Software Maintenance Release Note

Software Version sb275a07 For SwitchBlade 4000 Series Switches

Introduction

This software maintenance release note lists the issues addressed and enhancements made in maintenance version sb275a07 for Software Release 2.7.5A on existing models of SwitchBlade series switches. Release file details are listed in Table 1.

Table 1: Release file details for release sb275a07

Maintenance Release Date	17 January 2008
Compressed Release File Name	sb275a07.rez
Compressed Release File Size	3768296
GUI Resource File Name	d_sb8e33.rsc (8-slot chassis) d_sb4e33.rsc (4-slot chassis)

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

- the documentation you received with Software Release 2.7.5A
- the SwitchBlade Document Set for Software Release 2.7.3 (Document Number C613-03100-00 REV A), available from: www.alliedtelesis.co.nz/documentation/documentation.html

Caution: Using a software maintenance version for the wrong 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 Telesis 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 Telesis 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 Maintenance 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 version

To use this maintenance version you must have a base release license for Software Release 2.7.5A. Contact your distributor or reseller for more information.

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

```
enable rel=sb275a07.rez num=2.7.5
set install=pref rel=sb275a07.rez
```

Features in sb275a07

Software maintenance version sb275a07 includes all resolved issues and enhancements in earlier 2.7.5A versions, and the resolved issues and enhancements in the following tables.

Level 1

No level one issues

Level 2

CR	Module	Level	Description
CR00011907	**IP Gateway**	**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.
CR00018141	**Switch**	**2**	CPU utilisation could become very high under circumstances in which the switch needed to learn a large number of entries. For example, this could occur during a reboot when large numbers of MAC entries require learning. This issue has been resolved.

Level 3

No level three issues

Level 4

No level four issues

Enhancements

No enhancements

Features in sb275a06

Software maintenance version sb275a06 includes all resolved issues and enhancements in earlier 2.7.5A versions, and the resolved issues and enhancements in the following tables.

Level 1

No level one issues

Level 2

CR	Module	Level	Description
CR00013670	Trigger	2	If a "crash" trigger was configured, and an exception occurred, the trigger ran correctly when the switch came back up. However, if the user then performed warm restarts (by entering the command **restart switch**) after a switch exception, then the trigger ran again after each warm restart. This issue has been resolved. The trigger only runs the first time that the box starts after an exception.
CR00016727	TCP, Telnet	2	The speed of the output from the Telnet server has been increased.
CR00016779	IP Gateway	2	When two default routes existed and one was deleted, the switch did not add the second route to its hardware routing table. This issue has been resolved.
CR00016840	STP	2	Previously, when the switch was a Spanning Tree root bridge in a network and a user raised the switch's root bridge priority enough to stop the switch from being the root bridge, unnecessary delays in convergence occurred. This issue has been resolved.
CR00017184	Switching	2	If a faulty slave controller card was inserted into a SwitchBlade, the SwitchBlade would reboot. This issue has been resolved.
CR00018137	Switching, VLAN	2	Previously, multicast limiting did not limit the number of destination look-up failure packets or multicast packets destined to reserved IP multicast addresses. In a correctly-functioning network, rates of these packets are very low, but in a network with a loop, rates can be very high. This issue has been resolved. Multicast limiting now includes such packets.
CR00018145	RSTP	2	In RSTP BPDUs, the switch sent a Port ID of 8000 (zero) for its first port (generally port 1.1). This did not comply with IEEE Standard 802.1w-2001 Section 9.2.7, which states that the minimum port identifier should be 1. This could result in loops when interoperating with other networking devices. This issue has been resolved. The switch now uses a minimum Port ID of 8001 (one).

Level 3

CR	Module	Level	Description
CR00010136	IP Gateway	3	If an IP interface was added and deleted many times, an excessive number of memory buffers became full. Also, when an IP interface was deleted, the IGMP query timer (**set ip igmp int=*interface* querytimeout=*value***) sometimes continued running and later caused the switch to reboot. These issues have been resolved.
CR00016511	Switching	3	If a port on a linecard was a mirror port, and that card was hotswapped, the mirror port settings were not restored. Because of this, the mirror port was returned to the default VLAN. This issue has been resolved. Mirror port settings are now restored after hotswap.

Level 4

CR	Module	Level	Description
CR00013463	Ping	4	Previously, if you used the ? or Tab keys to obtain help about the **timeout** parameter for the **ping** command, the resulting help said that the maximum timeout was 65535. However, the correct maximum is 60 seconds. This issue has been resolved. The "?" help now displays the correct range of values.

Enhancements

CR	Module	Level	Description
CR00016978	STP, Switching	-	STP debugging has been enhanced to: ■ make it easier to see STP state information, and ■ only display information about Topology Change messages. For command syntax and output details, see "STP debugging enhancements (CR00016978)" on page 22.
CR00017826	BGP	-	The switch now supports the full AlliedWare BGP implementation, for a maximum of 150 routes. A new feature license has been created to enable this feature.

Features in sb275a05

Software maintenance version sb275a05 includes all resolved issues and enhancements in earlier 2.7.5A versions, and the resolved issues and enhancements in the following tables.

