Maintenance Release Note and Software Reference Supplement

AlliedWare Version 292-07

This software maintenance release note for Allied Telesis routers and switches describes:

- Software version files for each router and switch model ("Models and Version Files" on page 3)
- How to enable this new software version on your router or switch ("Enabling and Installing this Version" on page 4)
- New features and enhancements in maintenance version 292-07, followed by other new features and enhancements since Software Version 2.9.1—a supplement to the Software References for 2.9.1 ("Software Reference Supplement— New Features and Enhancements" on page 5)
- Issues resolved in maintenance version 292-07, followed by other issues resolves since Version 291-23 ("Issues Resolved in 292-07" on page 198)

Contents

Models and Version Files

Caution: Using a maintenance version file on the wrong model may cause unpredictable results, including disruption to the network.

Table 1: Switch and router models and software version files for this maintenance release

Models	Series	Release File	Date	Size (bytes)	GUI file
AR415S, AR440S, AR441S, AR442S, AR450S	AR400	54292-07.rez	Mar 2012	5063492	415s_292-07_en_d.rsc 440s_292-07_en_d.rsc 441s_292-07_en_d.rsc 442s_292-07_en_d.rsc 450s_292-07_en_d.rsc
AR750S, AR750S-DP, AR770S	AR7x0S	55292-07.rez	Mar 2012	4189352	750s_292-07_en_d.rsc (AR750S and AR750S-DP)
AR725, AR745	AR7x5	52292-07.rez	Mar 2012	4221652	_725_292-07_en_d.rsc _745_292-07_d.rsc
AT-8624T/2M, AT-8624PoE, AT-8648T/2SP	AT-8600	sr292-07.rez	Mar 2012	2563812	8624t_292-07_en_d.rsc 8624poe_292-07_en_d.rsc 8648t_292-07_en_d.rsc
AT-8724XL, AT-8748XL	AT-8700XL	87292-07.rez	Mar 2012	2472552	8724_292-07_en_d.rsc 8748_292-07_en_d.rsc
Rapier 24i, Rapier 48i, Rapier 16fi	Rapier i	86292-07.rez	Mar 2012	4699684	r24i_292-07_en_d.rsc r16i_292-07_en_d.rsc r48i_292-07_en_d.rsc
Rapier 48w	Rapier w	86292-07.rez	Mar 2012	4699684	-
AT-8824, AT-8848	AT-8800	86292-07.rez	Mar 2012	4699684	8824_292-07_en_d.rsc 8848_292-07_en_d.rsc
AT-8948, x900-48FE, x900-48FE-N	x900-48	89292-07.rez	Mar 2012	4990064	-
AT-9924T, AT-9924SP, AT-9924T/4SP	AT-9900	89292-07.rez	Mar 2012	4990064	9924_292-07_en_d.rsc
AT-9812T, AT-9816GB	AT-9800	sb292-07.rez	Mar 2012	4075596	9812_292-07_en_d.rsc 9816_292-07_en_d.rsc

Caution: 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.

Enabling and Installing this Version

To obtain the software version files (Table 1) for your routers and switches, contact your authorised Allied Telesis distributor or reseller. To use this maintenance release, you must have a release license that supports Software Release 2.9.2, or an 'any' release licence. Contact your distributor or reseller for more information about licences.

1. **Load the new release file.**

   For detailed information, see the *Managing Configuration Files and Software Versions* chapter in the *Software Reference*.

2. **Check the release.**

   To see which base release is already enabled on your router or switch, use the command:

   ```
   show release
   ```

   If this shows an **any** license, you do not need to specifically enable this new release. Go to step 4 to install this new version.

   If this shows a 2.9.1 base release license, you must enable this new release file. Go to step 3.

3. **Enable the release.**

   To enable this release, use the command:

   ```
   enable rel=xx292-07.rez num=2.9.2
   ```

4. **Install this as the preferred release.**

   To install this as the preferred release, use the command:

   ```
   set install=pref rel=xx292-07.rez
   ```

   where *xx* is the prefix to the filename, as shown in Table 1 on page 3.

For example, to install the release on an AT-8824 switch, use the commands:

```
enable rel=86292-07.rez num=2.9.2
set install=pref rel=86292-07.rez
```

Software Reference Supplement

New Features and Enhancements

This section describes all the features and enhancements in this AlliedWare release since the *AlliedWare™ Operating System Software Reference for Version 2.9.1* for supported routers or switches. To see an overview of the new features and enhancements in this software maintenance version, see Table 2.

In Table 2, for each product series:

- "Y" in a column indicates that the new feature or enhancement is available in this maintenance version for that product series.
- "-" in a column indicates that the feature or enhancement does not apply to that product series.

Table 2: Overview of new features and enhancements by software version

Feature or Enhancement	Module	AR44x/AR450S/ AR415S	AR7x5	AR750S/AR770S	Rapier i	Rapier w	AT-8800	AT-8600	AT-8700XL	AT-8948 / x900-48	AT-9900	AT-9800
New features and enhancements in 292-07 since 292-06												
"New show ipsec isakmp command (CR00035046)" on page 140	**IPSec, ISAKMP**	Y	Y	Y	Y	Y	Y	–	–	–	–	–
New features and enhancements in 292-05 since 292-04												
"ISAKMP responder rekey (CR00032324)" on page 141	**IPSec, ISAKMP**	Y	Y	Y	Y	Y	Y	–	–	–	–	–
New features and enhancements in 292-04 since 292-03												
"SQoS—virtual bandwith limit exceeded (CR00033115)" on page 95	**SQoS**	Y	Y	Y	Y	Y	–	–	–	–	–	–
"RSTP Slow convergence time agreement BPDU time (CR00033330)" on page 37	**STP**	–	–	–	Y	Y	Y	Y	Y	Y	Y	Y

Table 2: Overview of new features and enhancements by software version (cont.)

Feature or Enhancement	Module	AR44x/AR450S/ AR415S	AR7x5	AR750S/AR770S	Rapier i	Rapier w	AT-8800	AT-8600	AT-8700XL	AT-8948 / x900-48	AT-9900	AT-9800
"Filters to define acceptable X.509 certificates (CR00032322)" on page 149	**ISAKMP**	Y	Y	Y	Y	Y	Y	–	–	–	–	–
"CRL-DPs included in PKI X509 certificates are now decoded (CR00032323)" on page 144	**PKI**	Y	Y	Y	Y	Y	Y	–	–	–	–	–
"PPPOE Ignore Unknown Session (CR00032988 & CR00034376)" on page 52	**PPPoE**	Y	Y	Y	Y	Y	Y	–	–	Y	–	Y
"New PPP command parameter [PADRretry=0..10000] (CR00032805)" on page 56	**PPPoE**	Y	Y	Y	Y	Y	Y	–	–	Y	–	Y
"Reserved BGP IANA ASNs range increased (CR00033456)" on page 83	**BGP**	Y	Y	Y	Y	Y	Y	–	–	Y	Y	Y
"TPID in 802.1q tags sent from router ETH interface are now configurable (CR00032804)" on page 41	**Swi, Eth**	Y	Y	Y	–	–	–	–	–	–	–	–
New features and enhancements in 292-02 since 292-01												
"ISAKMP responder rekey (CR00032324)" on page 141	**ISAKMP**	Y	Y	Y	Y	Y	Y	–	–	–	–	–
"Longer PPP interface description (CR00032369)" on page 57	**PPP**	Y	Y	Y	Y	Y	Y	–	–	Y	Y	Y
"Ping and trace to domain (CR00032444)" on page 64	**DNS**	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
New features and enhancements in 292-01 since 291-23												
"DynDNS periodic update (CR00030779)" on page 67	**DNS**	Y	–	Y	–	–	–	–	–	–	–	–
"PPPoE AC improved interoperability (CR00030904)" on page 58	**PPP**	Y	Y	Y	Y	Y	Y	–	–	Y	–	Y
"Improved performance (CR00029835)" on page 49	**xDSL**	Y	–	–	–	–	–	–	–	–	–	–
"ARP flush for PPP interfaces (CR00030236)" on page 57	**PPP, ARP, IP**	Y	Y	Y	Y	Y	Y	–	–	Y	–	Y

Table 2: Overview of new features and enhancements by software version (cont.)

Feature or Enhancement	Module	AR44x/AR450S/ AR415S	AR7x5	AR750S/AR770S	Rapier i	Rapier w	AT-8800	AT-8600	AT-8700XL	AT-8948 / x900-48	AT-9900	AT-9800
"Error message displays IP address (CR00031970)" on page 73	**DHCPv4**	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
"Increase in positions available for IPsec policies (CR00032032)" on page 170	**IPsec**	Y	Y	Y	Y	Y	Y	–	–	–	–	–
"ARP security broadcast filter (CR00030472)" on page 74	**DHCP snooping**	–	–	–	–	–	–	–	–	Y	Y	–
"Switch port longer description (CR00031879)" on page 22	**L2 Switching**	–	–	–	Y	Y	Y	Y	Y	–	–	–
"Diffie-Hellman group and usepfkey parameter dependence (CR00028466)" on page 167	**IPsec**	Y	Y	Y	Y	Y	Y	–	–	–	–	–
"Router Port Link Disable (CR00028764)" on page 42	**Swi, Eth**	Y	Y	Y	–	–	–	–	–	–	–	–
"Security enhancement for untrusted private firewall interfaces (CR00029643)" on page 133	**Firewall**	Y	Y	Y	Y	Y	Y	–	–	–	–	Y
"IPsec Dead Peer Detection (DPD) (CR00027606)" on page 150	**IPsec**	Y	Y	Y	Y	Y	Y	–	–	–	–	–
"Firewall Application Detection System (ADS) (CR00029938)" on page 110	**Firewall**	Y	–	Y	–	–	–	–	–	–	–	–
"Loop Detection Frames with 802.1X and MAC-based Port Auth (CR00029957)" on page 23	**Switching**	–	–	–	Y	Y	Y	Y	Y	Y	Y	–
"Diffie-Hellman Groups 5 and 14 (CR00030097)" on page 161	**IPsec, Encryption**	Y	Y	Y	Y	Y	–	–	–	–	–	Y
New features and enhancements in 291-23 since 2.9.1* *Note: This section of the table lists all the new features and enhancements in 291-23 since 291-04. To see which 2.9.1 software maintenance version first supported particular features and enhancements, see the *Software Maintenance Release Note for Maintenance Version 291-23*, available from the Software Downloads section of http://www.alliedtelesis.com/support.												
"VLAN logical interfaces increased (CR00029290)" on page 23	**VLAN, Swi, IP**	–	–	–	Y	Y	Y	Y	Y	–	–	–
"Reverse Telnet transparent mode (CR00027944)" on page 179	**Telnet**	Y	Y	Y	Y	Y	Y	–	–	–	–	–

Table 2: Overview of new features and enhancements by software version (cont.)

Feature or Enhancement	Module	AR44x/AR450S/ AR415S	AR7x5	AR750S/AR770S	Rapier i	Rapier w	AT-8800	AT-8600	AT-8700XL	AT-8948 / x900-48	AT-9900	AT-9800
"IPsec Passthrough (CR00028385)" on page 115	**IPSec**	Y	Y	Y	Y	Y	Y	–	–	–	–	–
"Support VPN clients with no attributes in the final XAuth ack (CR00028456)" on page 167	**ISAKMP**	Y	Y	Y	Y	Y	Y	–	–	–	–	–
"AT SysInfo MIB support for memory OID (CR00024907)" on page 180	**SNMP MIB**	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
"Maximum number of IPsec bundles increased (CR00026765)" on page 168	**IPSec**	Y	Y	Y	Y	Y	Y	–	–	–	–	–
"Firewall router IP alert option (CR00027414)" on page 135	**Firewall**	Y	Y	Y	Y	Y	Y	Y	–	–	–	–
"Description parameter for Eth interfaces (CR00027921)" on page 47	**Eth**	Y	Y	Y	–	–	–	–	–	–	–	–
"Firewall Public Interface Dynamic Assigned IP Address (CR00023375)" on page 136	**Firewall**	Y	Y	Y	Y	Y	Y	–	–	–	–	Y
"MLD proxy (CR00023463)" on page 85	**IPv6 mullticast**	Y	Y	Y	Y	Y	Y	–	–	Y	Y	Y
"SNMP MIB enhancements for DHCP and Port Authentication (CR00025844)" on page 181	**DHCP, portauth, MIBs**	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
"Syslog start-up delay (CR00026520)" on page 177	**Log**	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
"MAC address format for MAC-based authentication (CR00026718)" on page 107	**Port Auth**	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
"User Authentication Password Enhancement (CR00020742)" on page 97	**User Authentication**	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
"DHCP snooping ARP security—disable port (CR00020926)" on page 75	**DHCP Snooping**	–	–	–	Y	Y	Y	Y	Y	Y	Y	–
"External Loop Detection and Termination (CR00026527)" on page 23	**Switching**	–	–	–	Y	Y	Y	Y	Y	Y	Y	–

Table 2: Overview of new features and enhancements by software version (cont.)

Feature or Enhancement	Module	AR44x/AR450S/ AR415S	AR7x5	AR750S/AR770S	Rapier i	Rapier w	AT-8800	AT-8600	AT-8700XL	AT-8948 / x900-48	AT-9900	AT-9800
"More DHCP snooping classifiers (CR00019005)" on page 75	**DHCP snooping**	–	–	–	–	–	–	–	–	Y	Y	–
"Denial of Service Attack Protection (CR00020057)" on page 109	**DoS Attack Prevention**	–	–	–	–	–	–	Y	–	–	–	–
"Compatibility with SAMSUNG SmartViewer 2.0 (CR00020882)" on page 137	**Firewall**	Y	Y	Y	Y	Y	Y	–	–	–	–	Y
"ADSL2 and ADSL2+ on AR441S (CR00021615)" on page 49	**ADSL, Core**	Y	–	–	–	–	–	–	–	–	–	–
"Support for the new AT-A65 expansion module (CR00023174)" on page 14	**Expansion module**	–	–	–	–	–	–	–	–	–	–	–
"Private VLAN uplink port increase (CR00023867)" on page 34	**Switching**	–	–	–	Y	Y	Y	Y	Y	–	–	–
"New ipfilter and ipfragment parameters for PPP templates (CR00023990)" on page 59	**PPP**	Y	Y	Y	Y	Y	Y	–	–	Y	Y	Y
"Borrowed IP address for PPP unnumbered IP address (CR00019706)" on page 60	**PPP**	Y	Y	Y	Y	Y	Y	–	–	Y	Y	Y
"DNS names in ISAKMP and IPsec policies (CR00021106)" on page 168	**IPsec, ISAKMP**	Y	Y	Y	Y	Y	Y	–	–	–	–	–
"Performance improvement (CR00021262)" on page 168	**IPsec**	Y	Y	Y	Y	Y	Y	–	–	–	–	–
"SNMP trap delay (CR00021769)" on page 174	**SNMP**	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
"Improved recovery time (CR00021852)" on page 172	**EPSR**	–	–	–	–	–	–	–	–	Y	Y	–
"Improved SHDSL train up time (CR00022331)" on page 50	**SHDSL**	Y	–	–	–	–	–	–	–	–	–	–
"Link status trap delay (CR00022832)" on page 175	**SNMP**	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
"No SSH feature licence required (CR00018895)" on page 108	**SSH**	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y

Table 2: Overview of new features and enhancements by software version (cont.)

Feature or Enhancement	Module	AR44x/AR450S/ AR415S	AR7x5	AR750S/AR770S	Rapier i	Rapier w	AT-8800	AT-8600	AT-8700XL	AT-8948 / x900-48	AT-9900	AT-9800
"Enhanced recovery from multiple link failure (CR00020566)" on page 172	**EPSR**	–	–	–	–	–	–	–	–	Y	Y	–
"Support for new switch and NSM models (CR00021061)" on page 15	**NSM**	–	–	–	Y	Y	–	–	–	–	–	–
"Improved VPN reliability (CR00021304)" on page 169	**IPsec**	Y	Y	Y	Y	Y	Y	–	–	–	–	–
"GUI displays SHDSL counters (CR00021752)" on page 50	**GUI**	Y	–	–	–	–	–	–	–	–	–	–
"Virtual activation of VLANs (CR00021896, CR00019547)" on page 34	**VLAN**	Y	–	Y	Y	Y	Y	Y	Y	Y	Y	Y
"Improved static server entries and debugging (CR00017819)" on page 77	**MACFF**	–	–	–	Y	Y	Y	Y	Y	Y	Y	–
"Support for AT-AR021v3 BRI-S/T PIC Models (CR00020309)" on page 16	**BRI**	Y	Y	Y	Y	Y	–	–	–	–	–	–
"Support for RoHS-compliant AT-G8T GBIC (CR00020370)" on page 16	**Switching**	–	–	–	–	–	–	–	–	–	–	Y
"IGMP Group MIB (CR00018418)" on page 194	**IGMP, MIB**	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
"Display PRI loopback and tests (CR00019548)" on page 48	**PRI**	Y	Y	Y	Y	Y	–	–	–	–	–	–
"Configure default multicast route operation (CR00019989)" on page 35	**Switching**	–	–	–	–	–	–	–	–	Y	Y	–
"Increased number of IP filters (CR00020146)" on page 68	**IP gateway**	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
"Log Eth link status change (CR00020171)" on page 47	**Eth**	Y	Y	Y	–	–	–	–	–	–	–	–
"ICMP Router Discovery Advertisements (CR00010614)" on page 68	**IP Gateway**	Y	Y	Y	–	–	–	–	–	Y	Y	–
"ADSL2 and ADSL2+ on AR440S (CR00015525)" on page 51	**ADSL, Core**	Y	–	–	–	–	–	–	–	–	–	–
"STP and MSTP debugging enhancements (CR00016978)" on page 37	**STP, MSTP, Switch**	–	–	–	Y	Y	Y	Y	Y	Y	Y	Y

Table 2: Overview of new features and enhancements by software version (cont.)

Feature or Enhancement	Module	AR44x/AR450S/ AR415S	AR7x5	AR750S/AR770S	Rapier i	Rapier w	AT-8800	AT-8600	AT-8700XL	AT-8948 / x900-48	AT-9900	AT-9800
"Acting on traffic for particular DHCP client (CR00017018)" on page 93	**Classifier, DHCP snooping**	–	–	–	–	–	–	–	–	Y	Y	–
"Routing header type 0 deprecated (CR00018144)" on page 84	**IPv6**	Y	Y	Y	Y	Y	Y	–	–	Y	Y	Y
"Nested VLAN port override (CR00018346)" on page 36	**VLAN**	–	–	–	–	–	–	–	–	Y	Y	–
"Bridging supports more ports (CR00019152)" on page 62	**Bridging**	Y	Y	Y	Y	Y	–	–	–	–	–	–
"Longer L2TP call name (CR00019377)" on page 63	**L2TP**	Y	Y	Y	Y	Y	Y	–	–	Y	Y	Y
"Increased maximum Link State Update size (CR00019749)" on page 82	**OSPF**	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
"CPU fan monitoring disabled by default (CR00018530)" on page 20	**Core**	–	–	–	–	–	–	–	–	Y	–	–
"BGP counter display (CR00012822)" on page 83	**BGP**	Y	Y	Y	Y	Y	Y	–	–	Y	Y	Y
"MAC-forced forwarding interoperation with access router (CR00016099)" on page 78	**MACFF, DHCP Snooping**	–	–	–	Y	Y	Y	Y	Y	–	–	–
"Support for x900-48FS (CR00016662)" on page 16	**Hardware**	–	–	–	–	–	–	–	–	Y	–	–
"Faster PPPoE client session re-establishment (CR00016913)" on page 60	**PPP**	Y	Y	Y	Y	Y	Y	–	–	Y	Y	Y
"RADIUS authentication of SSH sessions (CR00017197)" on page 108	**SSH, User, RADIUS**	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
"CR00017395: Accurate Maximum Segment Size (MSS) values for TCP sessions" on page 137	**Firewall**	Y	Y	Y	Y	Y	Y	–	–	–	–	Y
"IGMP snooping fast leave in multiple host mode (CR00017482)" on page 80	**IGMP Snooping**	Y	-	Y	Y	Y	Y	Y	Y	Y	Y	Y

Table 2: Overview of new features and enhancements by software version (cont.)

Feature or Enhancement	Module	AR44x/AR450S/ AR415S	AR7x5	AR750S/AR770S	Rapier i	Rapier w	AT-8800	AT-8600	AT-8700XL	AT-8948 / x900-48	AT-9900	AT-9800
"Load balancing on VLANs (CR00017532)" on page 171	**WAN Load Balancing**	Y	–	Y	–	–	–	–	–	–	–	–
"IGMP filtering (CR00017701)" on page 81	**IGMP**	–	–	–	–	–	–	Y	–	–	–	–
"Support for the new Rapier 48w switch (CR00017403)" on page 17	**Hardware**	–	–	–	–	Y	–	–	–	–	–	–
"ADSL connection option on Wizards page (CR00014288)" on page 19	**GUI**	Y	–	–	–	–	–	–	–	–	–	–
"CHAP authentication in slow networks (CR00014667)" on page 61	**PPP**	Y	Y	Y	Y	Y	Y	–	–	Y	Y	Y
"GUI displays ADSL statistics (CR00015432)" on page 19	**ADSL, GUI**	Y	–	–	–	–	–	–	–	–	–	–
"Software QoS on PPPoE interfaces (CR00016078)" on page 96	**Software QoS, PPP, Eth, VoIP**	Y	Y	Y	Y	Y	–	–	–	–	–	–
"Tunnelled IPsec connection for IPv6 (CR00016150)" on page 169	**IPsec, IPv6**	Y	Y	Y	Y	Y	Y	–	–	–	–	–
"Backing up the configuration with SNMP (CR00016221)" on page 195	**Load, MIBs**	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
"Log discarded ARP requests (CR00016234)" on page 76	**DHCP Snooping**	–	–	–	Y	Y	Y	Y	Y	Y	Y	–
"MAC-forced forwarding on non-private VLANs (CR00016285)" on page 79	**MACFF**	–	–	–	Y	Y	Y	Y	Y	Y	Y	–
"Support for AT-SPTX tri-speed Cu SFPs (CR00016361)" on page 18	**Switch**	–	–	–	–	–	–	–	–	Y	Y	–
"Full stop in MSTP config name (CR00016437)" on page 40	**MSTP**	–	–	–	Y	Y	Y	Y	Y	Y	Y	–
"SNMP ASN.01 BER padding (CR00016523)" on page 175	**SNMP**	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
"Bypass TCP state checking option for IP NAT (CR00016758)" on page 71	**IP NAT**	Y	Y	Y	–	–	–	–	–	–	–	–

Table 2: Overview of new features and enhancements by software version (cont.)

Feature or Enhancement	Module	AR44x/AR450S/ AR415S	AR7x5	AR750S/AR770S	Rapier i	Rapier w	AT-8800	AT-8600	AT-8700XL	AT-8948 / x900-48	AT-9900	AT-9800
"ARP silent roam for wireless roaming (CR00016776)" on page 72	**IP Gateway**	Y	–	Y	–	–	–	–	–	–	–	–
"Summertime for American Energy Policy Act 2005 (CR00016785)" on page 21	**Core**	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
"Aliases in script files (CR00016977)" on page 178	**Script**	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y

New in Hardware Support

This section describes software enhancements to support new models of switches, routers, and expansion options or to improve support for existing models.

Related enhancements include:

Support for the new AT-A65 expansion module (CR00023174)

Models

This enhancement is supported on:

- AT-8600

Description

The AT-A65 is a new expansion module for the AT-8624T/2M and AT-8624PoE switches. You can order these modules preinstalled in the switches or as separate units.

The AT-A65 expansion module can act as either a:

- 1000Base-X SFP expansion bay or
- 10/100/1000Base-T copper port with RJ-45 connection

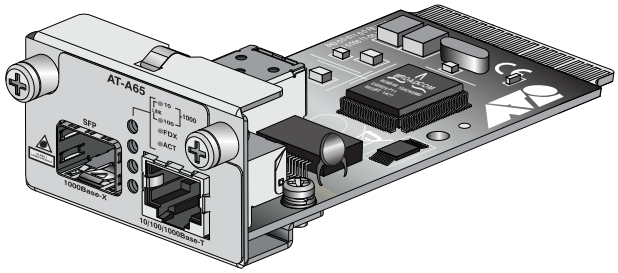
The module can automatically switch between the copper and fiber interface. When an SFP is installed in the AT-A65, the SFP port is considered the active port and the copper port becomes disabled. When there is no SFP installed then the copper port becomes the active port.

The SFP bay supports these SPF types: 1000Base-SX fiber, 1000Base-LX fiber, and 1000Base-ZX fiber.

The 10/100/1000Base-T copper port has the following qualities:

- 10, 100, and 1000Mbps auto-sensing
- half duplex and full duplex auto-negotiation at 10/100Mbps
- full duplex auto-negotiation at 1000Mbps
- auto-MDI / MDI-X

Figure 1: AT-A65 expansion module



For more information see the *AT-A65 Expansion Module Installation and Safety Guide*. This is available for download from your switch's product page (accessible from http://alliedtelesis.com/products/index) or from http://www.alliedtelesis.co.nz/documentation/.

Support for new switch and NSM models (CR00021061)

Models This enhancement is supported on:

- Rapier i, Rapier w

Module NSM

Description This software version includes support for new variants of the Rapier 24i and Rapier 48w switches, which have new NSM bay connectors. You can identify the new switch variants by the following board IDs:

Board ID	Name (as displayed by show system command)
311	AT-RP24i-B Rapier 24i NEBS
312	AT-RP24i-B Rapier 24i DC NEBS
302	AT-RP48w-B-15 Rapier 48w-AC
300	AT-RP48w-B-85 Rapier 48w

The new connectors are compatible with the following new NSM variants:

Board ID	Name
313	AT-AR040-B-00 NSM 4PIC
314	AT-AR048-B NSM DS3

Only the new switch variants can use the new NSMs. Other Rapier 24i and Rapier 48w switches continue to use the original NSMs (which have board IDs of 87 and 187).

Support for RoHS-compliant AT-G8T GBIC (CR00020370)

Models This enhancement is supported on:

- AT-9800

Module Switching

Description Support for the RoHS-compliant AT-G8T GBIC was added for AT-9800 series switches. Before this, the GBIC would fail to link up with the slide switch set to auto (its default position).

Support for AT-AR021v3 BRI-S/T PIC Models (CR00020309)

This enhancement is supported on:

- Rapier i, Rapier w
- AR44x, AR450S, AR415S
- AR725, AR745
- AR750S, AR770S

Module BRI

Description This release adds support for the v3 hardware revision of the AT-AR021 BRI-S/T Port Interface Card (PIC). The AT-AR021 V3 hardware revision is a plug-in replacement for the V2 hardware revision, which is no longer available. The AR021v3 has the same feature set and command set as the AR021v2, except that it does not support NT mode operation. Existing configurations for normal TE mode operation will run unchanged on the AR021v3.

The AR021v3 PIC can be installed in the following expansion bays:

- PIC bays on the AR415S, AR440S, AR441S, AR442S, AR725, AR745, AR750S, AR750S-DP, and AR770S routers
- AT-AR040 NSM installed in the AR745 router, Rapier 16fi, Rapier 24i, and Rapier 48w switches.

Support for x900-48FS (CR00016662)

Models This enhancement is supported on:

- x900-48

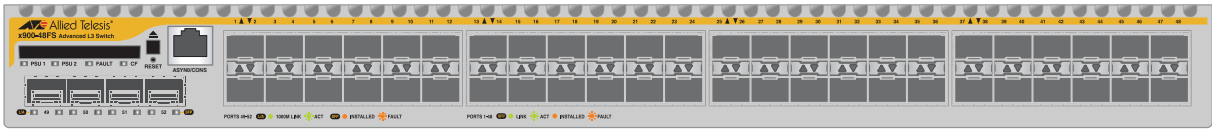
Module Hardware support

Description The x900-48FS is a new model in the x900 Series of layer 3 gigabit and fast Ethernet switches. Its key features are:

- Multi-layer Fast Ethernet switch
- 48-port 100BASE-X SFP sockets, 100 Mbps, full or half duplex
- 4-port 1000BASE-X SFP uplink sockets, 1000 Mbps, full duplex

- Support for hot-swappable SFP modules
- Hot-swappable, load sharing PSUs
- 1U height, rack-mountable
- Non-blocking Layer 2 and Layer 3 IP switching
- IPv6-ready hardware for accelerated unicast and multicast routing
- 4096 Layer 2 multicast entries
- 1024 Layer 3 IPv4 multicast entries
- 4096 logical IPv6 interfaces
- 32MBytes of fixed flash
- 256MBytes of Synchronous DRAM, expandable to 512MBytes with DIMM
- Compact Flash slot for hot-swappable expansion of flash memory up to 128MBytes

x900-48FS front panel



For more information about the x900 Series and expansion options, see the Hardware Reference. This is available for download from your switch's product page (accessible from http://alliedtelesis.com/products/index) or from http://www.alliedtelesis.co.nz/documentation/.

Support for the new Rapier 48w switch (CR00017403)

Models This enhancement is supported on:

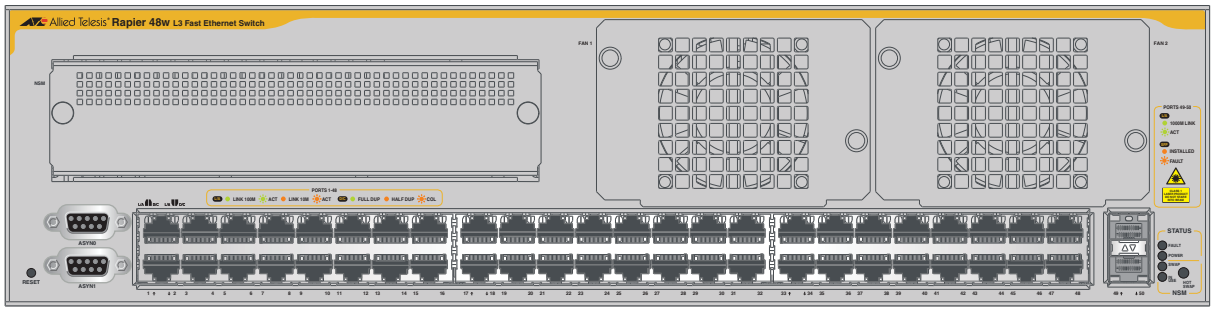
- Rapier w

Module Hardware support

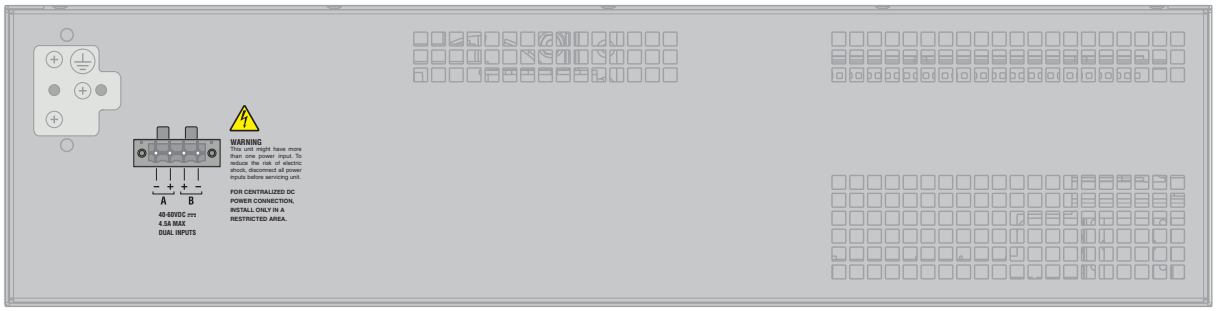
Description The Rapier 48w is a new model in the Rapier Series of layer 3 gigabit and fast Ethernet switches. Its key features are:

- 48-port 10BASE-T/100BASE-TX (RJ-45 connectors)
- Two 1000BASE SFP ports
- Two asynchronous serial console ports with DB9 connectors
- One Network Service Module bay, with support for various WAN interface cards
- Auto-negotiating Layer 3 Managed Switch
- Enhanced switching core
- Replaceable air filters and fan-only modules (FOMs) for NEBS applications

Rapier 48w front panel



Rapier 48w rear panel



For more information about the Rapier Series and expansion options, see the Hardware Reference. This is available for download from your switch's product page:
http://alliedtelesis.com/products/index) or from
http://www.alliedtelesis.co.nz/documentation/.

