Software Maintenance Release Note

# Version 321-03

# For AT-9924Ts, x900-24XT, x900-24XT-N, and x900-24XS Switches

## Introduction

This software maintenance release note lists the issues addressed and enhancements made in Maintenance Version 321-03 for Software Version 3.2.1 on AT-9924Ts, x900-24XT, x900-24XT-N, and x900-24XS (AT-9924SPsi) switches. Package file details are listed in the following table:

| | |
|---|---|
| **Maintenance Release Date** | 8 May 2008 |
| **Package File Name** | x900-24X_321-03.pkg |
| **GUI Resource File Names** | AT-9924Ts: 9924s_321-03_en_d.rsc<br>Others: x900-24x_321-03_en_d.rsc |
| **Package File Size** | 4465 kilobytes |

This maintenance release note should be read in conjunction with the following documents, available from:
www.alliedtelesis.co.nz/documentation/documentation.html

- Release Note for Software Version 3.2.1
- your switch's Document Set for Software Release 3.2.1

**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.

Allied Telesis™

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 Package

To use this maintenance version you must have a license for Software Version 3.2.1. Contact your distributor or reseller for more information. To enable this release and install it as the preferred release, use the commands:

```
enable base=x900-24X_321-03.pkg ver=3.2.1
set install=pref base=x900-24X_321-03.pkg
```

# Features in Version 321-03

Software Maintenance Version 321-03 includes the resolved issues and enhancements in earlier releases and in the following tables.

## Level 1

| CR | Module | Level | Description |
|---|---|---|---|
| **CR00013348** | **TTY** | **1** | Closing a telnet session to the switch caused the ASYN port to become unresponsive.<br>This issue has been resolved. |

## Level 2

| CR | Module | Level | Description |
|---|---|---|---|
| **CR00017581** | **Firewall** | **2** | Sometimes in congested networks, when processing certain out-of-order FTP or RSTP TCP packets the firewall could leak some memory.<br>This issue has been resolved. |
| **CR00016123** | **File management** | **2** | The switch could reboot when attempting to load files with a filename longer than 40 characters.<br>This issue has been resolved. |

| CR | Module | Level | Description |
|---|---|---|---|
| **CR00019424** | **Switching** | **2** | Jumbo frame support would not be switched on for tri-speed ports when they were set to 100M.<br>This issue has been resolved. |
| **CR00020618** | **Multicasting** | **2** | A reboot could occur whilst processing large numbers of simultaneous multicast streams with PIM and IGMP configured.<br>This issue has been resolved. |
| **CR00020914** | **DVMRP** | **2** | When using DVMRP for multicast traffic, if the switch received a leave request from the last remaining client in a multicast group before it could fully establish the DVMRP session for that group, the switch would not send a prune message to the upstream router and would continue to receive multicast traffic for that group. This issue has been resolved. |
| **CR00020934** | **DHCP snooping** | **2** | Under some configurations, enabling DHCP snooping debugging caused the switch to reboot when creating and adding a QoS policy to a port.<br>This issue has been resolved. |
| **CR00020937** | **QoS** | **2** | Under some configurations, the switch could reboot when:<br>■ applying a QoS policy to the same port twice (by using the command **set qos port=x policy=x**).<br>■ adding classifiers to a QoS flowgroup that has not been associated with a policy or traffic classifier.<br>These issues have been resolved. |
| **CR00021146** | **EPSR** | **2** | Previously, it was possible for non-EPSR messages such as IGMP snooping query solicitation messages to be sent on the EPSR control VLAN if the control VLAN was part of an STP topology. Since the control VLAN is designed as an intentional loop so that the master node can monitor the integrity of the loop, other messages on the control VLAN can form a packet storm.<br>This issue has been resolved. All switches in an EPSR ring now discard all non-EPSR messages on the control VLAN. |
| **CR00021163** | **DHCP snooping** | **2** | DHCP Snooping ARP Security should discard an ARP if the source MAC address in the Ethernet frame's MAC header does not match the sender hardware address in the ARP packet, but previously did not discard these. This issue has been resolved. |
| **CR00021342** | **BGP** | **2** | A small memory leak was occurring when receiving BGP update messages. This issue has been resolved. |
| **CR00021491** | **DVMRP** | **2** | When DVMRP had pruned an incoming multicast stream, if that stream continued to be transmitted and pruned correctly, after 24 hours the downstream DVMRP neighbour could stop successfully pruning that stream. At this point the downstream neighbour would be receiving the traffic on the interface even though it had no downstream receivers. This issue has been resolved. |
| **CR00021651** | **DHCP snooping** | **2** | When using DHCP Snooping ARP Security, maliciously formed ARPs destined for a unicast address would not be discarded. This issue has been resolved. |
| **CR00021664** | **IP gateway** | **2** | The switch would eventually reboot when utilising Jumbo packets (~9000 bytes) on ICMP echo request messages. This issue has been resolved. |

| CR | Module | Level | Description |
|---|---|---|---|
| **CR00021693** | **IP gateway** | **2** | If a Jumbo packet was received at the CPU for forwarding, the switch would reboot. This issue has been resolved. |
| **CR00019991** | **SNMP** | **2** | Previously, a corrupted SNMP request packet could cause the switch to reboot.<br>This issue has been resolved. |
| **CR00009885** | **Switch** | **2** | When the switch's Layer 2 MAC entry aged out, it did not maintain the correct linkage between Layer 2 MAC and Layer 3 IP entries.<br>This issue has been resolved. |
| **CR00013527** | **OSPF** | **2** | When the switch produced an OSPF type 7 LSA, it sometimes specified a route out of an interface that was down. This would stop the switch from forwarding traffic to the route's destination.<br>This issue has been resolved. |
| **CR00013548** | **EPSR** | **2** | Previously, if EPSR failed over, and some of the ports in the EPSR ring were trunked, and there were ARPs present on the non-master port, the ARPs would not be deleted. This meant that connectivity could be lost when the ring switched back.<br>This issue has been resolved. |
| **CR00013893** | **MSTP** | **2** | Executing the commands **disable mstp port=*number*** or **enable mstp port=*number*** would not disable or enable the port on all MSTIs.<br>This issue has been resolved. |
| **CR00014955** | **OSPF** | **2** | The switch sometimes rebooted when converting OSPF type 7 LSAs to type 5 LSAs. This issue has been resolved by increasing the robustness of the translation mechanism.<br>This issue has been resolved. |
| **CR00016262** | **Load** | **2** | When attempting to upload files from the switch using TFTP to an IPv4 server address, the switch reported an error if IPv6 was not enabled. It was not possible to upload files using TFTP to an IPv6 server address at all.<br>These issues have been resolved. |
| **CR00016303** | **Load** | **2** | The **upload** command did not always work if the **server** parameter was set with the **set load** command instead of being specified in the **upload** command.<br>This issue has been resolved. |
| **CR00017239** | **VLAN, IGMP Snooping** | **2** | When a user configured IGMP static router ports, the configuration file produced by the command **create config** could be invalid. When the switch ran the resulting configuration file on start-up, it produced an error instead of configuring the router ports.<br>This issue has been resolved. |
| **CR00017751** | **IGMP** | **2** | Previously, IGMP packets that had a source IP address of 0.0.0.0 were not accepted.<br>This issue has been resolved. Such packets are now accepted and processed. |

| CR | Module | Level | Description |
|---|---|---|---|
| **CR00018184** | **DHCP** | **2** | Previously, the switch did not have a minimum length for the Options field of DHCP messages. This conformed to RFC 2131, which states that the length of the Options field is variable, but did not conform to RFC 1531, in which the field has a minimum length of 312 bytes.<br>This issue has been resolved. To maintain interoperability with pre-RFC 2131 DHCP clients, the switch now pads the Options field to 312 bytes if it is less than this. |
| **CR00018270** | **Switch** | **2** | When aging out FDB MAC entries, it was possible for the FDB entry to be erased while there were still references to it. This could result in L3 switched traffic with a destination MAC of 00-00-00-00-00-00.<br>This issue has been resolved. |
| **CR00019713** | **OSPF** | **2** | If two or more ECMP routes from Type-5 LSAs were learned by the switch, only the route from the LSA with the highest Router ID would be inserted into the IP route table.<br>This issue has been resolved. All routes will now be inserted. |
| **CR00019923** | **LACP, VLAN** | **2** | The switch sometimes rebooted if a port was added to a private or nested VLAN when LACP was enabled.<br>This issue has been resolved. |
| **CR00020051** | **Switching** | **2** | If trunked ports were quickly removed from a device (for example, by powering off the device that the trunked ports were connected to), it was possible for the trunk's master port to become a port that was not a member of the trunk.<br>This issue has been resolved. |
| **CR00020240** | **PIM** | **2** | In PIM, if the RPF neighbour to the source or the RP changed as a result of a unicast route change, and there were slow route updates, and that meant a new route to the RPF could not be found within 5 seconds, then multicast traffic would not resume correctly once the new routing information was learned.<br>This issue has been resolved. |
| **CR00020266** | **Switching** | **2** | If a network event caused the switch to flush its layer 2 forwarding database (FDB) for a port, in some circumstances the switch also flushed hardware ARP entries that hardware layer 3 routes were still using. Possible triggers included an STP topology change somewhere else in the network, or a link flap on a port. Depending on the network configuration and/or network traffic, this issue could result in incorrectly layer 3 switched traffic.<br>This issue has been resolved. |
| **CR00020413** | **DHCP snooping, IGMP snooping** | **2** | IGMP snooping did not correctly snoop IGMP traffic that arrived on an untrusted DHCP snooping port.<br>This issue has been resolved. IGMP packets are processed now, unless IP filtering is enabled in DHCP snooping. Note that IP filtering is enabled by default, so the switch will drop IGMP packets by default if DHCP snooping does not have the source host as a current valid entry in the DHCP snooping database.<br>To disable or enable IP filtering in DHCP snooping, use the commands:<br>disable dhcpsnooping ipfiltering<br>enable dhcpsnooping ipfiltering<br>DHCP snooping must be enabled for IP filtering to take affect, but IP filtering cannot be disabled or enabled while DHCP snooping is enabled. |

