG, VRRP Level: 2

ARP requests received that matched a static ARP entry would overwrite the hardware switching tables for that entry. The static ARP in software (SHOW IP ARP) would remain as defined by the user, however. Now, if an ARP entry has been added statically, the hardware switching tables are not updated by the dynamic ARP information.

CR00008176 Module: FFS, FILE Level: 2

The flash file system could sometimes have duplicate copies of a file.

This issue has been resolved.

CR00008184 Module: IPG Level: 2

If an IP interface was assigned its IP address dynamically, and the IP that it was assigned matched the Network address of another interface on the device, then the device would drop packets destined for the remotely assigned IP interface.

This issue has been resolved. PCR40549

CR00008266 Module: CORE Level: 2

A reboot could occur if a device had an extremely large boot script.

This issue has been resolved.

CR00008280 Module: SYN Level: 2

SYN PICs suffered from severe data corruption when installed in an AR440S running 2.7.1 or 2.7.3 software release.

This issue has been resolved.

Level 3

CR00006086 Module: x25t Level: 3

IP interfaces over X25 were not operating correctly. This issue has been resolved.

No PCR number

CR00007476 Module: IPG Level: 3

The DNS relay has been changed to allow the relay of resource record types between 0x1d and 0xff. Previously packets with these types of resource records were dropped.

This issue has been resolved (No PCR number.)

CR00007521 Module: IPG Level: 3

DVMRP packets were being dropped due to packet length inconsistencies from other vendor devices.

This issue has been resolved. (No PCR number.)

CR00007716 Module: LOG Level: 3

Previously, when changing the password on a log output/receive definition to a shorter string, the log message exchange could fail.

This issue has been resolved. (PCR number: 50070)

Level 4

CR00006093 Module: FFS Level: 4

There was not enough information displayed to the user when the ACTIVATE FLASH COMPACTION command was entered at the same time as Flash was compacting.

This issue has been resolved. (No PCR number.)

Enhancements

CR00006652 Module: IKMP, IPSEC

Previously ISAKMP NAT-T was enabled by default on every ISAKMP policy created. NAT-T is now disabled by default on every ISAKMP policy.

No PCR number given.

CR00006953 Module: PPP

The ability to configure Van Jacobsen Header Compression over dynamic PPP interfaces has been added. To this end, the command parameter 'VJC={ON | OFF}' has been added to the CREATE and SET PPP TEMPLATE commands. (No PCR number.)

CR00008367 Module: FIREWALL

Support Japanese VoIP service using SIP (port 5060) where the VOIP phone's session setup is 5 packets or less and the keepalive is greater than 5 min. NB: if the keepalive is greater than the default udpTimeout of 20 minutes, then this will need to be configured for the policy. This check of the srcPort and dstPort is intended to be configurable once enh req 890 is done - this is just a temporary solution for 273-02.rez