Support for AT-SPTX tri-speed Cu SFPs (CR00016361)

Models This enhancement is supported on:

- AT-8948, x900-48
- AT-9900

Module Switch

Description AT-8948, AT-9900 and x900-48 series switches now support AT-SPTX tri-speed Cu SFPs.

New in Using the GUI

This section describes enhancements to the GUI as described in the *Using the Graphical User Interface (GUI)* chapter in the *Software Reference for Version 2.9.1* for your router or switch.

ADSL connection option on Wizards page (CR00014288)

Models This enhancement is supported on:

- AR44x

Module GUI

Description An ADSL connection option has been added to the Wizards page of the GUI for AR44xS routers. This option links to the xDSL configuration section, which lets you configure all basic ADSL or SHDSL settings on one convenient page.

If your router GUI does not open at the Wizards page, click on the Wizards button at the top of the left-hand menu to access it.

GUI displays ADSL statistics (CR00015432)

Models This enhancement is supported on:

- AR44x

Module GUI, ADSL

Description The GUI for AR440S and AR441S routers now displays statistics for the ADSL port. You can now see:

- a pop-up summary box, by clicking on the port on the System Status page
- ADSL port details, by selecting the new ADSL Statistics page in the Diagnostics menu
- ADSL port counters, by selecting the new ADSL Counters page under Layer 1 Counters in the Diagnostics menu

New in Configuring and Monitoring the System

This section describes new features and enhancements to system settings and monitoring, as described in the *Configuring and Monitoring the System* chapter in the *Software Reference for Version 2.9.1* for your router or switch.

CPU fan monitoring disabled by default (CR00018530)

Models This enhancement is supported on:

- AT-8948, x900-48

Module Core

Description CPU fan monitoring is now disabled by default on x900-48FE and x900-48FE-N switches. Monitoring the fan is unnecessary unless an accelerator card is installed on the switch, so disabling monitoring reduces the number of messages that the switch displays and logs.

To enable monitoring, use the command:

```
enable cpufanmonitoring
```

To disable it again, use the command:

```
disable cpufanmonitoring
```

When monitoring is enabled, the command **show system** displays the CPU fan status in the entry labelled "Main fan".

Summertime for American Energy Policy Act 2005 (CR00016785)

Models This enhancement is supported on:

- AT-8948, x900-48
- AT-9900
- AT-9800
- AT-8800
- AT-8600
- AT-8700XL
- Rapier i, Rapier w
- AR44x, AR450S, AR415S
- AR725, AR745
- AR750S, AR770S

Module Core

Description The default summertime dates have been updated to reflect the changes for North America made by the American Energy Policy Act of 2005.

By default, summertime now starts on the second Sunday in March and ends on the first Sunday in November.

New in Switching

This section describes new features and enhancements to Layer 1 and Layer 2 switching, as described in the *Switching* chapter in the *Software Reference for Version 2.9.1* for your router or switch.

Related enhancements include:

Switch port longer description (CR00031879)

Models This enhancement is supported on:

- AT-8800
- AT-8700XL
- Rapier i, Rapier w

Module L2 switching

Description Previously, the length of the description parameter for a switch port was limited to 47 characters. The limit has now been increased to 244 characters to allow for more extensive naming conventions for switch ports.

```
set switch port=<port> description=<descr>
```

VLAN logical interfaces increased (CR00029290)

Models This enhancement is supported on:

- Rapier i, Rapier w
- AT-8800

Module VLAN, Swi, IP

Description Previously, the number of logical IP interfaces that could be configured on a VLAN was limited to 16. This has been increased to 32 logical interfaces.

Loop Detection Frames with 802.1X and MAC-based Port Auth (CR00029957)

Models This enhancement is supported on:

- AR44x, AR450S, AR415S
- AR750S, AR770S

Module Switching

Description LDF (Loop Detection Frames) has been enhanced to work in conjunction with 802.1X and MAC-based Port Authentication. Previously, LDF and Port Authentication could not be configured on the same ports.

External Loop Detection and Termination (CR00026527)

Models This enhancement is supported on the following switch models:

- AT-8948, x900-48
- AT-9900
- AT-9800
- AT-8800
- AT-8600
- AT-8700XL
- Rapier i, Rapier w

Module Swi

Description Loop Detection and Protection serves as a fall-back feature to disable a port involved in a network loop in the event of failure of STP, or other higher layer protocol. It detects whether the device is receiving and transmitting packets that are contributing to a packet storm caused by a loop existing somewhere in its external network.

Operation

If this condition is detected, the switch will disable one or more of its ports in an attempt to terminate the storm by breaking the loop. The mechanism used in these checks operates independently and alongside conventional Ethernet loop spanning tree protocols that may be used to avoid data loops.

Methods employed

Two methods are employed to detect data loops:

- LDF Detection
- Receive Broadcast Counter Method

LDF detection

This method operates by transmitting Loop Detection Frames (LDF) from the external switch ports. An LDF is a VLAN tagged or untagged frame that contains the following:

- a unique and unregistered destination MAC address of a non-existent station. For example: FE-FF-FF-xx-xx-xx where the last 3 bytes used are the last 3 bytes of the source MAC address of the device.
- the sending MAC address of the initiating device
- an LDF data field comprising a unique test pattern

Because their destination MAC addresses will always be unknown, LDF frames will flood the network. If the device then receives an LDF on the same VLAN as that used when originally transmitted, a loop is assumed to exist somewhere downstream of the device's external ports. When a loop is detected the switch will apply the process that is specified by the action parameter of the **set switch loopdetection** command.

Receive broadcast counter method

If the device is part of a broadcast packet storm, one or more of the external ports will be receiving broadcast frames at, or close to, line rate. These frames will then flood the ingress VLAN of the device, and the transmit broadcast packet counters of the other external ports of this VLAN will increase to near line rate.

This method detects loops by monitoring the rate at which broadcast frames are received on the device's external ports, as recorded by the broadcast packet counter. If this rate exceeds that set by the BCthreshold parameter of the **set switch loopdetection** command, then an external loop is assumed to exist somewhere the device's external network. When a loop is detected the switch will apply the process that is specified by the action parameter of the **set switch loopdetection** command.

Actions if a loop is detected

If a loop is detected, a log message will be generated. Users are also able to configure whether the ports that participate in the loop will be disabled. A port disabled by this feature will remain disabled until it is either manually re-enabled, or a configurable timeout period elapses whereupon the CPU will re-enable the port. The **default** value of the configurable timeout period is **5 minutes**.

Commands

The following new commands are available:

- **set switch loopdetection** command on page 25
- **enable switch loopdetection** command on page 26

set switch loopdetection

Syntax

```
SET SWItch LOOPdetection=LDF [ACtion={NONE|DISableport}]
   [LDFinterval=10..1000000] [PDTO={1.. 86400|NONE}]
   [SECure={ON|OFF}]

SET SWItch LOOPdetection=BCcounter
   [ACtion={NONE|DISableport}]
   [BCthreshold=1..20000000][PDTO={1..86400|NONE}]
```

Description This command sets an operational parameter on a method of loop detection.

Parameter	Description
ACtion	Specifies the action to be taken when a port is deemed to be in a loop. If DISableport is specified, the port will be disabled, and will remain disabled for the time specified by the PDTO parameter of the **set switch loopdetection** command. However, once disabled, the user can re-enable the port at any time. If NONE is specified, no action will be taken. The default value is NONE.
BCthreshold	Specifies the receive broadcast packet port counter threshold, the units of which are frames per second. There is no default value for the BCTHRESHOLD parameter and as a result, this value must be specified before the BCCOUNTER method of loop detection can be enabled.
LDFinterval	Specifies the time interval in seconds between when a Loop Detection Frame (LDF) is sent out a port. A staggered start is used so that LDFs are not sent out all ports at the same time. The **default** is 120 seconds.
LOOPdetection	Specifies which method of loop detection will be set.
PDTO	The Port Disabled Time Out parameter specifies the length of time in seconds that a port remains in the disabled state after the port has been disabled by loop detection. If NONE is specified, the port will not be re-enabled by loop detection. Once a port has been disabled by loop detection, the port can be re-enabled at any time using the **enable switch port** command. Re-enabling a port will stop the timeout period. This parameter is only used if the DISABLEPORT action is specified. The **default** is 300 seconds.
SECure	Whether discard LDFs that are received out of sequence.

Examples To set the port disabled timeout to 60 seconds and to specify the disable port action on the LDF method of loop detection, use the command:

```
set swi loop=ldf ac=dis pdto=60
```

To set the port disabled timeout to the default 300 seconds and to specify the disable port action on the BCC method of loop detection, use the command:

```
set swi loop=bcc ac=dis pdto=none
```

Related commands
disable switch loopdetection
enable switch loopdetection
show switch loopdetection

enable switch loopdetection

Syntax

```
ENable SWItch LOOPdetection={BOTH|LDF|BCcounter}
   [ACtion={NONE|DISableport}] [POrt={port-list|ALL}]
```

Description

This command enables loop detection on the specified ports, or all ports if the PORT parameter is not specified.

Parameter	Description
ACtion	Specifies the action to be taken when a port is deemed to be in a loop. If DISableport is specified, the port will be disabled, and will remain disabled for the time specified by the PDTO parameter of the **set switch loopdetection** command. However, once disabled, the user can re-enable the port at any time. If NONE is specified, no action will be taken. The default value is NONE.
LOOPdetection	Specifies which method of loop detection will be enabled. If LDF is specified, Loop Detection Frames (LDF) will be periodically sent out the ports that loop detection is enabled on. If the switch receives these LDFs, then a loop has been formed. If BCCOUNTER is specified, the receive broadcast packet port counter will be checked against a user configurable threshold each second. If the rate equals or exceeds the threshold, the port will be deemed to be in a loop. The two methods operate independently of one another, and can be enabled simultaneously by specifying BOTH.
POrt	The list of ports that loop detection will be enabled on. If ALL is specified, then loop detection will be enabled on all the ports that loop detection is currently enabled on. The **default** value is ALL. Port numbers start at 1 and end at m, where m is the highest numbered Ethernet switch port, including uplink ports. Ports are identified by a port number.

Example

To enable loop detection using the bccounter method on ports 1 - 24, use the command:

```
ena swi loop=bcc port=1-24
```

Related commands
disable switch loopdetection
set switch loopdetection

show switch loopdetection

Syntax `SHow SWItch LOOPdetection[={LDF|Bccounter}] [Port={port-list|ALL}]`

Description This command displays loop detection information about one or more ports.

Figure 2: Example output from the **show switch loopdetection=ldf** command

```
Switch Loop Detection
-------------------------------------------------------------
LDF Method
Action ....................... Disable port
Secure ....................... OFF
LDF interval ................. 120 sec
Port disabled timeout ......... 300 sec

Rx port In loop   Disabled Re-enabling in Tx port  Debug mode
-------------------------------------------------------------
1       Yes       Yes      30              1         None
2       No        No        -              -         None
3       No        No        -              -         None
4       No        No        -              -         None
5       No        No        -              -         None
6       No        No        -              -         None
7       No        No        -              -         None
8       No        No        -              -         None
9       No        No        -              -         None
...

52      No        No        -              -         None
```

Figure 3: Example output from the **show switch loopdetection=bccounter** command

```
Switch Loop Detection
-------------------------------------------------------------------
BCCOUNTER Method
Action ......................... Disable port
Broadcast threshold ............ 100000 frames/sec
Port disabled timeout .......... 300 sec

Rx port In loop   Disabled  Rate detected Re-enabling in   Debug mode
-------------------------------------------------------------------
1       No        No        -             -               None
2       No        No        -             -               None
3       No        No        -             -               None
4       No        No        -             -               None
5       No        No        -             -               None
6       No        No        -             -               None
7       No        No        -             -               None
8       No        No        -             -               None
9       Yes       Yes       149764        288             None
10      No        No        -             -               None
11      No        No        -             -               None
12      No        No        -             -               None
13      No        No        -             -               None
14      No        No        -             -               None
15      Yes       Yes       149888        288             None
...

52      No        No        -             -           None
```

Table 3: Parameters displayed in the output of the **show switch loopdetection** command

Parameter	Description
ACtion	The action the switch will take when the LDF method indicates that the port is in a loop. One of: Disable port or None.
Secure	Indicates whether an out of sequence LDF is discarded by the switch. One of: ON or OFF.
LDF interval	The interval between the transmissions of LDFs in seconds.
Port disabled timeout	The duration that a port that is disabled by LDF method, remains disabled. Either a time in seconds or None.
Rx Port	A list of ports on which the LDF method is enabled.
In Loop	Whether the LDF healthcheck has detected a loop on the port; one of Yes or No.
Disabled	The time in seconds before the port is automatically re-enabled.
Re-enabling in	The time in seconds before the port is automatically re-enabled.
Tx Port	The switch has received an LDF that it transmitted.The LDF contains information regarding the port that the LDF was sent out of on the switch; this port number is displayed in this field.
Debug mode	The debug mode that is currently turned on for the port; one of LDFTxRx or None.
BCCOUNTER METHOD	
Action	The action the switch will take when the BCCounter method indicates that the port is in a loop; one of Disable port or None.

Table 3: Parameters displayed in the output of the **show switch loopdetection** command

Parameter	Description
Broadcast threshold	The broadcast threshold in frames per second.
Port disabled timeout	The duration that a port disabled by loop detection remains disabled. Can be specified by either a time in seconds, or continuous. In the continuous mode the port will remain disabled until it is manually enabled by using the **enable switch port** command.
Rx Port	A list of ports.
In Loop	A loop has been detected on the port by the BCCounter method; one of Yes or No.
Disabled	Whether port is currently disabled by the BCCounter method; one of Yes or No.
Rate detected	The number of the increase of the broadcast packets when the BCCOUNTER method determined that a port was in a broadcast storm.
Rate-enabling in	The time in seconds before the port is automatically re-enabled.
Debug mode	The debug mode currently turned on for the port: one of BCRate or None.

Examples To display the status of loop detection, use the command:

```
sh swi loop
```

Related commands
disable switch loopdetection
enable switch loopdetection
set switch loopdetection
show switch loopdetection counter

show switch loopdetection counter

Syntax `SHow SWItch LOOPdetection COUnter[Port={port-list|ALL}]`

Description This command displays counter information about loop detection.

Figure 4: Example output from the **show switch loopdetection counter po=1-52** command

```
Switch Loop Detection Counter
-------------------------------------------------------------------------
LDF Method
Port      Date/Time           Tx              Rx              Status
-------------------------------------------------------------------------
1    ----                    14              0               Disabled
1    ----                    0               0               Disabled
2    ----                    0               0               Disabled
3    ----                    0               0               Disabled
4    ----                    0               0               Disabled
5    ----                    0               0               Disabled
6    ----                    0               0               Disabled
7    ----                    0               0               Disabled
8    ----                    0               0               Disabled
9    ----                    14              0               Disabled
10   ----                    0               0               Disabled
11   ----                    0               0               Disabled
12   ----                    0               0               Disabled
13   ----                    0               0               Disabled
14   ----                    0               0               Disabled
15   ----                    0               1               Disabled
16   ----                    0               0               Disabled
...
52   ----                    0               0               Disabled
BCCOUNTER Method
Port     Date/Time          Threshold      Rate detected   Status
-------------------------------------------------------------------------
1    ----                    --              --              Enabled
2    ----                    --              --              Enabled
3    ----                    --              --              Enabled
4    ----                    --              --              Enabled
5    ----                    --              --              Enabled
6    ----                    --              --              Enabled
7    ----                    --              --              Enabled
8    ----                    --              --              Enabled
9    04-Aug-2009 13:53:42    1000000          70644581       Enabled
10   ----                    -                -              Enabled
11   ----                    -                -              Enabled
12   ----                    -                -              Enabled
13   ----                    -                -              Enabled
14   ----                    -                -              Enabled
15   04-Aug-2009 13:59:42    1000000         70647774        Enabled
16   ----                    0               0               Enabled
...
52   ----                    0               0               Enabled
```

Table 4: Parameters displayed in the output of the **show switch loopdetection counter** command

Parameter	Meaning
LDF METHOD	
Port	A list of ports.
Date/Time	The date and time when the LDF healthcheck last detected a loop was detected on the port.
Tx	The number of LDFs transmitted out of the port.

Table 4: Parameters displayed in the output of the **show switch loopdetection counter** command (cont.)

Parameter	Meaning
Rx	The number of LDFs received on the port.
Status	The current status of LDF method on the port; one of *Enabled* or *Disabled*.
BCCOUNTER METHOD	
Port	A list of ports.
Date/Time	The date and time when BCCountercheck last detected a loop on the port.
Threshold	The broadcast threshold in frames per second was set when the loop was detected.
Rate detected	The number of the increase of the broadcast packets when the BCCOUNTER method determined that a port was in a broadcast storm.
Status	The current status of BCCOUNTER method on the port; one of *Enabled* or *Disable*.

Examples To display the status of loop detection, use the command:

```
show swi loop=bc cou port=5
```

Related commands
disable switch loopdetection
enable switch loopdetection
set switch loopdetection
show switch loopdetection

disable switch loopdetection

Syntax

```
DISable SWItch
   LOOPdetection={LDF|BCcounter|BOTH}[POrt={port-list|ALL}]
```

Description This command disables loop detection on the specified ports, or all ports if the PORT parameter is not specified.

Parameter	Description	
LOOPdetection	Specifies which method of loop detection will be disabled.	
	LDF	Loop Detection Frames (LDF) will not be sent from ports with loop detection disabled.
	BCcounter	The broadcast packet port counter will not be monitored
	BOTH	Both LDF and BCcounter disabling will be disabled.
POrt	The ports that loop detection will be disabled on. Default: **ALL**	
	Port-list	Selects a list of port numbers in the range 1 to m, where m is the highest numbered Ethernet switch port, including uplink ports. Ports are identified either by a port number or a line card.port number.
	ALL	Selects all the ports.

Examples To enable loop detection using the bccounter method on the BCCOUNTER ports 1 - 24, use the command:

```
ena swi loop=bcc port=1-24
```

Related Commands
enable switch loopdetection
show switch loopdetection
set switch loopdetection
enable switch loopdetection

enable switch loopdetection debug

Syntax

```
ENable SWItch LOOPdetection DEBug={BCRate|LDFtxrx|ALL}
   [POrt={port-list|ALL}] [TIMEOut={1..10000|NONE}]
```

Description This command enables loop detection debugging on the specified ports, or all ports if the port parameter is not specified. Be aware that enabling debug could flood the receiving Telnet session or asynchronous port with raw data. The default value is for debug to be disabled on loop detection.

Parameter	Description
ALL	All loopdetection debug options.
BCRate	The rate of broadcast frames received over a fixed 1 second time interval. The number of broadcast frames that arrive during a 1second time period are compared with the number recorded for the previous period. If this count exceeds the value set by the **BCthreshold** parameter of the **set switch loopdetection** command, then the **bcrate** will be displayed in debug information.
DEBug	Specifies the loop detection debug mode to be enabled. The values for the **debug** parameter will be determined during implementation. If **all** is specified then all debug modes will be disabled.
LDFtxrx	Debug information will be displayed whenever an LDF frame is transmitted or received.
LOOPdetection	The **loopdetection** parameter specifies which method of loop detection will not have debugging. If **both** is specified, then both methods of loop detection will not have debugging.
POrt	Specifies the list of ports that loop detection debugging will be enabled on. If **ALL** is specified, then loop detection debugging will be enabled on all ports. The default value is all. Port numbers start at 1 and end at m, where m is the highest numbered Ethernet switch port, including uplink ports. Ports are identified by a port number.
TIMEout	The **timeout** parameter specifies the time in seconds for which any switch health check debugging is enabled. This reduces the risk of the switch and the display being overloaded with too much debugging information.

Examples To enable loop detection debug modes via BC rate method on port 1-24, use the command:

```
ena swi loop deb=bcr port=1-24
```

Related Commands
set switch loopdetection
show switch loopdetection

disable switch loopdetection debug

Syntax

```
DISable SWItch LOOPdetection={BOTH|LDF|BCcounter}
   DEBug={BCRate|LDFtxrx|ALL} [POrt={port-list|ALL}]
```

Description

This command disables loop detection debugging on the specified ports, or all ports if the PORT parameter is not specified. The default value is for debug to be disabled on loop detection.

Parameter	Description
BCRate	The rate of broadcast frames received over a fixed 1 second time interval. The number of broadcast frames that arrive during a 1 second time period are compared with the number recorded for the previous period. If this count exceeds the value set by the BCthreshold parameter of the set switch loopdetection command, then the BCRate will be displayed in debug information.
DEBug	Specifies the loop detection debug mode to be disabled. The values for the DEBUG parameter will be determined during implementation. If ALL is specified then all debug modes will be disabled.
LDFTxRx	Display of information whenever a LDF is transmitted or received.
LOOPdetection	The LOOPDETECTION parameter specifies which method of loop detection will not have debugging. If BOTH is specified, then both methods of loop detection will not have debugging.
POrt	Specifies the list of ports that loop detection debugging will be disabled on. If **ALL** is specified, then loop detection debugging will be disabled on all ports. The default value is all. Port numbers start at 1 and end at m, where m is the highest numbered Ethernet switch port, including uplink ports. Ports are identified by a port number.
ALL	All loopdetection debug options.

Examples

To disable loop detection debug modes via BC rate method on ports 1-24, use the command:

```
dis swi loop=bcc deb=bcr port=1-24
```

Related Commands

enable switch loopdetection
set switch loopdetection
show switch loopdetection

Private VLAN uplink port increase (CR00023867)

Models This enhancement is supported on:

- AT-8800
- AT-8600
- AT-8700XL
- Rapier i, Rapier w

Module Switching

Description The maximum number of uplink ports available for private VLANS has increased from 50 to 150.

Virtual activation of VLANs (CR00021896, CR00019547)

Models This enhancement is supported on:

- AT-8948, x900-48
- AT-9900
- AT-9800
- AT-8800
- AT-8600
- AT-8700XL
- Rapier i, Rapier w
- AR44x, AR450S, AR415S
- AR750S, AR770S

Module VLAN

Description 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.

VLAN activation is useful for VLANs that are reached through L2TP tunnels instead of through switch ports.

To turn virtual activation on or off, use the command:

```
SET VLAN={vlan-name|1..4094|ALL} VIRTActivation={Yes|No}
```

The default is **no**.

To see whether the VLAN has been activated virtually, use the command **show vlan** and check the new "Admin Active" field.

Configure default multicast route operation (CR00019989)

Models This enhancement is supported on:

- AT-8948, x900-48
- AT-9900

Module Switching

Description 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:

```
SET SWItch DEFAultmrouteoperation={TRap|ROUte|DEFault}
```

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**.

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.

To see the current setting, use the command **show switch** and check the entry called "Def. Multicast Route Op".

Nested VLAN port override (CR00018346)

Models This enhancement is supported on:

- AT-8948, x900-48
- AT-9900

Module VLAN

Description This enhancement adds a new parameter **nestedoverride** to the command **add vlan port**.

The **nestedoverride** parameter allows you to add the port to a non-nested VLAN as a tagged port even if the port has already been configured as a **customer** port in a nested VLAN. The **vlan** parameter specifies the non-nested VLAN to which you want to add the port. You must also specify **frame=tagged**. The port will behave as a normal customer port for the nested VLAN, and an egress-only port for the non-nested VLAN:

- Frames received on the port and tagged for the nested VLAN will be sent to the core ports of the nested VLAN, as normal.
- Frames received on the port and tagged for the non-nested VLAN will be sent to the core ports of the nested VLAN, and will not be sent to other ports of the non-nested VLAN.
- IGMP frames received on the port and tagged for the non-nested VLAN will be processed according to the IP multicasting configuration, instead of being discarded.
- Frames received on other ports of the non-nested VLAN will be transmitted from the port as tagged frames of the non-nested VLAN according to the FDB/multicast rules.

Caution: The **nestedoverride** parameter creates a non-standard configuration, and care should be taken when using this parameter in a live network. The **nestedoverride** and **uplink** parameters are mutually exclusive and cannot be specified in the same command.

An example configuration would be:

```
create vlan=v22 vid=22 nested
create vlan=v20 vid=20
add vlan=v22 port=1 nested=customer
add vlan=v20 port=1 frame=tagged nestedoverride
```

New in Spanning Trees

This section describes new features and enhancements to STP and MSTP, as described in the *Spanning Trees* chapter in the *Software Reference for Version 2.9.1* for your router or switch.

RSTP Slow convergence time agreement BPDU time (CR00033330)

Models This enhancement is supported on:

- AT-8948, x900-48
- AT-9900
- AT-9800
- AT-8800
- AT-8600
- AT-8700XL
- Rapier i, Rapier w

Module MSTP

Description Previously an STP BPDU with a lower priority vector than the port it arrived on would be discarded, therefore a fast port transition could not occur. This was in conformance with 802.1w-2001 Sec 17.19.8, which is now obsolete. 802.1D-2004 Sec.17.10 allows the fast transition to happen even if the priority vector is lower. This has been now implemented.

STP and MSTP debugging enhancements (CR00016978)

Models This enhancement is supported on:

- AT-8948, x900-48
- AT-9900
- AT-9800
- AT-8800
- AT-8600
- AT-8700XL
- Rapier i, Rapier w

Module STP, MSTP, Switch

Description STP and MSTP debugging has been enhanced to:

- make it easier to see state information, and
- only display information about Topology Change messages.

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, use the 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.

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

Full stop in MSTP config name (CR00016437)

Models This enhancement is supported on:

- AT-8948, x900-48
- AT-9900
- AT-8800
- AT-8600
- AT-8700XL
- Rapier i, Rapier w

Module MSTP

Description In the command **set mstp configname=*name***, the switch now accepts the character "." in the ***name***.

New in Interfaces

This section describes new features and enhancements to the management of Eth, synchronous, asynchronous, and DS3 physical interfaces, as described in the *Interfaces* chapter in the *Software Reference for Version 2.9.1* for your router or switch. Enhancements related to switch ports are described in "New in Switching" on page 22.

- "Router Port Link Disable (CR00028764)" on page 42
- "Description parameter for Eth interfaces (CR00027921)" on page 47
- "Log Eth link status change (CR00020171)" on page 47

Related enhancements include:

- "Link status trap delay (CR00022832)" on page 175
- "Software QoS on PPPoE interfaces (CR00016078)" on page 96
- "TPID in 802.1q tags sent from router ETH interface are now configurable (CR00032804)" on page 41

TPID in 802.1q tags sent from router ETH interface are now configurable (CR00032804)

A new **VLANTPID** parameter has been added to the existing interface command as follows:

```
set ip interface=<Eth interface> vlantag=<vlan id>
   vlanpriority=priority vlantpid=<value>
```

The display for the command **sh ip interface=eth<x>** has been modified to show the value of the new parameter:

```
Manager 450s> show ip int=eth1

Interface     Type     IP Address       Bc Fr PArp  Filt RIP Met.   SAMode  IPSc
Pri. Filt     Pol.Filt Network Mask     MTU   VJC   GRE  OSPF Met.  DBcast  Mul.
GArp VLAN Tag VLAN Pri VLAN TPID        InvArp      NotifyOSPFDown FlushARP
-------------------------------------------------------------------------------
eth1-0#       Static   192.168.2.15     1  n  On    ---  01         Pass    No
---           ---      255.255.255.0    1500  -     ---  0000000001 No      Rec
On   19       2        2134             -           Yes            -
-------------------------------------------------------------------------------
```

Operationally, the new parameter affects tagging of an interface as described below. When a packet is received on the ETH interface processing now occurs as follows:

- Check whether a standard tag exists.
  - If the standard tag is present in the header, then the packet is treated as tagged, otherwise:

- Check whether a non-standard, configured tag is present in the header
  - If the configured tag is present in the header, then the packet is treated as tagged. otherwise:
- The packet is not tagged.

When a packet is sent out on the ETH interface processing now occurs as follows:

- The vlan tag portion of the packet will contain the configured TPID.

For example;

```
set ip interface=eth0-x vlantpid=abcd
```

where ABCD is a hexadecimal number of up to 4 hex digits.

The default value of the TPID will remain 8100

Router Port Link Disable (CR00028764)

Models This enhancement is supported on the following router models:

- AR44x, AR415S
- AR450S—switch ports only
- AR750S, AR770S

Module SWI, ETH

Description Previously, router switch ports could only be disabled and enabled at a software level (enabled by default), and router Eth ports could not be disabled at all (always enabled). With this enhancement, you can disable and enable both router Eth ports and router switch ports at a hardware level (electrical link status) as well as at a software level. If the (hardware/electrical) link status is UP, the link partner considers the link to still be active. If the (hardware/electrical) link status is DOWN, the link partner knows that the port is inactive. This enhancement also provides a simple method of controlling WAN traffic over redundant links. On the AR450S, this enhancement applies to the router switch ports, but not to the Eth ports.

This enhancement adds the following new commands:

- “disable eth” on page 43
- “enable eth” on page 43

and modifies these commands:

- “disable switch port” on page 44
- “show switch port” on page 45
- “show eth state” on page 46

Log messages generated when links go down now also indicate whether they went down “by command“ or “by link loss“.

disable eth

Syntax `DISable ETH=n [LINk={ENAble|DISable}]`

where *n* is the number of the Ethernet interface.

Description This command disables the specified Ethernet interface (at a software level), and optionally also disables or enables the physical link belonging to the interface, ensuring that the link partner realises that the port is down. When an Ethernet port is disabled, it no longer sends or receives frames. Ethernet ports are enabled by default.

The **eth** parameter specifies the number of the Ethernet interface.

The **link** parameter specifies whether the Ethernet port is enabled or disabled at the hardware level. If **disable** is specified, this is the equivalent of disconnecting the cable. If the link parameter is not specified, the link remains physically and electrically enabled. On a disabled Ethernet port, the command:

```
disable eth=n link={enable}
```

brings the interface link up in hardware without re-enabling the port.

enable eth

Syntax `ENAble ETH=n`

where *n* is the number of the Ethernet interface.

Description This command enables an Ethernet interface. If an Ethernet port has had its hardware interface disabled by the command:

```
disable eth=n link=disable
```

then this command automatically re-enables the port at both hardware and software levels. Ethernet ports are enabled by default.

The **eth** parameter specifies the number of the Ethernet interface and must be specified.

disable switch port

The syntax and function of this command is modified by the addition of the **link** parameter.