# Level 3

| CR | Module | Level | Description |
|---|---|---|---|
| **CR00021585 CR00000671 CR00021008 CR00021621** | **GUI** | **3** | You can now configure and monitor x900-24XT, AT-9924Ts, and AT-9924Tsi switches through a powerful web-based GUI. For more information, see "Web-Based Graphical User Interface (GUI) (CR00021585)" on page 17. |
| **CR00010667** | **Asyn** | **3** | When the break key (Ctrl-Q) was entered, it would take a long time for the output to the Asyn (console) connection to stop displaying. This issue has been resolved. |
| **CR00011942** | **System** | **3** | When a user attempted to rename a file to a disallowed file type (for example, giving a .pkg file any other file extension), the switch displayed a misleading error message.<br>This issue has been resolved. The error message now reads "s056262: This change of filename extension is not allowed" |
| **CR00013952** | **SNMP, Port authentication** | **3** | Supplicant ports did not respond to SNMP Requests on objects in the private MIB atrPaeMib.<br>This issue has been resolved. |
| **CR00021320** | **EPSR, RSTP** | **3** | It was not possible to dynamically add VLANs on a EPSR ring port if the switch was running RSTP. VLANs could only be added by editing the boot configuration script and restarting the switch. This issue has been resolved. |
| **CR00009086** | **Switching** | **3** | When the commands **enable switch port=*number* automdi** and **disable switch port=*number* automdi** were executed from a telnet session, some INFO messages were output to the asyn0 console session instead of the telnet session.<br>This issue has been resolved. |
| **CR00013832** | **EPSR, SNMP** | **3** | When a user destroyed an EPSR domain, SNMP Requests returned information about the domain even though it no longer existed.<br>This issue has been resolved. |
| **CR00014159** | **RSTP** | **3** | RSTP (correctly) only uses the top 4 of the available 16 bits for the bridge priority. If a user enters a value that is not a multiple of 4096, the switch rounds the value down. Previously, the switch did not inform users when it rounded the value.<br>This issue has been resolved. The switch now displays an info message when it rounds the bridge priority.<br>Note that this only happens for RSTP. STP uses all 16 bits for the bridge priority. |
| **CR00017692** | **Core** | **3** | Stack dump information was not available in the **show debug** or **show system dump** commands after a fatal exception.<br>This issue has been resolved. |
| **CR00017744** | **Switch** | **3** | When switch ports were under a heavy traffic load, BPDUs could become corrupted (the CRC was missing from the end of the packet).<br>This issue has been resolved. |

| CR | Module | Level | Description |
|---|---|---|---|
| **CR00018949** | **Core** | **3** | When a PSU or FOM was hotswapped and replaced with a new unit of the same type, the switch did not update the serial number of the hotswapped unit. Output of the commands **show system** and **show log** displayed the serial number of the previous unit.<br>The same issue occurred with PICs in NSM units. For example, if you hot swapped out an NSM with a BRI PIC and then replaced that PIC with another identical PIC, and then hot swapped the NSM back into the bay, the new PIC's serial number was not displayed.<br>This issue has been resolved. |
| **CR00019207** | **Switching** | **3** | There was a small possibility that x900 and AT-9900s series switches could experience link problems for some ports with some SFPs.<br>This issue has been resolved. |
| **CR00020023** | **RSTP, SNMP** | **3** | If the STP state of a switch port in a Rapid Spanning Tree was monitored via SNMP using the BRIDGE-MIB, the value reported for a port in the Alternate role was Listening when it should have been Blocking. Similarly, Blocking was reported for a port in the Disabled role when it should have been Disabled.<br>This issue has been resolved. |
| **CR00020243** | **SNMP, IP gateway** | **3** | Previously, the switch would respond to SNMP requests destined for broadcast addresses.<br>This issue has been resolved. |
| **CR00020376** | **SNMP, IGMP** | **3** | SNMP could not always access all the group members in the IGMP interface group table.<br>This issue has been resolved. |

## Level 4

| CR | Module | Level | Description |
|---|---|---|---|
| **CR00014252** | **DDNS** | **4** | The ? help output for the command **set ddns port=?** displayed 0 to 65535 as valid values. In fact, the only valid values are 80 or 8245 for HTTP and 443 for HTTPS.<br>This issue has been resolved so that the ? help output is correct. |
| **CR00013167** | **TTY** | **4** | Using the Command Line Editor to modify a script file could cause the switch to become unresponsive, if all the characters of the script were deleted using the CTRL+Y keys, and an attempt was made to save the file using the CTRL+K+X keys.<br>This issue has been resolved. |
| **CR00013350** | **Trigger** | **4** | If a trigger was designed to activate when switch memory exceeded a given threshold, and that trigger was created when memory was above the threshold, the trigger activated as soon as it was created.<br>This issue has been resolved. Memory triggers now only activate when memory usage crosses the threshold. |

| CR | Module | Level | Description |
|---|---|---|---|
| **CR00015655** | **User, RADIUS** | **4** | Previously, the switch did not log a message if RADIUS authenticated a user logging in over telnet but RSO rejected the login.<br>This issue has been resolved.A message is now logged, with module USER, type RSO, and subtype RJCT. The message reads "Remote Security Officer access rejected from user <*name*> at <*ip-address*>." |
| **CR00017449** | **Switch** | **4** | The **set switch port speed** command incorrectly accepted a value of **1000mhalf** for tri-speed copper SFP ports.<br>This issue has been resolved. If you enter **1000mhalf**, the switch displays an error. |

## Enhancements

| CR | Module | Level | Description |
|---|---|---|---|
| **CR00017699** | **DHCP Snooping, MAC-Forced Forwarding, ARP Security** | **-** | This enhancement makes DHCP Snooping, ARP Security, and MAC-Forced Forwarding available on switches running version 321-03.<br>DHCP Snooping keeps a record of which IP addresses are currently allocated to hosts downstream of the ports on the switch, for traceability, and filters out packets from unknown hosts. With ARP security, DHCP snooping can also impose very strict control over which ARP packets are allowed into the network.<br>MAC-Forced Forwarding works in conjunction with private VLANs and DHCP snooping to increase layer 2 security. It stops hosts from seeing network traffic that is destined for other hosts.<br>For more information, see the *DHCP Snooping* and *MAC-Forced Forwarding* chapters of the *x900 Series Software Reference for Versions 2.9.1 & 3.2.1*, and the following How To Notes:<br>■ How To Use DHCP Snooping, Option 82, and Filtering on AT-9900 and x900-48 Series Switches<br>■ How To Use DHCP Snooping and ARP Security to Block ARP Poisoning Attacks<br>■ How To Use MAC-Forced Forwarding with DHCP Snooping to Create Enhanced Private VLANs<br>How To Notes are available from www.alliedtelesis.com/resources/literature/howto.aspx. |
| **CR00018895** | **SSH** | **-** | Secure Shell (SSH) no longer requires a feature licence. SSH server and client functionality now works when no feature licence is present. |
| **CR00020742** | **User Authentication** | **-** | This enhancement enables you to set rules for valid characters, lifetime, and history of passwords for user accounts in the User Authentication Database with manager or security officer privilege. These rules apply when connecting via Telnet or an asynchronous port and logging in to the command line interface, and you can apply the same rules to SSH clients by configuring SSH users to use passwords from the User Authentication Database.<br>For more information and command details, see "User Authentication Database Password Enhancement (CR00020742)" on page 19. |