Features in 86273-01

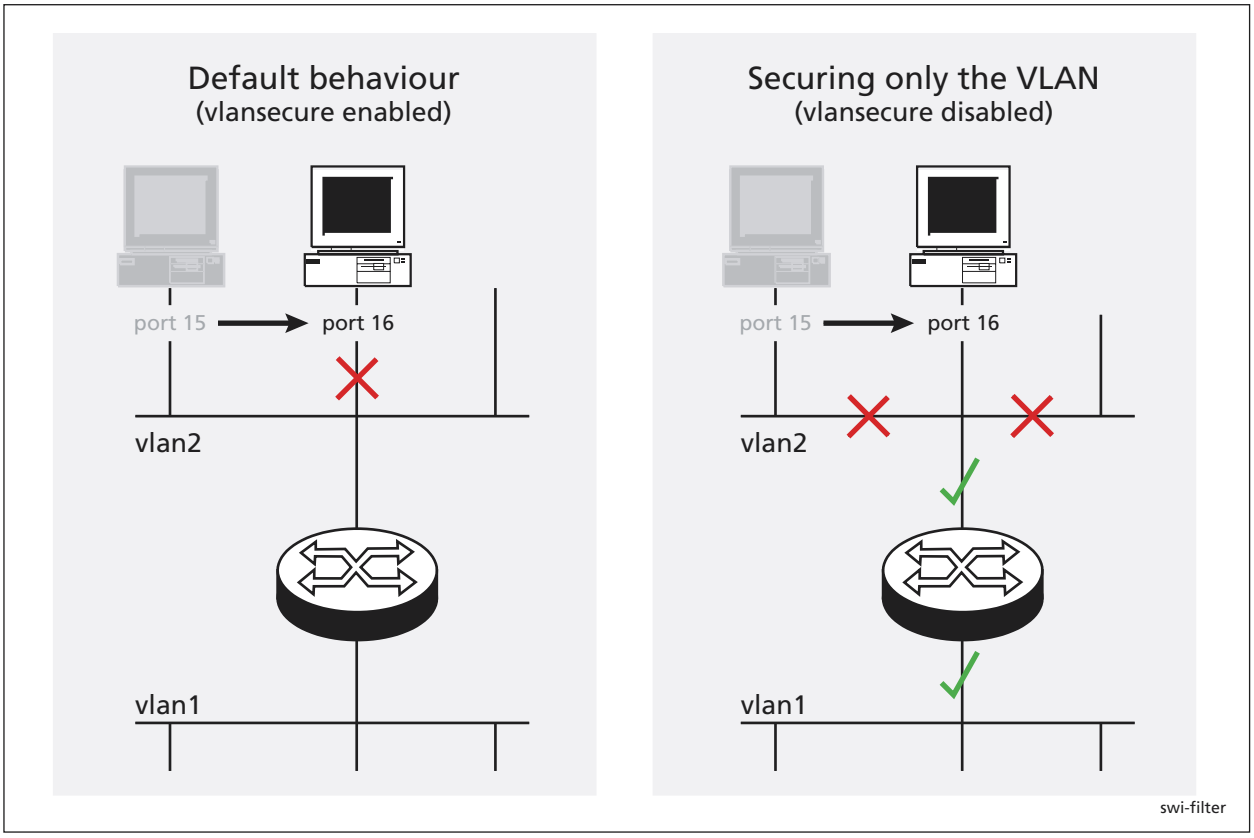
No release issued.

Securing a Single VLAN through Switch Filters (CR00011271)

On AT-8824 and Rapier 24i switches, this enhancement enables you to use switch filters to secure only the current VLAN, instead of securing all VLANs on the switch. To turn on this feature, a new command disables "vlansecure" for filters (see "Configuring vlansecure" on page 19). Without this enhancement (the default situation) a switch filter only allows a host to access the network through a particular port on the switch. For example, if you have a PC connected to port 15 in vlan2, and define the following filter, the PC can only communicate when it is connected to port 15:

```
add switch filter entry=0 dest=pc-mac-address vlan=2 port=15
   action=forward
```

With this enhancement, the above filter limits the host to accessing vlan2 through port 15, but does not prevent the host from accessing other VLANs through other ports in vlan2. For example, if the above filter exists and you move the PC to another port in vlan2, this enhancement prevents the PC from communicating with devices in vlan2 but allows it access to other VLANs on the switch. The following figure shows a PC that has been moved from port 15 to port 16 to illustrate the effect.



Configuring vlansecure

To turn off the default behaviour, so that the filter prevents access to only the current VLAN when you move the host, use the new command:

```
disable switch filter vlansecure
```

To return to the standard filter behaviour, use the new command:

```
enable switch filter vlansecure
```

To display which mode the filtering behaviour is in, use the existing command:

```
show switch filter
```

This command now displays the additional field "VlanSecure", which is either DISABLED or ENABLED.

Enhancements to MLD and MLD Snooping (CR00011490)

The following enhancements were made to MLD and MLD Snooping, in accordance with RFC 3810, *Multicast Listener Discovery Version 2 (MLDv2) for IPv6*.

MLD Packet Formats

MLD messages are now all sent with a hop limit of 1, a link-local source address, and the other format requirements of RFC 3810.

ICMP type for MLDv2 Reports

MLD Report messages now have an ICMP type of 143 by default, as specified by RFC 3810. The previous value was 255.

If you need to maintain backwards compatibility with earlier releases that use an ICMP type of 255, you can do so by using the new **draftcompat=yes** option in the command:

```
enable ipv6 mld interface=interface draftcompat={yes|no}
```

This enables the interface to receive MLDv2 reports with an ICMP type of 255. The default for **draftcompat** is **no**.

MLD Snooping Group Membership Display

The command **show mldsnooping** no longer displays the port members of the "All Routers" group. This change makes the output of this command more like output from the command **show igmpsnooping**.