Syntax

```
DISable SWItch POrt={port-list|All} [AUTOMDI]

DISable SWItch POrt={port-list|All} [FLOW]

DISable SWItch POrt={port-list|All} [LINk={ENAble|DISable}]
```

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

Description

This command allows the administrator to disable:

- a port or group of ports on the switch,
- the electrical link belonging to the specified ports, ensuring the link partner realises the port is down,
- the auto MDI/MDI-X function,
- the ports' flow control mechanism.

The **port** parameter specifies one or more ports to disable or which are to have their flow control or auto MDI/MDI-X functions disabled.

The **automdi** parameter disables auto MDI-MDI-X. This cannot be used with the link parameter.

The **flow** parameter specifies that flow control is disabled for the port. The type of flow control is full-duplex flow control or half-duplex flow back pressure. This cannot be used with the link parameter.

The **link** parameter specifies whether the switch port is enabled or disabled at the hardware level. If **disable** is specified, this is the equivalent of disconnecting the cable. If the link parameter is not specified, the link remains physically and electrically enabled. On a disabled switch port, entering the command disable switch **port**=*port-number* **link**=**enable** brings the interface link up in hardware without re-enabling the port. This cannot be used with either the **automdi** nor **flow** parameters.

show switch port

The output from this command is modified to include the method by which the physical link went down, either 'by command' or 'by link loss'. If the Link State is 'Up', there is no change to the output.

Syntax `SHow SWItch POrt[={port-list|All}]`

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

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

Figure 5: Example output from the **show switch port** command

```
Switch Port Information
------------------------------------------------------------
Port ............................ 1
  Description ................... -
  Status ........................ DISABLED
  Link State .................... Down, by command
  UpTime ........................ -
  Configured speed/duplex ....... Autonegotiate
  Actual speed/duplex ........... -
  Automatic MDI/MDI-X ........... Enabled
  Configured MDI/MDI-X .......... MDI-X
  Actual MDI/MDI-X .............. MDI-X
  Broadcast rate limit .......... -
  Multicast rate limit .......... -
  DLF rate limit ................ -
  Flow control .................. Enabled
  Send tagged pkts for VLAN(s) ... -
  Port-based VLAN ............... default (1)
  Ingress Filtering ............. OFF
  IGMP Filter ................... None
  Max-groups/Joined ............. Undefined/0
  IGMP Max-groups Action ........ Deny
------------------------------------------------------------
```

show eth state

The output from this command is modified to include a new Status line, and to also show the method by which the link went down, either 'by command' or 'by link loss'. If the Link State is 'Up', no method is shown.

Syntax `SHow ETH[=n] STATE`

where *n* is the number of the Ethernet interface.

Description This command displays general information about the Ethernet interface. If an interface number is not specified, information about all Ethernet interfaces is displayed.

Figure 6: Example output from the **show eth state** command

```
awplus# show eth=0 state
State for ETH instance 0:

 Status ............................ DISABLED
 Link .............................. down, by command
   Configured speed/duplex ......... Auto-negotiate
   Actual speed/duplex ............. unknown, unknown
   Auto-negotiation ................ in progress

   Link partner capabilities
     Auto-negotiation ............. unknown
     1000BASE-TX full duplex ..... unknown
     1000BASE-TX ................. unknown
     100BASE-TX full duplex ...... unknown
     100BASE-TX .................. unknown
     10BASE-T full duplex ........ unknown
     10BASE-T .................... unknown

PHY Port Information:
  00=1900 01=7849 02=0022 03=5521 04=01e1 05=0001 06=0004 07=2001 08=2001
  10=1800 11=1500 12=000f 13=0000 14=c000 15=0000 16=3fff 17=8000
  18=0000 19=00ff 1a=0000 1b=0000 1c=0044 1d=1000 1e=1a60 1f=0100
```

Description parameter for Eth interfaces (CR00027921)

Models This enhancement is supported on:

- AR44x, AR450S, AR415S
- AR725, AR745
- AR750S, AR770S

Module Eth

Description It is now possible to enter a 250 character description for an ETH interface (in the same manner as a switch port) by using a new parameter to the **set eth** command. The new parameter is **DESCription**. For example:

```
set eth=0 desc="I am a happy little ETH interface"
```

In addition, the **show interface=<*interface-id*>** command now outputs the ETH interface description.

Log Eth link status change (CR00020171)

Models This enhancement is supported on:

- AR44x, AR450S, AR415S
- AR725, AR745
- AR750S, AR770S

Module Eth

Description Log entries are now generated when Ethernet port links are taken up or down. Typical log entries are:

```
26 11:37:18 6 ETH  PINT  DOWN  ETH3: interface is DOWN
26 11:37:28 6 ETH  PINT  UP    ETH3: interface is UP
```

Note that AR022 PICs (ETH PICs) do not enter a log message after a restart if the link is up during that restart, but do enter a log message for each subsequent link transition.

New in ISDN

This section describes new features and enhancements to ISDN interface management, as described in the *Integrated Services Digital Network (ISDN)* chapter in the *Software Reference for Version 2.9.1* for your router or switch.

- "Display PRI loopback and tests (CR00019548)" on page 48

Related enhancements include:

- "Support for AT-AR021v3 BRI-S/T PIC Models (CR00020309)" on page 16

Display PRI loopback and tests (CR00019548)

Models This enhancement is supported on:

- Rapier i, Rapier w
- AR44x, AR450S, AR415S
- AR725, AR745
- AR750S, AR770S

Module PRI

Description With this enhancement, the **show pri state** command now displays any current loopback configuration and lists any running tests on PRI ports.

New in ATM over xDSL

This section describes new features and enhancements in ADSL, ADSL2, ADSL2+, SHDSL, and ATM interface management as described in the *ATM over xDSL* chapter in the *Software Reference for Version 2.9.1* for your router.

Related enhancements include:

Improved performance (CR00029835)

Models This enhancement is supported on:

- AR44x

Module xDSL

Description xDSL ATM data transmission performance has been improved.

ADSL2 and ADSL2+ on AR441S (CR00021615)

Models This enhancement is supported on:

- AR441S

Module ADSL, Core

Description With this software version, AR441S routers with a hardware revision of M1-2 (or later) will support ADSL2 and ADSL2+ connections. You can see the hardware revision of a router by entering the command **show system** and checking the "Rev" column for the "Base" board.

When running this software version, AR441S routers with rev M1-2:

- have the following new options for the command **set adsl standard**:
  - **adsl2**—connect only to devices offering ADSL2
  - **adsl2plus**—connect only to devices offering ADSL2+
  - **auto2plus**—connect at ADSL2+ if this is offered by the other end device (CO), or otherwise automatically fall back to what is offered

- have a default ADSL standard setting of **auto2plus**
- behave as they currently do for other ADSL standard settings

When running this software version, existing AR441S routers with a hardware revision of M1-1 or earlier:

- do not have the new options **adsl2**, **adsl2plus**, or **auto2plus** for the command **set adsl standard**
- still use the existing default ADSL standard setting of **auto**, which allows automatic fallback connection for ADSL standards only.

Improved SHDSL train up time (CR00022331)

Models This enhancement is supported on:

- AR442S

Module SHDSL

Description Previously on AR442S routers, SHDSL train up times were variable and frequently longer than one minute. This enhancement reduces this variability and minimises the train up time required.

GUI displays SHDSL counters (CR00021752)

Models This enhancement is supported on:

- AR442S

Module GUI

Description It is now possible to use the web-based GUI to display SHDSL counters and statistics on AR442S routers. The new pages are available from the left-hand menu under:

Diagnostics > Layer 1 Counters > SHDSL Counters

Diagnostics > SHDSL Statistics.

ADSL2 and ADSL2+ on AR440S (CR00015525)

Models This enhancement is supported on:

- AR440S

Module ADSL, Core

Description With this software version, AR440S routers with a hardware revision of M1-2 (or later) will support ADSL2 and ADSL2+ connections. You can see the hardware revision of a router by entering the command **show system** and checking the "Rev" column for the "Base" board.

When running this software version, AR440S routers with rev M1-2:

- have the following new options for the command **set adsl standard**:
  - **adsl2** —connect only to devices offering ADSL2
  - **adsl2plus** —connect only to devices offering ADSL2+
  - **auto2plus** —connect at ADSL2+ if this is offered by the other end device (CO), or otherwise automatically fall back to what is offered
- have a default ADSL standard setting of **auto2plus**
- behave as they currently do for other ADSL standard settings

When running this software version, existing AR440S routers with a hardware revision of M1-1 or earlier:

- do not have the new options **adsl2**, **adsl2plus**, or **auto2plus** for the command **set adsl standard**
- still use the existing default ADSL standard setting of **auto**, which allows automatic fallback connection for ADSL standards only.

New in PPP

This section describes new features and enhancements to PPP as described in the *Point-to-Point Protocol (PPP)* chapter in the *Software Reference for Version 2.9.1* for your router or switch.

Related enhancements include:

PPPOE Ignore Unknown Session (CR00032988 & CR00034376)

Models This enhancement is supported on:

- AT-8948, x900-48
- AT-9900
- AT-9800
- AT-8800
- Rapier i, Rapier w
- AR44x, AR450S, AR415S
- AR725, AR745
- AR750S, AR770S

Module PPP

Description A single new optional PPPoE configuration parameter PADTUnknown has been added to optionally indicate that PPPoE can be set to either ignore packets containing session ids which have not yet been established or respond with PADT (Session Termination). The default is ON (send PADT for unknown sessions).

The new option can be defined either when creating a new PPPoE interface or the option after creation of the PPPoE interface. This option only applies to PPPoE so the 'over' interface must be either Vlan or ETH. An error is produced if it is not applied to a PPPOE interface.

The PADTUnknown parameter is also available in PPP Templates from Maintenance Software Release 292-06 onwards.

Create ppp

syntax

```
CREATE PPP=ppp-interface OVER=physical-interface
   [AUTHENTICATION={CHAP|EITHER|PAP|NONE}] [AUTHMODE={IN|
   OUT|INOUT}] [BAP={ON|OFF}] [BAPMODE={CALL|CALLBACK}]
   [CBDELAY=1..100] [CBMODE={ACCEPT|OFF|REQUEST}]
   [CBNUMBER=e164number] [CBOPERATION={E164NUMBER|
   USERAUTH}] [COMPALGORITHM={PREDICTOR|STACLZS}]
   [COMPRESSION={ON|OFF|LINK}] [CONFIGURE={value|
   CONTINUOUS}] [DEBUGMAXBYTES=16..256]
   [DESCRIPTION=description] [DOWNRATE=0..100]
   [DOWNTIME=time] [ECHO={ON|OFF|period}] [ENCRYPTION={ON|
   OFF}] [FRAGMENT={ON|OFF}] [FRAGOVERHEAD=0..100]
   [IDLE={ON|OFF|time}] [INDATALIMIT={NONE|1..65535}]
   [IPPOOL={pool-name|NONE}] [IPREQUEST={ON|OFF}]
   [LQR={ON|OFF|period}] [MAGIC={ON|OFF}] [MODEM={ON|OFF}]
   [MRU={ON|OFF|256..1656}] [MSSheader=40..200]
   [NULLFRAGTIMER=time] [NUMBER=number]
   [ONLINELIMIT={NONE|1..65535}] [OUTDATALIMIT={NONE|
   1..65535}] [PADRretry=0..10000] [PASSWORD=password]
   [PREDCHECK={CRC16| CRCCCITT}]
   [RECHALLENGE={ON=|OFF|360..3600}] [RESTART=time]
   [STACCHECK={LCB|SEQUENCE}] [STARENTITY=1..255]
   [TERMINATE={value|CONTINUOUS}]
   [TOTALDATALIMIT={NONE|1..65535}] [TYPE={DEMAND|PRIMARY|
   SECONDARY}] [UPRATE=0..100] [UPTIME=time]
   [USERNAME=username][PADTUnknown={ON|OFF}]
```

Parameter	Description
PADTUnknown	This is an optional parameter allowed only when defining a PPP over Ethernet interface, i.e. only if the interface is over VLAN or ETH. When set, any PPPoE packets received with a session id which is unknown (i.e. the session is not yet known to be established) will be responded to with a PPPoE Active Discovery Termination packet to ensure the peer clears down this session. This is the default behaviour. The parameter can also be set OFF. In this case, any PPPoE packets received with an unknown session ID will simply be ignored. This option may be required for compatibility with certain hosts which may begin to use a session ID early before the PPPoE Discovery procedure has fully completed and therefore before the session id has been validated. If a packet with an unknown session is detected, PADT will not be sent if PADTUknown is set to OFF, however a counter is incremented. The value of this counter is displayed in the **show ppp pppoe** command under the heading 'Unknown Session packets'.
Examples	In this example, the PPPoE interface has been set to indicate that PADT should not be sent for any PPPoE packets which contains session IDs which are unknown. `create ppp=0 over=ETH-any PADTUnknown=OFF`

set ppp

Syntax

```
SET PPP [DNSPRIMARY=ipadd] [DNSSECONDARY=ipadd]
    [WINSPRIMARY=ipadd] [WINSSECONDARY=ipadd] SET PPP=ppp-
    interface [OVER=physical-interface]
    [AUTHENTICATION={CHAP|EITHER|PAP|NONE}] [AUTHMODE={IN|
    OUT|INOUT}] [BAP={ON|OFF}] [BAPMODE={CALL|CALLBACK}]
    [CBDELAY=1..100] [CBMODE={ACCEPT|OFF|REQUEST}]
    [CBNUMBER=e164number] [CBOPERATION={E164NUMBER| USERAUTH}]
    [COMPALGORITHM={PREDICTOR|STACLZS}]
    [COMPRESSION={ON|OFF|LINK}] [CONFIGURE={value| CONTINUOUS}]
    [DEBUGMAXBYTES=16..256] [DESCRIPTION=description]
    [DOWNRATE=0..100] [DOWNTIME=time] [ECHO={ON|OFF|period}]
    [ENCRYPTION={ON| OFF}] [FRAGMENT={ON|OFF}]
    [FRAGOVERHEAD=0.100] [IDLE={ON|OFF|time}]
    [INDATALIMIT={NONE|1..65535}] [IPPOOL={pool-name|NONE}]
    [IPREQUEST={ON|OFF}] [LQR={ON|OFF|period}] [MAGIC={ON|OFF}]
    [MAXLINKS=1..64] [MODEM={ON|OFF}] [MRU={ON|OFF|256..1656}]
    [MSSheader=40..200] [NULLFRAGTIMER=time]
    [ONLINELIMIT={NONE|1..65535}] [OUTDATALIMIT={NONE| 1..65535}]
    [PADRRetry=0..10000] [PADTUnknown={ON|OFF}]
    [PASSWORD=password] [PREDCHECK={CRC16|CRCCCITT}]
    [RECHALLENGE={ON|OFF|360..3600}][RESTART=time]
    [STACCHECK={LCB|SEQUENCE}][STARENTITY=1..255]
    [TERMINATE={value|CONTINUOUS}]
    [TOTALDATALIMIT={NONE|1..65535}] [TYPE={DEMAND|PRIMARY|
    SECONDARY}] [UPRATE=0..100] [UPTIME=time] [USERNAME=username]
```

A single new optional parameter PADTUnknown is added to optionally indicate that PPPoE can be set to either ignore packets containing session IDs which have not yet been established or respond with PADT (Session Termination). The default is ON (send PADT for unknown sessions).

Where:

Parameter	Description
PADTUnknown	This is an optional parameter allowed only when defining a PPP over Ethernet interface, i.e.: only if the interface is over Vlan or ETH. When set, any PPPoE packets received with a session id which is unknown (i.e: the session is not yet known to be established) will be responded to with a PPPoE Active Discovery Termination packet to ensure the peer clears down this session. This is the default behaviour, The parameter can also be set OFF. In this case, any PPPoE packets received with an unknown session id will simply be ignored. This option may be required for compatibility with certain hosts which may begin to use a session id early before the PPPoE Discovery procedure has fully completed and therefore before the session ID has been validated. If a packet with an unknown session is detected, PADT will not be sent if PADTUknown is set to OFF, however a counter is incremented. The value of this counter is displayed in the **show ppp pppoe** command under the heading 'Unknown Session packets'. Default: ON
Examples	In this example, the PPPoE interface has been set to indicate that PADT should not be sent for any PPPoE packets which contains session IDs which are unknown. `set ppp=0 PADTUnknown=OFF`

show ppp conf

The **show ppp conf** command syntax is not altered. The output is modified to show the current setting for the PADTUnknown configuration.

Figure 7: Example output from the show ppp conf command

```
Interface - description
    Parameter                        Configured                 Negotiated
  ------------------------------------------------------------------------------
  ppp0 -
                                                              Local             Peer
    Bandwidth Allocation Protocol          OFF
    Bandwidth Allocation Call Mode        CALL
    Multilink Fragmentation                OFF
    Acceptable Fragment Overhead (%)         5
    Null Fragment Timer (seconds)            3
    Session Timer (seconds)                OFF
    Idle Timer (seconds)                   OFF
    Maximum Receive Unit (bytes)            ON             NONE              NONE
    Compression                            OFF
    Username                           internet1
    Password                                SET
    Bundle Endpoint Discr Class               0
    Bundle Endpoint Discr Value              []
    Bundle Username                    NOT SET
  eth0-any
    Type                                primary
    Restart Timer (seconds)                  3
    Max-Configure                     continuous
    Max-Terminate                            2
    Echo Request Timer (seconds)            10
    Callback Mode                          OFF
    Link Compression                       OFF              OFF               OFF
    LQR Timer (seconds)                    OFF              OFF               OFF
    Magic Number                            ON              OFF               OFF
    Link Discriminator                    0000              OFF               OFF
    Link Endpoint Discr Class                0
    Link Endpoint Discr Value
    Authentication                         NONE             NONE              NONE
    Authentication Mode                   INOUT
    Utilisation (%)                          0
  IP
    IP Compression Protocol                NONE             NONE              NONE
    IP Pool                            NOT SET
    IP Address Request                      ON
    IP Address Borrowing                   OFF
    IP Address                           0.0.0.0            NONE              NONE
    Primary DNS Address                NOT SET              NONE              NONE
    Secondary DNS Address              NOT SET              NONE              NONE
    Primary WinS Address               NOT SET                                NONE
    Secondary WinS Address             NOT SET                                NONE
  PPPoE
    Session ID                             NONE
    MAC Address of AC                                                         NONE
    PADR Retry Limit                         15
    Send PADT for Unknown Session          OFF
  Debug
    Maximum packet bytes to display          60
  ------------------------------------------------------------------------------
```

New PPP command parameter [PADRretry=0..10000] (CR00032805)

Models This enhancement is supported on:

- AT-8948, x900-48
- AT-9900
- AT-9800
- AT-8800
- Rapier i, Rapier w
- AR44x, AR450S, AR415S
- AR725, AR745
- AR750S, AR770S

Module PPP

Description If a PPPoE Access Concentrator (AC) responds to a host's PADI (PPPoE Active Discovery Initiation) with a PADO (PPPoE Active Discovery Offer) but does not respond to the host's request to setup a connection on this AC, then there is a limit to the number of times the host will resend the request (ie:the host sends PPPoE Active Discovery Request and expects an PPPoE ActiveDiscovery Session confirmation). Previously this limit was fixed at 15.

This enhancement introduces a new PPP command parameter [PADRretry=0..10000]

which allows this limit to be set from 1 to 10,000 using a new optional parameter PADRRetry in the PPPoE interface configuration.

The special value of 0 is also supported, which indicates there is no limit and requests will be resent until it is explicitly stopped or a connection is completed. The default value is 15, which retains the existing behaviour in configurations which do not specify the new parameter.

Longer PPP interface description (CR00032369)

Models This enhancement is supported on:

- AT-8948, x900-48
- AT-9900
- AT-9800
- AT-8800
- Rapier i, Rapier w
- AR44x, AR450S, AR415S
- AR725, AR745
- AR750S, AR770S

Module PPP

Description Previously, when configuring a PPP interface using the **create ppp** and **set ppp** command, the optional parameter **description** had a maximum limit of 70 characters. This has been increased to 254 characters.

```
CREATE PPP=ppp-interface OVER=physical-interface
   [DESCRIPTION=description] [other-ppp-parameters]

SET PPP=ppp-interface [OVER=physical-interface]
   [DESCRIPTION=description] [other-ppp-parameters]
```

where:

- *description* is a character string 1 to 254 characters long. Valid characters are any printable character.

ARP flush for PPP interfaces (CR00030236)

Models This enhancement is supported on:

- AT-8948, x900-48
- AT-9800
- AT-8800
- Rapier i, Rapier w
- AR44x, AR450S, AR415S
- AR725, AR745
- AR750S, AR770S

Module ARP, PPP, IP

Description When a new IP interface becomes available, any dynamic ARPs learned on other interfaces are discarded and relearned. This is RFC compliant behaviour and is performed in order for the ARP cache to reflect the changed network topology. However, when the ARP cache is being repopulated, ARP messages can arrive very rapidly, and some messages may be discarded. In order to avoid this in a dynamic environment with many PPP over ISDN interfaces changing state regularly, a new parameter has been added to the **add ip interface** and **set ip interface** commands:

```
ADD IP INTerface=interface IPaddress={ipadd|DHCP}
   [FLUSHArp={ON|OFF}] [other-ppp-parameters]
```

```
SET IP INTerface=interface [FLUSHArp={ON|OFF}] [other-ppp-
   parameters]
```

The **flusharp** parameter determines whether (**on**) or not (**off**) to flush all dynamic entries from the ARP table when a link status change is recognized on the specified PPP interface. The default is **on**.

For example, to set the device to retain dynamic entries in the ARP table when it detects a change in the link status of the ppp0 interface, use the command:

```
add ip interface=ppp0 ip=0.0.0.0 mask=0.0.0.0 flusharp=off
```

To set the device to flush dynamic entries from the ARP table when it detects a change in the link status of the ppp0 interface (that is, to restore the default setting), use the command:

```
set ip interface=ppp0 ip=0.0.0.0 mask=0.0.0.0 flusharp=on
```

The output from the s**how ip interface** command now also displays the setting of the **flusharp** parameter.

PPPoE AC improved interoperability (CR00030904)

Models This enhancement is supported on:

- AT-8948, x900-48
- AT-9800
- AT-8800
- Rapier i, Rapier w
- AR44x, AR450S, AR415S
- AR725, AR745
- AR750S, AR770S

Module PPP

Description Previously, if the device was configured as a PPPoE Access Concentrator, it originated PPP Link Control Protocol (LCP) Configure Request messages that also included options Endpoint Discriminator (EPD) and Maximum Received Reconstructed Unit (MRRU).

Since dynamic multilink is not supported over PPPoE, these options are no longer included in the PPP LCP configure request messages when the device is operating as a PPPoE Access Concentrator. This change in behavior improves interoperability with other devices, by removing unnecessary PPP negotiation exchanges.

New ipfilter and ipfragment parameters for PPP templates (CR00023990)

Models This enhancement is supported on:

- AT-8948, x900-48
- AT-9900
- AT-9800
- AT-8800
- Rapier i, Rapier w
- AR44x, AR450S, AR415S
- AR725, AR745
- AR750S, AR770S

Module PPP

Description Two new parameters, **ipfilter** and **ipfragment**, are now available for the **create ppp template** and **set ppp template** commands:

```
create ppp template=ppp-template [ipfilter=NONE|0..999]
   [ipfragment=ON|OFf|True|False|Yes|No]

set ppp template=ppp-template [ipfilter=NONE|0..999]
   [ipfragment=ON|OFf|True|False|Yes|No]
```

These parameters are useful when a dynamic IP interface is created over the dynamic PPP interface. The shortest valid strings are **ipfi** for **ipfilter** and **ipfr** for **ipfragment**.

The **ipfilter** parameter specifies the traffic filter to apply to IP packets transmitted or received over the dynamic IP interface. The filter must already have been defined with the **add ip filter** command. The dynamic IP interface may have a maximum of one traffic filter but the same traffic filter can be assigned to more than one interface. Traffic filters are applied to packets received via the dynamic IP interface. The default is to not apply a filter.

The **ipfragment** parameter specifies whether the "Do not fragment" bit is obeyed for outgoing IP packets that are larger than the MTU of the interface. If **yes**, the "Do not fragment" bit is ignored and outgoing IP packets larger than the MTU of the interface are fragmented. This is particularly useful for interfaces configured with GRE, SA, or IPsec encapsulation, which can potentially increase packet sizes beyond the MTU of the interface. If **no**, the "Do not fragment" bit is obeyed and IP packets larger than the MTU are discarded. This is normal behaviour for IP. The fragment parameter has no effect on packets smaller than the interface MTU. The default is **no**.

Borrowed IP address for PPP unnumbered IP address (CR00019706)

Models This enhancement is supported on:

- AT-8948, x900-48
- AT-9900
- AT-9800
- AT-8800
- Rapier i, Rapier w
- AR44x, AR450S, AR415S
- AR725, AR745
- AR750S, AR770S

Module PPP

Description A new parameter **ipborrow** has been added to the **create ppp** and **set ppp** commands. You can set the **ipborrow** parameter to the values: **yes | on | true | no | off | false**.

This parameter is required in the following situation: the PPP interface has been configured as an unnumbered IP interface (i.e. configured with IP address 0.0.0.0), but you do not want the PPP peer to allocate an IP address to be used on the local PPP interface (i.e. **iprequest=no**). In this case, the switch needs to present a non-zero IP address to the peer during IPCP negotiation. The solution to this problem is to use another IP address that has been configured on the switch (invariably another interface on the device will have been configured with a non-zero IP address). With the **ipborrow** parameter, you can configure the unnumbered PPP interface to 'borrow' this other interface's IP address to use as the IP address it presents to the peer during IPCP negotiation.

If there are multiple non-zero IP interfaces on the switch, you cannot specify which interface's IP address the unnumbered PPP will borrow; it will simply borrow the IP address from the interface with the lowest ifindex.

Faster PPPoE client session re-establishment (CR00016913)

Models This enhancement is supported on:

- AT-8948, x900-48
- AT-9900
- AT-9800
- AT-8800
- Rapier i, Rapier w
- AR44x, AR450S, AR415S
- AR725, AR745
- AR750S, AR770S

Module PPP

Description This enhancement enables the PPPoE client to establish a session promptly after a restart or power cycle. This is done by sending a PPPoE Active Discovery Terminate (PADT) frame in response to a frame received with an unknown PPPoE session ID.

CHAP authentication in slow networks (CR00014667)

Models This enhancement is supported on:

- AT-8948, x900-48
- AT-9900
- AT-9800
- AT-8800
- Rapier i, Rapier w
- AR44x, AR450S, AR415S
- AR725, AR745
- AR750S, AR770S

Module PPP

Description This enhancement increases the amount of time that the switch waits for a CHAP Success message. This enables the switch to successfully complete authentication, even in particularly slow networks.

The first authentication attempt still times out after 3 seconds, but the second attempt takes 6 seconds to time out, and any further attempts take 9 seconds.

New in Bridging

This section describes enhancements to bridging, as described in the *Bridging* chapter in the *Software Reference for Version 2.9.1* for your router or switch.

Bridging supports more ports (CR00019152)

Models This enhancement is supported on:

- Rapier i, Rapier w
- AR44x, AR450S, AR415S
- AR725, AR745
- AR750S, AR770S

Module Bridging

Description The number of ports supported by Bridging has been increased from 32 to 512.

New in L2TP

This section describes enhancements to the L2TP, as described in the *Layer Two Tunnelling Protocol (L2TP)* chapter in the *Software Reference for Version 2.9.1* for your router or switch.

Longer L2TP call name (CR00019377)

Models This enhancement is supported on:

- AT-8948, x900-48
- AT-9900
- AT-9800
- AT-8800
- Rapier i, Rapier w
- AR44x, AR450S, AR415S
- AR725, AR745
- AR750S, AR770S

Module L2TP

Description Previously, the length of the L2TP call name was limited to 15 characters. This limit has been increased to 19 characters.

New in Internet Protocol (IP)

This section describes new features and enhancements to IP support as described in the *Internet Protocol (IP)* chapter in the *Software Reference for Version 2.9.1* for your router or switch.

Related enhancements include:

Ping and trace to domain (CR00032444)

Models This enhancement is supported on:

- AT-8948, x900-48
- AT-9900
- AT-9800
- AT-8800
- AT-8600
- AT-8700XL
- Rapier i, Rapier w
- AR44x, AR450S, AR415S
- AR725, AR745
- AR750S, AR770S

Module DNS

Description The ping and trace commands have been enhanced so that if the system name is in the form *switchname.<domain>*, then when the **ping** or **trace** commands are used to ping or trace a hostname, the DNS lookup is for the hostname within the same domain, that is: *hostname.<domain>*. The **telnet** command already behaved like this; with this enhancement, the **ping** and **trace** commands do too.

The following commands are enhanced:

ping

The syntax of this command has not changed, but the description of the address parameter has changed: the *host* can now be a full domain name or a host name in the same domain as the system.

```
PING [[IPADDRESS=]{ipadd|ipv6add[%interface]|host}]
    [DELAY=seconds] [LENGTH=number]
    [NUMBER={number|CONTINUOUS}] [PATTERN=hexnum]
    [SIPADDRESS={ipadd|ipv6add}]
    [SCREENOUTPUT={OFF|ON|NO|YES}] [TIMEOUT=1..65535]
    [TOS=number]
```

where:

- *host* is a host name from the host name table, a full domain name or a host name in the same domain as the system.

The **ipaddress** parameter specifies the destination address for ping packets for IP. You can specify a valid IP address, a host name defined in the host name table, a full qualified domain name or a hostname which is in the same domain as the system name (see below for an explanation) as the destination IP address. To add a host to the host name table, use the **add ip host** command. To configure a DNS for the switch to use to resolve domain names, use the **add ip dns** command.

If the sysName MIB is set to the switch or routers's fully qualified domain name (eg: switch.company.com) by using the **set system name** command and a name server has been defined by using the **set ip nameserver** command, then the command:

```
ping mainhost
```

will attempt to ping the host 'mainhost.company.com', provided 'mainhost' is not an IP nickname (IP nicknames take precedence) and provided the host 'mainhost.company.com' can be translated to an IP address using a DNS lookup.

If a domain name is specified, the switch sends a request to a name server to translate the domain name into an IP address. This may take several seconds during which time the normal switch prompt disappears. When the name server responds (or fails to respond), a message is displayed indicating that the lookup was successful (or unsuccessful). If successful, then the ping proceeds to ping the IP address.

```
Info (1005327): Resolving host name "my.domain.com" to IP address.

Info (1005328): Host name resolved to 192.168.100.1.

Echo reply 1 from my.domain.com (192.168.100.1) time delay 20 ms
```

trace

The syntax of this command has not changed, but the description of the **ipaddress** parameter has changed: the *host* can now be a full domain name or a host name in the same domain as the system.

Syntax

```
TRAce [[IPaddress=]ipadd] [ADDROnly={No|OFf|ON|Yes}]
   [MAXTtl=number] [MINTtl=number] [NUMber=number]
   [POrt=1..65535] [SCReenoutput={No|OFf|ON|Yes}]
   [SOurce=ipadd] [TIMEOut=number] [TOS=0..255]
```

where:

- *ipadd* is an IPv4 address in dotted decimal notation, a valid IPv6 address, or a host name from the host name table or a host name in the same domain as the system.

Description

The **ipaddress** parameter specifies the destination IP address; this command traces the route to this IP address. If you do not specify an IP address here or in the set trace command then a trace is not performed and an error message is displayed. To configure a DNS for the router to use to resolve domain names, use the **add ip dns command**. You can specify a valid IP address, a host name defined in the host name table, a full qualified domain name or a hostname which is in the same domain as the system name as the destination IP address. To add a host to the host name table, use the **add ip host** command. To configure a DNS for the switch to use to resolve domain names, use the **add ip dns** command.