| CR | Module | Level | Description |
|---|---|---|---|
| **CR00021896** | **VLAN** | **-** | This enhancement enables administrative (virtual) activation of VLANs. When a VLAN is activated virtually, its IP interface is active (and therefore usable) even if all its ports are physically disconnected. The IP interface associated with the virtually activated VLAN can be operated by protocols such as OSPF, BGP, and RIP.<br>VLAN activation is useful for VLANs that are reached through L2TP tunnels instead of through switch ports.<br>To turn virtual activation on or off, use the command:<br>SET VLAN={*vlan-name*\|1..4094\|ALL} VIRTActivation ={Yes\|No}<br>The default is **no**.<br>To see whether the VLAN has been activated virtually, use the command **show vlan** and check the new "Admin Active" field.<br>This enhancement was previously only available on Rapier, AT-8800, AT-8600 and AT-8700XL switches. Now it is available on all devices that support VLANs. |
| **CR00020926** | **DHCP Snooping** | **-** | A new feature has been added to DHCP Snooping that allows a port to be disabled if DHCP Snooping ARP Security discards an ARP.<br>To turn this feature on, use the command:<br>set dhcpsnooping arpsecurity action=disable<br>To turn it off, use the command:<br>set dhcpsnooping arpsecurity action=none |
| **CR00014172** | **BOOTP** | **-** | This enhancement enables you to associate a BOOTP relay destination with a given interface. To do this, use the new optional **interface** parameter in the command:<br>ADD BOOTp RELAy=*ipadd* INTerface=*interface*<br>BOOTP packets received on this interface are relayed to the specified relay destination only. You can define the same interface for multiple relay destinations; the switch relays any BOOTP packets received to each relay destination.<br>If you do not specify an interface, the destination becomes a "generic" destination. If the switch receives a BOOTP message on an interface for which no specific destination is defined, the switch relays the message to all generic destinations. This is the same as the behaviour prior to this enhancement.<br>To remove a destination that is associated with an interface, use the command:<br>DELete BOOTp RELAy=*ipadd* INTerface=*interface*<br>To see the interfaces that each destination is associated with, use the pre-existing command:<br>SHow BOOTp RELAy |
| **CR00016978** | **STP, MSTP, Switch** | **-** | STP and MSTP debugging has been enhanced to:<br>■ make it easier to see state information, and<br>■ only display information about Topology Change messages.<br>For command syntax and output details, see "STP and MSTP debugging enhancements (CR00016978)" on page 29. |
| **CR00017482** | **IGMP Snooping** | **-** | The IGMP snooping fast leave option has been enhanced, to make it available when multiple clients are attached to a single port on the snooping switch. For configuration information, see "IGMP snooping fast leave in multiple host mode (CR00017482)" on page 30. |

| CR | Module | Level | Description |
|---|---|---|---|
| **CR00018418** | **IGMP, MIB** | **-** | AlliedWare now includes an IGMP Group MIB. This MIB is available in the file at-igmp.mib. It has the object identifier prefix igmp ({ modules 139 }), and contains a collection of objects and traps for monitoring IGMP group membership. For more information, see "IGMP Group MIB (CR00018418)" on page 32. |
| **CR00019547** | **VLAN** | **-** | This enhancement enables administrative (virtual) activation of VLANs. When a VLAN is activated virtually, its IP interface is active (and therefore usable) even if all its ports are physically disconnected. The IP interface associated with the virtually activated VLAN can be operated by protocols such as OSPF, BGP, and RIP.<br>VLAN activation is useful for VLANs that are reached through L2TP tunnels instead of through switch ports.<br>To turn virtual activation on or off, use the command:<br>SET VLAN={*vlan-name*\|1..4094\|ALL} VIRTActivation ={Yes\|No}<br>The default is **no**.<br>To see whether the VLAN has been activated virtually, use the command **show vlan** and check the new "Admin Active" field. |
| **CR00019749** | **OSPF** | **-** | This enhancement increased the maximum acceptable payload size of an OSPF Link State Update from 1452 bytes to 1992 bytes. As an example, previously the maximum number of Router LSAs that could be received in one Link State Update was 119. This has increased to 164. |
| **CR00019989** | **Switching** | **-** | A new command has been added to modify the operation of the switch when a packet uses the default hardware multicast route. This usually happens when the switch receives new unregistered multicast traffic. The command syntax is:<br>SET SWItch DEFAultmrouteoperation={TRap\|ROUte\|DEFault}<br>The **defaultmrouteoperation** parameter specifies the operation to perform on the first packet received for a multicast stream. If you specify **trap** or **default**, the packet is copied to the CPU for processing, and is also flooded to other ports in the VLAN. Under some circumstances, especially when an L3 multicast routing protocol such as PIM is configured, the packet may not be flooded correctly to other ports on the receiving upstream VLAN. If you specify **route**, the packet is copied to the CPU and also routed on the receiving upstream VLAN. In some circumstances this may change the packet's VLAN tag. The default is **trap**.<br>**Important:** Setting this command to **route** changes the default behaviour of the switch hardware, may change the VLAN tag, and may cause issues in private VLAN configurations. We recommend that you only change this setting if clients on the receiving VLAN are not receiving the first packet of a new multicast stream and this is affecting the multicast service.<br>To see the current setting, use the command **show switch** and check the entry called "Def. Multicast Route Op". |
| **CR00020146** | **IP gateway** | **-** | The upper limit on the number of entries in an IP filter has been increased from 255 to 3072. |
| **CR00020171** | **Eth** | **-** | Log entries are now generated when Ethernet port links are taken up or down. Typical log entries are:<br>26 11:37:18 6 ETH PINT DOWN ETH0: interface is DOWN<br>26 11:37:28 6 ETH PINT UP ETH0: interface is UP |

# Features in Version 321-02

Software Maintenance Version 321-02 includes the resolved issues and enhancements in earlier releases and in the following tables.

## Level 1

| CR | Module | Level | Description |
|---|---|---|---|
| CR00013963 | Switch | 1 | Under heavy broadcast traffic, it was possible for the switch forwarding database (FDB) to lock up.<br>This issue has been resolved. |
| CR00014302 | TTY | 1 | If the switch configuration file contained the command **set tty idle**, the switch continually rebooted.<br>This issue has been resolved. |

## Level 2

| CR | Module | Level | Description |
|---|---|---|---|
| CR00010511 | BGP | 2 | Turning **defaultoriginate** on or off for a BGP peer (by using the command a**dd bgp peer**) did not cause BGP to generate an update, even if automatic updating was enabled (**enable bgp autosoftupdate**).<br>This issue has been resolved. |
| CR00013137 | File System, Hardware Management | 2 | The command **clear card totally** would not work reliably if it was the first command to access the SD card since inserting the SD card in the card slot.<br>This issue has been resolved. |
| CR00013500 | User, 802.1x | 2 | If the reauthentication period for 802.1x port authentication was set to less than 20 seconds, the switch sometimes rebooted.<br>This issue has been resolved. |
| CR00013556 | Hardware Management | 2 | Previously, if an x900-24XS (AT-9924SPsi) switch had many SPFs and XEMs installed, management of these SFP/XFPs would use approximately 20% of the available CPU resource.<br>This issue has been resolved. SFP/XFP management now has no noticable impact on CPU usage. |
| CR00014177 | STP | 2 | If a port was a tagged member of multiple VLANs, and was held in a blocking state by STP, then removing the port from one of its VLANs would cause the port to start forwarding packets. This would result in a packet storm on the looped network.<br>This issue has been resolved. |
| CR00014197 | Switch | 2 | The switch rebooted when executing the command **show switch table=port instance=*instance-number***, where *instance-number* is the instance of an installed 10Gbps XEM.<br>This issue has been resolved. |
| CR00014263 | Switch | 2 | Previously, a newly inserted SFP always used the default duplex/speed mode for that type of SFP.<br>This issue has been resolved. When a SFP is inserted, it now attempts to set its duplex/speed mode to the port's previous state. |