Level 1

No level one issues

Level 2

CR	Module	Level	Description
CR00009347	GUI	2	It was not possible to use the GUI to add untagged ports to the default VLAN. This issue has been resolved.
CR00010874	IP Gateway OSPF	2	Previously, the switch discarded multicast OSPF packets that it received on unnumbered PPP interfaces. This prevented OSPF from working across unnumbered PPP interfaces. This issue has been resolved.
CR00013466	Switch	2	Previously, if a JDSU XFP was used in the AT-SB4541 10G line card, the switch rebooted when executing the command **show switch port**. This issue has been resolved. Also, the XFP LED on the 10G line card used to flash amber when many types of XFPs were installed without a link. This issue has also been resolved. When an XFP is installed, enabled, and without a link, the XFP LED is now solid green.
CR00013678	GUI File System	2	It was not always possible to save the switch configuration by using the Save button on the GUI. Sometimes the GUI reported the following error instead of saving the configuration: "Save failed: SYSR busy, try create config file when transfer complete" This issue has been resolved.
CR00013823	Switch	2	In very rare circumstances, a port could stop transmitting traffic if its speed was modified or it was reset while under heavy traffic load. This issue has been resolved.
CR00013862	IP Gateway	2	If a network loop lasted for a day or longer, the switch ran out of memory and rebooted. This issue has been resolved. The switch now conserves memory in these extreme circumstances.
CR00014124	Switch	2	When the master switch controller was in slot B and a slave controller was in slot A, the Layer 2 multicast table for AT-SB4541 10G line cards could become incorrect. This caused loss of connectivity. This issue has been resolved. The Layer 2 multicast table now reflects the correct configuration when the master controller is in slot A or slot B.

CR	Module	Level	Description
CR00015071	IP Gateway	2	Routing over a PPP interface could fail if the switch had a default route out an Ethernet port. The default route switched all packets, even those destined for the PPP interface. This issue has been resolved. The resolution involves adding routes over the PPP interface to the switch hardware tables with an instruction to trap these packets to the CPU. Therefore these routes now appear in the hardware tables, and can be displayed by using the command **show switch table=ip**.
CR00015132	Switch GUI	2	If a trunk group did not have any ports associated with it, viewing the Trunk page in the GUI caused the switch to reboot. This issue has been resolved.
CR00015190	Switch	2	When multicast data was being forwarded at L2 through the switch during startup and a slave switch controller was present, the switch sometimes rebooted. This issue has been resolved.
CR00015697	Switch	2	Mirroring the traffic on port 1 of any line card caused the switch to lose packets.

Level 3

CR	Module	Level	Description
CR00011444	Asyn	3	If information was sent to a console (asyn) port that had no cable plugged into it, excessive CPU usage occurred. This issue has been resolved.
CR00012858	DHCP	3	Previously, it was not possible to have multiple static DHCP entries with the same client ID (MAC address), even if the static entries were for different DHCP ranges. This issue has been resolved. You can now add static DHCP entries for a given MAC address to multiple ranges. Note that you cannot have multiple entries for a given MAC address on the same range.

Level 4

No level four issues

Enhancements

CR	Module	Level	Description
CR00013351	IGMP snooping, EPSR, RSTP	-	A new feature has been added to IGMP snooping, to minimise loss of multicast data after a topology change on networks that use EPSR or spanning tree (STP, RSTP, or MSTP) for loop protection and IGMP snooping. For more information, see "IGMP Snooping Query Solicitation (CR00013351)" on page 24.
CR00014222	IGMP snooping, Switch, VLAN	-	IGMP snooping learns which ports have routers attached to them, so it can forward relevant IGMP messages out those ports. By default, snooping identifies router ports by looking for ports that receive specific multicast packets (such as IGMP queries, PIM messages, OSPF messages, and RIP messages). In some network configurations, this learning process cannot identify all router ports. For such networks, this enhancement enables you to statically configure particular ports as multicast router ports. To specify the static router ports, use the new command: add igmpsnooping vlan={*vlan-name*|1..4094} routerport=*port-list* To stop ports from being static router ports, use the new command: delete igmpsnooping vlan={*vlan-name*|1..4094} routerport=*port-list* To list the static router ports, use the existing command: show igmpsnooping and check the new "Static Router Ports" field.

Features in sb275a04

Software maintenance version sb275a04 includes all resolved issues and enhancements in earlier 2.7.5A versions, and the resolved issues and enhancements in the following tables.