If the sysName MIB is set to the switch's fully qualified domain name (e.g., switch.company.com) by using the **set system name** command and a name server has been defined by using the **set ip nameserver** command, then the command:

```
trace mainhost
```

will attempt to trace the path to the host 'mainhost.company.com', provided 'mainhost' is not an IP nickname (IP nicknames take precedence) and provided the host 'mainhost.company.com' can be translated to an IP address using a DNS lookup.

If a domain name is specified, the switch sends a request to a name server to translate the domain name into an IP address. This may take several seconds during which time the normal switch prompt disappears. When the name server responds (or fails to respond), a message is displayed indicating that the lookup was successful (or unsuccessful). If successful, then the trace proceeds to trace the route to the IP address.

```
SecOff systemname.co.nz> trace alliedtelesis

Info (1005327): Resolving host name "my.domain.com" to IP address.

Info (1005328): Host name resolved to 192.168.100.1.

Trace from 192.168.1.102 to my.domain.com (192.168.100.1), 1-30 hops
 0.     1      2      3 (ms) 192.168.1.1
 1.     ?      ?      ? (ms) ***
 2.    29     33     40 (ms) 192.168.110.1
 3.    37     39     41 (ms) 192.168.120.1
 4.    36     39     43 (ms) 192.168.130.1
 5.    26     26     27 (ms) 192.168.140.1
 6.    52     54     57 (ms) 192.168.150.1
 7.    43     43     44 (ms) 192.168.150.2
 8.    50     54     60 (ms) 192.168.160.1
 9.     ?      ?      ? (ms) ***
10.     ?      ?      ? (ms) ***
11.     ?      ?      ? (ms) ***
12.     ?      ?      ? (ms) ***
```

DynDNS periodic update (CR00030779)

Models This enhancement is supported on:

- AR44x, AR450S, AR415S
- AR750S, AR770S

Module DNS

Description The DynDNS client on the routers now supports a keepalive feature to prevent it from timing out. When the router is configured as a dynamic DNS client, it sends a DynDNS update message to the dynamic DNS service (DynDNS.com) when the **activate ddns update** command is entered. If a host registered on the DynDNS site is not updated within 30 days, it expires and is automatically removed from the DynDNS system. To prevent these expiries, the dynamic DNS client can now be configured to automatically send regular update messages to the dynamic DNS service by using a new parameter in the **set ddns** command:

```
SET DDNS [PERIodicupdate]={ON|OFF|days}] [other-ddns-
   parameters]
```

The **periodicupdate** parameter controls the DynDNS keep-alive feature. If **off** is specified, the router does not automatically send DynDNS update message. If **on** is specified, the router sends the DynDNS update message every twenty-eight (28) days. If a number of days (1 to 60) is specified, the router sends the DynDNS update message at intervals of this number of days. The default is **on**.

Example To set the router to not send the DynDNS update packet regularly, use the command:

```
set ddns periodicupdate=off
```

The output from the **show ddns** command now also displays the setting of the **periodicupdate** parameter, and the number of days elapsed since the last successful update, or since the router DDNS was enabled.

For more information about the Dynamic DNS Client on the router, see the *Internet Protocol* chapter in the *Software Reference*.

Increased number of IP filters (CR00020146)

Models This enhancement is supported on:

- AT-8948, x900-48
- AT-9900
- AT-9800
- AT-8800
- AT-8600
- AT-8700XL
- Rapier i, Rapier w
- AR44x, AR450S, AR415S
- AR725, AR745
- AR750S, AR770S

Module IP gateway

Description The upper limit on the number of entries in an IP filter has been increased from 255 to 3072.

ICMP Router Discovery Advertisements (CR00010614)

Models This enhancement is supported on:

- AT-8948, x900-48
- AT-9900
- AR44x, AR450S, AR415S
- AR725, AR745
- AR750S, AR770S

Note that the other layer 3 switches already supported this feature.

Module IP Gateway

Description

Router discovery

The switch or router now supports all *RFC 1256, ICMP Router Discovery Messages* as it applies to routers. If this feature is configured, the switch sends router advertisements periodically and in response to router solicitations. It does not support the Host Specification section of this RFC.

Benefits Before an IP host can send an IP packet, it has to know the IP address of a neighbouring router that can forward it to its destination. ICMP Router Discovery messages let routers automatically advertise themselves to hosts. Other methods either require someone to manually keep these addresses up to date, or require DHCP to send the router address, or require the hosts to be able

to eavesdrop on whatever routing protocol messages are being used on the LAN.

Router discovery process

The following table summarises what happens when Router Discovery advertisements are enabled for interfaces on the switch.

When...	Then...
Router Discovery advertising starts on a switch interface because: - the switch starts up, or - advertisements are enabled on the switch or on an interface	the switch multicasts a router advertisement and continues to multicast them periodically until router advertising is disabled.
a host starts up	the host may send a router solicitation message.
the switch receives a router solicitation	the switch multicasts an early router advertisement on the multicast interface on which it received the router solicitation.
a host receives a router advertisement	the host stores the IP address and preference level for the advertisement lifetime.
the lifetime of all existing router advertisements on a host expires	the host sends a router solicitation.
a host does not receive a router advertisement after sending a small number of router solicitations	the host waits for the next unsolicited router advertisement
a host needs a default router address	the host uses the IP address of the router or L3 switch with the highest preference level.
Router Discovery advertising is deleted from the physical interface (**delete ip advertise** command), or the logical interface has **advertise** set to **no** (**set ip interface** command)	the switch multicasts a router advertisement with the IP address(es) that stopped advertising, and a lifetime of zero. It continues to periodically multicast router advertisements for other interfaces.
the switch receives a router advertisement from another router	the switch does nothing but silently discards the message.

Advertisement messages

A *router advertisement* is an ICMP (type 10) message that contains the following:

- in the destination address field of the IP header, the interface's configured advertisement address, either 224.0.0.1 (**all**) or 255.255.255.255 (**limited**).
- in the lifetime field, the interface's configured advertisement lifetime.
- in the Router Address and Preference Level fields, the addresses and preference levels of all the logical interfaces that are set to advertise.

The switch does not send router advertisements by default.

Solicitation messages

A *router solicitation* is an ICMP (type 10) message containing:

- source Address: an IP address belonging to the interface from which the message is sent
- destination Address: the configured Solicitation Address, and
- Time-to-Live: 1 if the Destination Address is an IP multicast address; at least 1 otherwise.

Advertisement interval The router advertisement *interval* is the time between router advertisements. For the first few advertisements sent from an interface (up to 3), the switch sends the router advertisements at intervals of at most 16 seconds. After these initial transmissions, it sends router advertisements at random intervals between the minimum and maximum intervals that the user configures, to reduce the probability of synchronization with the advertisements from other routers on the same link. By default the minimum is 450 seconds (7.5 minutes), and the maximum is 600 seconds (10 minutes).

Preference level The *preference level* is the preference of the advertised address as a default router address relative to other router addresses on the same subnet. By default, all routers and layer 3 switches have the same preference level, zero. While it is entered as a decimal from -2147483648 to 2147483647, it is encoded in router advertisements as a twos-complement hex integer from 0x8000000 to 0x7fffffff. A higher preference level is preferred over a lower value.

Lifetime The *lifetime* of a router advertisement is how long the information in the advertisement is valid. By default, the lifetime of all advertisements is 1800 seconds (30 minutes).

Configuration procedure

Do the following to configure the switch to send router advertisements.

1. **Set the physical interface to advertise.**

   For each physical interface that is to send advertisements, add the interface. In most cases the default advertising parameters work well, but you can change them if required. By default, the switch sends advertisements every 7.5 to 10 minutes, with a lifetime of 30 minutes. These settings are likely to work in most situations and not cause extra traffic, even if there are several switches on the LAN. If you change these settings, keep the following proportions:

   ```
   lifetime=3 x maxadvertisementinterval

   minadvertisementinverval=0.75 x maxadvertisementinterval
   ```

   To change these settings, use one of the commands:

   ```
   add ip advertise interface=interface
       [advertisementaddress={all|limited}]
       [maxadvertisementinterval=4..1800]
       [minadvertisementinterval=3..maxadvertisementinterval]
       [lifetime=maxadvertisementinterval..9000]

   set ip advertise interface=interface
       [advertisementaddress={all|limited}]
       [maxadvertisementinterval=4..1800]
       [minadvertisementinterval=3..maxadvertisementinterval]
       [lifetime=maxadvertisementinterval..9000]
   ```

2. **Stop advertising on other logical interfaces.**

   By default, logical interfaces are set to advertise if their physical interface is set to advertise. If the physical interface has more than one logical interface (IP multihoming), and you only want some of them to advertise, set the other logical interfaces not to advertise with one of the commands:

   ```
   add ip interface=interface ipaddress={ipadd|dhcp}
       advertise=no [other-ip-parameters]

   set ip interface=interface advertise=no
       [other-ip-parameters]
   ```

3. **Set preference levels.**

   By default, every logical interface has the same preference for becoming a default router (mid range, 0). To give a logical interface a higher preference, increase **preferencelevel**. To give it a lower preference, decrease this value. If it should never be used as a default router, set it to **notdefault**.

   ```
   add ip interface=interface ipaddress={ipadd|dhcp}
      preferencelevel={-2147483648..2147483647|notdefault}
      [other-ip-parameters]
   set ip interface=interface
      [preferencelevel={-2147483648..2147483647|notdefault}]
      [other-ip-parameters]
   ```

4. **Enable advertising.**

   To enable router advertisements on all configured advertising interfaces, use the command:

   ```
   enable ip advertise
   ```

5. **Check advertise settings.**

   To check the router advertisement settings, use the command:

   ```
   show ip advertise
   ```

Bypass TCP state checking option for IP NAT (CR00016758)

Models This enhancement is supported on:

- AR44x, AR450S, AR415S
- AR725, AR745
- AR750S, AR770S

Module IP NAT

Description This enhancement enables you to turn off TCP state and sequence checking in IP NAT. It also allows all ICMP packets go through IP NAT.

To do this, use the command:

```
enable ip nat bypasstcp
```

When **bypasstcp** is enabled, IP NAT performs IP address and port translation for TCP packets and forwards the packets, regardless of the TCP sequence number and the current TCP state. It also allows ICMP echo reply and other ICMP packets to initiate a session and get forwarded.

To disable the bypassing, use the command:

```
disable ip nat bypasstcp
```

Bypassing is disabled by default because it degrades the security of IP NAT. However, it is useful when you need NAT on VRRP routers.

Note that this enhancement does not apply to firewall NAT.

ARP silent roam for wireless roaming (CR00016776)

Models This enhancement is supported on:

- AR44x, AR450S, AR415S
- AR750S, AR770S

Module IP Gateway

Description This enhancement allows ARPs to move between ports on the router's VLAN interfaces.This assists with wireless station roaming.

To enable this feature, use the command:

```
enable ip arp silentroam
```

To disable it, use the command:

```
disable ip arp silentroam
```

New in DHCP

This section describes enhancements to DHCP support, as described in the *Dynamic Host Configuration Protocol (DHCP)* chapter in the *Software Reference for Version 2.9.1* for your router or switch.

■ "Error message displays IP address (CR00031970)" on page 73

Related enhancements include:

■ "SNMP MIB enhancements for DHCP and Port Authentication (CR00025844)" on page 181

Error message displays IP address (CR00031970)

Models This enhancement is supported on:

- AT-8948, x900-48
- AT-9900
- AT-9800
- AT-8800
- AT-8600
- AT-8700XL
- Rapier i, Rapier w
- AR44x, AR450S, AR415S
- AR725, AR745
- AR750S, AR770S

Module DHCPv4

Description If you attempt to add a static DHCP entry (**add dhcp range** command) to bind an IP address to a MAC address when the MAC address is already bound to a different IP address, an error message is displayed.

This error message has been enhanced—the error message now also displays the IP address that is already bound to the MAC address.

New in DHCP Snooping

This section describes new features and enhancements to DHCP snooping as described in the *DHCP Snooping* chapter in the *Software Reference for Version 2.9.1* for your router or switch.

Related enhancements include:

ARP security broadcast filter (CR00030472)

Models This enhancement is supported on:

- AT-8948, x900-48
- AT-9900

Module DHCP snooping

Description Previously, the **enable dhcpsnooping arpsecurity** command enabled filtering of all ARP packets.

A new parameter **type** has been added:

```
enable dhcpsnooping arpsecurity [type={all|broadcast}]
```

to allow the user to set the device to filter all ARP packets (**type=all** default) or to filter broadcast ARP packets only (**type=broadcast**). The **broadcast** option uses fewer entries in the device's hardware filter table.

DHCP snooping ARP security—disable port (CR00020926)

Models This enhancement is supported on:

- AT-8948, x900-48
- AT-9900
- AT-8800
- AT-8600
- AT-8700XL
- Rapier i, Rapier w

Module DHCP Snooping

Description A new feature has been added to DHCP Snooping that allows a port to be disabled if DHCP Snooping ARP Security discards an ARP. To turn this feature on, use the command:

```
set dhcpsnooping arpsecurity action=disable
```

To turn it off, use the command:

```
set dhcpsnooping arpsecurity action=none
```

More DHCP snooping classifiers (CR00019005)

Models This enhancement is supported on:

- AT-8948, x900-48
- AT-9900

Module DHCP snooping

Description Previously, the range of classifier numbering for DHCP snooping was restricted to 1 to 100. The restriction has been removed. You can now specify a classifier number from 1 to 9999 when creating a DHCP snooping classifier (**create classifier** command).

Also, the maximum number of DHCP snooping classifiers you can create has increased to 520.

Log discarded ARP requests (CR00016234)

Models This enhancement is supported on:

- AT-8948, x900-48
- AT-9900
- AT-8800
- AT-8600
- AT-8700XL
- Rapier i, Rapier w

Module DHCP Snooping

Description This enhancement enables the switch to log discarded ARP requests when ARP security is enabled. By default, discarded ARP requests are not logged. To turn logging on, use the command:

```
enable dhcpsnooping log=arpsecurity
```

To turn it off, use the command:

```
disable dhcpsnooping log=arpsecurity
```

To see whether it is enabled, use the existing command:

```
show dhcpsnooping
```

and check the new “Logging enabled” entry.

To view the log entries, use the command:

```
show log
```

New in MAC-Forced Forwarding

This section describes enhancements to MAC-Forced Forwarding support, as described in the *MAC-Forced Forwarding* chapter in the *Software Reference for Version 2.9.1* for your router or switch.

Improved static server entries and debugging (CR00017819)

Models This enhancement is supported on:

- AT-8948, x900-48
- AT-9900
- AT-8800
- AT-8600
- AT-8700XL
- Rapier i, Rapier w

Module MACFF

Description This enhancement improves MAC-forced forwarding in the following ways:

- The commands **add** and **set macff server** both now allow you to optionally specify a MAC and/or IP address for the static entry. The complete syntax is now:

```
add macff server interface=vlan [description=description]
    [ipaddress=ipadd] [macaddress=macadd]

set macff server interface=vlan [description=description]
    [ipaddress=ipadd] [macaddress=macadd]
```

- The IP address is the main identifier in the static entry. It must be unique. You can specify the add command multiple times to specify multiple IP addresses for a single MAC address. It is also possible to have a single IP address resolve itself to duplicate MAC addresses, although not recommended.
- If you specify a MAC address without specifying an IP address, this associates the MAC address with an IP address of 0.0.0.0. You can only associate one MAC address with the IP address 0.0.0.0. The switch will make no attempt to resolve the MAC address.
- If you specify an IP address without specifying a MAC address, the switch attempts to resolve the address by ARPing. If there are multiple MAC addresses for the IP address, the switch uses the first ARP reply.
- If you specify both an IP address and a MAC address, the switch does not attempt to resolve the addresses. Even if it later dynamically learns a different IP address for that MAC address, the static entry takes precedence. However, if the switch learns of a discrepancy, it now produces a log entry. You should investigate the discrepancy—it is likely to be because of a configuration error.

- The command **delete macff server** now allows you to identify the server to delete by entering only its IP address. If the MAC address is not associated with an IP address, you can instead enter only the MAC address.
- Debugging is now on a global basis, not a per-interface basis. Therefore, the commands are now **enable macff debug=*options*** and **disable macff debug=*options***. Also, information about debugging options has been removed from the output of **show macff interface** and instead put in the output of **show macff [counters]**.

MAC-forced forwarding interoperation with access router (CR00016099)

Models This enhancement is supported on:

- AT-8800
- AT-8600
- AT-8700XL
- Rapier i, Rapier w

Module MACFF, DHCP Snooping

Description MAC-forced forwarding has been enhanced for use in a hospitality situation, such as a hotel. The enhanced solution allows hotel guests to connect to the network without having to change their IP settings, while still ensuring privacy for each guest. Typically some guests will obtain their IP address from the hotel's DHCP server and others will have statically configured IP addresses in their PCs.

The solution is designed to interoperate with a specialised Access Router that is able to deal with the full range of IP addresses that will be in use on the guests' PCs. The Nomadix Access Gateway (from www.nomadix.com) is an example of such a specialised access router.

Configuration of the new feature is similar to the existing MAC-forced forwarding configuration. On each edge switch, you also need to enter the following new command before enabling DHCP snooping:

```
disable dhcpsnooping ipfiltering
```

You also need to turn on ARP security and allow authorised clients to send only unicast packets, by entering the following commands:

```
enable dhcpsnooping arpsecurity
enable dhcpsnooping strictunicast
```

This enhancement also introduces the ability to add MACFF servers with static MAC addresses, rather than relying on ARP to determine them based on IP addresses. To do this, enter the command:

```
add macff server mac=macaddr
```

MAC-forced forwarding on non-private VLANs (CR00016285)

Models This enhancement is supported on:

- AT-8948, x900-48
- AT-9900
- AT-8800
- AT-8600
- AT-8700XL
- Rapier i, Rapier w

Module MACFF

Description It is now possible to use MAC-forced forwarding on non-private VLANs. Because MAC-forced forwarding is primarily a security feature, the switch displays a warning message if you do so.

This enhancement allows you to use MAC-forced forwarding to limit broadcast traffic in a network where private VLANs are not appropriate.

New in IP Multicasting

This section describes new features and enhancements to IGMP, PIM, and DVMRP, as described in the *IP Multicasting* chapter in the *Software Reference for Version 2.9.1* for your router or switch.

Related enhancements include:

IGMP snooping fast leave in multiple host mode (CR00017482)

Models This enhancement is supported on:

- AT-8948, x900-48
- AT-9900
- AT-9800
- AT-8800
- AT-8600
- AT-8700XL
- Rapier i, Rapier w
- AR44x, AR450S, AR415S
- AR750S, AR770S

Module IGMP Snooping

Description 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 filtering (CR00017701)

Models This enhancement is supported on:

- AT-8600

Module IGMP

Description IGMP filtering is now available on AT-8600 series switches.

For more information, see the *IP Multicasting* chapter of the switch's Software Reference, or *How To Configure IGMP for Multicasting on Routers and Managed Layer 3 Switches*. This is available for download from your switch's product page (accessible from http://alliedtelesis.com/products/index), or from http://www.alliedtelesis.co.nz/documentation/.

New in OSPF

This section describes enhancements to OSPF, as described in the *Open Shortest Path First (OSPF)* chapter in the *Software Reference for Version 2.9.1* for your router or switch.

Increased maximum Link State Update size (CR00019749)

Models This enhancement is supported on:

- AT-8948, x900-48
- AT-9900
- AT-9800
- AT-8800
- AT-8600
- AT-8700XL
- Rapier i, Rapier w
- AR44x, AR450S, AR415S
- AR725, AR745
- AR750S, AR770S

Module OSPF

Description 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.

New in BGP-4

This section describes enhancements to BGP support as described in the *Border Gateway Protocol version 4 (BGP-4)* chapter in the *Software Reference for Version 2.9.1* for your router or switch.

Reserved BGP IANA ASNs range increased (CR00033456)

The configurable range of BGP IANA ASN's has been increased for existing BGP commands, and now includes all IANA reserved BGP ASNs between the range of 64512 through 65535 inclusive as defined in RFC 1930, section 10 in addition to public ASNs.

The effected existing commands with increased range limits are:

```
SET IP AUtonomous=1..65535
ADD BGP PEer=ipadd REMoteas=1..65535
SET BGP PEer=ipadd REMoteas=1..65535
```

For example:

```
add bgp peer=192.168.1.1 remoteas=65535
set ip auto=65535
```

BGP counter display (CR00012822)

Models This enhancement is supported on:

- AT-8948, x900-48
- AT-9900
- AT-9800
- AT-8800
- Rapier i, Rapier w
- AR44x, AR450S, AR415S
- AR725, AR745
- AR750S, AR770S

Module BGP

Description The BGP counter output display has been significantly improved. Also, the command **show bgp counter=all** now displays the RIB, UPDATE, DB and PROCESS counters.

New in IPv6

This section describes new features and enhancements to IPv6 support as described in the *Internet Protocol version 6 (IPv6)* chapter in the *Software Reference for Version 2.9.1* for your router or switch.

- "Routing header type 0 deprecated (CR00018144)" on page 84

Related enhancements include:

- "Tunnelled IPsec connection for IPv6 (CR00016150)" on page 169

Routing header type 0 deprecated (CR00018144)

Models This enhancement is supported on:

- AT-8948, x900-48
- AT-9900
- AT-9800
- AT-8800
- Rapier i, Rapier w
- AR44x, AR450S, AR415S
- AR725, AR745
- AR750S, AR770S

Module IPv6

Description Routing Header type 0 has been deprecated for IPv6 due to security concerns, as described in the Internet Draft at http://tools.ietf.org/id/draft-ietf-ipv6-deprecate-rh0-01.txt.

When the switch receives a packet addressed to it that contains RH type 0, it now responds as if it does not understand the header, as specified in RFC 2460. That is, it ignores the header if the number of segments left is zero, or it replies to the sender with an ICMPv6 incorrect parameters error message.

New in IPv6 Multicasting

This section describes new features and enhancements to IPv6 MLD and PIM multicast protocols as described in the *IPv6 Multicasting* chapter in the *Software Reference for Version 2.9.1* for your router or switch.

MLD proxy (CR00023463)

Models This enhancement is supported on:

- AT-8948, x900-48
- AT-9900
- AT-9800
- AT-8800
- Rapier i, Rapier w
- AR44x, AR450S, AR415S
- AR725, AR745
- AR750S, AR770S

Module IPv6, IPv6 Multicasting

Description This feature allows the router or switch to be configured as a simple proxy device to forward multicast traffic. It performs the host portion of the MLDv2 protocol on a single upstream interface and the router portion of the MLDv2 protocol on a number of downstream interfaces. The implementation is based on RFC 4605.

Modified commands:

- "enable ipv6 mld interface" on page 86
- "set ipv6 mld interface" on page 86
- "show ipv6 mld counters" on page 87
- "enable ipv6 mld debug" on page 87
- "show ipv6 mld debug" on page 88

New commands:

- "disable ipv6 mld proxy" on page 88
- "show ipv6 mld proxy" on page 89
- "show ipv6 mld proxy interface" on page 91
- "enable ipv6 mld proxy" on page 88

Modified Commands

A new optional parameter has been added to the **enable ipv6 mld int** and **set ipv6 mld int** commands. The parameter allows the user to specify the MLD interface as participating in the MLD proxy configuration. The default is **off**.

enable ipv6 mld interface

Syntax

```
ENABLE IPV6 MLD INTERFACE=interface
   [PROxy={OFF|UPstream|DOWNstream}
   [FORCEFORward={YES|NO}]]
```

where:

- *interface* is an interface name

Description

The interface parameter specifies the interface on which MLD is to be enabled. The interface must already be assigned and configured. Valid interfaces are:

- eth (such as eth0)
- PPP (such as ppp0)
- VLAN (such as vlan1)
- frame relay (such as fr0)
- virtual tunnel (such as virt9)

The PROXY parameter specifies whether the MLD interface as participating in the MLD proxy configuration. The default is OFF.

The FORCEFORWARD parameter specifies whether the MLD interface should always forward traffic regardless of whether the device wins the MLD Querier election on the given interface. The default is No.

Examples

To configure an interface for MLD proxy, use the command:

```
ENABLE IPV6 MLD INTERFACE=vlan1 PROXY=upstream
```

To force a downstream interface to forward traffic even if it loses the MLD Querier election on that interface use

```
ENABLE IPV6 MLD INTERFACE=vlan2 PROXY=downstream
   FORCEFORWARD=yes
```

See Also

disable ipv6 mld interface

set ipv6 mld interface

Syntax

```
SET IPV6 MLD INTERFACE=interface
   [PROxy={OFF|UPstream|DOWNstream}
   [FORCEFORward={YES|NO}]]
```

where:

- *interface* is an interface name.

Description

The interface parameter specifies the interface on which MLD is enabled. The interface must already be assigned and configured. Valid interfaces are:

- eth (such as eth0)
- PPP (such as ppp0)
- VLAN (such as vlan1)
- frame relay (such as fr0)
- virtual tunnel (such as virt9)

The PROXY parameter specifies whether the MLD interface as participating in the MLD proxy configuration. The default is OFF.

The FORCEFORWARD parameter specifies whether the MLD interface should always forward traffic regardless of whether the device wins the MLD Querier election on the given interface. The default is No.

Examples To change the proxy status for interface vlan1, use the command:

```
set ipv6 mld interface=vlan1 proxy=downstream
```

See Also disable ipv6 mld interface
set ipv6 mld interface

show ipv6 mld counters

Syntax `SHOW IPV6 MLD COUnters`

Description This command displays the MLD counters

Figure 8: Example output from the **show ipv6 mld counters** command

```
MLD counters
-----------------------------------------------------------
eth0:

  inQueryV1 ....................... 0     outQueryV1 ....................... 0
  inReportV1 ...................... 0     outReportV1 ...................... 0
  inDoneV1 ........................ 0     outDoneV1 ........................ 0
  inQueryV2 ....................... 0     outQueryV2 ....................... 0
  inReportV2 ...................... 0     outReportV2 ...................... 14

eth1:

  inQueryV1 ....................... 0     outQueryV1 ....................... 0
  inReportV1 ..................... 104    outReportV1 ...................... 0
  inDoneV1 ........................ 1     outDoneV1 ........................ 0
  inQueryV2 ....................... 0     outQueryV2 ....................... 61
  inReportV2 ..................... 62     outReportV2 ...................... 0
-----------------------------------------------------------
```

See Also disable ipv6 mld interface
set ipv6 mld interface

enable ipv6 mld debug

Syntax `ENABLE IPV6 MLD DEBug [TIMEOut={0..3600}|None] [DETAILED]`

Description This command enables MLD debugging.

The TIMEOUT parameter specifies how many seconds to output MLD debug messages for. The default is NONE, meaning the MLD debug will continue forever.

The DETAILED parameter allows the user to enable enhanced, more detailed debug message to be printed out.

See Also disable ipv6 mld debug
show ipv6 mld debug

show ipv6 mld debug

Syntax `SHOW IPV6 MLD DEBug`

Description This command displays the current state of MLD debugging.

Figure 9: Example output from the **show ipv6 mld debug** command

```
MLD debug
-------------------------------------------------------------
Status: Enabled, detailed
Timeout in: 34 seconds
```

See Also disable ipv6 mld debug
show ipv6 mld debug

New Commands

The following new commands are added to support MLD Proxy.

enable ipv6 mld proxy

Syntax `ENABLE IPV6 MLD PROxy`

Description Enables the MLD proxy software.

Examples To enable forwarding of IPv6 multicast data from the configured upstream interface to the downstream interfaces, use the command:

```
enable ipv6 mld proxy
```

See Also disable ipv6 mld proxy
enable ipv6 mld interface
set ipv6 mld interface

disable ipv6 mld proxy

Syntax `DISABLE IPV6 MLD PROxy`

Description Disables the MLD proxy software.

Examples To disable forwarding of IPv6 multicast data from the configured upstream interface to the downstream interfaces, use the command:

```
disable ipv6 mld proxy
```

See Also enable ipv6 mld proxy
enable ipv6 mld interface
set ipv6 mld interface

show ipv6 mld proxy

Syntax `SHOW IPV6 MLD PROxy`

Description This command displays information about the current state of the MLD Proxy.

Figure 10: Example output from the **show ipv6 mld proxy** command

```
MLD Proxy
-------------------------------------------------------------
MLD Proxy configuration:
  Status ............................. Enabled
  Number of downstream interfaces ..... 2
  Upstream interface .................. vlan1
  Downstream interfaces ............... vlan2, vlan3

Interface: vlan1 (upstream interface)
-------------------------------------------------------------
  Link local address ............... fe80::0200:cdff:fe1d:7d7d
  Multicast Address ................ ff02::0001:ff15:0ae6
    Filter mode .................... Exclude
  Multicast Address ................ ff02::0001:ff5e:970a
    Filter mode .................... Exclude
  Multicast Address ................ ff02::0001:ffa6:385c
    Filter mode .................... Exclude
  Multicast Address ................ ff02::0001:ff00:0002
    Filter mode .................... Exclude
  Multicast Address ................ ff02::0001:ff00:0003
    Filter mode .................... Exclude
  Multicast Address ................ ff02::0001:ff00:0004
    Filter mode .................... Exclude
  Multicast Address ................ ff08::0001
    Filter mode .................... Exclude

Interface: vlan2 (downstream interface)
-------------------------------------------------------------
  Version ......................... 2
  V2 Draft Compatible ............. NO
  Is querier ...................... YES
  Force forwarding ................ YES
  Link local address ............... fe80::0200:cdff:fe1d:7d7d
  Multicast Address ................ ff02::0001:ff15:0ae6
    Filter mode .................... Exclude
    MA timer ....................... 243
    Version ........................ 2
  Multicast Address ................ ff02::0001:ff5e:970a
    Filter mode .................... Exclude
    MA timer ....................... 241
    Version ........................ 2
  Multicast Address ................ ff02::0001:ff00:0002
    Filter mode .................... Exclude
    MA timer ....................... 241
    Version ........................ 2
  Multicast Address ................ ff02::0001:ff00:0003
    Filter mode .................... Exclude
    MA timer ....................... 243
    Version ........................ 2
  Multicast Address ................ ff08::0001
    Filter mode .................... Exclude
    MA timer ....................... 243
    Version ........................ 2
```

Figure 10: Example output from the **show ipv6 mld proxy** command (cont.)

```
Interface: vlan3 (downstream interface)
-------------------------------------------------------------
  Version ......................... 2
  V2 Draft Compatible ............. NO
  Is querier ...................... YES
  Force forwarding ................ NO
  Link local address .............. fe80::0200:cdff:fe1d:7d7d
  Multicast Address ............... ff02::0001:ffa6:385c
    Filter mode ................... Exclude
    MA timer ...................... 257 secs
    Version ....................... 1
  Multicast Address ............... ff02::0001:ff00:0004
    Filter mode ................... Exclude
    MA timer ...................... 257 secs
    Version ....................... 1
  Multicast Address ............... ff02::0001:ff00:0002
    Filter mode ................... Exclude
    MA timer ...................... 252 secs
    Version ....................... 1
  Multicast Address ............... ff08::0001
    Filter mode ................... Exclude
    MA timer ...................... 258 secs
    Version ....................... 1
-------------------------------------------------------------
```

Table 5: Parameters displayed in the output of the **show ipv6 mld proxy** command

Parameter	Meaning
Status	Displays whether the MLD Proxy is enabled or disabled
Number of downstream interfaces	Displays the number of downstream interfaces configured for the proxy
Upstream interface	Displays the interface configured as the proxy's upstream interface
Downstream interfaces	Displays the list of interfaces configured as downstream interfaces for the proxy
Force forwarding	Displays whether an interface has overridden the requirement that only devices that win the MLD Querier election on a given interface may forward traffic onto that interface.