| CR | Module | Level | Description |
|---|---|---|---|
| CR00014824 | User | 2 | The RADIUS backup feature did not work—the **radiusbackup** parameter in the **add user** and **set user** commands had no effect.<br>This issue has been resolved. |
| CR00015736 | Switch | 2 | Sometimes IP routed traffic would be sent out the correct port, but with the destination MAC of another device on the network. This issue was most likely to occur in configurations that use multi-homed interfaces on multiple VLANs for end devices.<br>This issue has been resolved. |
| CR00015743 | Switching, Environment Monitoring | 2 | Fibre SFPs installed in the base unit of an x900-24XS (AT-9924SPsi) switch occasionally unexpectedly went into a link-down state and stayed in that state.<br>This issue has been resolved. |
| CR00015936 | Switch | 2 | It was not possible to set a tri-speed SFP to a fixed speed in the configuration script that the AT-9924SP switch runs when it starts up.<br>This issue has been resolved, so the SFP can be set to a fixed speed from the configuration script<br>Also, it was possible to use the command **set swi port=*number* speed** on an empty SFP bay. The command reported that the operation had been successful, but an inserted SFP was instead set to its previous or default setting.<br>This issue has been resolved. It is no longer possible to set the speed of an empty SFP bay. |
| CR00015949 | IPv6 | 2 | Sometimes, when a switch received an IPv6 router advertisement message, it incorrectly created a duplicate of an already-existing interface route. If a user then deleted the IPv6 interface that these two routes belonged to, the switch could reboot.<br>This issue has been resolved. |
| CR00016060 | IGMP | 2 | If a port was disabled from being an All Routers group port for IGMP, and that port received All Routers group traffic, it would incorrectly be added to the All Routers group.<br>This issue has been resolved. |
| CR00016063 | Switch | 2 | The x900-24XT switch was not sending pause flow control frames when it was configured to do so.<br>This issue has been resolved. |
| CR00016576 | IPv6 | 2 | The switch sometimes rebooted after receiving an IPv6 router advertisement, or after the command **set ipv6 interface** was entered.<br>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.<br>This issue has been resolved. |
| CR00017031 | IGMP Snooping | 2 | If a port on the switch joined and left many IP multicast groups, the switch sometimes did not transmit all multicast packets to all receivers.<br>This issue has been resolved. |

| CR | Module | Level | Description |
|---|---|---|---|
| CR00017256 | Switching | 2 | When using multi-homed IP interfaces on a VLAN, it was possible that L3 hardware switching would stop for all multi-homed interfaces on that VLAN, if one of the multi-homed interfaces was removed or went into an administratively down state.<br>This issue has been resolved. |

## Level 3

| CR | Module | Level | Description |
|---|---|---|---|
| CR00000671 | GUI | 3 | When a port was the mirror port, the port maps on GUI pages incorrectly displayed that port as available for configuration.<br>This issue has been resolved. |
| CR00007404 | MSTP | 3 | If a network running MSTP was connected to a network running RSTP and MSTP message debugging was enabled on a switch, the debug output could loop for a very long time with invalid data.<br>This issue has been resolved. |
| CR00008357 | File System, Hardware Management | 3 | Copying a large file within Flash memory or from SD card to Flash memory can take up to several minutes, and the CLI cannot be used until the copying is finished. Previously, the CLI did not warn the user of this.<br>This issue has been resolved. For command sessions on terminals directly connected to the console port asyn0, the CLI now displays a warning message that indicates how long the copying will take. |
| CR00010668 | Hardware Management, Logging | 3 | When a power supply module was hot swapped by the user, no informational messages were displayed on the console terminal to show that the hot swapping had happened.<br>This issue has been resolved. |
| CR00010971 | Hardware Management | 3 | If the switch is started up with an unsupported or incompatible type of expansion module plugged into it, it now creates a warning message in the switch log as well as on the console terminal. |
| CR00011629 | PIM, PIM6, ECMP | 3 | Previously, the switch's count of PIM4 and PIM6 bad Bootstrap Messages (BSMs) could be high, because the switch forwarded BSMs over interfaces that contained an Equal Cost Multipath (ECMP) route to the receiving interface.<br>This issue has been resolved. BSMs are no longer forwarded via all interfaces contained in an ECMP group, but only via one interface in the group. |
| CR00012230 | IP Gateway | 3 | When running the boot ROM release, it was possible to configure the switch as a DHCP client by using the command **add ip interface=*int* ip=dhcp**. However, the boot ROM release does not include the DHCP client feature, so the switch did not receive an IP address via DHCP.<br>This issue has been resolved. It is no longer possible to configure the switch as a DHCP client when running the boot ROM release. |
| CR00012495 | IGMP | 3 | When an IGMP filter was destroyed, switch ports that used the filter did not have their IGMP filter setting returned to "None".<br>This issue has been resolved. |

| CR | Module | Level | Description |
|---|---|---|---|
| CR00012585 | User | 3 | When authenticating users via RADIUS, the number of times that the switch attempts to contact the RADIUS server is determined by the Server Retransmit Count (displayed in output of the command **show radius**). Previously, this count incorrectly included the initial request. For example, a Retransmit Count of 3 meant that up to 3 attempts were made to contact the server.<br>This issue has been resolved, so that the Retransmit Count no longer counts the initial request. For example, a Retransmit Count of 3 now means that up to 4 attempts are made to contact the server. |
| CR00013213 | Triggers | 3 | The command **create trigger time** accepted invalid dates such as 00-dec-2000.<br>This issue has been resolved. |
| CR00013694 | Switch, IP Gateway | 3 | For layer 3 Jumbo frames, this software version improves initial layer 3 flow setup and handling of flows that exceed the layer 3 MTU mid-flow. |
| CR00014312 | Switch | 3 | Unnecessary interrupts could cause high CPU utilisation in networks that carry multicast traffic.<br>This issue has been resolved. |
| CR00014328 | IP Gateway, Switch | 3 | If a port had static ARP entries defined for a VLAN, then adding the port to another VLAN made those static ARP entries inactive.<br>Also, deleting a port from a VLAN would delete all static ARP entries that were defined on that port, including entries for other VLANs. Note that this deletion issue did not occur on Rapier i, AT-8800, AT-8700XL, or AT-8600 Series switches.<br>Both of these issues have been resolved. |
| CR00014930 | Test | 3 | Previously, if a test on an interface did not complete, output from the command **show test** displayed the test result as "good".<br>This issue has been resolved. If a test could not complete, it now returns a result of "BAD". |
| CR00015126 | IP Gateway | 3 | For IP filters of **type=routing**, the first filter entry could not be set to match on the following IP address/mask pair:<br>source=0.0.0.0 smask=255.255.255.255<br>This IP address/mask pair corresponds to the default route.<br>This issue has been resolved. You can now match on the default route in the first entry of a filter. |
| CR00016286 | Environmental Monitoring, Hardware Management | 3 | Hot swaps of power supply modules were not reported correctly in the Installed Hardware section of the **show system** command output, or in the switch log.<br>This issue has been resolved. |
| CR00016536 | Switch, QoS | 3 | The "?" help description for switch commands that accept a value in bytes (or similar units such as kbytes or bytes/s) incorrectly indicated that the units were bps. This applied to a number of commands, including:<br>create qos trafficclass=*value* maxburst=?<br>create qos policy=*value* dtcmaxburst=?<br>set qos red=*value* start1=?<br>set swi port=*value* bcl=?<br>set swi dlfl=?<br>This issue has been resolved. The "?" help description now displays the correct units. |

## Level 4

| CR | Module | Level | Description |
|---|---|---|---|
| CR00013976 | IGMP | 4 | The list of parameters output by the "?" help for **show ip igmp ?** incorrectly included "IGMP".<br>This issue has been resolved. |
| CR00014250 | LLDP | 4 | In output of the command **show lldp localdata**, the field lldpLocSysDesc gives information about the switch model and software version. Previously, this information was sometimes split incorrectly across 3 rows.<br>This issue has been resolved. The information now displays correctly. |
| CR00016126 | QoS, Switch | 4 | When a QoS policy was associated with a port that was set to a speed less than the maximum speed of the port, a warning message would be displayed on the console session and in the log when the port state changed to UP. This message stated that the QoS policy operation may be affected by the speed setting of the port. Having this message displayed on the console was considered unnecessary and potentially confusing.<br>This issue has been resolved.The message is now only displayed in the log. |

## Enhancements

| CR | Module | Level | Description |
|---|---|---|---|
| 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).<br>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.<br>To specify the static router ports, use the new command:<br>add igmpsnooping vlan={*vlan-name*\|1..4094} routerport=*port-list*<br>To stop ports from being static router ports, use the new command:<br>delete igmpsnooping vlan={*vlan-name*\|1..4094} routerport=*port-list*<br>To list the static router ports, use the existing command:<br>show igmpsnooping<br>and check the new "Static Router Ports" field. |
| CR00015269 | Switch, EPSR | - | EPSR uses a classifier-based hardware filter to select packets in the control VLAN. The hardware filter now only uses 2 of the available 16 bytes to match packets. This increases the number of other classifier-based features you can use when running EPSR. |
| CR00015671 | Time Service, Logging, NTP | - | This enhancement enables you to set the switch's timezone and summertime settings. For more information, see "Timezone and Summertime (CR00015671)" on page 33. |

| CR | Module | Level | Description |
|---|---|---|---|
| CR00016221 | Load, MIBs | - | With this enhancement, you can use SNMP to:<br>■ set parameters for uploading files from the switch, and<br>■ upload files to a TFTP server<br>SNMP already lets you save the current configuration to a file on the switch. You can use this with the new options to back up the configuration to a TFTP server.<br>For more information, see "Backing up the configuration with SNMP (CR00016221)" on page 36. |
| CR00017197 | SSH, User, RADIUS | - | SSH sessions to the switch can now be authenticated via RADIUS. The switch attempts to authenticate an SSH user via RADIUS if the user to be authenticated is not configured in the local user database and the switch has RADIUS configured. |

# Features in Version 321-01

Software Maintenance Version 321-01 includes the resolved issues and enhancements in the following tables.