Level 1

No level one issues

Level 2

CR	Module	Level	Description
CR00007522 **CR00012896**	**IP Gateway**	**2**	The switch's hardware IP route table occasionally did not contain the most optimal route to a destination. This meant packets were sometimes sent via sub-optimal routes. An additional effect was that when multiple equal-cost routes existed a less than complete set of those routes would be utilised. This issue has been resolved, so that the switch forwards packets via the best IP route(s) available.
CR00009026	**IP Gateway, OSPF**	**2**	The IP route cache (and therefore the Layer 3 IP routing table in hardware) was sometimes refreshed unnecessarily when OSPF SPF recalculation took place as a result of OSPF receiving a router LSA update. This issue has been resolved.
CR00009347	**GUI**	**2**	It was not possible to use the GUI to add untagged ports to the default VLAN. This issue has been resolved.
CR00009826	**IP Gateway**	**2**	When a static ARP is deleted, the switch sends out an ARP request to attempt to create a dynamic ARP for that IP address. Previously, the switch did not process the ARP response correctly and therefore did not add the ARP to its ARP table. This issue has been resolved. When a static ARP is deleted, the switch attempts to create a dynamic ARP for that IP address, and will successfully add it to the ARP table if a device responds.
CR00010170	**OSPF**	**2**	Route maps did not filter static routes of external type 2 when redistributing them into OSPF. This issue has been resolved.
CR00010598	**OSPF**	**2**	When filtering OSPF routes, IP route filters did not filter out intra-area interface routes. This issue has been resolved.
CR00010827	**OSPF**	**2**	Previously, OSPF would advertise LSU packets to the wrong area when a stub area was altered. This issue has been resolved.
CR00011219	**IPv4**	**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.

CR	Module	Level	Description
CR00011585	OSPF	2	Adding the same OSPF stub or host twice caused OSPF to suspend its operation, causing neighbour relationships to eventually fail. This issue has been resolved.
CR00012067	OSPF	2	A summary LSA was not turned into a route if the destination and mask fell inside one of the switch's active ranges, unless it exactly matched the active range's address and mask. This complied with RFC 1583 section 16.2. However, the recommended behaviour has been modified in RFC 2328 section 16.2. To comply with this, the LSA is now calculated if it falls inside one of the switch's active ranges.
CR00012606	STP	2	Processing of an invalid STP packet could result in an STP timeout value being incorrectly set to 0. This issue has been resolved, so the timeout can never be set to 0.
CR00012783	VLAN	2	When the mirror port was specified on the switch, untagged ports would start to transmit tagged traffic. This issue has been resolved.
CR00013178	Switch	2	In packet storm conditions, involving a high percentage of routing protocol packets, the switch could become very low on resources, and reboot. This issue has been resolved.
CR00013275	Firewall	2	If a firewall policy had a list attached to it (by using the command **add firewall policy=*policy-name* list=*list-name***), destroying the policy would cause the switch to reboot. This issue has been resolved.
CR00013380	IP Gateway	2	In certain unusual network configurations, the switch would respond to ICMP messages addressed to it with the wrong source IP address in the reply. This issue has been resolved.
CR00013598	IP Gateway	2	If the switch had multiple default routes with the same nexthop (such as one static default route and a default route learnt by RIP) and one of those default routes was withdrawn, then the hardware entry for the default route would be removed. This meant that traffic destined to that route was forwarded to the CPU, which could result in a performance degradation. This issue has been resolved.
CR00014044	IGMP	2	When large numbers of multicast streams were passing through the switch and there was no multicast routing protocol running (such as PIM or DVMRP), the CPU would experience regular periods of extended high utilisation. This could result in lost control packets and network instability. This issue has been resolved.

Level 3

CR	Module	Level	Description
CR00000133 CR00008167	**Log**	**3**	Messages in the permanent log were lost after changing the queue length for the permanent log. This issue has been resolved.
CR00002589 CR00011829	**IPX**	**3**	Previously, an IPX circuit sometimes incorrectly displayed its link status as UP, when it was actually in a DOWN state. This issue has been resolved.
CR00009817	**Ping**	**3**	The command **purge ping totally** did not purge all the information about ping polling. This issue has been resolved.
CR00010183	**OSPF**	**3**	If a route had already been learnt by OSPF, and then the inroutemap on OSPF was configured in such a way that the properties of this route should be altered as it is imported into the IP route table, the route would not be altered even if the SPF calculation was repeated. This issue has been resolved.
CR00010184	**OSPF**	**3**	If route map filtering altered the type of a AS-External route, the metric format was not also appropriately altered. This issue has been resolved, so that the metric format will also be altered to be appropriate for the route type.
CR00011652	**GUI**	**3**	It was not possible to use the GUI to edit a file (through the Management > Configuration Files > Edit page) if the filename contained a hyphen (such as test-1.cfg). The browser returned a "page not found" error. This issue has been resolved. You can now edit such files.
CR00012130	**IP Gateway**	**3**	The command **set ip route preference=*value* protocol=*protocol*** did not correctly update the preference of all routes learned by the specified protocol. This issue has been resolved.
CR00012427 CR00002887	**Logging**	**3**	If a user modified the permanent log by destroying it and creating a new one, and then saved the configuration with the command **create config**, the resulting configuration file included the command **destroy log output=permanent**. Therefore when the switch restarted it destroyed the log and all entries. This issue has been resolved. The command **create config** now writes the command **set log output=permanent** to the configuration file instead of the **destroy** and **create** commands.
CR00012947	**Log**	**3**	When a user entered the command **show log receive=*ipadd* mask=*mask***, the switch displayed an error message that said **mask** was not a valid parameter. This issue has been resolved. The **mask** parameter is now valid for this command.
CR00013048	**Firewall**	**3**	When IP NAT or firewall NAT was used, the switch sometimes generated ICMP messages that specified the wrong source IP address. This meant that the response to traceroute could be incorrect. This issue has been resolved.