Note: All other parameters are as for the SHOIPV6 MLD command output.

Examples To see the current state of the MLD Proxy, use the command:

```
show ipv6 mld proxy
```

show ipv6 mld proxy interface

Syntax `SHOW IPV6 MLD PROXY INTERFACE=`*`interface`*

where:

- *interface* is an interface name.

Description The interface parameter specifies the interface on which MLD is enabled. The interface must already be assigned and configured. Valid interfaces are:

- eth (such as eth0)
- PPP (such as ppp0)
- VLAN (such as vlan1)
- Frame relay (such as fr0)
- virtual tunnel (such as virt9)

This command displays information about the current state of a particular interface involved in the MLD Proxy.

Figure 11: Example output from the **show ipv6 mld proxy interface** command

```
MLD Proxy
---------------------------------------------------------------
MLD Proxy configuration:
  Status ............................. Enabled
  Number of downstream interfaces ..... 3
  Upstream interface .................. vlan1
  Downstream interfaces ............... vlan2, vlan3

Interface: vlan1 (upstream interface)
---------------------------------------------------------------
  Link local address ............... fe80::0200:cdff:fe1d:7d7d
  Multicast Address ................ ff02::0001:ff15:0ae6
    Filter mode .................... Exclude
  Multicast Address ................ ff02::0001:ff5e:970a
    Filter mode .................... Exclude
  Multicast Address ................ ff02::0001:ffa6:385c
    Filter mode .................... Exclude
  Multicast Address ................ ff02::0001:ff00:0002
    Filter mode .................... Exclude
  Multicast Address ................ ff02::0001:ff00:0003
    Filter mode .................... Exclude
  Multicast Address ................ ff02::0001:ff00:0004
    Filter mode .................... Exclude
  Multicast Address ................ ff08::0001
    Filter mode .................... Exclude
```

Table 6: Parameters displayed in the output of the **show ipv6 mld proxy interface** command

Parameter	Meaning
Status	Displays whether the MLD Proxy is enabled or disabled
Number of downstream interfaces	Displays the number of downstream interfaces configured for the proxy
Upstream interface	Displays the interface configured as the proxy's upstream interface
Downstream interfaces	Displays the list of interfaces configured as downstream interfaces for the proxy
Force forwarding	Displays whether an interface has overridden the requirement that only devices that win the MLD Querier election on a given interface may forward traffic onto that interface.

Note: All other parameters are as for the SHOIPV6 MLD command output.

Examples To see the current state of the MLD Proxy, use the command:

```
show ipv6 mld proxy interface=vlan1
```

New in Generic Packet Classifiers

This section describes new features and enhancements to classifiers (used with filtering and QoS) as described in the *Generic Packet Classifier* chapter in the *Software Reference for Version 2.9.1* for your router or switch.

- "Acting on traffic for particular DHCP client (CR00017018)" on page 93

Related enhancements include:

- "More DHCP snooping classifiers (CR00019005)" on page 75

Acting on traffic for particular DHCP client (CR00017018)

Models This enhancement is supported on:

- AT-8948, x900-48
- AT-9900

Module Classifier, DHCP snooping

Description This enhancement enables you to act on traffic that is received on an uplink port and is destined for a particular DHCP client. It expands the classifier functionality so that the switch can use DHCP snooping records to determine which traffic is destined for each client. Once the classifier has identified the traffic, you can apply a QoS policy or hardware filters to it.

For example, you can use the new functionality to track how much traffic each user receives via an uplink port. This enables you to track traffic usage at the uplink port, even if destination IP addresses are dynamically assigned by DHCP and traffic for multiple users is in the same VLAN.

To configure such tracking:

1. **Configure DHCP snooping.**
2. **Create the required classifiers.**

   For each DHCP client, create a classifier using the following new options:

   ```
   create classifier=id ipdaddress=dhcpsnooping
      snoopport=port-number snoopvlan=vlan-id
   ```

   The **dhcpsnooping** option for the **ipdaddress** parameter causes the switch to dynamically create appropriate classifiers when DHCP snooping deems that an appropriate DHCP lease event has occurred.

   The **snoopport** parameter specifies the switch port that traffic egresses for the target DHCP client.

   The **snoopvlan** parameter specifies the VLAN for traffic to that client.

3. **Put the classifiers into a QoS heirarchy.**
4. **Apply the QoS policy to the uplink port.**

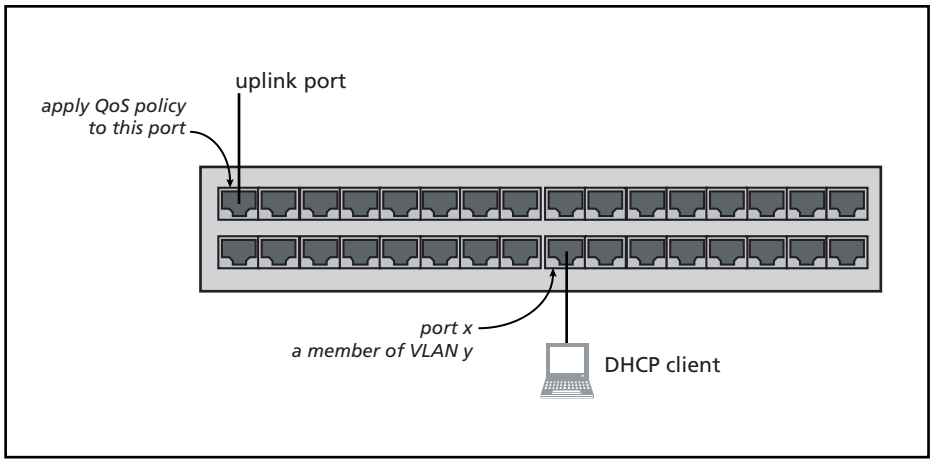
5. **Use the traffic class counters to see how much traffic is destined for each client.**

The new options have also been added to the **set classifier** command and output of the **show classifier** command.

Example For example, consider the following figure. In this example, the QoS policy on the uplink port includes the following classifier:

```
create classifier=1 ip=dhcpsnooping snoopport=x snoopvlan=y
```

When the client receives a DHCP lease, all traffic that comes in through the uplink port and is destined for the client will match classifier 1.



New in Software QoS

This section describes new features and enhancements to Software QoS support as described in the Software Quality of Service (QoS) chapter in the *Software Reference for Version 2.9.1* for your router or switch.

SQoS—virtual bandwith limit exceeded (CR00033115)

Models This enhancement is supported on:

- Rapier i, Rapier w
- AR44x, AR450S, AR415S
- AR725, AR745
- AR750S

Module Software QoS

Description An undesireable burst of traffic after a period of inactivity that would exceed the limit set by Virtual Bandwidth has been rectified.

A new command parameter has been added tailing the existing SQoS Virtual Bandwidth parameter that sets up the minimal burst metering. The parameter is called **MINBurst** and has values of ON, OFF, YES, and NO.

When the Virtual Bandwidth meter is created or updated, the software checks if the MINBurst is TRUE, and will reduce the max burst size relative to 1 second metered time interval. Otherwise, it defaults to the value relative to a 60 second period.

For example:

```
Manager > create  sqos trafficclass=10 virtbw=20mbps ?
 DESCription
 RED
 METer
 BWClass3acti
 PAUSETime
 PREMARKDscp
 PREMARKBwcla
 REMarking
 REMARKVlanpr
 MINBurst
 MAXQlen
 QUEUEDrop
 PRIOrity
 WEIght
 WEIGHTSchedu
 QLIMITExceed
 PAUSEAction
 <enter>      Process command as is, as long as required
parameters are present
```

```
Manager > cre sqos tr=10 virtbw=20mbps minburst=?
required -  Yes No ON OFf
```

This issue has been resolved.

Software QoS on PPPoE interfaces (CR00016078)

Models This enhancement is supported on:

- Rapier i, Rapier w
- AR44x, AR450S, AR415S
- AR725, AR745
- AR750S

Module Software QoS, PPP, Ethernet, VoIP

Description The switch now supports software QoS on PPPoE interfaces.

New in User Authentication

This section describes enhancements to user authentication and the user authentication database as described in the *User Authentication* chapter in the *Software Reference for Version 2.9.1* for your router or switch.

■ "User Authentication Password Enhancement (CR00020742)" on page 97

Related enhancements include:

■ "RADIUS authentication of SSH sessions (CR00017197)" on page 108

User Authentication Password Enhancement (CR00020742)

Models This enhancement is supported on:

- AT-8948, x900-48
- AT-9900
- AT-9800
- AT-8800
- AT-8600
- AT-8700XL
- Rapier i, Rapier w
- AR44x, AR450S, AR415S
- AR725, AR745
- AR750S, AR770S

Module User Authentication

Description 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

Table 7: New and modified commands

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 (Figure 12, Table 8). 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 13 on page 104, Table 9 on page 104).

Figure 12: 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 8: 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 13: 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 9: 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 (Figure on page 105, Table 10 on page 105).

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

Figure 14: 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 10: 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 (Figure 15 on page 106, Table 11 on page 106).

The output of this command includes new fields.

Figure 15: 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 11: 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".

New in Port Authentication

This section describes new features and enhancements to 802.1X and MAC-based port authentication as described in the *Port Authentication* chapter in the *Software Reference for Version 2.9.1* for your router or switch.

- "MAC address format for MAC-based authentication (CR00026718)" on page 107

Related enhancements include:

- "SNMP MIB enhancements for DHCP and Port Authentication (CR00025844)" on page 181

MAC address format for MAC-based authentication (CR00026718)

Models This enhancement is supported on:

- AT-8948, x900-48
- AT-9900
- AT-9800
- AT-8800
- AT-8600
- AT-8700XL
- Rapier i, Rapier w
- AR44x, AR450S, AR415S
- AR725, AR745
- AR750S, AR770S

Module Port Auth

Description It is now possible to configure a device so that when MAC-based authentication sends a request for a MAC address to be authorised, the username and password (which are the MAC address) can now be formatted either with hyphens (i.e. 00-00-cd-12-34-56) or without hyphens, (ie. 0000cd123456).

New in Secure Shell (SSH)

This section describes enhancements to Secure Shell session management as described in the *Secure Shell* chapter in the *Software Reference for Version 2.9.1* for your router or switch.

No SSH feature licence required (CR00018895)

Models This enhancement is supported on:

- AT-8948, x900-48
- AT-9900
- AT-9800
- AT-8800
- AT-8600
- AT-8700XL
- Rapier i, Rapier w
- AR44x, AR450S, AR415S
- AR725, AR745
- AR750S, AR770S

Module SSH

Description Secure Shell (SSH) no longer requires a feature licence. SSH server and client functionality now works when no feature licence is present.

RADIUS authentication of SSH sessions (CR00017197)

Models This enhancement is supported on:

- AT-8948, x900-48
- AT-9900
- AT-9800
- AT-8800
- AT-8600
- AT-8700XL
- Rapier i, Rapier w
- AR44x, AR450S, AR415S
- AR725, AR745
- AR750S, AR770S

Module SSH, User, RADIUS

Description SSH sessions to the switch or router can now be authenticated via RADIUS. The switch or router 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 or router has RADIUS configured.

New in DoS Attack Prevention

This section summarises the new DoS Attack Prevention feature as described in the *Denial of Service (DoS) Attack Prevention chapter in the Software Reference for Version 2.9.1* DoS Attack Prevention Edition (C613-03127-00 REV B) for the AT-8600 switch.

■ "Denial of Service Attack Protection (CR00020057)" on page 109

Denial of Service Attack Protection (CR00020057)

Models This enhancement is supported on:

■ AT-8600

Module DoS Attack Prevention

Description The AlliedWare™ Operating System now includes a Denial of Service Attack Protection feature for AT-8600 Series switches. This enhancement allows you to configure specific defences against the following types of DoS attacks:

■ IP Options

■ LAND Attack

■ Ping of Death Attack

■ Smurf Attack

■ SYN Flood Attack

■ Teardrop Attack

For more information about configuring DoS Attack Prevention, see the *Denial of Service (DoS) Attack Prevention* chapter in the *Security* part in the *AlliedWare™ Operating System Software Reference for Version 2.9.1 DoS Attack Prevention Edition* (C613-03127-00 REV B) available for AT-8600 Series switches. This is available for download from your switch's product page (accessible from http://alliedtelesis.com/products/index) or from http://www.alliedtelesis.co.nz/documentation/.

New in Firewall

This section describes new features and enhancements to the Firewall as described in the *Firewall* chapter in the *Software Reference for Version 2.9.1* for your router or switch.

Firewall Application Detection System (ADS) (CR00029938)

Models This enhancement is supported on the following models:

- AR44x, AR450S, AR415S
- AR750S, AR770S

Module Firewall

Description Peer-to-Peer (P2P) application exchanges can expose a network to risks of excess bandwidth being used by the P2P application, of virus distribution via the application, and of private information being unintentionally distributed on the Internet. With this Application Detection System (ADS) enhancement, the firewall can be configured to detect, filter, and log traffic from Winny (v2.0b7.1), a peer-to-peer (P2P) file-sharing application most commonly used in Japan. ADS can be used in networks such as in Internet hotels and Internet apartments to reduce the security risks from this application.

Use the following new commands to configure P2P filtering:

- **enable firewall policy p2pfilter** command on page 111
- **disable firewall policy p2pfilter** command on page 112

Use the following new and modified commands to display the P2P filtering configuration and events:

- **show firewall policy** command on page 113
- **show firewall policy p2pfilter** command on page 114
- **show firewall event** command on page 115

enable firewall policy p2pfilter

This new command enables the Application Detection System (ADS) to detect traffic from a peer-to-peer (P2P) application for the specified firewall policy, and sets the action and threshold to apply to such traffic. By default, P2P filtering is disabled. If ADS is already enabled for the application, use this command to modify the settings.

Syntax

```
ENAble FIREwall POLIcy=policy P2PFILTER={WINNY}
   ACTION={NOTIFY|DENY} [THRESHOLD=1..255]
```

Table 12: Parameters in the **enable firewall policy p2pfilter** command

Parameter	Description	
POLIcy	The name firewall policy to add the P2P filtering to. *policy* is a character string, 1 to 15 characters in length. Valid characters are uppercase letters (A-Z), lowercase letters (a-z), digits (0-9), the underscore character ("_"), the hyphen character ("-"). Wildcards are not allowed.	
P2PFILTER	The peer-to-peer application to filter for: WINNY—Winny v2.0b7.1.	
ACTION	The action to take when the firewall detects a packet from the P2P application.	
	NOTIFY	When packets from the specified P2P application are detected, generate firewall events and log messages. Do not discard packets from the application or remove the firewall session.
	DENY	When packets from the P2P application are detected, remove the corresponding firewall session and generate corresponding firewall events and log messages.
THRESHOLD	The number of packets to check at the beginning of a TCP session (after the TCP 3-way handshake is completed) to determine whether they come from the specified P2P application. If no packets from the application are detected within this threshold, then no further filtering for the application is applied for the rest of the session. If packets from the application are detected within the threshold, then the **action** parameter determines what will happen. If the **action** is **deny**, the firewall session is removed immediately. If the **action** is **notify**, then events and messages are generated, and the firewall continues to check the session for more application packets till the threshold is reached. Default: **20** (Winny)	

Example To enable P2P filtering and to discard all traffic from the P2P application *Winny* for the policy *mypolicy*, use the command:

```
ena fire poli=mypolicy p2pfilter=winny action=deny
```

See Also

disable firewall policy p2pfilter
show firewall policy
show firewall policy p2pfilter
show firewall event

disable firewall policy p2pfilter

This new command disables Application Detection System (ADS) filtering of traffic from the specified peer-to-peer (P2P) application in the firewall policy. By default, P2P filtering is disabled.

Syntax `DISable FIREwall POLIcy=`*`policy`* `P2PFILTER={WINNY}`

Table 13: Parameters in the **enable firewall policy p2pfilter** command

Parameter	Description
POLIcy	The firewall policy to disable the P2P filtering in. *policy* is a character string, 1 to 15 characters in length. Valid characters are uppercase letters (A-Z), lowercase letters (a-z), digits (0-9), the underscore character ("_"), the hyphen character ("-"). Wildcards are not allowed.
P2PFILTER	The P2P application to disable filtering for: WINNY.

Examples To disable P2P filtering of traffic for the application *Winny* in the policy *mypolicy,* use the command:

```
dis fire poli=mypolicy p2pfilter=winny
```

See Also
enable firewall policy p2pfilter
show firewall policy
show firewall policy p2pfilter
show firewall event

show firewall policy

In addition to other firewall policy configuration, this command now also displays the status of filtering for a peer-to-peer (P2P) application.

Syntax `SHow FIREwall POLIcy[=`*`policy`*`]`

Figure 16: Example output from the show firewall policy command

```
Policy : test
  TCP Timeout (s) ................... 3600
  UDP Timeout (s) ................... 1200
  Other Timeout (s) ................. 1200
  ICMP Unreachable Timeout (s) ...... 0
  TCP Handshake Timeout Mode ........ Normal
  MAC Cache Timeout (m) ............. 1440
  RADIUS Limit ...................... 100
  Accounting ........................ disabled
  Enabled Logging Options ........... none
  Enabled Debug Options ............. none
  Enabled Debug Modes ............... none
  Enabled Debug IP Address .......... none
  Identification Protocol Proxy ..... enabled
  Enabled IP options ................ none
  Enhanced Fragment Handling ........ none
  Enabled ICMP forwarding ........... none
  Receive of ICMP PINGS ............. enabled
  Number of Notifications ........... 0
  Number of Deny Events ............. 0
  Number of Allow Events ............ 0
  Number of Active TCP Opens ........ 0
  Number of Active Sessions ......... 0


  Cache Hits ........................ 0
  Discarded ICMP Packets ............ 0
  SMTP Domain ....................... not set
  FTP Data Port ..................... RFC enforced
  TCP Setup Proxy ................... enabled
  TCP MSS Adjustment ................ disabled
  UPNP .............................. disabled
    WAN interfaces .................. none
    LAN interfaces .................. none
    Maximum port maps ............... 250
  SIP ALG ........................... disabled
  P2P Filter ........................ enabled
  Number of Limitrules .............. 0
  Private Interfaces : none currently defined
  Public Interface  : none currently defined
```

Table 14: New parameter displayed in the output of the **show firewall policy** command

Parameter	Meaning	
P2P Filter	The current P2P filter status.	
	enabled	Displayed when filtering is enabled for the policy for any P2P application.
	disabled	Displayed when there is no P2P filtering enabled for the policy.

Examples To display information about firewall policy *mypolicy*, including the status of P2P filtering, use the command:

```
sh fire poli=mypolicy
```

See Also
disable firewall policy p2pfilter
enable firewall policy p2pfilter
show firewall policy p2pfilter
show firewall event

show firewall policy p2pfilter

This new command displays configuration settings for peer-to-peer (P2P) filtering for the specified policy, or for all firewall policies.

Syntax `SHow FIREwall POLIcy[=`*`policy`*`] P2PFILTER`

Figure 17: Example output from the **show firewall policy p2pfilter** command

```
Policy : test
Current P2P Filter Setup

Application           Threshold       Hits          Status
-------------------------------------------------------------
Winny                 20              160           notify
-------------------------------------------------------------
```

Table 15: Parameters displayed in the output of the **show firewall policy p2pfilter** command

Parameter	Meaning	
Application	The P2P application name.	
Threshold	The threshold value configured.	
Hits	Detected number of P2P packets detected since the P2P filtering in the firewall policy was enabled.	
Status	Status information.	
	notify	Displayed when P2P action was notify.
	deny	Displayed when P2P action was deny.
	disabled	Displayed when P2P filter is disabled.

Examples To display information about P2P filtering for the policy *mypolicy*, use the command:

```
sh fire poli=mypolicy p2pfilter
```

See Also
disable firewall policy p2pfilter
enable firewall policy p2pfilter
show firewall policy
show firewall event

show firewall event

This command now also displays firewall events related to filtering for a peer-to-peer (P2P) application.

Syntax `SHow FIREwall EVent[={ALLOw|DENY|NOTify}] [POLIcy=`*`policy-name`*`] [REVerse=`*`number`*`] [TAil=`*`number`*`]`

Figure 18: Example output from the **show firewall event** command

```
Policy : net - Notify Events:
Date/Time   Dir Prot Number IP:Port <map> Dest IP:Port /Reason /IP header
-------------------------------------------------------------------------------
 4 06:01:57 OUT TCP       1 192.168.1.50:3618 5413 192.168.0.2:5320
                P2P communication found
-------------------------------------------------------------------------------

Policy : net - Deny Events:
Date/Time   Dir Prot Number IP:Port <map> Dest IP:Port /Reason /IP header
-------------------------------------------------------------------------------
4 06:00:42 OUT TCP       1 192.168.1.50:3587 11171 192.168.0.2:5320
                P2P communication discarded
-------------------------------------------------------------------------------

Policy : net - Allow Events:
Date/Time   Dir Prot Number IP:Port <map> Dest IP:Port /Reason /IP header
  No event information currently recorded
```

IPsec Passthrough (CR00028385)

Models This enhancement is supported on:

- AT-8800
- Rapier i, Rapier w
- AR44x, AR450S, AR415S
- AR725, AR745
- AR750S, AR770S

Module Firewall, IPsec

Description IPSec Passthrough is implemented as another form of ENAT specifically for the ESP protocol in the firewall. The feature is an enhancement of current firewall capabilities which implements an IPSec Application Level Gateway function to support IPSec connections from the private LAN, through the router and towards the public internet. The ALG functionality and IPSec co-exist (i.e. IPSec connections may just pass through the router or they may also terminate on the router. Both configurations are simultaneously possible.)

- IPSec Passthrough is controlled by command handler extensions to the firewall command handler.
- IPSec Passthrough is enabled by applying the translation to an entire interface (interface based) or subsets of traffic (rule based). It is automatically enabled if a firewall rule exists and disabled if the firewall rules are removed.

- A separate show command is used to display active connections. Connections are terminated by a timeout without activity or explicitly via command.
- Once the connection is through the firewall, it still may terminate on the router itself. There is no limitation to the use of IPsec Passthrough and IPsec hosting or peering simultaneously on the same router.
- IP Sec Passthrough functionality is configured using the add firewall policy rule command and removed from configuration using the delete firewall policy rule command.
- The commands are extended to allow protocol=ESP when action=NAT and nattype=ENHANCED. No other combinations are valid for protocol ESP.
- The interface to which this rule is applied must be a public interface. Applying it to a private interface has no effect.
- The specification of GBLIP is optional. If not specified, then the IP address of the public interface will be used.

The syntax of the command is changed as follows. The changed/new portions are highlighted in bold.

add firewall policy rule

Syntax

```
ADD FIREwall POLIcy=policy-name RUle=rule-id
   ACtion={ALLOw|DENY|NAT|NONat} INTerface=interface
   PROTocol={protocol|ALL|EGP|GRE|ICmp|OSPF|SA|TCP|UDP|ESP}
   [AFTer=hh:mm] [BEFore=hh:mm]
   [DAYs={ALL|MON|TUE|WED|THU|FRI|SAT|SUN|WEEKDay|WEEKEnd}
   [,...]] [ENCapsulation={NONE|IPSec}] [GBLIP=ipadd]
   [GBLPort={ALL|port[-port]|service-name}]
   [GBLRemoteip=ipadd[-ipadd]] [IP=ipadd[-ipadd]]
   [LISt={list-name|RADius|MACRADius}]
   [NATType={DOuble|ENAPt|ENHanced|NApt|REVerse|STAndard}]
   [NATMask=ipadd] [POrt={ALL|port[-port]|service-name}]
   [REMoteip=ipadd[-ipadd]] [SOurceport={ALL|port[-port]}]
   [TTL=hh:mm]
```

With rule based NAT and **nattype**=**enhanced** and **protocol**=**ESP**, the meaning of the **ip**, **gblip** are modified for IPSec Passthrough. The **port** parameters are not relevant for IPSec Passthrough and are not used.

Table 16: Meaning of parameters modified by this enhancement

Rule-based NAT type	Interface	Type of address or port	Match	Translate to
Enhanced NAT (**nattype**= **enhanced**) Protocol=ESP	Private: outgoing traffic	Source IP	**ip**	**gblip** (required)
		Destination IP	**remoteip**	Not translated
		Source port	n/a	n/a
		Destination port	n/a	n/a

Examples In this example, you have a public interface to which you want to allow TCP/UDP sessions using enhanced NAT and you also wish to configure IPSec Passthrough for VPN connections originating from the private side to the public side.

To configure this, use the commands:

Figure 19: Example configuration extract

```
# Firewall configuration
enable firewall
create firewall policy="internet"
add firewall policy="internet" int=eth0 type=public
add firewall policy="internet" int=vlan1 type=private
# An interface based rule may exist but this is only to define UDP/TCP # NATing
add firewall poli="internet" nat=enhanced int=vlan1 gblint=eth0
# An Allow rule is required for UDP:500 for ISAKMP messages to reach
# the initiator on the private side
add firewall poli="internet" ru=1 ac=allo int=eth0 prot=udp
ip=<eth0_internet_address> po=500 gblip=<eth0_internet_address> gblport=500
# A rule based NAT for ESP extends or defines NAT for ESP only. It
# implies an allow rule for prot=ESP and so no explicit allow rule
# is required.
add firewall poli="internet" ru=2 ac=nat nattype=enhanced int=eth0 prot=esp
```

In this example, you have a public interface to which you want to allow IPSec Passthrough for VPN access only using enhanced NAT.

To configure this, use the commands:

Figure 20: Example configuration extract

```
# Firewall configuration
enable firewall
create firewall policy="internet"
add firewall policy="internet" int=eth0 type=public
add firewall policy="internet" int=vlan1 type=private
# An Allow rule is required for UDP:500 for ISAKMP messages to reach
# the initiator on the private side
add firewall poli="internet" ru=1 ac=allo int=eth0 prot=udp
ip=<eth0_internet_address> po=500 gblip=<eth0_internet_address> gblport=500
# A rule based NAT defines NAT for ESP only. It
# implies an allow rule for prot=ESP and so no explicit allow rule
# is required.
add firewall poli="internet" ru=2 ac=nat nattype=enhanced int=eth0 prot=esp
```

Session Management

show firewall

The **show firewall** command syntax is not altered, however the output of the show firewall command is modified to include summary statistics about IPSec Passthrough (ESP) sessions.

The **show firewall** command will display summary statistics about the number of ESP sessions if at least 1 policy is configured that enables IPSec Passthrough, The **show firewall** command displays the current number in use and the peak over the course of the running of the router.

Peak and **Active** are reset to 0 if the configuration which enables IPSec Passthrough is removed from the configuration. The output below shows the **show firewall** command if ESP NAT is configured on at least one policy.

Figure 21: Example output from the **show firewall** command

```
SecOff IPSecPthruGW> sh firewall


Firewall Configuration

Status ..................... enabled
Enabled Notify Options .... manager
SIP ALG enabled ........... FALSE
SNMP Session Report ....... enabled
Maximum Packet Fragments .. 20
Sessions:
  Maximum ................. 29433
  Peak .................... 1
  Active .................. 0
  Peak ESP . …..............5
  Active ESP …..............1
```

Table 17: New parameters in the output from the **show firewall** command

Parameter	Description
Peak	The highest number of simultaneous IPSec Passthrough sessions on all policies on the device at one time.
Active	The total number of sessions currently active on the device

show firewall session

The syntax of the **show firewall session** command is modified to allow the selection of sessions started for protocol ESP (IPSec Passthrough).

Syntax

```
SHow FIREwall SEssion[=session-number] [POLIcy=policy-name]
   [COUnter] [IP=ipadd[-ipadd]] [POrt={port[-port]|service-
   name}]
   [PROTocol={protocol|ALL|EGP|GRE|ICmp|OSPF|TCP|UDP|ESP}]
   [SUMmary] [UPNP]
```

For sessions which have been started for protocol ESP, the output of the **show firewall session** command is modified to show parameters which are relevant for IPSec Passthrough sessions.

The IP, Remote IP, GBL IP or GBL Remote IP addresses:

- have the same meanings as for TCP sessions.
- are not followed by a port number
- are followed by:
  - the initiator Security Parameter Index (SPI), after the IP and GBL IP addresses
  - the responder SPI if it is known, after the Remote IP and GBL Remote IP address (only if the state of the ESP session is **established**). If it is not yet known, then 0 is displayed (in state **initiated**)

Table 18: Example output

```
Policy : ipsecpthru
Current Sessions
--------------------------------------------------------------------------------
e0ee ESP   IP: 192.168.3.5:4120155611    Rem IP: 202.178.178.177:4120155611
       Gbl IP: 202.178.178.178:0      Gbl Rem IP: 202.178.178.177:0
     ESP state ............................ initialised
     Start time ........................... 12:53:42 15-Dec-2009
     Seconds to deletion .................. 54
--------------------------------------------------------------------------------
```

Table 19: Example output

```
Policy : ipsecpthru
Current Sessions
--------------------------------------------------------------------------------
4860 ESP   IP: 192.168.3.5:3785540529    Rem IP: 202.178.178.177:3785540529
       Gbl IP: 202.178.178.178:101480477 Gbl Rem IP: 202.178.178.177:101480477
     ESP state ............................ established
     Start time ........................... 12:12:41 15-Dec-2009
     Seconds to deletion .................. 900
--------------------------------------------------------------------------------
```

Table 20: Example output

```
Policy : ipsecpthru
Current Sessions
--------------------------------------------------------------------------------
a8ca UDP      IP: 192.168.3.5:500           Remote IP: 202.178.178.177:500
          Gbl IP: 202.178.178.178:43210 Gbl Remote IP: 202.178.178.177:500
d4e0 UDP      IP: 192.168.3.5:49289         Remote IP: 202.178.178.177:1701
          Gbl IP: 202.178.178.178:54496 Gbl Remote IP: 202.178.178.177:1701
b18e ESP   IP: 192.168.3.5:2041892766    Rem IP: 202.178.178.177:2041892766
       Gbl IP: 202.178.178.178:151433019 Gbl Rem IP: 202.178.178.177:151433019
--------------------------------------------------------------------------------
```

Table 21: Parameters in the output from the **show firewall session** command

Parameter	Description
Policy	The name of the policy.
Hex-num	The session identifier.
TCP/UDP/**ESP**/number	The IP protocol (either TCP, UDP, **ESP** or an IP protocol number), followed by the source address:port, the global IP address:mapped port, and the destination IP address:port. **If the protocol= 50 (ESP), the IP address is followed by the Security Parameter Index (SPI) and not a port.**
IP	This IP address is the source address of outbound packets and the destination address of inbound packets in this session, as seen on the private side of the firewall.
Remote IP/**Rem IP**	This IP address is the destination address of outbound packets and the source address of inbound packets in this session, as seen on the private side of the firewall.