## Level 1

No level one issues.

## Level 2

| CR | Module | Level | Description |
|---|---|---|---|
| CR00015628 | Switch | 2 | The latest revision of the AT-SPTX SPF was not fully recognised by the switch, so not all the features of the SFP could be utilised.<br>This issue has been resolved. |

## Level 3

No level three issues.

## Level 4

No level four issues.

## Enhancements

No enhancements.

# Web-Based Graphical User Interface (GUI) (CR00021585)

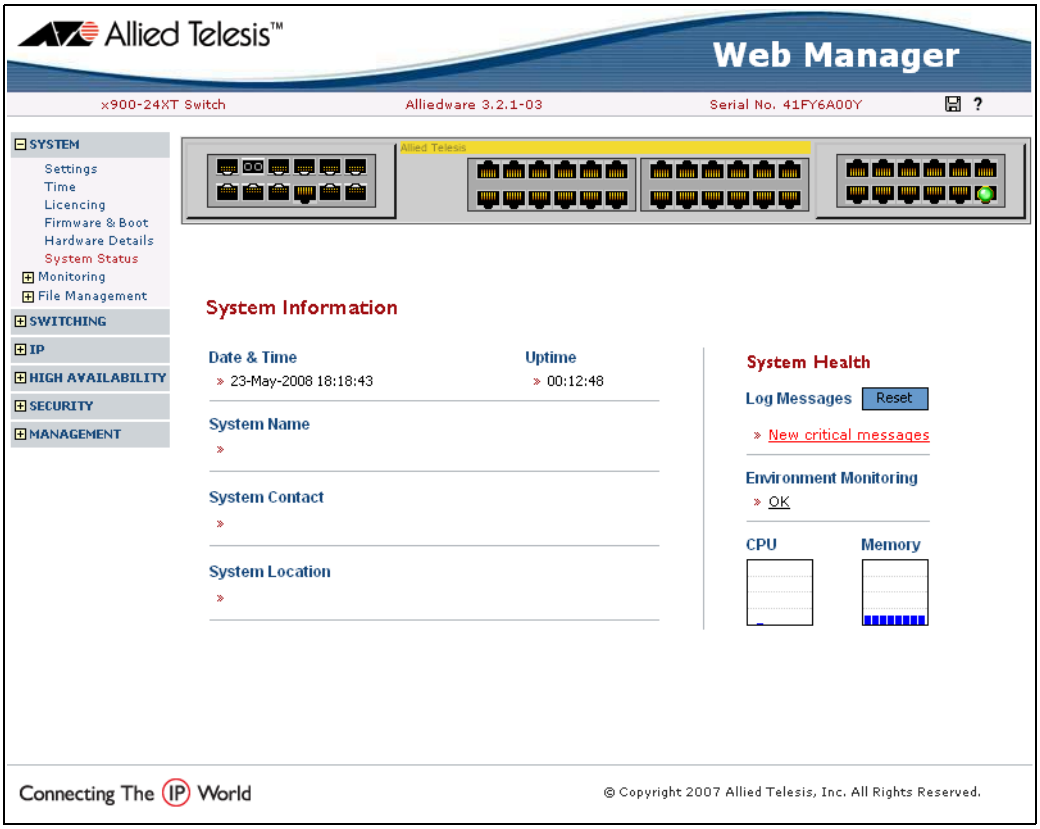
You can now configure, manage and monitor x900-24XT, AT-9924Ts, and AT-9924Tsi switches through a web-based graphical user interface (GUI).

To install and use the GUI:

6. Connect the switch into your LAN appropriately.
7. Upgrade to the current release file and restart the switch.
8. Load the current GUI resource file (.rsc) file onto the switch. The file is available from the same location as the release file (for example, from www.alliedtelesis.co.nz/support/updates/patches.html).
9. Install and enable the GUI, by entering the commands **set install=pref gui=<*filename*>** and **enable gui**.
10. Assign an IP address to VLAN 1, and set up a suitable default route.
11. Open your web browser and browse to the IP address. If you are browsing through a proxy server, you need to bypass it.
12. For that IP address, ensure that Javascript is enabled, cookies are enabled, and pop-ups are allowed. Parts of the GUI require these.

For more information, see the "Using the Graphical User Interface (GUI) on AT-9900 Series Switches" chapter of the Software Reference. The GUI looks different to the GUI for the AT-9900, but the access method is the same.

The following screenshot shows the System Status page, which opens when you first log into the switch. This page gives a quick overview of the switch port status, the environmental monitoring status, and the memory and CPU usage.



The following screenshots show the GUI menu, and therefore the available features.

# User Authentication Database Password Enhancement (CR00020742)

This enhancement enables you to set rules for valid characters, lifetime, and history of passwords for user accounts in the User Authentication Database with manager or security officer privilege. These rules apply when connecting via Telnet or an asynchronous port and logging in to the command line interface. They do not apply to user accounts used for authenticating calls.

You can also apply the same rules to SSH clients by configuring SSH users to use passwords from the User Authentication Database.

## Valid Password Characters

Valid password characters are divided into four categories:

- uppercase letters (A–Z)
- lowercase letters (a–z)
- digits (0–9)
- special symbols (any printable character not covered by one of the other categories)

You can set the minimum number of character categories that must be present in a password, by using the command:

```
set user pwdmincat=1..4 [other-options...]
```

The **pwdmincat** parameter sets the minimum number of character categories that must be present in a password. The default is 1.

For example, if you set the minimum number of categories to 2, the following passwords are valid:

- ABCDefgh
- ABCD1234
- 1234!#$%
- ABCDef12
- abcd12#$

and the following passwords are invalid:

- ABCDEFGH
- abcdefgh
- 12345678
- !#$%^&*(

If you try to set a password with less than the minimum number of character categories using the **add user**, **set user** or **set password** commands, an error message is displayed and the password is rejected.

You can display the global setting for the minimum number of character categories by using the command:

```
show user configuration
```

## Password Lifetime and Expiry

You can force passwords for all manager and security officer accounts to expire after a set number of days, using the command:

```
set user pwdlifetime={0..1000} [other-options...]
```

The **pwdlifetime** parameter sets the lifetime of the password, in days. The default is 0, which means passwords have an unlimited lifetime and never expire. The lifetime is calculated in days from 00:00 local time on the day the password lifetime is set. This lifetime applies to current and new passwords.

The current lifetime for each user is saved in the file `userpwd.sec` in either NVS or flash memory, and is retained over a power cycle or restart. On the SwitchBlade 4000 Series, the file is synchronised between switch controller cards. You can not view the file, or move it from the device.

When a user with manager or security officer privilege logs in, a message is displayed showing the number of days remaining until the password expires.

If users try to log in via the command line interface with a password that has expired, they will be allowed to log in, but they will be reminded to change their password:

```
B1L2 login: manager
Password:

Warning (2045309): User password has expired, please change
password.


Manager B1L2>
```

You can force users to change an expired password immediately after logging in, using the command:

```
set user pwdforce={yes|no|on|off|true|false}
   [other-options...]
```

Then, when users log in with an expired password, they are immediately prompted for a new password:

```
B1L2 login: manager
Password:

Warning (2045310): User password has expired, please enter a
new password.

New password:
Confirm:


Manager B1L2>
```

Users cannot log in via the GUI using an expired password.

When you change the password lifetime, your current password is checked against the new setting. If your password doesn't comply with the new setting, you are prompted to change your password.

You can display the global settings for password lifetime using the command:

```
show user configuration
```

## Password History

When you configure a password lifetime, you can prevent users from re-using old passwords by enabling password history, using the command:

```
set user pwdhistory={0|1..15} [other-options...]
```

The **pwdhistory** parameter sets the number of passwords to save for each user. A separate password history is created for each manager and security officer account. The password history includes the current password and all previous passwords up to the limit set. The default is 0, which disables password histories.

The password histories are saved in the file `userpwd.sec` in either NVS or flash memory, which is retained over a power cycle or restart. On the SwitchBlade 4000 Series, the file is synchronised between switch controller cards. You can not view the file, or move it from the device. The file size is limited to 30 KBytes. You can not add a user if it would increase the file size beyond this limit. In this case, you can either delete a user that is no longer required, or reduce the size of the password history.

When password history is enabled and users try to change their password using the **set user** or **set password** commands, the new password is checked against previous passwords saved in the password history. If an identical password is found in the history, the password is rejected.