CR	Module	Level	Description
CR00014021	Switch	3	In certain circumstances, if the switch was configured with IP filters and STP, then some traffic would be incorrectly blocked. This issue has been resolved.

Level 4

CR	Module	Level	Description
CR00002394	IP Gateway	4	RIP would try to send route update packets when the lower link layer was down. This issue has been resolved, so that RIP no longer tries to send packets when the lower link layer is down.
CR00008006	OSPF	4	Previously, the maximum metric value for OSPF route redistribution was 16777215. This has been changed to 16777214.
CR00010399	IP Gateway	4	Previously, the ? help for some IP commands showed duplicate options. This issue has been resolved.
CR00010540	TTY	4	Sometimes, output from the CLI ? help is long enough for the page scrolling mechanism to take effect. This produces the prompt: --More-- (<space> = next page, <CR> = one line, C = continuous, Q = quit) Previously, if a user entered q in response to this prompt, the command was lost instead of regenerated. Also, commands terminated with the ? or Tab characters were added to the command history with the ? or Tab character present, which is not desirable behaviour. These issues have been resolved.
CR00010584	OSPF	4	The "operation successful" message was not produced after the command **reset ospf spf** was successfully carried out. This issue has been resolved.
CR00011743	Core, GUI	4	The GUI sometimes displayed a value above 100% for the peak utilisation of a port. This issue has been resolved.
CR00012192	Core, Utility	4	If the ? is entered at the end of an incomplete command (to obtain help), but the partially-entered command contains an error, then an error message is displayed. Previously, the incomplete command was not then re-presented to the user for editing. This issue has been resolved, so that the incomplete command is now presented to the user again after the error message.
CR00012774	IP Gateway, TCP	4	In an unusual network configuration where the IP subnet on one interface was a subset of that on another interface, it was possible for the results of a trace route to show erroneous information. This issue has been resolved. A search for an interface using an address within the interface's subnet now finds the most specific match for the address.

CR	Module	Level	Description
CR00012946	**Log**	**4**	When a user entered the command **show log receive=*ipadd***, information about all IP addresses was displayed unless the user also entered the **mask** parameter. This issue has been resolved. Specifying an IP address without a mask now limits the display to information about that IP address.
CR00013332	**Core**	**4**	When insufficient arguments were entered in the command **set interface**, an error message was not produced. This issue has been resolved, so that an error message is now correctly output.
CR00013334	**TCP**	**4**	The **delete tcp** command did not output a success message after successfully completing. The **enable tcp debug** command produced messages with the wrong module ID. These issues have been resolved.
CR00013336	**Core, NVS, TCP, TTY**	**4**	If parameters were incorrectly entered twice in some **set** or **show** commands, the resulting error message was corrupted and included meaningless characters. This issue has been resolved.
CR00013442	**Switch**	**4**	When the user attempted to enable CPU Tx health checking on an instance in the SwitchBlade controller (by using the command **enable switch healthcheck=cputx**), the switch correctly rejected this command. However, the output of the **show config dynamic** or **create config** commands included this rejected command. This issue has been resolved.

Enhancements

CR	Module	Level	Description
CR00013349	IP Gateway	-	It is now possible to specify a timeout value when enabling IP debugging. After the timeout expires, IP debugging will be automatically disabled. This helps to prevent problems from too much IP debugging clogging up the display. To specify the timeout, use the new optional **timeout** parameter in the command: enable ip debug={all|arp|packet|advertise|upnp} [timeout={none|1..2400}] The **timeout** units are seconds. The parameter is only valid if you specify an option on the **debug** parameter, because otherwise output is logged instead of being displayed. For example, to view ARP debugging information onscreen for the next 25 seconds, use the command: enable ip debug=arp timeout=25
CR00013444	IP Gateway	-	RIPv2 can now use authentication passwords that contain almost any printable character, including characters such as $, % and &. The ? character is interpreted as asking for parameter help, so this is not usable anywhere inside a password. Also, a password cannot contain double quotes (") as the first character of the string. The RIP password length is now strictly enforced at 16 characters. The command handler no longer accepts a password with more characters than this.

Features in sb275a03

Software maintenance version sb275a03 was not released.

Features in sb275a02

Software maintenance version sb275a02 includes all resolved issues and enhancements in earlier 2.7.5A versions, and the resolved issues and enhancements in the following tables.