Table 21: Parameters in the output from the **show firewall session** command

Parameter	Description
Gbl IP	This IP address is the source address of outbound packets and the destination address of inbound packets in this session, as seen on the public side of the firewall.
Gbl Remote IP/**Gbl Rem IP**	This IP address is the destination address of outbound packets and the source address of inbound packets in this session, as seen on the public side of the firewall.
ESP state	The state of the ESP session; either 'initiated' or 'established'.
Seconds to deletion	If the ESP state is **established**, the **Seconds to deletion** is the time until the session is removed if there is no activity on this session. If the ESP state is **initiated**, the **Seconds to deletion** is the time until the session is removed if there is no IPSec response received from the responding router that matches the initiated session. A response matches if the source IP address of the responder matches the global remote IP address and the destination IP address of the response matches the global IP address of the session.

Note that the display of the IP addresses and SPIs is more free format than for other sessions and will not necessarily line up with the display of types of other sessions.

delete firewall session

The syntax of the **delete firewall session** command is not modified but it now also supports the deletion of sessions which have been started for IPSec Passthrough. Sessions are identified for deletion by the session ID.

show firewall policy

The syntax of the **show firewall policy** command is not modified. The show output is modified to display the value of the configured (or default if not configured) **epstimeout** value.

Table 22: Example output from the show firewall policy command

```
Policy : internet
  TCP Timeout (s) ................... 3600
  UDP Timeout (s) ................... 1200
  ESP Timeout (s) ................... 1200
  Other Timeout (s) ................. 1200
  ICMP Unreachable Timeout (s) ...... 0
  TCP Handshake Timeout Mode ........ Normal
  MAC Cache Timeout (m) ............. 1440
  RADIUS Limit ...................... 100
  Accounting ........................ disabled
  Enabled Logging Options ........... espalg
  Enabled Debug Options ............. none
  Enabled Debug Modes ............... none
  Enabled Debug IP Address .......... none
  Identification Protocol Proxy ..... enabled
  Enabled IP options ................ none
  Enhanced Fragment Handling ........ none
  Enabled ICMP forwarding ........... none
  Receive of ICMP PINGS ............. enabled
  Number of Notifications ........... 0
  Number of Deny Events ............. 1
  Number of Allow Events ............ 1
  Number of Active TCP Opens ........ 0
  Number of Active Sessions ......... 1
  Cache Hits ........................ 0
  Discarded ICMP Packets ............ 0
  SMTP Domain ....................... not set
  FTP Data Port ..................... RFC enforced
  TCP Setup Proxy ................... enabled
  TCP MSS Adjustment ................ disabled
  UPNP .............................. disabled
    WAN interfaces .................. none
    LAN interfaces .................. none
    Maximum port maps ............... 250
  SIP ALG ........................... disabled
Number of Limitrules ............... 0
Private Interface : vlan2
    Trust Private ................... yes
    Rule ............................ 6
      Action ........................ nat
      NAT type ...................... enhanced
      Protocol ...................... ESP
      Global IP ..................... 202.178.178.178
      Days .......................... all
  Public Interface  : eth0
    Method .......................... dynamic
    NAT ............................. enhanced
      Method ........................ enhanced dynamic
Private Interface ............. vlan2
      Global IP ..................... 202.178.178.178
```

show firewall policy counter

The command syntax for **show firewall policy counter** is not modified. The output is modified to include:

- the **epstimeout** value (as for the **show firewall policy** command)
- if the public interface has an enhanced NAT with protocol=ESP (50) defined, then additional counters are displayed.

Table 23: Example output from the show firewall policy counter command

```
Policy : internet
  TCP Timeout (s) ................... 3600
  UDP Timeout (s) ................... 1200
  ESP Timeout (s) ................... 1200
  Other Timeout (s) ................. 1200
  ICMP Unreachable Timeout (s) ...... 0
  TCP Handshake Timeout Mode ........ Normal
  MAC Cache Timeout (m) ............. 1440
  RADIUS Limit ...................... 100
  Accounting ........................ disabled
  Enabled Logging Options ........... espalg
  Enabled Debug Options ............. none
  Enabled Debug Modes ............... none
  Enabled Debug IP Address .......... none
  Identification Protocol Proxy ..... enabled
  Enabled IP options ................ none
  Enhanced Fragment Handling ........ none
  Enabled ICMP forwarding ........... none
  Receive of ICMP PINGS ............. enabled
  Number of Notifications ........... 0
  Number of Deny Events ............. 2
  Number of Allow Events ............ 4
  Number of Active TCP Opens ........ 0
  Number of Active Sessions ......... 4
  Cache Hits ........................ 66
  Discarded ICMP Packets ............ 0
  SMTP Domain ....................... not set
  FTP Data Port ..................... RFC enforced
  TCP Setup Proxy ................... enabled
  TCP MSS Adjustment ................ disabled
  UPNP .............................. disabled
    WAN interfaces .................. none
    LAN interfaces .................. none
    Maximum port maps ............... 250
    Number Port Mappings ............ 0
    Spawned Sessions ................ 0
  SIP ALG ........................... disabled
  Number of Limitrules .............. 0
```

Table 23: Example output from the show firewall policy counter command (cont.)

```
Private Interface : vlan2
    Total Packets Received .......... 68
    Number Flows Started ............ 4
    Number Cache Hits ............... 64
    Number Dropped Packets .......... 0
    Number Unknown IP Protocols ..... 0
    Number Bad ICMP Packets ......... 0
Number Dumped ICMP Packets ...... 0
    Number Spoofing Packets ......... 0
    Number Dropped GBLIP is Zero .... 0
    Number No Spare Entries ......... 0
    Number FTP Port Commands ........ 0
    Number Bad FTP Port Commands .... 0
    Number ESP Sessions Initiated ... 2
    Number ESP Sessions Established . 2
    Number ESP Sessions Peak ........ 2
    Number ESP Sessions ............. 2
    Number Ambiguous ESP Sessions ... 0
    Rule ............................ 6
      Action ........................ nat
      NAT type ...................... enhanced
      Protocol ...................... ESP
      Global IP ..................... 202.178.178.178
      Number Hits ................... 2
      Days .......................... all
  Public Interface  : eth0
    Method ......................... dynamic
    Total Packets Received .......... 8
    Number Flows Started ............ 0
    Number Cache Hits ............... 4
    Number Dropped Packets .......... 2
    Number Unknown IP Protocols ..... 0
    Number Bad ICMP Packets ......... 0
    Number Dumped ICMP Packets ...... 0
    Number Spoofing Packets ......... 0
    Number Dropped GBLIP is Zero .... 0
    Number No Spare Entries ......... 0
    Number FTP Port Commands ........ 0
    Number Bad FTP Port Commands .... 0
    Number ESP Dropped Packets ...... 0
    NAT ............................. enhanced
      Method ........................ enhanced dynamic
      Private Interface ............. vlan2
      Global IP ..................... 202.178.178.178
```

Table 24: New parameters in the output from the **show firewall policy counter** command

Parameter	Meaning
General information about the policy	
ESP Timeout (s)	The length of time, in seconds, for which the firewall maintains inactive ESP sessions.
Information about private and public interfaces	
Public Interface	The name of a public interface that is attached to the policy. If the interface is dynamic, the template name and username follow this entry.

Table 24: New parameters in the output from the **show firewall policy counter** command

Parameter	Meaning
Number ESP Session Initiated	The number of ESP messages detected from the private to the public interface which did not yet have a session and a new session was initiated.
Number ESP Sessions established	The number of ESP initiated sessions which received a reply from the remote host which resulted in a session moving to the established state.
Number of ESP Session peak	The highest number of simultaneous ESP Sessions established on this interface for this policy.
Number ESP Sessions	The current number of established ESP Sessions on this interface for this policy.
Number Ambiguous ESP Sessions	The number of sessions which were established for which there were requests outstanding which were indistinguishable. A session is indistinguishable if there is more than 1 session in the initiated state to the same destination. The returning message from the destination may be intended for either of the initiated sources. IPSec Passthrough ALG will automatically establish the session with the source request which has been waiting the longest, however, this may be an incorrect choice and the counter is incremented so that these occurrences may be monitored. If the selection criteria is incorrect, then all subsequent packets are cross-wired to the respective clients. Once cross-wired, IPSec Passthrough ALG will deliver the wrong stream of packets to the wrong client, resulting in a likely failed connection as the encryption will fail. It is also possible, though considered a rarer case, where two different hosts behind the firewall initiate a session to the same destination host using the same SPI value (because they are different clients, they are not aware of the SPI selected by other clients). This case is the same as the case mentioned above from the point of view of establishing the session and the count is incremented by 1. However, this case is further complicated in that every incoming packet will be directed to a single host since the established sessions are indistinguishable. The likely result is that one of the IPSec connections will time out as it will receive no packets, while the other may stay up but reject all of the packets belonging to its twin or fail due to the reception of indecipherable packets.
Number ESP Dropped Packets	The number of ESP packets received from the public side for which there is no corresponding established ESP sessions. (ESP Packets received from the private side when there is no established ESP Session will initiate a new session, which is the normal case).

set firewall policy esptimeout

In order to provide ESP session resources in a timely manner after the session is no longer active, the ESP Session idle timer is configurable using a new parameter **esptimeout** in the command **set firewall policy** command. The syntax of the command is similar to other firewall session timers; the time is specified in minutes.

The idle timer value represents the time which IPSec Passthrough Application Layer Gateway (ALG) waits after the last packet has been received for the session before terminating the session and freeing its resources. Each packet received for the session resets the timer. At least one packet must be received during the idle timer period in order to maintain the session.

A session stops receiving packets if the two ends have terminated the IPSec connection or if one end abandons the connection for any reason. IPSec Passthrough ALG cannot detect the end of the IPSec Connection and so the timer is relied upon to end the session and release and return resources.

IPSec Passthrough ALG also cannot detect the session timer negotiated by IPSec so the setting of the **ESPTimeout** value must be engineered as a compromise between responsiveness to failed or ended connections and providing the expected IPSec service between the two negotiated ends.

Note: The idle timer may be set low, so that the detection of unused connections is quick and resources are returned quickly to the pool. However, setting it too low may disconnect a session in a period where there are no packets exchanged on an otherwise active connection. Setting the value high may use additional resources to hold sessions which are no longer active.

set firewall policy

Syntax

```
SET FIREwall POLIcy=policy-name [FTPDataport={RFC|ANY}]
   [ICMPUnreachabletimeout=0..65535]
   [MACCachetimeout=1..43200] [MAXupnpportmaps={0..1000}]
   [OTHERTimeout=0..43200] [RADIuslimit=1..500]
   [TCPTimeout=0..43200] [UDPTimeout=0..43200]
   [ESPTimeout=0..43200]
   [UPNP={ON|OFF|YES|NO|ENAbled|DIsabled}]
```

Description

This command sets various timeout periods and limits for a firewall policy. The firewall times out inactive sessions after the set period. This command also optionally enables the specified policy for UPnP. You can also use this command to set a limit to the number of port maps for UPnP.

If you enable the load balancer, the value configured for the load balancer's **orphantimeout** parameter (see the **set loadbalancer** command in the Server Load Balancing chapter in the Software Reference for your switch) overwrites values set for the **tcptimeout**, **udptimeout**, **othertimeout** and **esptimeout** parameters.

You can either specify a minimum of 30 **seconds** (0), or from 1 min to 43200 **minutes** in 1 minute increments etc.

Table 25: New parameter in the **set firewall policy** command

Parameter	Description	
ESPTimeout	The idle timeout period for an ESP Session. The session is terminated if no packets are exchanged on this session for the idle timeout period. Default: **20** minutes	
	0	The ESP session times out after 30 seconds.
	1..43200	Time in minutes after which the session times out after the last message has been detected.

Logging

Logging in firewall takes place on two levels.

- Event logging, which is displayed using the command **show firewall event**. There are three kinds of event displayed for each policy: ALLOW, DENY or NOTIFY
- In addition, certain events will also result in Firewall logs, which will provide more detail. Firewall event logging has three different types of events, Notify, Deny and Allow events.

'Allow events' are for flows or sessions which have been allowed based on the policy settings and which have been created.

'Deny events' are for flows or sessions which have been disallowed based on policy settings or other reasons.

'Notify events' are informational and usually associated with an existing session other than for the establishment or denial of a session or flow, for example if the session is terminated for other than normal reasons or an activity has been detected and noted for security reasons or an action is undertaken as a result of detection (for example a TCP SYN attack).

Any packets which are received with the ESP protocol which are discarded because of any firewall rule will be recorded as a log. (In Firewall terminology, this will be a 'deny event'). Deny event generation itself is throttled to ensure that the event logs are not overflowed.

An ESP packet which is dropped for other reasons than a firewall rule will also be logged as a NOTIFY event. The only case is when an ESP packet is received from the public interface which does not match a session in the initiated state. All ESP sessions which do not match an existing session will be assumed to matching a newly initiated session. This is because it is never known if an incoming ESP packet is part of an existing session until a search is made of all sessions and it matches an existing session. If it does not match an existing session, then it is assumed to be a matching entry for a new session and this check is done later in the processing.

Each session established is logged as an 'allow event'. Session termination if it is normally terminated is not recorded. Session creation and termination however, both generate priority 0 (debug) logs. Since these are below priority 3, they are not normally visible from the 'show log' command. To enable these logs the command 'ADD LOG OUTPUT=TEMPORARY TYPE=036 SUBTYPE=ESPALG' should first be entered.

Note that firewall logging is selectable on a per policy basis and is normally off by default. So, in addition to setting a filter for the new log types of priority=0, a new log option must be enabled (ESPALG) for the policy using the command 'enable firewall policy log=espalg'.

The command details for enabling, viewing the new logs and events for IPSec Passthrough are detailed in the following sections.

enable firewall policy log

The **enable firewall policy** command is modified to include enabling of logs for IPSec Passthrough.

enable firewall policy

Syntax

```
ENAble FIREwall POLIcy=policy-name [ACCounting]
   [FRAgment={ICMP|UDP|OTHER}[,...]]
   [ICMP_Forwarding={ALL|PARAmeter|PING|SOURcequench|
   TIMEExceeded|TIMEStamp|UNREachable}]
   [LOG={ALLOw|DENY|DENYDump|EVERYDeny|INAIcmp|INALlow|
   INAOther|INATcp|INAUdp|INDDIcmp|INDDOther|INDDTcp|
   INDDUdp| INDDump|INDEny|INDIcmp|INDOther|INDTcp|INDUdp|
   OUTAIcmp|OUTAllow|OUTAOther|OUTATcp|OUTAUdp|OUTDDIcmp|
   OUTDDOther|OUTDDTcp|OUTDDUdp|OUTDDump|OUTDEny|OUTDIcmp|
   OUTDOther|OUTDTcp|OUTDUdp|SIPAlg|ESPAlg}]
   [OPtions={ALL|RECord_route|SECUrity|SOURcerouting|
   TIMEStamp}] [PING]
```

A new parameter is added to the LOG options to enable logging from the IPsec Passthrough ALG function.

Table 26: New parameter in the **enable firewall policy** command

Parameter	Meaning
ESPAlg	Logs produced by the IPSec Passthrough ALG function.

Allow event/Session establishment

When a session is established, the following event will be generated:

```
Policy : internet - Allow Events:
Date/Time   Dir Prot Number IP:Port <map> Dest IP:Port /Reason /IP header
-------------------------------------------------------------------------------
14 17:08:54 OUT UDP       1 192.168.3.5:500 5451 202.78.78.77:500
                UDP flow started
14 17:08:55 OUT ESP       1 192.168.3.5:2564985687 202.78.78.77:44200366
                ESP session started
-------------------------------------------------------------------------------
```

All allow events for IPSec Passthrough are in direction OUT. In the case of direction OUT the following fields are displayed:

Table 27: New parameter meanings event/session establishment

Parameter	Meaning
IP	Originating port on the private side
Port	This is the Initiator SPI for the ESP session
Dest IP	ESP host on the public side
Dest Port	This is the Responder SPI for this ESP session.
Reason/IP Header	Not used for ESP.

A log with severity DEBUG(0) is also generated to indicate ESP Session start.

```
SecOff ipsecpthru_gw> sh log sev=0 full

Date/Time    Mod  Type  SType Dev   Origin           MSGID Source File/Line
-------------------------------------------------------------------------------
17:08:55  0  FIRE FIRE  ESPAL 00000 Local            00075 fwutil.c:2172
14-DEC-2009  FW               LOCTIME
             ESP 192.168.3.5:2564985687 202.78.78.77:44200366 session started
-------------------------------------------------------------------------------
```

The log displays the same information as the 'allow' event.

Normal Session Termination/Notify Event

When the session is terminated there is no event generated. The following are some reasons why sessions are terminated:

4. Normal session timeout because session has been idle too long.
5. Session is removed because the firewall policy is removed by command.
6. Session is deleted explicitly by command using the 'delete firewall session' command.
7. Firewall is disabled.

A log with severity DEBUG(0) is generated for ESP Sessions ended.

```
SecOff ipsecpthru_gw> sh log sev=0 full

Date/Time    Mod  Type  SType Dev   Origin           MSGID Source File/Line
-------------------------------------------------------------------------------
17:08:55  0  FIRE FIRE  ESPAL 00000 Local            00075 fwutil.c:2172
14-DEC-2009  FW               LOCTIME
             ESP 192.168.3.5:2564985687 202.78.78.77:44200366 session started
17:55:44  0  FIRE FIRE  ESPAL 00000 Local            00086 fwutil.c:2172
14-DEC-2009  FW               LOCTIME
             ESP 192.168.3.5:2564985687 202.78.78.77:44200366 session ended
-------------------------------------------------------------------------------
```

Abnormal Session/Notify Event

If a packet is received on the public interface for which there is no corresponding match of an 'established' session or a packet cannot be matched to an 'initiated' session then a notify event is also generated.

Since sessions are not expected to be started from the public to the private side or we do not expect responses from servers which were not recorded as the destination address, this can be considered an IN DENY event. Since this is unexpected, it is treated as a Notify Event, as it could be a type of DOS attack.

```
Policy : internet - Notify Events:
Date/Time   Dir Prot Number IP:Port <map> Dest IP:Port /Reason /IP header
-------------------------------------------------------------------------------
14 14:59:47 IN  ESP       1 202.78.78.78:0 0.0.0.0:0
                No ESP session
                45000058 334a0000 403215f2 ca4e4e4d ca4e4e4e 0ca8fb58 0000008b
                4b0147d9 97f94939 b763d4ca 6461cb83 33ec7743 57a71c47 61482193 1
21e4d42
                d1616038
```

A log with severity NOTICE(4) is also generated with any additional details. This log is enabled with LOG option=ESPAlg (enable firewall policy log=ESPAlg).

Table 28: New reason in the **enable firewall policy log=ESPAlg** command

Log Reason	Meaning
unsolicited packet received - no session	The ESP packet's source ip address did not match any established session's destination address or there are no established sessions or it does not match any initiated session's destination address or there are no sessions in 'initiated' state.

Consistent with firewall logging, only the first 4 events are logged and if required, a fifth log is generated with the number of repeated messages following the first four.

Viewing logs of priority 0

For the ESP logs of severity 0 (debug), additional commands are required to generate and view these logs since they are below priority 3. This command must be entered in addition to having ESPALG logs enabled from the policy for which the logs are required to be viewed or monitored.

Table 29: Additional configuration in the ESP logs of severity 0

Option	Additional Configuration
ESPALG	ADD LOG OUTPUT=TEMPORARY TYPE=036 SUBTYPE=ESPALG.

Deny Event/Session Denial

When an ESP session is denied by the firewall for a policy reason, the following event is generated:

```
Policy : test - Deny Events:
Date/Time   Dir Prot Number IP:Port <map> Dest IP:Port /Reason /IP header
-------------------------------------------------------------------------------
31 18:17:01 OUT  ESP      1 192.168.1.1:05f13e05 210.0.0.2:0
            Policy rejected
            45000028 a2164000 800633bb 0a1449aa c3be0d82 10750050 e6a283db
19010223 50114470 affd0000
```

For example, this may occur if there is no allow or enhanced NAT rule for protocol=ESP and an ESP message is detected in the outgoing direction.

Diagnostics

Debugging commands for IPSec Passthrough

A new option for tracing IPSec Passthrough activity through the firewall is available by extending the available options for debug. A new option 'ESPALG' is added and can be added on a per policy basis.

enable firewall policy debug

Syntax

```
ENAble FIREwall POLIcy[=policy-name]
   DEBug={ALL|ARP|CHecksum|ESPAlg|HTTP|IDentproxy|
   LIMitrule|PACKet|PKT|PRocess|PROXy|RADius|SIPAlg|SMTP|
   TCP|UPNP}[DEBUGMode={ALL|ERRORcode|MESSage|PARSing|
   TRAce}] IP=ipadd[-ipadd]]
```

Table 30: New parameter option in the **enable/disable firewall policy debug** commands

Parameter	Meaning	
DEBug	Specifies one or more types of debugging to be enabled. You can specify a single type or a comma-separated list of types. This parameter is not retained over a reboot.	
	Default: no default	
	...	
	ESPALg	**Displays information about the processing of ESP packets through the firewall implementing the IPSec Passthrough functionality**.
	...	

disable firewall policy debug

Syntax DISable FIREwall
POLIcy[=*policyname*]DEBug={ALL|ARP|CHecksum|**ESPAlg**|HTTP|IDentproxy|LIMitrule|PACKet|PKT|PRocess|PROXy|RADius|SIPAlg|SMTP|TCP|UPNP}[DEBUGMode={ALL|ERRORcode|MESSage|PARSing|TRAce}]

Example outputs from IPSec Passthrough debug

Figure 22: Example debug output with espalg debug enabled—session establishment

```
SecOff ipsecpthru_gw> ena fire poli=internet deb=espalg

Info (1077003): Operation successful.

SecOff ipsecpthru_gw> FIREWALL ESP search for established session - fail dir=IN
FIREWALL ESP search for initialised session - fail dir=IN
FIREWALL ESP Policy=internet id=46ba iSPI=861056255 state=initialised dir=OUT
FIREWALL ESP search for established session - fail dir=IN
FIREWALL ESP Search for initialised session - matched Policy=internet id=46ba di
r=IN
FIREWALL ESP Policy=internet id=46ba rSPI=266595965 state=established dir=IN

SecOff ipsecpthru_gw> sh fire sess

Policy : internet
Current Sessions
------------------------------------------------------------------------------
2b76 UDP      IP: 192.168.3.5:500           Remote IP: 202.178.178.177:500
          Gbl IP: 202.178.178.178:11126 Gbl Remote IP: 202.178.178.177:500
     Start time ........................... 15:33:15 03-Feb-2010
     Seconds to deletion .................. 1176
46ba ESP   IP: 192.168.3.5:861056255     Rem IP: 202.178.178.177:861056255
       Gbl IP: 202.178.178.178:266595965 Gbl Rem IP: 202.178.178.177:266595965
     ESP state ............................ established
     Start time ........................... 15:33:16 03-Feb-2010
     Seconds to deletion .................. 1200
------------------------------------------------------------------------------

SecOff ipsecpthru_gw>
```

Figure 23: Example debug output with espalg and packet debug enabled

```
SecOff ipsecpthru_gw> ena fire poli=internet deb=espalg

Info (1077003): Operation successful.

SecOff ipsecpthru_gw> ena fire poli=internet deb=packet

Info (1077003): Operation successful.

SecOff ipsecpthru_gw> sh fire poli=internet

Policy : internet
  TCP Timeout (s) ..................... 3600
  UDP Timeout (s) ..................... 1200
  ESP Timeout (s) ..................... 1200
  Other Timeout (s) ................... 1200
  ICMP Unreachable Timeout (s) ...... 0
  TCP Handshake Timeout Mode ........ Normal
  MAC Cache Timeout (m) ............... 1440
  RADIUS Limit ........................ 100
  Accounting .......................... disabled
  Enabled Logging Options ............ espalg
  Enabled Debug Options ..............  packet espalg
  Enabled Debug Modes ................ none
  Enabled Debug IP Address ........... none
  Identification Protocol Proxy ..... enabled

SecOff ipsecpthru_gw>
FIRE ESP   45000050 b18c0000 403287de c0a80305 cab2b2b1 3352acff 0000002a
           847c21a5 4b18dfbc 2130f993 8be6c4ed 9447573e ed672e58 2a4eba3c
           46749333 ac875002 4a7db293 ada584e4 fe3f329b 382eace3
FIREWALL ESP OUT via session id=46ba

FIRE ESP   45000050 b18c0000 4032ce26 cab2b2b2 cab2b2b1 3352acff 0000002a
           847c21a5 4b18dfbc 2130f993 8be6c4ed 9447573e ed672e58 2a4eba3c
           46749333 ac875002 4a7db293 ada584e4 fe3f329b 382eace3
FIREWALL ESP session match id=46ba SPI=0fe3ee7d dir=IN

FIRE ESP   45000050 a6450000 4032d96d cab2b2b1 cab2b2b2 0fe3ee7d 00000017
           34e61ac6 60b845ca 22e15a90 a92a9c86 1a3c0299 d60f2fda 64f6d060
           99874338 d37408dd 58dd6ea0 d17863cc b2a0eefd 9a0729c1
FIREWALL ESP IN via Session id=46ba

FIRE ESP   45000050 a6450000 40329325 cab2b2b1 c0a80305 0fe3ee7d 00000017
           34e61ac6 60b845ca 22e15a90 a92a9c86 1a3c0299 d60f2fda 64f6d060
           99874338 d37408dd 58dd6ea0 d17863cc b2a0eefd 9a0729c1

SecOff ipsecpthru_gw>
```

Security enhancement for untrusted private firewall interfaces (CR00029643)

Models This enhancement is supported on:

- AT-9800
- AT-8800
- Rapier i, Rapier w
- AR44x, AR450S, AR415S
- AR725, AR745
- AR750S, AR770S

Module Firewall

Description This enhancement provides a more secure firewall for untrusted private interfaces, such as may be used in semi-public settings like Internet cafes. The effect of the **trustprivate** parameter in the **add firewall policy interface** command has changed. A static or dynamic private untrusted interface is added to a firewall policy by using the command:

```
ADD FIREwall POLIcy=policy-name INTerface=interface
   TYpe=PRIVate TRUstprivate=NO
```

With this enhancement, traffic that is received on a private untrusted interface and that is destined for an IP address owned by the router or switch itself (that is, either an IP address of the local loopback interface or an IP address of any local interface) is denied by default. Previously, such traffic was allowed by default, which may have allowed some unintended access to the router or switch. For example, Telnet or Secure Shell management access to the router or switch via a private interface set to **trustprivate**=**no** was previously allowed by default, but is now denied by default (that is, unless a specific firewall policy rule allows it).

Previously, static private interfaces added to a firewall policy were trusted (**trustprivate**=**yes**) by default and dynamic private interfaces were untrusted (**trustprivate**=**no**) by default. With this enhancement, both static and dynamic private interfaces are trusted (**trustprivate**=**yes**) by default. This default setting allows access to the router or switch itself from the private interfaces, and suits most situations.

The behaviour for untrusted private interfaces can be modified by explicitly allowing certain traffic to the router or switch according to firewall policy rules configured by the **add firewall policy rule** command.

- If you require any access to the router or switch via an untrusted (**trustprivate**=**no**) private interface, for example, if an IT manager connected to the interface requires Telnet or Secure Shell access to the router or switch, you must now add new firewall policy rules to allow access for the trusted host or permitted protocol.
- If your configuration includes firewall policy rules to explicitly deny traffic from untrusted (**trustprivate**=**no**) private interfaces to the router or switch itself, these rules are now redundant—they have no effect on the traffic.

As before, traffic that is received on a private untrusted interface, and that is destined to be forwarded out a public interface is inspected by the firewall and allowed by default); if it is destined to be forwarded out another private interface, then it is not inspected by the firewall (not a firewall session—always allowed).

In the Firewall policy in the following example configuration extract:

- *vlan1* is added to the firewall policy as a static private untrusted interface.
- A dynamic untrusted private interface is added to the policy for "roadwarriors".
- The trusted system administrator at IP address 192.168.1.2 is allowed to telnet to the router via the static untrusted interface *vlan1*.

Figure 24: Example firewall configuration extract

```
# Enable the firewall.
enable firewall
# Create a firewall policy to control access to the network.
create firewall policy="school"
# Create a dynamic interface template for this firewall policy.
create firewall policy="school" dynamic=roadwarriors
# Allow any authenticated username to use the dynamic interface template for the
# policy.
add firewall policy="school" dynamic=roadwarriors user=any
# Add vlan1 to this policy as a static private untrusted interface.
add firewall policy="school" interface=vlan1 type=private trustprivate=no
# Add a dynamic private untrusted interface to allow incoming PPP/L2TP
# connections (roadwarriors).
add firewall policy="school" int=dyn-roadwarriors type=private trustprivate=no
# Add eth1 to the policy as a public interface.
add firewall policy="school" interface=eth1 type=public
# Add a Network Address Translation (NAT) from the private interface (vlan1) to
# the public interface (eth1).
add firewall policy="school" nattype=enhanced interface=vlan1 gblinterface=eth1
# Rule 1 allows in the dynamic L2TP connection:
add fire poli="school" rule=1 action=allow int=eth1 prot=udp port=1701
ip=172.33.0.1 gblip=172.33.0.1 gblport=1701
# Rule 2 allows the trusted host at 192.168.1.2 to have telnet access, even
# though this is an untrusted interface:
add fire poli="school" rule=2 act=allow int=vlan1 prot=tcp port=23
ip=192.168.1.2
```

Firewall router IP alert option (CR00027414)

Models This enhancement is supported on:

- AT-9800
- AT-8800
- Rapier i, Rapier w
- AR44x, AR450S, AR415S
- AR725, AR745
- AR750S, AR770S

Module Firewall

Description By default the firewall module drops packets with an IP option. However, a policy may be configured to allow the passage of IP packets with specific options. This enhancement adds the **router IP alert** option to the short list of options that may be allowed for a firewall policy.

This results in a new option being added to both the enable and disable firewall policy commands.

Note that the value "ALL" means all of the individual option types accepted by the command and not all possible IP options. The options types accepted are by no means a complete list of IP options.

enable firewall policy

Syntax

```
ENAble FIREwall POLIcy=policy-name [ACCounting]
   [FRAgment={ICMP|UDP|OTHER}[,...]]
   [ICMP_Forwarding={ALL|PARAmeter|PING|SOURcequench|
   TIMEExceeded|TIMEStamp|UNREachable}]
   [LOG={ALLOw|DENY|DENYDump|EVERYDeny|INAIcmp|INALlow|
   INAOther|INATcp|INAUdp|INDDIcmp|INDDOther|INDDTcp|
   INDDUdp|INDDump|INDEny|INDIcmp|INDOther|INDTcp|INDUdp|
   OUTAIcmp|OUTAllow|OUTAOther|OUTATcp|OUTAUdp|OUTDDIcmp|
   OUTDDOther|OUTDDTcp|OUTDDUdp|OUTDDump|OUTDEny|OUTDIcmp|
   OUTDOther|OUTDTcp|OUTDUdp|SIPAlg}]
   [OPtions={ALL|ROUter_alert|RECord_route|SECUrity|
   SOURcerouting|TIMEStamp}] [PING]
```

disable firewall policy

Syntax

```
DISable FIREwall POLIcy=name [ACCcouting]
   [FRAgment={ICMP|UDP|OTHER}[,...]]
   [ICMP_Forwarding={ALL|PARAmeter|PING|SOURcequench|
   TIMEExceeded|TIMEStamp|UNREachable}]
   [LOG={ALLOw|DENY|DENYDump|EVERYDeny|INAIcmp|INALlow|
   INAOther|INATcp|INAUdp|INDDIcmp|INDDOther|INDDTcp|
   INDDUdp|INDDump|INDEny|INDIcmp|INDOther|INDTcp|INDUdp|
   OUTAIcmp|OUTAllow|OUTAOther|OUTATcp|OUTAUdp|OUTDDIcmp|
   OUTDDOther|OUTDDTcp|OUTDDUdp|OUTDDump|OUTDEny|OUTDIcmp|
   OUTDOther|OUTDTcp|OUTDUdp|SIPAlg}]
   [OPtions={ALL|ROUter_alert|RECord_route|SECUrity|
   SOURcerouting|TIMEStamp}] [PING]
```

The **options** parameter disables the forwarding of packets with the specified IP option or options to the next level of firewall checking. The value may be a single option or a comma-separated list of options. The default is not to forward packets with IP options.