When you enable password history, each user's current password is added to the password history.

If you reduce the size of the password history by setting **pwdhistory** to a lower value, and an account has a password history with more entries than the new limit, then the oldest passwords are removed from the account's password history until the password history is reduced to the new limit.

If you disable password history by setting **pwdhistory** to 0, all existing password histories are destroyed.

The password history for an account is also destroyed when you:

- delete the user
- purge the user
- change the user's privilege level from manager or security officer to user.

You can display the global setting for password history using the command:

```
show user configuration
```

## Secure Shell Users

Secure Shell maintains its own user database separate from the User Authentication Database. However, you can apply the rules for minimum length, valid characters, lifetime, and history of passwords from the User Authentication Database to an SSH user by configuring the SSH user to use a password from the User Authentication Database.

To apply password rules to SSH users:

1. Set the password rules:

```
set user [pwdforce={yes|no|on|off|true|false}]
    [pwdhistory=0..15] [pwdlifetime=0..1000]
    [pwdmincat=1..4] [other-options...]
```

2. Create a user in the User Authentication Database with manager or security officer privilege:

```
add user=username password=password
    privilege={manager|securityofficer} [other-options...]
```

3. Create an SSH user with the same name and configure it to use the password from the User Authentication Database:

```
add ssh user=username useuserpwd [other-options...]
```

You can modify an existing SSH user, by using the command:

```
set ssh user=username
    [{password=password|keyid=key-id|useuserpwd}]
    [ipaddress={ipadd|ipv6add}] [mask=mask]
```

You can display information about SSH users, including which users are configured to use a password from the User Authentication Database, by using the commands:

```
show ssh user
show ssh user=username
```

## Command Changes

The following table summarises the new and modified commands:

Table 1:

| Command | Change |
|---|---|
| **add ssh user** | New parameter **useuserpwd**. |
| **set ssh user** | New parameter **useuserpwd**. |
| **set user** | New parameters **pwdforce**, **pwdhistory**, **pwdlifetime**, and **pwdmincat**. |
| **show ssh user** | Asterisk indicates that the SSH user uses a password from the User Authentication Database. |
| **show user** | New field **Password Lifetime**. |
| **show user configuration** | New fields **minimum password categories to match**, **previous passwords to match**, **password lifetime**, and **force password change at logon.** |

# Command Reference Updates

This section describes each new command and the changed portions of modified commands and output screens. For modified commands and output, the new parameters, options, and fields are shown in bold.

## add ssh user

### Syntax

```
ADD SSH USER=username {PASSword=password|KEYid=key-
   id|USEuserpwd} [IPaddress={ipadd|ipv6add}] [MASk=mask]
```

### Description

This command adds a user to the list of registered users who can connect and log in via Secure Shell. If the registered user is also a member of the User Authentication Database, then the user has the associated privileges. If the SSH session username is not found in the list of registered users, and one or more RADIUS servers are defined, the user is authenticated using RADIUS. If authentication fails, the Secure Shell server will not accept the connection.

This command requires a user with security officer privilege when the device is in security mode.

The **useuserpwd** parameter specifies that the password for the corresponding user in the User Authentication Database password will be used for Secure Shell authentication. The corresponding user must exist. The parameters **password**, **keyid** and **useuserpwd** are mutually exclusive—you can only specify one.

### Examples

To create an SSH user named Admin and use the password from the User Authentication Database, use the command:

```
add ssh user=Admin use
```

## set ssh user

### Syntax

```
SET SSH USER=username [{PASSword=password|KEYid=key-
   id|USEuserpwd}] [IPaddress={ipadd|ipv6add}] [MASk=mask]
```

### Description

This command modifies a user in the list of registered users who can connect and log in via Secure Shell. This command requires a user with security officer privilege when the device is in security mode.

The **useuserpwd** parameter specifies that the password for the corresponding user in the User Authentication Database password will be used for Secure Shell authentication. The corresponding user must exist. The parameters **password**, **keyid** and **useuserpwd** are mutually exclusive—you can only specify one. To stop using the password from the User Authentication

Database, you must specify an alternative authentication method using either **password** or **keyid**.

### Examples

To modify the SSH user named Admin to use the password from the User Authentication Database, use the command:

```
set ssh user=Admin use
```

## set user

### Syntax

```
SET USEr [LOgin={True|False|ON|OFf|Yes|No}]
   [LOGINFail=1..10] [LOCkoutpd=1..30000]
   [MANpwdfail=1..5] [MInpwdlen=1..23]
   [PWDForce={Yes|No|ON|OFf|True|False}]
   [PWDHistory=0..15] [PWDLifetime=0..1000]
   [PWDMincat=1..4] [Securedelay=10..3600]
   [TACRetries=0..10] [TACTimeout=1..60]
```

### Description

This command modifies global parameters affecting the User Authentication Facility. It requires a user with security officer privilege when the switch is in security mode.

The **pwdforce** parameter specifies whether users are forced to enter a new password after logging in with an expired password. If you specify **yes**, users are forced to set a new password immediately after they log in with an expired password. If you specify **no**, a message is displayed asking the user to set a new password, but the user is not forced to set a new password. The **pwdforce** parameter applies only to users with manager and security officer privilege, and is only valid when a password lifetime has been set using the **pwdlifetime** parameter.

The **pwdhistory** parameter specifies the number of passwords to save in a password history for each user with manager or security officer privilege. Specify 0 to disable password histories. The default is 0. When you enable password histories and a user with manager or security officer privilege changes their password, the new password is checked against the list of previous passwords in the user's password history. If an identical password is found in the history, the password is rejected.

The **pwdlifetime** parameter specifies the lifetime, in days, of passwords for users with manager or security officer privilege. Specify 0 to disable password histories. The default is 0, which means passwords have an unlimited lifetime and never expire. When you set a password lifetime, and a user with manager or security officer privilege logs in, a message is displayed showing the number of days left until the password expires. When a user logs in with a password that has expired, they are prompted to change the password. If **pwdforce** is set to **yes**, the user is forced to change the password immediately after logging in.

The **pwdmincat** parameter specifies the minimum number of character categories that must be present in passwords for users with manager or

security officer privilege. The default is 1. Valid password characters are divided into four categories:

- uppercase letters (A–Z)
- lowercase letters (a–z)
- digits (0–9)
- special symbols (any printable character not covered by one of the other categories)

### Examples

To force users with manager or security officer privilege to combine uppercase and lowercase letters, digits, and special characters in their passwords, use the command:

```
set user pwdmincat=4
```

To set a password lifetime of 60 days, save a history of the last five passwords, and force a user logging in with an expired password to change the password immediately, use the command:

```
set user pwdlifetime=60 pwdhistory=5 pwdforce=yes
```

## show ssh user

### Syntax

SHow SSH USER[=*username*]

### Description

This command displays information about the users allowed to make connections to the Secure Shell server.

The **user** parameter specifies the user name being displayed.

If a user is not specified, summary information about all users is displayed. The **Auth** field now includes an asterisk if the password used is from the User Authentication Database.

If a user is specified, details are displayed about that user.

Figure 35: Example output from the **show ssh user** command

```
Secure Shell User List

User     IpAddr                        Auth  KeyId  Status
-------------------------------------------------------------
test4    fe80:230:84ff:fe0e:263e       Pass      0  enabled
test2    fe80:230:84ff:fe0e:263d       Pass      0  enabled
secoff   0.0.0.0                       RSA       5  enabled
800      0.0.0.0                       RSA       4  enabled
admin    0.0.0.0                       RSA       7  disabled
john     192.168.2.1                   Pass*     0  enabled
```

Table 3: Modified parameters in output of the **show ssh user** command

| Parameter | Meaning |
|---|---|
| Auth | The authentication method; one of "RSA" or "Pass" (password). Pass is followed by an asterisk ("*") if the password from the User Authentication Database is used. |

Figure 36: Example output from the **show ssh user** command for a specific user

```
User..................... john
Status................... Enabled
Authorisation method..... Password (user database)
RSA key ID............... 0
Shell.................... Yes
IpAddress................ 192.168.2.1
Mask..................... 255.255.255.255
Failed Logins............ 0
```

Table 4: Modified parameters in output of the **show ssh user** command for a specific user

| Parameter | Meaning |
|---|---|
| Authorisation method | The authentication method; one of "RSA" or "Password". Password is followed by "(user database)" if the password from the User Authentication Database is used. |

## show user

### Syntax

`SHow USEr[=`*`login-name`*`]`

### Description

This command displays the contents of the User Authentication Database.

The output of this command includes a new **Password Lifetime** field.