Level 1

No level one issues

Level 2

CR	Module	Level	Description
CR00006503	IP Gateway	2	Large UDP packets sometimes caused a memory corruption, which could cause unexpected switch behaviour, including reboots. This issue has been resolved.
CR00012264	IP Gateway	2	Multicast packets were incorrectly being sent to the CPU when the switch received them on an IP interface that did not have DVMRP or PIM enabled on it. This could result in unexpectedly high CPU usage statistics. This issue has been resolved.
CR00012417	Switch, Utility	2	The switch sometimes did not process ARP requests fast enough to prevent VRRP from changing mastership in the network. This issue has been resolved.
CR00012455	BOOTP, IP Gateway	2	When the switch's BOOTP relay agent relayed a DHCP offer to a locally-attached DHCP client, the switch added an ARP entry with an incorrect port number. This meant packets from clients were forwarded by the CPU instead of being switched in hardware. This issue has been resolved.
CR00012504	BOOTP	2	There was a synchronisation issue between the software IP ARP table and the hardware IP table, when a switch was configured for BOOTP relay and multihoming concurrently. This could cause packets destined for clients to be forwarded by the CPU or dropped instead of being switched in hardware. This issue has been resolved.
CR00012725	IP Gateway, Switch	2	If a destination could be reached by both an interface route and a backup route (a static route with the same destination as the network address of the interface), in some circumstances the switch did not add either route to its hardware route table. This stopped the switch from sending traffic via either the interface or the backup route. This situation has been resolved. The switch now correctly uses the interface route when the interface is up and the backup route when the interface is down.

CR	Module	Level	Description
CR00012726	IP Gateway, VLAN, VRRP	2	Previously, if a VLAN had been configured for use as the primary interface for a VRID within VRRP, it was possible to delete the VLAN's IP interface. Also, if the IP address of the VLAN was changed (by using the command **set ip**), the priority of the VRID was not recalculated. These issues have been resolved, resulting in the following VRRP behaviour: ■ An IP interface cannot be deleted if it is one of the primary interfaces already configured for VRRP ■ An IP interface can still be deleted if it is a monitored interface, because VRRP is only monitoring the state of the interface and does not need the interface to have an IP address. ■ A VLAN cannot be destroyed if it is a monitored interface of VRRP. ■ The command **set ip** can be used to change the IP address of the interface even if VRRP is active. VRRP will recalculate the priority of the specific VRIDs using this interface. However, the IP address of the VRID cannot be changed.
CR00012782	Switch, VLAN, VRRP	2	If a VRRP interface (including the virtual VRRP MAC address) is elected as the VRRP master for a VLAN, and that VLAN has no ports on a given switch instance, the VRRP interface is not added to that switch instance. This is correct behaviour. However, if a user later added ports to the VLAN on that switch instance, the VRRP interface was still not added. This meant the switch did not respond to ARP traffic destined for the VRRP MAC address if the traffic came via that switch instance. Also, the VRRP interface was not always correctly deleted from switch instances. These issues have been resolved.
CR00012961	Switch	2	In very rare circumstances, the switch rebooted when it attempted to update the downstream port members of a layer 3 multicast stream. This issue has been resolved.

Level 3

CR	Module	Level	Description
CR00009379	Appletalk	3	When the switch was using AppleTalk, it occasionally failed to process traffic. When this occurred, entering AppleTalk commands could cause the switch to reboot. This issue has been resolved.
CR00010377	Switch	3	Inserting a slave control card into slot A of a SwitchBlade chassis reduced the number of external IP and IPX interfaces that could be created on all line cards. This issue has been resolved. The insertion of a slave control card into slot A of a SwitchBlade chassis now does not change the number of external IP and IPX interfaces that can be created on all line cards.
CR00010798	GUI	3	The web-based GUI enables users to manage switch ports by using icons to represent each port. Previously, for 8-port line cards, alternating RJ-45 port icons did not display. This issue has been resolved.
CR00011308	File, Install	3	On the slave switch controller, the list of files that the command **show file** displayed sometimes included two entries for the file **temp.ins**. This file is part of the switch's management of temporary install records. This issue has been resolved. The command now correctly shows only one entry for **temp.ins**.
CR00011774	Switch	3	The dot1qTpFdbPort MIB entry displays the ports on which the switch has learned MAC addresses. Previously, the switch started the list of ports at port 0 instead of port 1. This issue has been resolved.
CR00011849	Alarm	3	When a port was disconnected, the "Port Failure" indicator on the GUI remained in alarm state until the port was reconnected. This gave the incorrect impression that an alarm condition existed. This issue has been resolved.
CR00012323	Switch, VLAN	3	Ports were not always numbered correctly in the SNMP tables dot1dStpPortTable, dot1dTpPortTable, dot1qPortVlanTable, dot1dBasePortTable, and swiPortTable. This issue has been resolved. The switch now numbers ports in these tables consistently, with the correct indexes.
CR00012609	IP Gateway, Switch, VLAN	3	The switch sometimes flooded IGMP packets that were destined for the All Routers multicast address, instead of transmitting them correctly. This occurred when the switch had a hardware filter with an action of **forward** and the filter matched on packets with a source IP address in a particular subnet. This issue has been resolved.
CR00012651	IP Gateway	3	When the switch used IP filters, it dropped packets if they were routed out the interface on which they arrived, or if they were routed between two different logical interfaces in an interface (such as vlan2-1 and vlan2-2). This issue has been resolved. The switch now forwards packets correctly when IP filters are configured.