Related command `show fire policy`

Firewall Public Interface Dynamic Assigned IP Address (CR00023375)

Models This enhancement is supported on:

- AT-9800
- AT-8800
- Rapier i, Rapier w
- AR44x, AR450S, AR415S
- AR725, AR745
- AR750S, AR770S

Module Firewall

Description When a firewall public interface is being dynamically assigned an IP address, and therefore does not have pre-assigned ip address, and Enhanced NAT is defined on this interface, rules which specify global ip ({gblip}) normally set {gblip=0.0.0.0}. When the router learns the ip address of the interface then the {gblip} is set to this value and private traffic's source address is substituted with this value when it is sent out through the public interface.

If in a rule, the {ip} address parameter is also specified, then incoming packets which match the rule are directed to the private interface which bears that IP address. If the desire is that traffic being allowed inwards is to terminate on the address of the public interface (but because the interface is being dynamically assigned its IP address, this address is not known at configuration time), then it is now possible to specify {ip=0.0.0.0} in the rule. When both {gblip=0.0.0.0} and {ip=0.0.0.0} then packets received matching this rule will be terminated on the public interface i.e.: {ip}={gblip}=address of the public interface.

Compatibility with SAMSUNG SmartViewer 2.0 (CR00020882)

Models This enhancement is supported on:

- AT-9800
- AT-8800
- Rapier i, Rapier w
- AR44x, AR450S, AR415S
- AR725, AR745
- AR750S, AR770S

Module Firewall

Description A new compatibility mode allows the firewall to interoperate with the SAMSUNG SmartViewer 2.0 for ProDVR application. This application uses RSTP over TCP to communicate with SAMSUNG IP security cameras.

To use this application on a switch with a firewall configured, you must add a new application rule for RTSP to your firewall policy:

```
add firewall policy=[policy-name] apprule=app-rule-id
   action=allow interface=[interface] application=rtsp
   compatibility=smartviewer
```

CR00017395: Accurate Maximum Segment Size (MSS) values for TCP sessions

Models This enhancement is supported on:

- AT-9800
- AT-8800
- Rapier i, Rapier w
- AR44x, AR450S, AR415S
- AR725, AR745
- AR750S, AR770S

Module Firewall

Description This enhancement enables the firewall to establish accurate MSS (Maximum Segment Size) values for TCP sessions without using the MTU discovery process. MTU discovery depends on ICMP error packets, so does not work in networks that do not forward ICMP error packets.

To enable this feature, use the command:

```
enable firewall policy=name adjusttcpmss
```

The **adjusttcpmss** parameter enables the firewall to adjust the MSS value stored inside incoming TCP SYN packets, to reflect the lower of the two MTU values on the ingress and egress interfaces. Normally, for example, if a TCP SYN packet arrives from an interface with an MTU of 1500 and leaves on an interface with an MTU of 1000, the MSS inside the SYN packet will remain at 1460. When this feature is enabled, the MSS will be adjusted to 960 because the firewall knows that the egress interface has a smaller MTU. Note that the firewall does not change the original MSS value if it is already lower than the values of the ingress and egress interfaces.

To disable this feature, use the command:

```
disable firewall policy=name adjusttcpmss
```

This feature is disabled by default.

New in IPsec

This section describes new features and enhancements to IPsec, ISAKMP, IKE, and related features as described in the *IP Security (IPsec)* chapter in the *Software Reference for Version 2.9.1* for your router or switch.

Related features include:

New show ipsec isakmp command (CR00035046)

Models This enhancement is supported on:

- AT-8800
- Rapier i, Rapier w
- AR44x, AR450S, AR415S
- AR725, AR745
- AR750S, AR770S

Module IPsec, ISAKMP

Description Previously, IPSec and ISAKMP information was displayed separately and multiple commands were required to find out all the information about a single connection. Some of this information has now been combined into a single command to make debugging IPSec connections easier.

show ipsec isakmp

Syntax: Show IPSec ISAkmp

Description This command displays information about the current IPSec SAs (Security Associations) and their associated ISAKMP SAs.

Figure 25: Example output from the **show ipsec isakmp** command

```
IPSEC                    ISAKMP                      Expiry Limits - hard/soft/used
SA Id  NAT-OA            SA Id  Peer Address     DPD    ISAKMP SA Lifetime (secs)
-------------------------------------------------------------------------------
    0  -                     1  203.179.85.33    Act    86400/82076/356
    1  -                     2  222.228.212.43   Act    86400/75590/356
    5  N/A (Tnl Mode)        7  200.200.200.254  IdlQR  600/569/304
    6  N/A (Tnl Mode)        7  200.200.200.254  IdlQR  600/569/304
   12  N/A (Tnl Mode)       13  200.200.200.254  IdlQR  600/567/291
   13  192.168.34.252       14  200.200.200.254  None   28800/27345/256
   15  10.0.0.2             16  10.255.255.3     Act    3600/3413/49
-------------------------------------------------------------------------------
```

Table 31: Parameters in the output from the **show ipsec isakmp** command

Parameter	Meaning
IPSec SA Id	The identification number for the IPSec SA.
NAT-OA	Information about the original IP address (unless in Tunnel mode)
ISAKMP SA Id	The identification number of the associated ISAKMP SA.
Peer Address	The IP address of the peer for the ISAKMP SA.

Table 31: Parameters in the output from the **show ipsec isakmp** command

Parameter	Meaning
DPD	The current state of Dead Peer Detection; one of the following: Act: Active—Only displayed when DPD Mode is BOTH. The connection is actively being monitored for idleness and the DPD Idle Timer is running. If a valid IPSec packet is not received on the connection in 'Idle Expiry Limit (seconds)', then the connection will be considered idle and will initiate a query for liveliness. ActRx: ActiveReceive—If DPDMode=Receive, then DPD will always display this state indicating its readiness to respond to peer queries for liveliness. IdlQy: IdleQuery—DPDMode=BOTH and 'Idle Expiry (seconds)' has reduced to 0 and a query for liveliness (sending R-U-THERE Notify) has been initiated. IdlQR: IdleQueryRetry—DPDMode=BOTH and the first attempt to reach the peer has expired and subsequent attempts are being tried. 'Retry Count' indicates how many times it has already retried. Dead: The maximum number of retries without receiving a response has been attempted and the connection is declared dead and will be deleted. This state is a brief transitional state and will rarely be seen since the SA being queried is the one which is declared dead and will be deleted. None: This is the state displayed when DPDMode is BOTH, but the peer's DPDMode is NONE. [Blank:] DPDMode is NONE, that is, not enabled.
Expiry Limits ISAKMP SA Lifetime	The expiry time of the ISAKMP SA in seconds: hard: The time before this SA is deleted. soft: The time before this SA is renegotiated. used: The number of seconds since this SA was created.

Example To display all current IPSec SAs and their associated ISAKMP SA information, use the command:

```
sh ips isa
```

Related commands: show ipsec sa
show isakmp sa

ISAKMP responder rekey (CR00032324)

Models This enhancement is supported on:

- AT-8800
- Rapier i, Rapier w
- AR44x, AR450S, AR415S
- AR725, AR745
- AR750S, AR770S

Module ISAKMP

Description Previously, when an ISAKMP policy was configured with **peer=any**, as it would be when configuring the router or switch as a security access server for servicing multiple incoming secure client connections, it relied on the client to renegotiate secure keys if they expired during an active connection. A new option in the ISAKMP policy configuration gives the option of renewing secure keys from the server side.

The following commands are modified to include the new option:

- **create/set isakmp policy** command on page 142
- **show isakmp policy** command on page 143

create/set isakmp policy

These commands have a single new parameter **rekey** to specify whether the ISAKMP Responder Rekey option is set or not. The new **rekey** parameter is only valid if **peer** is set to **any**.

```
CREate ISAkmp POLicy=name PEer=ANy
   [ENCalg={3DES2key|3DESInner|3DESOuter|DES|AES128|
   AES192|AES256}] [KEY=0..65535]
   [REKey={ON|OFf|TRue|FAlse}] [other-isakmp-params]

SET ISAkmp POLicy=name PEer=ANy
   [ENCalg={3DES2key|3DESInner|3DESOuter|DES|AES128|
   AES192|AES256}] [KEY=0..65535]
   [REKey={ON|OFf|TRue|FAlse}] [other-isakmp-params]
```

Table 32: New parameter in the **create** and **set isakmp policy** commands

Parameter	Description	
REKey	Whether ISAKMP Responder Rekeying is enabled or disabled for the ISAKMP policy. This option is only valid if **peer=any**. By default if **peer=any**, ISAKMP is performing a responder function and under these conditions if the ISAKMP Security Authorisation expires before the User renews the key, ISAKMP will not renegotiate the key. When this option is set, ISAKMP will renegotiate a new key if the local expiration timer is set lower than the user expiration. This is useful if the client device ignores expiration timer negotiation (and therefore does not set its timer to expire before the responder) or does not support some form of Dead Peer detection (heartbeat or Dead Peer Discovery). Default: off	
	Off, FAlse	ISAKMP Responder Rekey is disabled for the ISAKMP policy.
	On, TRue	ISAKMP Responder Rekey is enabled for the ISAKMP policy.

Examples In this example, the ISAKMP policy has been configured as a responder with **peer=any** and therefore the **rekey** option can be specified. Here the ISAKMP responder rekey option enabled:

```
create isakmp poli="keys" peer=any group=2 enc=3desouter key=1
   rek=true
```

In this example, the ISAKMP policy has been configured as a responder with **peer=any** and therefore the **rekey** option can be specified. However, the

responder rekeying option is not desirable so it is not specified and therefore the ISAKMP responder rekey option is disabled by default:

```
create isakmp poli="keys" peer=any group=2 enc=3desouter key=1
```

In this example, the ISAKMP policy is being changed to be configured as a responder with peer=any and therefore the REKEY option can be specified. Here the ISAKMP responder rekey option enabled.

```
set isakmp poli="keys" peer=any rek=true
```

In this example, the ISAKMP policy is being changed to be configured as a responder with **peer**=**any** and therefore the **rekey** option can be specified. However the ISAKMP responder rekey option is not required so it is ommitted. ISAKMP Responder Rekey option is automatically set to be disabled:

```
set isakmp poli="keys" peer=any
```

In this example, the ISAKMP policy was set to **peer**=**any** and **rekey**=**true** and is now being set to **peer**=202.36.163.161. The **rekey** option is not required (and not valid) and the **rekey** option will automatically be disabled:

```
set isakmp poli="keys" peer=202.36.163.161
```

show isakmp policy

The syntax of this command is not changed; however the output is modified to include the current configuration of the ISAKMP Responder Rekey option. The ISAKMP Responder Rekey option is only valid if **peer**=**any** and the current setting is displayed if **peer**=**any** and not shown otherwise.

Note that ISAKMP Responder Rekey is a policy option and not part of the SA specification, so it is shown in the ISAKMP Policy portion of the show command.

Figure 26: Example output from the **show isakmp policy** command

```
ISAKMP Policy
  Name ................................ my_isakmp_policy
  Peer Address ........................ ANY
  Phase1 Mode ......................... IDPROT
  Authentication Type ................. PRESHARED
  Extended Authentication ............. NONE
  Extended Authentication Type ........ -
  Extended Authentication User Name ..... -
  Extended Authentication Password ..... -
  Key Id .............................. 30
  Local RSA key ....................... -
  Peer Certificate Id ................. -
  Phase 2 Exchanges Limit ............. NONE
  PreNegotiate ........................ TRUE
  DOI ................................. IPSEC
  Send Notify Messages ................ TRUE
  Send Delete Messages ................ FALSE
  Always Send ID Messages ............. FALSE
  Commit Bit .......................... FALSE
```

Figure 26: Example output from the **show isakmp policy** command (cont.)

```
   Message Retry Limit ................... 5
   Message Time Out ...................... 20
   Message Back-off ...................... Incremental
   Exchange Delete Delay ................. 30
   Source Interface ...................... -
   VPN Client Policy File Name ........... -
   Local ID .............................. -
   Remote ID ............................. IPv4:192.68.1.2
   DebugFlag ............................. 00000000
   Retry IKE Attempts .................... 0
   Current IKE Retries ................... 0
   Required IKE Retry Phase .............. No Phases
   Rekey on SA Soft Expiry ............... TRUE

SA Specification
.
.
.
```

CRL-DPs included in PKI X509 certificates are now decoded (CR00032323)

Models This enhancement is supported on:

- AT-8800
- Rapier i, Rapier w
- AR44x, AR450S, AR415S
- AR725, AR745
- AR750S, AR770S

Introduction

The Certificate Revocation List - Distribution Point (CRL-DP) extension field of PKI X.509 certificates is now automatically configured. This enhancement primarily enhances usability with Android smart phones.

New Commands

set pki crlsource

Syntax SET PKI CRLSource={COMmand | CRLDp}

Description This command allows the user to globally change the order of which set of CRLs are searched first when validating a certificate. The two sets of CRLs are defined as those added manually using the "ADD PKI CRL=…" command, and those added automatically using a certificate's CRL-DP field.

The **CRLSource** parameter specifies which set of CRLs are searched first. "CRLSource=COMmand" causes those CRLs added manually to be searched first (this is the default setting), while "CRLSource=CRLDp" causes those CRLs added automatically

Examples The following command sets the CRLs loaded automatically to be searched first.

```
set pki crls=crldp
```

See Also

```
add pki crl
add pki cert
show pki
show pki crl
```

Modified Commands

show pki

Syntax

```
SHow PKI [COUnters]
```

Description This command displays information about the PKI module.

Figure 27: Example output from the SHOW PKI command

```
PKI Module general information:
  subjectAltName ..........
  CRL update period ....... 24 hours
  CRL source precedence ... CRLDP <<< new line
  CMP retry period ........ 5 seconds
  CMP maximum retries ..... 1
  Max. # of certificates .. 24
  Debug device ............ 16
  Debug types enabled: none
```

Table 33: new parameters displayed in the output of the **show pki** command

Parameter	Meaning	
CRL source precedence	COMMAND	CRLs entered manually
	CRL-DP	CRLs obtained automatically are searched first

Examples To display general information about the PKI module, use the command:

```
sh pki
```

See also

```
set pki crlsource
```

show pki crl

Syntax

SHow PKI CRL=[name]

where *name* is a string 1 to 24 characters long.

Description This command displays information about a particular CRL or all CRLs in the router's CRL database.

Figure 28: Example output from the **show pki crl=name** command

```
PKI CRL: ca1
  State ..................... UPTODATE
  Minutes to next update ... 1434
  Number of updates ........ 1

  Type ...................... CRL-DP
    in certificate ......... router1 << new line
  Version ................... V1
  Issuer .................... cn=Test CA 1, ou=Web test, o=SSH Communications
                              Security, c=FI
  Signature algorithm ...... SHA1 with RSA
  Number of entries ........ 21
  This update ............... 04:54:01 - 14-Mar-2001 (GMT)
  Next update ............... 06:00:00 - 14-Mar-2001 (GMT)

  Source Location:
    file ............... ca1.crl
  Certificate List:
    Certificate Serial Number Revocation Date Revocation Reason
    ------------------------------------------------------------
    380f 893a [940542266] 13:01:51 - 19-Oct-1999 unused
    3817 4a1f [941050399] 18:53:19 - 27-Oct-1999 unused
    3818 9c41 [941136961] 18:56:01 - 28-Oct-1999 unused
    3869 5da3 [946429347] 01:02:28 - 29-Dec-1999 unused
    389f 59b0 [949967280] 23:48:00 - 07-Feb-2000 unused
    38a0 5ca4 [950033572] 18:12:53 - 08-Feb-2000 unused
    38b8 cdc8 [951635400] 07:10:01 - 27-Feb-2000 unused
    38ba 124d [951718477] 06:14:37 - 28-Feb-2000 unused
    38ff 3486 [956249222] 16:47:02 - 20-Apr-2000 unused
    3922 d125 [958583077] 17:04:37 - 17-May-2000 unused
    3934 2329 [959718185] 20:23:06 - 30-May-2000 unused
    3950 2941 [961554753] 02:32:33 - 21-Jun-2000 unused
    3950 656f [961570159] 06:49:19 - 21-Jun-2000 unused
    ------------------------------------------------------------
```

Table 34: New parameters displayed in the output of the show pki crl=name command

Parameter	Meaning
In certificate	If the CRL type is CRL-DP, indicating it was added automatically, then this line shows the name of the certificate containing the CRL-DP field that downloaded the CRL

Examples To display general information about the PKI module, use the command:

```
sh pki
```

See Also add pki crl
add pki cert
show pki
show pki crl

show pki certificate

Syntax `SHow PKI CERtificate[=`*name*`]`

where *name* is a string 1 to 24 characters long.

Description This command displays information about a particular certificate or all certificates in the router's certificate database.

Figure 29: Example output from the show pki certificate=name command

```
Certificate:
  name ................ router1
  state ............... TRUSTED
  manually trusted .... FALSE
  type ................ EE
  source .............. COMMAND

  version ............. V3
  serial number ....... 3bf1 c141 [1005699393]
  signature alg ....... SHA1 with RSA
  public key alg ...... RSA
  not valid before .... 03:55:03 - 14-Nov-2001 (GMT)
  not valid after ..... 04:25:03 - 14-Nov-2002 (GMT)
  subject ............. cn=router1, dc=foo, dc=bar, dc=com

  issuer .............. dc=foo, dc=bar, dc=com

  MD5 fingerprint ..... e81e bb17 deb3 664d 91e3 5c58 c890 aae1
  SHA1 fingerprint .... d662 ba63 ecb9 be83 0962 9ca1 5888 1bee d96b 67d6
  key fingerprint ..... 49d4 4919 106f ea71 21c7 7bef ab69 48c1 0ca8 99d2

  key usage ........... Digital Signature
  subject key ID ...... e70d3c808b6d747f2a415ccf7efc8e16a94c9f8d
  authority key ID .... dcc16049a4e158dcda046cecb90b91c9a94c6800

  CRL Distribution Points                                              )
    Distribution Point  1 (CRL: cdp0)                                  )
      {1} Type ........ HTTP                                           )
          Address ..... 192.168.100.200                          new section
          HTTP file ... cacrl1.crl                                     )
      CRL Issuer ...... dc=foo, dc=bar, dc=com                         )
      Reasons (05) .... Key Compromise                                 )
                        CA Compromise                                  )

  validation path ..... <- foobar[ manually trusted, self-signed ]

  Source Location:
    type .............. LDAP
    IP address ........ 192.168.100.200
    distinguished name cn=router1, dc=foo, dc=bar, dc=com
```

Table 35: New parameters displayed in the output of the SHOW PKI

Parameter	Meaning
CRL Distribution Points	Header for the CRL-DP extension information section.
Distribution Point	A certificate can contain a CRL-DP for more than one CRL. This shows the index of this DP and the CRL name given by the router's dynamic retrieval system for this CRL

Table 35: New parameters displayed in the output of the SHOW PKI

Parameter	Meaning
{1} Type	Each CRL-DP can define more than one location to retrieve the CRL from. This shows the index {n} and type (either HTTP or LDAP) of this location.
Address	Shows the IP address of the location's host. This could alternatively be a URL for the host.
HTTP file	The name of the CRL file to download from the server.
CRL Issuer	The distinguished name of the issuer of the CRL.
Reasons (xx)	The set of reasons the certificate(s) in the CRL have been revoked. The xx is the encoded value of the field.

Examples To display information about a particular certificate, use the command:

```
sh pki cert=name
```

See Also

```
add pki crl
add pki cert
show pki
show pki crl
```

GUI pages

There are no GUI requirements for this enhancement.

Log Message Descriptions

One log message has been added to the PKI module.

Name:

Module: PKI

Type: LOG_TYPE_PKI,50,PKI

Subtype: LOG_STY_PKI_CRL,,2,"CRL"

Severity: LOG_SEV_IMPORTANT

Description This message indicates that the CRL Issuer specified in a certificate's CRL-DP field does not match that in the corresponding CRL, which has therefore been invalidated.

```
Reference field:
String Format
CRL-DP Issuer in SSL certificate %s does not match Issuer in CRL
%s.
Parameters
<%s>Name of the certificate containing the CRL-DP field
<%s>Name of the CRL being downloaded.
Routine(s) logged from: pkiCrlInfoRetrieved

Recommended action: Check authenticity of the certificate and CRL
and their sources.
```

Filters to define acceptable X.509 certificates (CR00032322)

Models This enhancement is supported on:

- AT-8800
- Rapier i, Rapier w
- AR44x, AR450S, AR415S
- AR725, AR745
- AR750S, AR770S

Module PKI

Description Certificate acceptance has been modified to allow the administrator to filter certificates according to subject values.

```
ADD PKI CERTFilter=[1-20] {ENTry=[1-100]} {parameters}
```

and the parameters are:

```
ACtion=[ALLOw|DENY] LOG=[ON|OFF|YES|NO|TRUE|FALSE]
```

with the following Subject parameters being a maximum of 16 characters, but also allowing a '*' wildcard:

- CN Common Name
- C Country
- L Location
- O Organisation
- OU Organisational Unit
- ST State

Except for CERTFilter, all parameters are optional.

If ENTry is excluded, the filter is simply added sequentially. In fact, if the next entry specified is not sequential, the entry is reallocated to the next sequential number. If the subject parameters are excluded, they default to the '*' wildcard.

The ACTion and LOG parameters default to 'ALLOW' and 'YES' respectively.

You can view the certificate filters by:

```
SHow PKI CERTFilter{=[1-20]}
```

You can also change the filters using:

```
SET PKI CERTFilter
```

in much the same way as the ADD command.

And there is the delete command:

```
DELete PKI CERTFilter=[1-20] {ENTry=[1-100]}
```

Finally, the filters need to be assigned to an ISAKMP policy using:

```
SET ISAkmp POLicy=xxx CERTFilter=[1-20|NOne]
```

Only one certificate filter per policy, and it works on a first-match basis

IPsec Dead Peer Detection (DPD) (CR00027606)

Models This enhancement is supported on:

- AT-8800
- Rapier i, Rapier w
- AR44x, AR450S, AR415S
- AR725, AR745
- AR750S, AR770S

Module IPsec, Encryption

Description IPsec Dead Peer Detection (DPD) is a query and response mechanism to determine peer liveliness, based on *RFC 3706, A Traffic-Based Method of Detecting Dead Internet Key Exchange (IKE) Peers, 2004*, which is supported by multiple vendors. Only the side interested in the liveliness of the far end initiates the query and response exchange, and queries are sent as needed, rather than periodically. This means relatively few messages need to be exchanged, and the solution is scalable.

The IPsec peer that is interested in the liveliness of an ISAKMP SA (called a DPD peer Initiator) sends an R-U-THERE query to the peer (called a DPD peer responder), and either the peer responds with an R-U-THERE-ACK message, or, if it does not respond after a configurable number of retries, the secure connection is considered to be dead.

The AlliedWare router or switch can be configured to function as a DPD peer responder or as both a DPD peer initiator and a DPD peer responder as specified in *RFC 3706*. (It cannot be an initiator only.) Timers and retry parameters can be configured to suit your network. This DPD function and the ISAKMP heartbeat function cannot both be enabled on the same policy.

New configuration parameters have been added to these commands to configure IPsec DPD:

- **create isakmp policy** command on page 152
- **set isakmp policy** command on page 154

The output from these commands now also display information about IPsec DPD:

- **show isakmp policy** command on page 155
- **show isakmp sa** command on page 156
- **show isakmp counters** command on page 158
- **show isakmp exchange** command on page 159

For more information about configuring IPsec and ISAKMP, see the *IP Security (IPsec)* chapter in the *Software Reference*.

Table 36: How IPsec DPD works

Role	When...	Then...
ISAKMP peer; any device supporting IPsec and ISAKMP	It negotiates a security association (SA)	It specifies its capabilities, including whether it supports DPD. If it specifies that it supports DPD, it must minimally be able to function as a DPD peer responder, and may also support the DPD peer initiator role.
DPD peer responder; either an AlliedWare router or switch with **dpdmode**=**receive** or **both** or another device supporting DPD	It receives an R-U-THERE message from an IPsec peer	It responds by sending an R-U-THERE-ACK message back to the peer.
AlliedWare router or switch configured as a DPD peer initiator (**dpdmode**=**both**) (Other devices supporting the DPD peer initiator role may use different criteria for sending R-U-THERE queries, and for deleting an SA.)	It receives a valid, encrypted message from the IPsec peer for the SA.	It starts or restarts a configurable DPD idle timer (**dpdidletimer**).
	The DPD idle time expires	It sends an R-U-THERE IKE notify message to the peer to test for liveliness.
	It receives an R-U-THERE-ACK message in response from the peer	It restarts the DPD idle timer.
	It does not receive an R-U-THERE-ACK message from the peer in response to the R-U-THERE message	It resends (retries) R-U-THERE messages according to the **msgretrylimit**, **messagebackoff**, and **msgtimeout** parameters.
	It does not receive an R-U-THERE-ACK message from the peer in response to the maximum number of retries	It considers the secure connection to be dead, deletes the IPsec SA and the ISAKMP SA. Note: If the **msgetrylimit** is set to 0, no R-U-THERE message will be sent and the connection will immediately fail when the DPD idle timer first expires.

create isakmp policy

Two new parameters have been added to this command to configure the IPSec Dead Peer Detection (DPD): **dpdidletimer** and **dpdmode**. The parameters **msgbackoff**, and **msgretrylimit**, and **msgtimeout** now also apply to DPD operation.

Syntax

```
CREate ISAkmp POLicy=name PEer={ipv4add|ipv6add|ANy}
   [AUTHType={PREshared|RSAEncr|RSASig}]
   [DELETedelay=0..30] [DHExponentlength=160..1023]
   [DPDIdletimer=1..86400] [DPDMode={Both|None|Receive}]
   [ENCalg={3DES2key|3DESInner|3DESOuter|DES|AES128|AES192|
   AES256}] [EXPIRYKbytes=1..1000]
   [EXPIRYSeconds=600..31449600] [GROup={0|1|2}]
   [HAShalg={SHa|MD5}]
   [HEARtbeatmode={Both|None|Receive|Send}]
   [HYBRIDxauth={ON|OFf|TRue|FAlse}] [IPVersion={4|6}]
   [KEY=0..65535]
   [LOCALID={ipv4add|ipv6add|domainname|user-domainname|
   dist-name}] [LOCALRsakey=0..65535]
   [MODe={MAIn|AGGressive}] [MSGBACkoff={INCREMental|NONE}]
   [MSGRetrylimit=0..1024] [MSGTImeout=1..86400]
   [NATTraversal={ON|OFf|TRue|FAlse}]
   [PHASE2xchglimit={NOne|1..1024}]
   [POLICYFilename=filename]
   [PREnegotiate={ON|OFf|TRue|FAlse}]
   [REMOTEId={ipv4add|ipv6add|domainname|user-domainname|
   dist-name}] [RETRYIKEattempts={0..16|CONTinuous}]
   [SENDDeletes={ON|OFf|TRue|FAlse}]
   [SENDNotify={ON|OFf|TRue|FAlse}]
   [SENDIdalways={ON|OFf|TRue|FAlse}]
   [SETCommitbit={ON|OFf|TRue|FAlse}]
   [SRCInterface=interface] [XAUth={CLient|SErver|NONE}]
   [XAUTHName=username] [XAUTHPasswd=password]
   [XAUTHType={GEneric|RAdius}]
```

Table 37: New parameters in the **create isakmp policy** command:

Parameter	Description
DPDIdletimer	The number of seconds (1..86400) after the last message received on a secure connection before the local side of the Secure Association initiates the sending of an IPSec Dead Peer Detection query (ie: a Informational exchange containing an R-U-THERE Notify payload). The local side initiates this to detect the liveliness of the Secure Association peer. This query is sent only if the DPDMode is set to **Both**. Default: **20**

Table 37: New parameters in the **create isakmp policy** command:

Parameter	Description	
DPDMode	Controls the level of Dead Peer Detection supported. If the **heartbeatmode** parameter is set to **both**, **receive**, or **send**, then **dpdmode** can only be set to **none**. Default: **None**	
	Both	Dead Peer Detection is enabled. Dead Peer Detection capability is indicated to IPsec peers on secure association establishment. R-U-THERE queries from the IPsec peer will be responded to with R-U-THERE-ACK if the secure association exists. R-U-THERE queries to test for liveliness when the DPDIdleTimer expires are initiated. On failed tests for liveliness, established Secure Associations with the dead peer are removed.
	None	Dead Peer Detection is not enabled. Dead Peer Detection capability will not be indicated to IPsec peers on secure association establishment.
	Receive	Dead Peer Detection is supported. Dead Peer Detection capability is indicated to IPsec peers on secure association establishment. R-U-THERE queries from the IPSec peer will be responded to with R-U-THERE-ACK if the secure association exists. No R-U-THERE queries are initiated and connection idleness is not monitored.

For more information about the **create isakmp policy** command, including existing parameters that now also apply to DPD (**msgbackoff**, **msgretrylimit**, and **msgtimeout**), see the *IP Security (IPsec)* chapter in the *Software Reference* for your router or switch.

Examples In this example, the ISAKMP policy has Dead Peer Detection enabled to both respond to and initiate queries for liveliness. The DPD Idle interval is not set, therefore DPD uses the default parameter for **dpdidletimer** (20 seconds).

```
create isakmp poli="keys" peer=any group=2 enc=3desouter key=1
   dpdmode=both
```

In this example, the ISAKMP policy has Dead Peer Detection enabled to both respond to and initiate queries for liveliness. It sets the specific DPD Idle interval to 5 minutes.

```
create isakmp poli="keys" peer=any group=2 enc=3desouter key=1
   dpdmode=both dpdidletimer=300
```

In this example, the ISAKMP policy has Dead Peer Detection set to only respond to queries for liveliness from its peer. DPDIdleTimer is allowed to be set but it is not used.

```
create isakmp poli="keys" peer=any group=2 enc=3desouter key=1
   dpdmode=receive
```

In this example, the ISAKMP policy does not have Dead Peer Detection enabled (default).

```
create isakmp poli="keys" peer=any group=2 enc=3desouter key=1
```

set isakmp policy

The same two new parameters have been added to this command as to the **create isakmp policy** command above: **dpdidletimer** and **dpdmode**. The parameters **msgbackoff**, and **msgretrylimit**, and **msgtimeout** now also apply to DPD operation.