Figure 1-59: Example output from the **show user** command

```
Number of logged in Security Officers currently active.....1

Number of Radius-backup users..... 0

User Authentication Database
-------------------------------------------------------------------------------
Username: dave ()
   Status: enabled    Privilege: Sec Off   Telnet: yes   Login: yes   RBU: no
   Callback number: 0061393546786
   Calling number: 5554491
   Logins: 2          Fails: 0        Sent: 0            Rcvd: 0
   Authentications: 0 Fails: 0
   Password Lifetime: expired
Username: manager (Manager Account)
   Status: enabled    Privilege: manager   Telnet: yes   Login: yes   RBU: no
   Logins: 4          Fails: 0        Sent: 0            Rcvd: 0
   Authentications: 0 Fails: 0
   Password Lifetime: 1 days
Username: tony ()
   Status: enabled    Privilege: user      Telnet: no    Login: no    RBU: no
   Ip address: 192.168.1.5      Netmask: 255.255.255.0    Mtu: 1500
   IPX network: c0e7230f
   Apple network: 22   Apple zone: Finance
   Logins: 0          Fails: 2        Sent: 0            Rcvd: 0
   Authentications: 0 Fails: 0
-------------------------------------------------------------------------------


Active (logged in) Users
------------------------

User           Port/Device
    Login Time               Location
-------------------------------------------------------------------------
manager        Asyn 0
    14:33:22 18-Apr-2002     local
manager        Telnet 1
    14:33:22 18-Apr-2002     10.1.1.1
-------------------------------------------------------------------------
```

Table 5: New parameters in output of the **show user** command

| Parameter | Meaning |
|---|---|
| Password Lifetime | The number of days left until the user's password expires, or "expired" if the password has expired. |

## show user configuration

### Syntax

```
SHow USEr Configuration
```

### Description

This command displays global configuration parameters and counters for the User Authentication Facility.

The output of this command includes new fields.

Figure 1-60: Example output from the **show user configuration** command

```
User module configuration and counters
------------------------------------------------------------------------------
Security parameters
  login failures before lockout ............     4            (LOGINFAIL)
  lockout period ...........................    20 seconds    (LOCKOUTPD)
  manager password failures before logoff ..     3            (MANPWDFAIL)
  maximum security command interval ........    30 seconds    (SECUREDELAY)
  minimum password length ..................     6 characters (MINPWDLEN)
  TACACS retries ...........................     3            (TACRETRIES)
  TACACS timeout period ....................     5 seconds    (TACTIMEOUT)
  minimum password categories to match .....     1            (PWDMINCAT)
  previous passwords to match ..............    15            (PWDHISTORY)
  password lifetime ........................    38 days       (PWDLIFETIME)
  force password change at logon ........... enabled          (PWDFORCE)
  semi-permanent manager port .............. none

Security counters
  logins                          7     authentications               23
  managerPwdChanges               0     defaultAcctRecoveries          0
  unknownLoginNames               1     tacacsLoginReqs                1
  totalPwdFails                   5     tacacsLoginRejs                1
  managerPwdFails                 3     tacacsReqTimeouts              0
  securityCmdLogoffs              1     tacacsReqFails                 0
  loginLockouts                   1     databaseClearTotallys          0
------------------------------------------------------------------------------
```

Table 6: New parameters in output of the **show user configuration** command

| Parameter | Meaning |
|---|---|
| minimum password categories to match | The minimum number of character categories that must be present in passwords for users with manager or security officer privilege. |
| previous passwords to match | The number of passwords to save in a password history for each user with manager or security officer privilege, or "disabled" if password histories are disabled. |
| password lifetime | The lifetime, in days, of passwords for users with manager or security officer privilege, or "disabled" if passwords do not expire. |
| force password change at logon | Whether users with manager or security officer privilege logging in using an expired password are forced to change their password immediately; either "enabled" or "disabled". |

# STP and MSTP debugging enhancements (CR00016978)

## Debugging command and output enhancements

STP and MSTP debugging have been enhanced in the following ways:

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

  ```
  enable stp[={stp-name|ALL}] debug=swi

  enable mstp 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.

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

  ```
  enable switch debug={stp|mstp}
  ```

- 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 one of the commands:

  ```
  enable stp[={stp-name|ALL}] debug=msg
     tconly={on|off|yes|no}

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

  The default is **off**.

- All STP and MSTP debugging output is now time-stamped.

## New *show* commands

The following new commands display the current port states (in hardware) of all ports that are taking part in STP or MSTP:

```
show switch stp
show switch mstp
```

The following example shows the output of the **show switch stp** command.

```
Switch STP Port State Information at 12:09:52:
ST   Port        State
--   ----        -----
0    2            Fo
0    3            Fo
0    5            Bl
0    6            Li
```

The following example shows the output of the **show switch mstp** command.

```
Switch MSTP Port State Information
Switch STP Port State Information at 04:50:37:
ST   Port   State
--   ----   -----
1    33     Fo
1    48     Fo
2    33     Fo
2    48     Fo
3    33     Fo
3    48     Fo
```

The following table lists the fields in this output.

Table 1-1:

| Parameter | Meaning | |
|---|---|---|
| ST | The ID number of the Spanning Tree that the port belongs to. | |
| Port | The switch port whose state is displayed. | |
| State | The STP state of the port. | |
| | Bl | **Blocking**: forwarding disabled, learning disabled, BPDUs received |
| | Li | **Listening**: forwarding disabled, learning disabled, BPDUs received (only on AT-9800 series switches) |
| | 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 fast leave in multiple host mode (CR00017482)

The IGMP snooping fast leave option has been enhanced, to make it available when multiple clients are attached to a single port on the snooping switch. Fast leave now has two modes available:

- **multiple host mode**—the new feature. In multiple host mode, the snooper tracks which clients are joined to a given IP multicast group on a given port. As soon as the last client leaves a group on a port, the snooper shuts off the multicast to that port.
- **single host mode**—the existing functionality. In single host mode, as soon as the snooper receives a leave message for a group on a port, it shuts off

the multicast. This mode assumes that there are no other clients on the port that are still interested in receiving the multicast, so is suitable only when clients are directly attached to the snooper.

To specify the new multiple mode, use the command:

```
set igmpsnooping vlan={vlan-name|1..4094|all}
   fastleave=multiple
```

To specify single mode, use either of the commands:

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

The command **show igmpsnooping vlan** has also been enhanced. The new command syntax is:

```
show igmpsnooping vlan={vlan-name|1..4094|all}
   [group={multicast-ip-address|allgroups}] [detail]
```

The **group** parameter lets you display information for only one group or for only the All Groups port (the **allgroups** option).

The **detail** parameter displays more detailed information, including expiry times for each port, and in the case of multiple host fast leave mode, the list of hosts on a port. The following example shows this.

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

Vlan Name (vlan id) ..... default (1)
Fast Leave ............... Multiple Host Topology
Query Solicitation ...... Off
Static Router Ports ..... None
Group List ............... 2 groups

  Group 224.0.1.22                          Timeout in 256 secs
    Port 24                                 Timeout in 257 secs
      Hosts: 1
        00-00-cd-27-be-f5 (172.20.176.200)  Timeout in 257 secs

  Group 239.255.255.250                     Timeout in 258 secs
    Port 24                                 Timeout in 259 secs
      Hosts: 1
        00-00-cd-27-be-f5 (172.20.176.200)  Timeout in 259 secs
```

# IGMP Group MIB (CR00018418)

AlliedWare now includes an IGMP Group MIB. This MIB is available in the file at-igmp.mib.

The IGMP Group has the object identifier prefix igmp ({ modules 139 }), and contains a collection of objects and traps for monitoring IGMP group membership.

The following objects are defined:

- igmpIntInfo ({ igmp 1 }) is a collection of objects for managing IGMP-capable interfaces:
  - igmpInterfaceTable ({ igmpIntInfo 1 }) is a table of IGMP-capable IP interfaces, indexed by interface.
  - igmpIntStatsTable ({ igmpIntInfo 2}) is a table of statistics for IGMP-capable IP interfaces.
- igmpIntMember ({ igmp 9 }) is a collection of objects for managing IGMP group membership:
  - igmpIntGroupTable ({ igmpIntMember 1 }) is a table of IP multicast group memberships.
- igmpSnooping ({ igmp 10 }) is a collection of objects for managing IGMP snooping:
  - igmpSnoopAdminInfo ({ igmpSnooping 1 })
  - igmpSnoopAdminEnabled ({ igmpSnoopAdminInfo(1) 1 }) is a boolean value indicating whether IGMP Snooping is globally enabled.
  - igmpSnoopVlanTable ({ igmpSnooping 2 }) is a table of layer 2 interfaces performing IGMP snooping.
  - igmpSnoopGroupTable ({ igmpSnooping 3 }) is a table of IGMP groups snooped on layer 2 interfaces.
  - igmpSnoopPortTable ({ igmpSnooping 4 }) is a table of ports in layer 2 interfaces that are currently members of multicast groups.
  - igmpSnoopHostTable ({ igmpSnooping 5 }) is a table of hosts receiving multicast data.

# Timezone and Summertime (CR00015671)

With this enhancement, you can:

- set an internationally recognised timezone and set that timezone's UTC offset
- define and enable summer time settings, including the offset value that summer time uses alongside the UTC offset.

## Setting a timezone

You can define a timezone for the switch to use. Once defined, the system uses this timezone's time for operation.

To set a timezone, use the command:

```
set timezone[=time-zone-name]
   [utcoffset=std-utc-offset]
```

| Parameter | Description |
|---|---|
| TIMEzone | The timezone the switch should use. *time-zone-name* is a character string from 1 to 7 characters representing the abbreviation for this timezone's Standard Time, for example NZST.<br>Default: No default. |
| UTCoffset | The time difference between local time on the switch's clock and UTC/GMT. The offset is used to calculate UTC time system-wide. *std-utc-offset* is a positive or negative number in the format hh[:mm], where hh=0-23 and mm=0-59. If hours are specified then mm is optional.<br>Default: 0 |

To see the current timezone settings, use the command:

```
show timezone
```

To clear the existing timezone settings, and return the UTC offset to its default value of 0, use the command:

```
clear timezone
```

## Configuring summer time

Summer time is also known as Daylight Saving Time. When enabled, the system automatically sets the clock ahead when summer time begins, and sets the clock back when it ends.

You can enable summer time, specify when summer time starts and ends, and define a summer time offset value.

To enable summer time, use the command:

```
enable summertime
```

When summer time is enabled, but no summer time definition is set with the **set summertime** command, the switch uses North American settings as the

default. Therefore, in North America, summer time values do not need to be defined, just enabled.

Two formats can define the beginning and end of summer time, and only one may be used at a time.

| For this format... | Then... |
|---|---|
| non-recurring fixed dates using the **startdate** and **enddate** parameter. | these dates apply only once on the dates given, and you must set new dates for the following year. |
| a recurring rule specifying the month, numbered week of the month, and day of the week | it stays in effect until it is either changed or reset. The date when summer time starts and ends is automatically recalculated each year. |

To set a recurring summer time definition, use the command:

```
set summertime[=summertime-zone-name] startmonth=month
   startweek=week startday=day starttime=hh:mm endmonth=month
   endweek=week endday=day endtime=hh:mm offset=offset
```

To set a non-recurring fixed summer time definition, use the command:

```
set summertime[=summertime-zone-name] startdate=date
   starttime=hh:mm enddate=date endtime=hh:mm offset=offset
```

| Parameter | Description |
|---|---|
| SUMMertime | The abbreviation used to represent summer time for this time zone, for example, **nzdt**.<br>Default: **dst** |
| STARTDAte | The absolute summer time start date. *Date* is in the d-mmm-yyyy, dd-mmm-yy, or dd-mmm-yyyy format. *month* is the first three letters of the month, for example, **apr**.<br>If you specify a **startdate**, you must specify an **enddate**. |
| STARTMonth | The start month for a recurring rule. *month* is the first three letters of the month, for example, **jan**.<br>Default: **apr** |
| STARTWeek | The start week for a recurring rule. *week* is the number of the week within its month, a number between 1 and 5. The value 5 always means the last week in the month and can be used in any month.<br>Default: **1** |
| STARTDay | The start day for a recurring rule. *day* is the name of a day of the week using the first three letters of the day only, for example **mon**, **tue**, **wed**.<br>Default: **sun** |
| STARTTIme | The start time. *time* is the time in hh:mm:ss format, where **hh**=0-23 **mm**=0-59, and **ss**=0-59. If **hh** is specified then **mm** is optional. If **mm** is specified then **ss** is optional.<br>Default: **02:00** (2:00am) |
| ENDDate | The absolute summer time end date. *Date* is in the d-mmm-yyyy, dd-mmm-yy, or dd-mmm-yyyy format. *month* is the first three letters of the month, for example, **jun**.<br>If you specify an **enddate**, you must specify a **startdate**. |
| ENDMonth | The end month for a recurring rule. *name* is the first three letters of the month, for example **jun**.<br>Default: **jun** |

| Parameter | Description |
|---|---|
| ENDWeek | The end week for a recurring rule. *week* is the number of the week within its month, a number between 1 and 5.<br>Default: **5** |
| ENDDay | The end day for a recurring rule. *day* is the name of a day of the week using the first three letters of the day only, for example **mon**, **tue**, **wed**.<br>Default: **sun** |
| ENDTime | The end time. *time* is the time in hh:mm:ss format, where **hh**=0-23 **mm**=0-59, and **ss**=0-59. If **hh** is specified then **mm** is optional. If **mm** is specified then **ss** is optional.<br>Default: **02:00** (2:00am) |
| Offset | The offset value, from 0 to 120 minutes. The value entered in this parameter is the amount of time by which Standard Time changes when summer time begins and ends.<br>Default: **60** |

To see the current summertime settings, use the command:

```
show summertime
```

To disable summer time, use the command:

```
disable summertime
```

To clear the existing summer time UTC offset and settings, and reset the default North American summer time definition, use the command:

```
clear summertime
```

You still need to set the local time using the command:

```
set system time
```

If you set the time **before** you configure summer time settings, we suggest you set the time to standard time because the switch automatically changes the time to summer time when applicable. If you set the time **after** configuring summer time, we suggest you set the time to the current local time—either summer time or standard time, whichever applies.

# Backing up the configuration with SNMP (CR00016221)

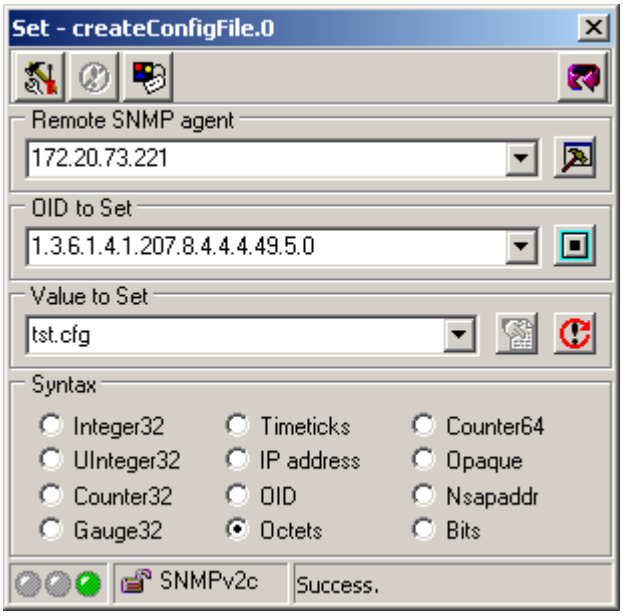
With this enhancement, you can use SNMP to:

- set parameters for uploading files from the switch, and
- upload files to a TFTP server

SNMP already lets you save the current configuration to a file on the switch. You can use this with the new options to back up the configuration to a TFTP server. To do this, perform the following steps.

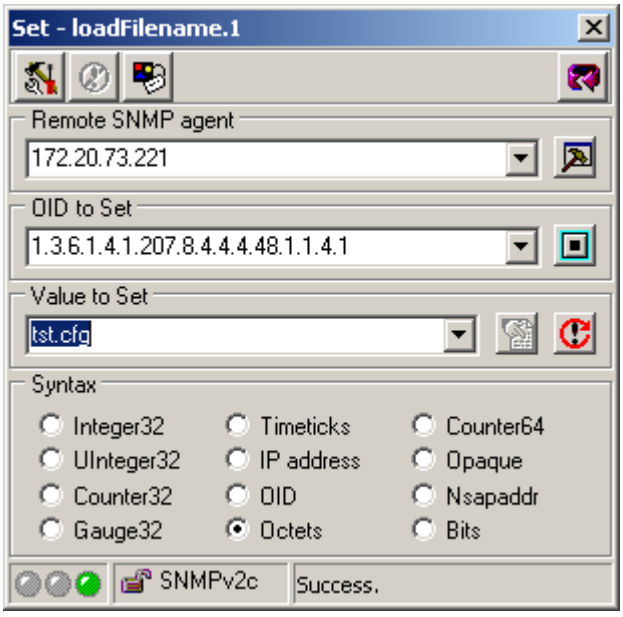
## 1. Save the configuration

To save the current configuration, use SNMP SET createConfigFile. The following screenshot shows this for a file called tst.cfg.



## 2. Set the load parameters

To specify the server IP address, use SNMP SET loadServer. To set the filename, use SNMP SET loadFilename. The following screenshot shows setting the filename to tst.cfg.




## 3. Upload the file

To upload the file, use SNMP SET loadStatus and set it to a value of 8. The following screenshot shows this.