CR	Module	Level	Description
CR00012747	File	3	The **upload** command (**upload server=*x.x.x.x* file=*filename.ext***) did not allow files with KEY, CER or CSR extensions to be uploaded from the switch. This issue has been resolved, so these file types can now be uploaded.
CR00012786	IP Gateway	3	When a link that had RIP configured on it went down, so that the switch used an alternative route, output from the command **show ip route** sometimes displayed incorrect information when the link came back up. When the link first comes back up, the route's RIP metric is still 16, so the alternative route is still the "best" route to the target. However, **show ip route** sometimes displayed a disabled route over the original link, with a RIP metric of 16, as the best route, even though the switch correctly used the alternative route. This issue has been resolved.

Level 4

No level four issues

Enhancements

CR	Module	Level	Description
CR00012616	Core, CURE, File, Show	-	Monitoring of CPU utilisation has been enhanced. You can now set the switch to capture data about which specific functions the CPU is executing, and what level of instantaneous usage the CPU is experiencing. This allows you, in conjunction with your authorised distributor or reseller, to diagnose the causes of high rates of CPU utilisation on the switch. For more information and the new commands, see "Extended Monitoring of CPU Utilisation (CR00012616)" on page 26.

Features in sb275a01

Software maintenance release sb275a01.rez includes the resolved issues and enhancements in the following tables.

Level 1

CR	Module	Level	Description
CR00004954	Switch	1	Previously, if the switch relearned a MAC address on a new switch instance from a VLAN-tagged frame, it forwarded all frames for that MAC address as tagged frames. This happened even if the destination port was untagged. This issue has been resolved.
CR00010870	LACP	1	Previously, if LACP was enabled, resetting a line card could cause the switch to reboot. This issue has been resolved.
CR00011417	SYSR	1	The switch occasionally lost communication with the slave switch controller, for example, if the master controller took more than 30 seconds to reboot. This issue has been resolved.
CR00011601	HealthCheck	1	When the switch was receiving traffic at a high rate and processing it in the CPU (for example, during a broadcast storm) hot-swapping, resetting blades and health checks sometimes failed. This issue has been resolved.

Level 2

CR	Module	Level	Description
CR00005408	IGMP	2	Sometimes a delay of up to 40 seconds occurred before the switch sent unknown IGMP packets to the CPU for processing. This issue has been resolved.
CR00008791	PIM4	2	Previously, L2 switching of multicast traffic did not always operate correctly when L2 and L3 multicast were being used at the same time. This issue has been resolved.
CR00009693	GUI Agent	2	Previously, using the GUI to view the ARP cache could cause the switch to reboot if the ARP cache contained many thousands of records. This issue has been resolved.
CR00010029	SYSR	2	If a slave switch controller initialised with an older SYSR version than the master switch controller, and the slave switch controller contained an invalid release licence, the master controller would reboot. This issue has been resolved.

CR	Module	Level	Description
CR00010052	Switch	2	The maximum number of IP interfaces that can be defined on a line card switch instance is 60. An incorrect error message was displayed when more than 60 IP interfaces were defined on a line card switch instance. This issue has been resolved.
CR00010765	SYSR	2	Previously, the switch incorrectly allowed users to enable features on the master controller when the slave controller did not have a matching licence. This meant that the slave and the master could not synchronise. This issue has been resolved. Attempting to enable a feature on the master controller now gives an error if the slave controller does not have a matching licence for that feature.
CR00010996	Port Authentication	2	When port authentication was using a RADIUS server, it sometimes stopped working after several hours. This was because port authentication generated RADIUS Accounting Request (STOP) messages with an incorrect Acct-Session-Time value. This issue has been resolved.
CR00011002	TCP	2	When loading a file using the HTTP method, occasionally the file would not load if too many out of sequence TCP packets were received. This issue has been resolved.
CR00011247	GUI Agent	2	Previously, using the GUI to configure the output log caused the switch to reboot. This issue has been resolved.
CR00011273	SYSR	2	When Flash memory on the master switch controller contained many large files, SYSR sometimes reset itself prematurely. This issue has been resolved.
CR00011337	Environment Monitoring	2	Previously, the switch did not record the system temperature, and therefore output of the command **show system** displayed the temperature as 0°C. This issue has been resolved.
CR00011485	SYSR	2	Previously, enabling health checks and setting **time3action** to **blade** could cause the switch to reboot. This happened if a web browser was also connected to the GUI. This issue has been resolved.
CR00011600	GUI Agent	2	Previously, the GUI's "Restore Configuration" functionality did not operate correctly. This issue has been resolved.
CR00011822	HTTP Server	2	When loading a file via HTTP, the switch sometimes rebooted. This issue has been resolved.
CR00011880	GUI	2	Using the GUI to configure STP ports caused the switch to reboot. This issue has been resolved.

Level 3

CR	Module	Level	Description
CR00007863	IPv4 ICMP	3	Previously, SwitchBlade v2 linecards did not generate an ICMP redirect message in response to the first ICMP request they received. This issue has been resolved.
CR00011316	Operations	3	Previously, entering the command **set summertime** could cause extra digits to appear in the output of the commands **show ip interface** and **show config dynam=trigger**. This issue has been resolved.
CR00011339	Port Trunking	3	The command **create switch trunk** appeared twice in the configuration file created by the command **create config**—in both the switch pre-VLAN and post-VLAN sections. This issue has been resolved, so that the command now only appears in the post-VLAN section.
CR00011480	DHCPv4 Server	3	BOOTP Relay and the DHCP server cannot operate at the same time. Previously, if an attempt was made to enable one of these services and the other service was already operational, the second service was made operational. The first service stopped operating, but the switch did not report this. Now, the switch reports an error instead of enabling the second service.

Level 4

CR	Module	Level	Description
CR00011127	SYSLOG	4	System log messages of type "switch" are now indicated by the number 3 and the text "SWI", as shown in bold in the following example: 09 10:27:05 **3** SWCX **SWI** SILIC Soft reset on Port 2.3
CR00011184	HealthCheck	4	The command **show switch loopdetection** now shows all ports in both the LDF Method and BCCOUNTER Method sections of the output. Previously, the BCCOUNTER Method section only showed the ports for which **loop=bcc** was enabled.
CR00011651	Board Hotswap	4	When the command **reset switch blade** was entered with a blade number that was too high, the error message sometimes said that the maximum blade value was 10. The error message now correctly says that the maximum blade value is 8.

Enhancements

CR	Module	Level	Description
CR00011621	SYSR	-	The **show sys sysr slave** command now shows the slave switch controller's synchronisation status and the last event that occurred on the slave controller. This information is updated every 5 seconds.

STP debugging enhancements (CR00016978)

STP debugging has been enhanced in the following ways:

- A new STP debugging option turns on real-time switch port state debugging. This option displays a message every time STP asks for the state of a port to be changed. To enable the new STP debugging, use the command:

  ```
  enable stp debug=swi
  ```

  The output takes the form "<timestamp> <port> <new state>". For example, the output "13:37:47/6.4/Discarding" shows that port 6.4 moved in to the discarding state at 13:37:47.

- A new switch debugging option reports the same output as the new STP debug option, but displays the output when the STP state changes within the switching module, instead of within the STP module. Therefore, the STP debugging shows the change that STP asked for and the switch debugging shows the change that switching made. These two changes should be compatible. To enable the new switch debugging, use the command:

  ```
  enable switch debug=stp
  ```

- A new **tconly** parameter limits message debugging so that an incoming or outgoing message is only displayed if it is a topology change message (the TC-flag is set within the message). This is useful when debugging IGMP topology change notification. To turn this feature on and off, use the command:

  ```
  enable stp debug=msg tconly={on|off|yes|no}
  ```

  The default is **off**.

- All STP debugging output is now time-stamped.

- The following new command displays the current port states (in hardware) of all ports that are taking part in the STP:

  ```
  show switch stp
  ```

  The following example shows the output of this command.

```
Switch STP Port State Information at 12:09:52:
ST   Port        State
--   ----        -----
0    1.21         Fo
0    1.29         Fo
0    1.33         Bl
0    1.41         Li
```

The following table lists the fields in this output.

Parameter	Meaning	
ST	The ID number of the Spanning Tree that the port belongs to. SwitchBlades only support one Spanning Tree, numbered 0.	
Port	The switch port whose state is displayed.	
State	The STP state of the port; one of:	
	Bl	**Blocking**: forwarding disabled, learning disabled, BPDUs received
	Li	**Listening**: forwarding disabled, learning disabled, BPDUs received
	Le	**Learning**: forwarding disabled, learning enabled, BPDUs received
	Fo	**Forwarding**: forwarding enabled, learning enabled, BPDUs received
	Di	**Disabled**: forwarding disabled, learning disabled, BPDUs discarded

IGMP Snooping Query Solicitation (CR00013351)

Query solicitation minimises loss of multicast data after a topology change on networks that use EPSR or spanning tree (STP, RSTP, or MSTP) for loop protection and IGMP snooping.

When IGMP snooping is enabled on a VLAN, and EPSR or Spanning Tree (STP, RSTP, or MSTP) changes the underlying link layer topology of that VLAN, this can interrupt multicast data flow for a significant length of time. Query solicitation prevents this by monitoring the VLAN for any topology changes. When it detects a change, it generates a special IGMP Leave message known as a Query Solicit, and floods the Query Solicit message to all ports. When the IGMP Querier receives the message, it responds by sending a General Query. This refreshes snooped group membership information in the network.

Query solicitation functions by default (without you enabling it) on the root bridge in an STP topology and the master node in an EPSR topology. By default, the root bridge or master node always sends a Query Solicit message when the topology changes.

On other switches in the network, the query solicitation is disabled by default, but you can enable it by using the command:

```
set igmpsnooping vlan={vlan-name|1..4094|all}
   querysolicit={on|yes|true}
```

If you enable query solicitation on a switch other than the STP root bridge or EPSR master node, both that switch and the root or master send a Query Solicit message.

Once the Querier receives the Query Solicit message, it sends out a General Query and waits for responses, which update the snooping information throughout the network. If necessary, you can reduce the time this takes by tuning the IGMP timers, especially the **queryresponseinterval** parameter. For more information, see the “IGMP Timers and Counters” section of “How To Configure IGMP on Allied Telesyn Routers and Switches for Multicasting”. This How To Note is available from www.alliedtelesyn.co.uk/en-gb/solutions/techdocs.asp?area=howto

Disabling Query Solicitation and Display Settings

On any switch, you can disable query solicitation by using the command:

```
set igmpsnooping vlan={vlan-name|1..4094|all}
   querysolicit={off|no|false}
```

To see whether query solicitation is on or off, use the command:

```
show igmpsnooping
```

Check the new Query Solicitation field, as shown in the following figure.

```
IGMP Snooping
-------------------------------------------------------------------------
Status ........................... Enabled
Disabled All-groups ports ........ None

Vlan Name (vlan id) ..... default (1)
Fast Leave .............. Off
Query Solicitation ...... Off
Group List ..............

  No group memberships.

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

Changes to IGMP Snooping Fast Leave Command Syntax

The command syntax for the Fast Leave feature has also been changed, to make it more like the syntax for the query solicitation feature.

To enable Fast Leave on a specific VLAN, or all VLANs on the switch, the new syntax is:

```
set igmpsnooping vlan={vlan-name|1..4094|all}
   fastleave={on|yes|true}
```

To disable Fast Leave on a specific VLAN, or all VLANs on the switch, the new syntax is:

```
set igmpsnooping vlan={vlan-name|1..4094|all}
   fastleave={off|no|false}
```

The original syntax was:

```
set igmpsnooping fastleave={on|yes|true|off|no|false}
   [interface=vlan])
```

This original syntax is still valid, but we recommend using the new syntax instead.

Extended Monitoring of CPU Utilisation (CR00012616)

This Software Version includes a new feature for monitoring CPU utilisation. You can now set the switch to capture data about which specific functions the CPU is executing, and what level of instantaneous usage the CPU is experiencing. This allows you, in conjunction with your authorised distributor or reseller, to diagnose the causes of high rates of CPU utilisation on the switch.

You can set the switch to capture data continuously, or only when the CPU experiences a specific level of instantaneous usage. The switch holds up to 500 entries (10 seconds) of data about CPU utilisation.

To capture data when the CPU is experiencing a specific amount of instantaneous usage, set the start and start percentages with the command:

```
activate cpu extended start=1..100 [stop=1..100]
```

When a start percentage is set, the switch automatically disables extended monitoring once it has 500 data entries.

To enable extended monitoring, use the command:

```
enable cpu extended
```

This command also lets you capture data immediately, without first setting start and stop percentages. This adds data entries continuously, until you stop it. Only the last 10 seconds of data entries are stored.

To stop capturing data, and reset the **start** and **stop** parameters if they are set, use the command:

```
disable cpu extended
```

To remove data entries and reset the **start** and **stop** parameters in the **activate cpu extended** command, use the command:

```
reset cpu utilisation
```

This command interrupts active data capturing for a specific event. However, monitoring remains enabled, and continues to collect data. This means you can capture data for a particular event without having to disable and re-enable this feature.

To see the extended CPU utilisation information (Figure 1, Table 1), use the new optional **extended** parameter in the command:

```
show cpu extended
```

Figure 1: Example output from the **show cpu extended** command

```
CPU Utilisation ( as a percentage )
-----------------------------------
Maximum since router restarted ..... 100
Maximum over last 5 minutes ........ 100
Average since router restarted ..... 5
Average over last 5 minutes ........ 6
Average over last minute ........... 7
Average over last 10 seconds ....... 41
Average over last second ........... 100
-----------------------------------

Extended CPU Information
------------------------------------------------------------
State ............... Enabled
Current Time ........ 21:44:49 (04aa9a34 / 2573941241)
Current Install ..... 54-281.rez (5012892)
Start percent ....... -
Stop percent ........ -

msSM      Timestamp Util   Caller  Return1  Return2  Return3
------------------------------------------------------------
04aa9a34 2573927208  100 0021a384 00031c0c 00027e8c 0021a57c
04aa9a20 2573907218  100 0021a384 00031c0c 00027e8c 0021a57c
04aa9a0c 2573887230  100 0021a4b0 00031c0c 00027e8c 0021a57c
.
.
.
```

Table 1: New parameters in output of the **show cpu=extended** command

Parameter	Meaning
State	Whether extended CPU utilisation is enabled.
Current Time	Current time in hh:mm:ss format. The time in milliseconds since midnight, and the current timestamp are also in brackets.
Current Install	Current installed release, with the size of the release in brackets.
Start percent	Percentage of utilisation that the CPU must reach, if any, before the switch can begin capturing extended CPU utilisation data. A "-" shows if no percentage is set.
Stop percent	Percentage of utilisation that the CPU must fall below before the switch stops capturing extended CPU utilisation data.
msSM	Time since midnight shown in milliseconds, hexadecimal format.
Timestamp	Number of microseconds since the switch last restarted. This figure wraps at 4 294 967 295 to return to 0.
Util	Percentage of instantaneous CPU utilisation.
Caller	Return address of the function that the CPU is executing.
Return 1, Return 2, Return 3	Return addresses for function calls on the CPU stack.