Syntax

```
SET ISAkmp POLicy=name [PEer={ipv4add|ipv6add|ANy}]
   [AUTHType={PREshared|RSAEncr|RSASig}] [DELETedelay=10]
   [DHExponentlength=160..1023] [DPDIdletimer=1..86400]
   [DPDMode={Both|None|Receive}]
   [ENCalg={3DES2key|3DESInner|3DESOuter|DES|AES128|AES192|
   AES256}] [EXPIRYKbytes=1..1000]
   [EXPIRYSeconds=600..31449600] [GROup={0|1|2}]
   [HAShalg={SHa|MD5}]
   [HEARtbeatmode={Both|None|Receive|Send}]
   [HYBRIDxauth={ON|OFf|TRue|FAlse}] [IPVersion={4|6}]
   [KEY=0..65535]
   [LOCALID={ipv4add|ipv6add|domainname|user-domainname|
   dist-name}] [LOCALRsakey=0..65535]
   [MODe={MAIn|AGGressive}] [MSGBACkoff={INCREMental|NONE}]
   [MSGRetrylimit=0..1024] [MSGTImeout=1..86400]
   [NATTraversal={ON|OFf|TRue|FAlse}]
   [PHASE2xchglimit={NOne|1..1024}]
   [POLICYFilename=filename]
   [PREnegotiate={ON|OFf|TRue|FAlse}]
   [REMOTEId={ipv4add|ipv6add|domainname|userdomainname|
   dist-name}] [RETRYIKEattempts={0..16|CONTinuous}]
   [SENDDeletes={ON|OFf|TRue|FAlse}]
   [SENDIdalways={ON|OFf|TRue|FAlse}]
   [SENDNotify={ON|OFf|TRue|FAlse}]
   [SETCommitbit={ON|OFf|TRue|FAlse}]
   [SRCInterface=interface] [XAUth={CLient|SErver|NOne}]
   [XAUTHName=username] [XAUTHPasswd=
```

show isakmp policy

The output from the **show isakmp policy** command for a specified policy is modified to display the current Dead Peer Detection (DPD) configuration.

Figure 30: Example output from the **show isakmp policy** command

```
ISAKMP Policy
  Name ................................ my_isakmp_policy
  Peer Address ........................ 202.36.163.201
  Phase1 Mode ......................... IDPROT
  Authentication Type ................. PRESHARED
  Extended Authentication ............. NONE
  Extended Authentication Type ........ -
  Extended Authentication User Name ..... -
  Extended Authentication Password ..... -
  Key Id .............................. 30
  Local RSA key ....................... -
  Peer Certificate Id ................. -
  Phase 2 Exchanges Limit ............. NONE
  PreNegotiate ........................ TRUE
  DOI ................................. IPSEC
  Send Notify Messages ................ TRUE
  Send Delete Messages ................ FALSE
  Always Send ID Messages ............. FALSE
  Commit Bit .......................... FALSE
  Message Retry Limit ................. 5
  Message Time Out .................... 20
  Message Back-off .................... Incremental
  Exchange Delete Delay ............... 30
  Source Interface .................... -
  VPN Client Policy File Name ......... -
  Local ID ............................ -
  Remote ID ........................... IPv4:192.68.1.2
  DebugFlag ........................... 00000000
  Retry IKE Attempts .................. 0
  Current IKE Retries ................. 0
  Required IKE Retry Phase ............ No Phases


SA Specification
  Encryption Algorithm ................ DES - 56 bit
  Hash Algorithm ...................... SHA
  Group Description ................... 1
  DH Private Exponent Bits ............ 767
  Heartbeat Mode ...................... NONE
  DPD Mode ............................ BOTH
  DPD Idle Timeout .................... 300
  Group Type .......................... MODP
  Expiry Seconds ...................... 86400
  Expiry Kilobytes .................... 1000
  NAT Traversal ....................... TRUE
```

show isakmp sa

The output from the **show isakmp sa** command for a specified SA is modified to display the current Dead Peer Detection (DPD) configuration the current operational sequence numbers being maintained for initiation and reception of DPD Notify messages.

Figure 31: Example output from the **show isakmp sa** command

```
SA Id ................................ 1
  Initiator Cookie ................... e418dba372510e53
  Responder Cookie ................... 80c30ff4f2cb3f29
  DOI ................................ IPSEC
  Policy name ........................ main
  State .............................. ACTIVE
  Local address ...................... 202.36.163.161
  Remote Address ..................... 202.36.163.201
  Time of establishment ..............
  Commit bit set ..................... FALSE
  Send notifies ...................... TRUE
  Send deletes ....................... FALSE
  Message Retry Limit ................ 5
  Initial Message Retry Timeout (s) ... 20
  Message Back-off ................... None
  Exchange Delete Delay (s) .......... 30
  Do Xauth ........................... FALSE
    Xauth Finished ................... TRUE
  Expiry Limit (bytes) ............... 1024000
  Soft Expiry Limit (bytes) .......... 896000
  Bytes seen ......................... 304
  Expiry Limit (seconds) ............. 86400
  Soft Expiry Limit (seconds) ........ 75600
  Seconds since creation ............. 2117
  Number of Phase 2 exchanges allowed . 4294967295
  Number of acquires queued .......... 0
Sa Definition Information:
  Authentication Type ................ PRESHARED
  Encryption Algorithm ............... DES - 56 bit
  Hash Algorithm ..................... SHA
  group Type ......................... MODP
  group Description .................. MODP768
  DH Private Exponent Bits ........... 767
  expiry seconds ..................... 86400
  expiry kilobytes ................... 1000
XAuth Information:
  Id ................................. 0
  Next Message ....................... UNKNOWN
  Status ............................. FAIL
  Type ............................... Generic
  Max Failed Attempts ................ 0
  Failed Attempts .................... 0
NAT-Traversal Information:
  NAT-T enabled ...................... YES
  Peer NAT-T capable ................. YES
  NAT discovered ..................... REMOTE
Heartbeat information:
  Send Heartbeats .................... NO
  Next sequence number tx ............ 1
  Receive Heartbeats ................. NO
  Last sequence number rx ............ 0
```

Figure 31: Example output from the **show isakmp sa** command (cont.)

```
DPD information:
  DPD Mode ........................... BOTH
  State .............................. Active
  Retry Count ........................ 0
  Idle Expiry (seconds)............... 300
  Next sequence number tx ............ 12516
  Last sequence number rx ............ 9743
```

Table 38: New parameters in output of the **show isakmp sa** command for a specified Security Association

Parameter	Meaning	
DPD Information	Information relating to the IPSec Dead Peer Detection	
DPD Mode	The configuration of the Dead Peer Detection capability.	
	Both	DPD will receive and respond to queries for liveliness from its peer. DPD will also initiate queries for liveliness if the DPD Idle Timer expires.
	Receive	DPD will receive and respond to queries for liveliness from its peer but will not initiate queries. DPD Idle Timer does not run and Idle Expiry Limit (seconds) is always 0. State will always be 'ActiveReceive'. Retry Count will always be 0.
	None	DPD is not configured.
State	The current state of Dead Peer Detection; one of the following:	
	Active	Only displayed when DPD Mode is BOTH. The connection is actively being monitored for idleness and the DPD Idle Timer is running. If a valid IPSec packet is not received on the connection in 'Idle Expiry Limit (seconds)', then the connection will be considered idle and will initiate a query for liveliness.
	ActiveReceive	If DPD Mode = Receive, then DPD will always display this state indicating its readiness to respond to peer queries for liveliness.
	IdleQuery	DPD Mode = BOTH and 'Idle Expiry (seconds)' has reduced to 0 and a query for liveliness (sending R-U-THERE Notify) has been initiated.
	IdleQueryRetry	DPD Mode = BOTH and the first attempt to reach the peer has expired and subsequent attempts are being tried. 'Retry Count' indicates how many times it has already retried.
	Dead	The maximum number of retries without receiving a response has been attempted and the connection is declared dead and will be deleted. This state is a brief transitional state and will rarely be seen since the SA being queried is the one which is declared dead and will be deleted.
	None	This is the state displayed when DPDMode is NONE, that is, not enabled.

Table 38: New parameters in output of the **show isakmp sa** command for a specified Security Association (cont.)

Parameter	Meaning
Retry Count	If the DPD idle timer has expired and the peer is being queried for liveliness, the retry count represents the number of times that the R-U-THERE query has been sent without a response. If the DPD State is Active or ActiveReceive or None, this count is always 0. If the count reaches the Message Retry Limit, then the SA will be declared dead and deleted.
Idle Expiry (seconds)	When DPD State = Active, the number of seconds remaining before the connection is considered idle and the query for liveliness begins. In any other state than Active, this value is 0
Next sequence number tx	Sequence number to be used in the next DPD Notify payload sent.
Last sequence number rx	Sequence number received in the last DPD Notify payload. The value is 0 if no DPD Notify payload has yet been received. The receiving end expects the sequence number to be incremented by 1 for each new exchange following the first one. An exchange (and therefore subsequently the connection to which it refers) will fail if the expected sequence number is not received after the maximum number of retries are attempted. This is a security aspect of Dead Peer Detection which prevents replay attacks.

show isakmp counters

This command now includes a new option for displaying Dead Peer Detection(DPD) counters.

Syntax

```
SHow ISAkmp
   COUnters[={AGGressive|GENeral|DPD|HEArtbeat|INFo|IPSec|M
   AIn|NETwork|QUIck|SAD|SPD|TRAnsaction|XDB}]
```

Table 39: New option in the **show isakmp counters** command

Parameter	Description	
COUnters	The category or categories of counters to display. Multiple categories can be specified as a comma-separated list. Default: displays all ISAKMP counters under this command.	
	DPD	Displays IPSec Dead Peer Detection counters.

Table 40: Example output from the **show isakmp counters** command

```
DPD Mode Counters:

startXchgInitiator     0     startXchgResponder     0
initXchgComplete       0     respXchgComplete       0
initXchgFail           0     respXchgFail           0
rxRUTMsg               0     txRUTAMsg              0
txRUTMsg               0     rxRUTAMsg              0
rxInvalidSeqno         0     rxNotifyPayInvalid     0
```

Table 41: Parameters in output from the **show isakmp counters=dpd** command

Parameter	Meaning
startXchgInitiator	Number of times a DPD exchange started as the Initiator of the liveliness query (R-U-THERE is sent)
startXchgResponder	Number of times a DPD exchange started as the Responder to a liveliness query (R-U-THERE-ACK is sent in response to R-U-THERE)
initXchgComplete	Number of times a DPD exchange as an initiator is completed successfully (R-U-THERE-ACK is received in response to an R-U-THERE)
respXchgComplete	Number of times a DPD exchange as a responder is completed successfully (R-U-THERE-ACK is sent in response to an R-U-THERE)
initXchgFail	The number of times a DPD exchange started as the initiator is not completed successfully indicating a dead peer and resulting in local IPSec Secure Association deletion.
respXchgFail	The number of times a DPD exchange started as the responder is not completed successfully. Either the received message is invalid or there was a problem in sending a response.
rxRUTMsg	The number of R-U-THERE messages received.
txRUTAMsg	The number of R-U-THERE-ACK messages sent.
txRUTMsg	The number of R-U-THERE messages sent.
rxRUTAMsg	The number of R-U-THERE-ACK messages received.
rxInvalidSeqNo	The number of DPD payloads received with an invalid sequence number.
rxNotifyPayInvalid	The number of DPD messages received with an invalid Notify payload (where notify type can be identified as IPSec DPD).

show isakmp exchange

Informational exchange gets a new state machine for DPD exchanges and therefore exchanges of type INFO have new states which can be viewed with the **show isakmp exchange** command. The syntax of the command has not changed. The number of possible states displayed has been increased. It is no longer true that for informational exchanges that the state is always 'IDLE'.

Syntax `SHow ISAkmp EXChange[=`*`exchange-id`*`]`

Where the states possible has been changed as follows. These changes apply for the command to show all exchanges in summary form 'show isakmp exchange' as well as the command to display a specific exchange in more detail ('show isakmp exchange=<exchange-id>'):

Table 42: Parameters in output from the **show isakmp exchange** command

Parameter	Meaning
Id	Identification number used to identify the Exchange.
Phase	Current phase of the exchange; either 1, 1.5, or 2.

Table 42: Parameters in output from the **show isakmp exchange** command (cont.)

Parameter	Meaning
State	Current state of the exchange.
	For Main mode exchanges:
	IDLE
	SASENT
	SARECV
	KESENT
	KERECV
	AUTHSENT
	AUTHRECV
	UP
	For Quick mode exchanges:
	STARTING
	WAIT_HASH_SA_NONCE
	WAIT_HASH
	RECEIVING_MESSAGE
	SENDING_HASH_SA_NONCE
	SENDING_HASH
	DONE
	For Aggressive mode exchanges:
	IDLE
	SAKESENT
	SAKERECV
	SAKEAUTHSENT
	SAKEAUTHRECV
	AUTHSENT
	AUTHRECV
	UP
	For Transaction exchanges:
	IDLE
	REQSENT
	REQRECV
	REPSENT
	REPRECV
	SETSENT
	SETRECV
	ACKSENT
	ACKRECV
	UP

Table 42: Parameters in output from the **show isakmp exchange** command (cont.)

Parameter	Meaning
	For Informational exchanges:
	IDLE
	SEND_RUT
	WAIT_RUTA
	SEND_RUTA
	DONE

Diffie-Hellman Groups 5 and 14 (CR00030097)

Models This enhancement is supported on:

- AT-8800
- Rapier i, Rapier w
- AR44x, AR450S, AR415S
- AR725, AR745
- AR750S, AR770S

Module IPsec, Encryption

Description IPsec and ISAKMP on the routers and switches now support additional Diffie-Hellman Modular Exponential (MODP) Groups for the Internet Key Exchange (IKE) protocol. These new stronger groups allow for stronger encryption by the Advanced Encryption Standard (AES). The new groups supported are:

- MODP group 5 (1536-bit exponent length)
- MODP group 14 (2048-bit exponent length)

as specified in *RFC 3526, More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE), 2003*.

Parameter changes have been made to these commands to configure the new options:

- **create isakmp policy** command on page 162
- **set isakmp policy** command on page 163
- **create ipsec policy** command on page 164
- **set ipsec policy** command on page 165

The output from these **show** commands for IPsec, ISAKMP, and Encryption Services now also display information about the new options:

- **show isakmp policy** command on page 165
- **show isakmp exchange** command on page 165
- **show isakmp sa** command on page 166
- **show ipsec policy** command on page 166
- **show enco channel** command on page 166

For more information about IPsec and ISAKMP, and how to configure it on your router or switch, see the *IP Security (IPsec)* chapter in the *Software Reference*.

create isakmp policy

The parameters **dhexponentlength** and **group** are modified as described below.

Syntax

```
CREate ISAkmp POLicy=name PEer={ipv4add|ipv6add|ANy}
   [AUTHType={PREshared|RSAEncr|RSASig}]
   [DELETedelay=0..30] [DHExponentlength=160..2048]
   [DPDIdleTimer=1..86400] [DPDMode={Both|None|Receive}]
   [ENCalg={3DES2key|3DESInner|3DESOuter|DES|AES128|AES192|
   AES256}] [EXPIRYKbytes=1..1000]
   [EXPIRYSeconds=600..31449600] [GROup={0|1|2|5|14}]
   [HAShalg={SHa|MD5}]
   [HEARtbeatmode={Both|None|Receive|Send}]
   [HYBRIDxauth={ON|OFf|TRue|FAlse}] [IPVersion={4|6}]
   [KEY=0..65535]
   [LOCALID={ipv4add|ipv6add|domainname|user-domainname|
   dist-name}] [LOCALRsakey=0..65535]
   [MODe={MAIn|AGGressive}] [MSGBACkoff={INCREMental|NONE}]
   [MSGRETrylimit=0..1024] [MSGTImeout=1..86400]
   [NATTraversal={ON|OFf|TRue|FAlse}]
   [PHASE2xchglimit={NOne|1..1024}]
   [POLICYFilename=filename]
   [PREnegotiate={ON|OFf|TRue|FAlse}]
   [REMOTEId={ipv4add|ipv6add|domainname|
   user-domainname|dist-name}]
   [RETRYIKEattempts={0..16|CONTinuous}]
   [SENDDeletes={ON|OFf|TRue|FAlse}]
   [SENDNotify={ON|OFf|TRue|FAlse}]
   [SENDIdalways={ON|OFf|TRue|FAlse}]
   [SETCommitbit={ON|OFf|TRue|FAlse}]
   [SRCInterface=interface] [XAUth={CLient|SErver|NONE}]
   [XAUTHName=username] [XAUTHPasswd=password]
   [XAUTHType={GEneric|RAdius}]
```

Table 43: Modified parameters in the **create isakmp policy** command:

Parameter	Description
DHExponentlength	The length in bits of the Diffie-Hellman private exponent. A large private exponent increases the security of generated keys. A small private exponent shortens the time taken for the Diffie-Hellman key exchange. The minimum for all five Diffie-Hellman groups is 160 bits. The maximum allowable values are: 512 bits for group 0; 768 bits for group 1;1024 bits for group 2;**1536 for group 5** and **2048 for group 14**. Default: 160
GROup	The Diffie-Hellman group to use when negotiating session keys. Groups 0, 1, 2, 5 and 14 are MODP groups, each allowing for a progressively increasing length in the number of bits used for the exponent component of the MODP calculation. Group 0 allows up to 512 bits, group 1 - 768 bits, group 2 - 1024 bits, **group 5 - 1536 bits** and group **14 - 2048 bits**. Larger exponent size results in higher security, but at the expense of encryption time. Default: 1

set isakmp policy

The parameters **dhexponentlength** and **group** are modified, as described for the **create isakmp policy** command above.

Syntax

```
SET ISAkmp POLicy=name [PEer={ipv4add|ipv6add|ANy}]
   [AUTHType={PREshared|RSAEncr|RSASig}] [DELETedelay=10]
   [DHExponentlength=160..2048]  [DPDIdleTimer=1..86400]
   [DPDMode={Both|None|Receive}]
   [ENCalg={3DES2key|3DESInner|3DESOuter|DES|AES128|AES192|
   AES256}] [EXPIRYKbytes=1..1000]
   [EXPIRYSeconds=600..31449600] [GROup={0|1|2|5|14}]
   [HAShalg={SHa|MD5}]
   [HEARtbeatmode={Both|None|Receive|Send}]
   [HYBRIDxauth={ON|OFf|TRue|FAlse}] [IPVersion={4|6}]
   [KEY=0..65535]
   [LOCALID={ipv4add|ipv6add|domainname|user-domainname|
   dist-name}] [LOCALRsakey=0..65535]
   [MODe={MAIn|AGGressive}] [MSGBACkoff={INCREMental|NONE}]
   [MSGRetrylimit=0..1024] [MSGTImeout=1..86400]
   [NATTraversal={ON|OFf|TRue|FAlse}]
   [PHASE2xchglimit={NOne|1..1024}]
   [POLICYFilename=filename]
   [PREnegotiate={ON|OFf|TRue|FAlse}]
   [REMOTEId={ipv4add|ipv6add|domainname|userdomainname|
   dist-name}] [RETRYIKEattempts={0..16|CONTinuous}]
   [SENDDeletes={ON|OFf|TRue|FAlse}]
   [SENDIdalways={ON|OFf|TRue|FAlse}]
   [SENDNotify={ON|OFf|TRue|FAlse}]
   [SETCommitbit={ON|OFf|TRue|FAlse}]
   [SRCInterface=interface] [XAUth={CLient|SErver|NOne}]
   [XAUTHName=username] [XAUTHPasswd=password]
   [XAUTHType={GEneric|RAdius}]
```

create ipsec policy

New options have been added to the **group** parameter.

Syntax

```
CREate IPSec POLicy=name INTerface=interface
   ACtion={DEny|IPsec|PErmit} [IPVersion={4|6}]
   [BUNDlespecification=bundlespecification-id]
   [DFBit={SEt|COpy|CLear}] [GROup={0|1|2|5|14}]
   [ICmptype={list|NDALL}] [IPROUtetemplate=template-name]
   [ISAkmppolicy=isakmp-policy-name]
   [KEYmanagement={ISakmp|MAnual}]
   [LADdress={ANy|ipv4add[-ipv4add]|
   ipv6add[/prefix-length]|ipv6addipv6add}] [LMAsk=ipv4add]
   [LNAme={ANy|system-name}] [LPort={ANy|OPaque|port}]
   [PEERaddress={ipv4add|ipv6add|ANy|DYnamic}]
   [POSition=1..100] [RADdress={ANY|ipv4add[-ipv4add]|
   ipv6add[/prefix-length]|ipv6addipv6add}]
   [RESPondbadspi={True|False}] [RMAsk=ipv4add]
   [RNAme={ANy|system-name}] [RPort={ANy|port|OPaque}]
   [SASElectorfrompkt={ALL|LADdress|LPort|NONE|RADdress|
   RPort|TRAnsportprotocol}] [SRCInterface=interface]
   [TRAnsportprotocol={ANy|EGp|ESp|GRe|ICmp|OPaque|OSpf|
   RSvp|TCp|UDp|protocol}] [UDPHeartbeat={True|False}]
   [UDPPort=port] [UDPTunnel={True|False}]
   [USEPFSKey={True|False}]
```

Table 44: Modified parameter in the **create ipsec policy** command

Parameter	Description
GROup	The group used for the Diffie-Hellman key exchange by ISAKMP/IKE for Perfect Forward Secrecy. Groups 0, 1, 2, **5** and **14** are MODP groups, each allowing for a progressively increasing length in the number of bits used for the exponent component of the MODP calculation. Group 0 allows up to 512 bits, group 1 - 768 bits, group 2 - 1024 bits, **group 5 - 1536 bits** and **group 14 - 2048 bits**. Larger exponent size results in higher security but at the expense of encryption time. This parameter is only used if the **usepfskey** parameter is set to true. Default: **1**

set ipsec policy

New options have been added to the group parameter, as described for the **create ipsec policy** command above.

Syntax

```
SET IPSec POLIcy=name [ACtion={DEny|IPSec|PErmit}]
   [BUNDlespecification=bundlespecification-id]
   [DFBit={SEt|COpy|CLear}] [GROup={0|1|2|5|14}]
   [ICmptype={list|NDall}] [IPROUtetemplate=template-name]
   [IPVersion={4|6}] [ISAkmppolicy=isakmp-policy-name]
   [LADdress={ANy|ipv4add[-ipv4add]|
   ipv6add[/prefixlength]|ipv6add-ipv6add}] [LMAsk=ipv4add]
   [LNAme={ANy|system-name}] [LPort={ANy|OPaque|port}]
   [PEERaddress={ipv4add|ipv6add|ANy|DYNAMIC}]
   [PKTDebuglength=1..1500] [POSition=1..100]
   [RADdress={ANy|ipv4add[-ipv4add]|
   ipv6add[/prefixlength]|ipv6add-ipv6add}]
   [RESPondbadspi={True|False}] [RMASK=ipv4add]
   [RNAme={ANy|system-name}] [RPort={ANy|port|OPaque}]
   [SASElectorfrompkt={ALL|LADdress|LPort|NONE|RADdress|
   RPort|TRAnsportprotocol}] [SRCInterface=interface]
   [TRAnsportprotocol={ANy|EGp|ESp|GRe|ICmp|OPaque|OSpf|
   RSvp|TCp|UDp|protocol}] [UDPHeartbeat={True|False}]
   [UDPPort=port] [UDPTunnel={True|False}]
   [USEPFSKey={True|False}]
```

show isakmp policy

The output from this command displays the Diffie-Hellman group number, including the new values if they are configured, as follows.

Table 45: Modified parameter in the output from the **show isakmp policy** command

Parameter	Description
Group Description	Whether the Diffie-Hellman group number is 0, 1, 2, **5**, or **14**.

show isakmp exchange

The output from this command displays the Diffie-Hellman group description, including the new values if they are configured, as follows.

Table 46: Modified parameter in the output from the **show isakmp exchange** command

Parameter	Description
Main and Aggressive Mode	Information about a Main mode or Aggressive mode exchange
Group Description	The Diffie-Hellman group identification: 512 768 1024 **1536** **2048** INVALID

Table 46: Modified parameter in the output from the **show isakmp exchange** command

Parameter	Description
Sa Definition Information	Information about the Security Association definition for the exchange
Group Description	The Diffie-Hellman group identification; either MODP512, MODP768, MODP1024, **MOD1536**, **MOD2048**, or INVALID.

show isakmp sa

The output from this command displays the Diffie-Hellman group description, including the new values if they are configured, as follows.

Table 47: Modified parameter in the output from the **show isakmp sa** command

Parameter	Description
Group Description	The Diffie-Hellman group identification: 512 768 1024 **1536** **2048** INVALID

show ipsec policy

The output from this command displays the Diffie-Hellman group number, including the new values if they are configured.

show enco channel

The output from this command displays the Diffie-Hellman group description, including the new values if they are configured, as follows.

Table 48: Modified parameter in the output from the **show enco channel** command

Parameter	Description
Group	[Diffie-Hellman] Whether the Diffie-Hellman group is 768-bit MODP, 1024-bit MODP, **1536-bit MODP** or **2048-bit MODP**.

Diffie-Hellman group and usepfkey parameter dependence (CR00028466)

Models This enhancement is supported on:

- AT-8800
- Rapier i, Rapier w
- AR44x, AR450S, AR415S
- AR725, AR745
- AR750S, AR770S

Module IPsec

Description Previously, when creating or modifying the parameters for an IPsec policy using either the **create ipsec policy** command or the **set ipsec policy** command, the Diffie-Hellman **group** parameter could only be specified if the **usepfkey** parameter was set to **true**.

```
CREate IPSec POLicy=name INTerface=interface
   ACtion={DEny|IPsec|PErmit} GROup={0|1|2} USEPFSKey=True
   [<other-ipsec-policy-params>]
```

This dependence has been removed: the **group** parameter can now be specified independently of the **usepfkey** parameter.

```
CREate IPSec POLicy=name INTerface=interface
   ACtion={DEny|IPsec|PErmit} GROup={0|1|2}
   [<other-ipsec-policy-params>]
```

Support VPN clients with no attributes in the final XAuth ack (CR00028456)

Models This enhancement is supported on:

- AT-8800
- Rapier i, Rapier w
- AR44x, AR450S, AR415S
- AR725, AR745
- AR750S, AR770S

Module ISAKMP

Description Added support for VPN clients that do not have attributes supplied in the final XAuth acknowledge message e.g. The Greenbow VPN client.

Maximum number of IPsec bundles increased (CR00026765)

Models This enhancement is supported on:

- AT-8800
- Rapier i, Rapier w
- AR44x, AR450S, AR415S
- AR725, AR745
- AR750S, AR770S

Module IPsec

Description Previously the maximum number of IPsec bundles that could be attached to a policy was 100. This has been increased to 200.

DNS names in ISAKMP and IPsec policies (CR00021106)

Models This enhancement is supported on:

- AT-8800
- Rapier i, Rapier w
- AR44x, AR450S, AR415S
- AR725, AR745
- AR750S, AR770S

Module IPsec, ISAKMP

Description You can now specify peers in ISAKMP and IPsec policies using a DNS name. Previously, you could only specify the peers using an IP address. Corresponding **show** commands now also display the DNS name.

Performance improvement (CR00021262)

Models This enhancement is supported on:

- AT-8800
- Rapier i, Rapier w
- AR44x, AR450S, AR415S
- AR725, AR745
- AR750S, AR770S

Module IPsec

Description This enhancement has improved switch performance when:

- multiple IPsec policies exist. In particular, having two policies causes much less of a reduction in performance.
- a single channel exists with bidirectional traffic (i.e. the single channel is both encoding and decoding packets).

Improved VPN reliability (CR00021304)

Models This enhancement is supported on:

- AT-8800
- Rapier i, Rapier w
- AR44x, AR450S, AR415S
- AR725, AR745
- AR750S, AR770S

Module IPsec

Description Changes have been made to reduce the risk of packet loss over a VPN under very high traffic levels and corresponding high-to-overload CPU conditions.

- The number of input buffers allowed for IPsec message processing has been increased, to mitigate brief (<50ms) periods of CPU overload where the arrival of IPsec packets can exceed the switch's ability to process them in real time. This prevents packet loss.
- Processing of the ISAKMP heartbeat between two peer switches has been given the highest priority over packet stream encryption, to ensure that the security authorisation synchronisation is not lost during high traffic rates. Loss of synchronisation results in packet loss until a resynchronisation completes.

Tunnelled IPsec connection for IPv6 (CR00016150)

Models This enhancement is supported on:

- AT-8800
- Rapier i, Rapier w
- AR44x, AR450S, AR415S
- AR725, AR745
- AR750S, AR770S

Module IPsec, IPv6

Description To establish a tunnelled IPsec connection for IPv6, you may need to specify the source IP interface in the IPsec and ISAKMP policies. This enhancement enables you to do so.

To specify the source interface, use the **srcinterface** parameter in the commands:

```
create ipsec policy=name <other parameters>
set ipsec policy=name <other parameters>
create isakmp policy=name <other parameters>
set isakmp policy=name <other parameters>
```

The global address of the source interface (if available) will be used as the local address of the policy.

Increase in positions available for IPsec policies (CR00032032)

Models This enhancement is supported on:

- AT-8948, x900-48
- AT-9900
- AT-9800
- AT-8800
- AT-8600
- AT-8700XL
- Rapier i, Rapier w
- AR44x, AR450S, AR415S
- AR725, AR745
- AR750S, AR770S

Module IPsec

Description Previously, the number of positions available for altering the relative position of an IPsec policy (the **position** parameter in the **create ipsec policy** and **set ipsec policy** commands) used to be limited to 100. This has been increased to 1000.

New in WAN Load Balancing

This section describes enhancements to WAN load balancing support as described in the *WAN Load Balancing* chapter in the *Software Reference for Version 2.9.1* for your router or switch.

Load balancing on VLANs (CR00017532)

Models This enhancement is supported on:

- AR44x, AR450S, AR415S
- AR750S, AR770S

Module WAN Load Balancing

Description WAN load balancing can now also balance traffic across IP interfaces that are configured on VLANs. This means it is now available for the following IP interfaces:

- eth (such as eth0)
- ppp (such as ppp0)
- vlan (such as vlan1)

New in EPSR

This section describes enhancements to EPSR as described in the *Ethernet Protection Switching Ring (EPSR)* chapter in the *Software Reference for Version 2.9.1* for your router or switch.

Improved recovery time (CR00021852)

Models This enhancement is supported on:

- AT-8948, x900-48
- AT-9900

Module EPSR

Description An enhancement has been made to EPSR to speed up recovery time in situations where the master switch is isolated or down. In these situations, if any links between transit nodes go down and are restored, the transit nodes are now able to put the recovered ports back into a forwarding state even without messaging from the master switch. This means that connectivity around the ring can be partially restored before communication with the master has been restored.

The mechanism by which the transit nodes make this decision operates in a way that prevents the possibility of the ring ever becoming unprotected.

Enhanced recovery from multiple link failure (CR00020566)

Models This enhancement is supported on:

- AT-8948, x900-48
- AT-9900

Module EPSR

Description This software version includes support for EPSR+ with enhanced multiple link recovery. This enhancement enables an EPSR ring to recover from simultaneous failure of multiple links or units, no matter where in the ring these failures occur.

With enhanced recovery, if a ring has multiple points of failure, and then one point recovers, the recovered point will start processing traffic even if other points are still down. This keeps as much of the ring available as possible.

To enable enhanced recovery, use one of the commands:

```
create epsr=<id> enhance=on
set epsr=<id> enhance=on
```

Note that you must enable enhanced recovery on the master node **and** every transit node within the EPSR domain.

Enhanced recovery is disabled by default, to allow interoperation with other implementations that are based on RFC 3619.

To disable enhanced recovery, use one of the commands:

```
create epsr=<id> enhance=off
```

```
set epsr=<id> enhance=off
```

To see whether it is enabled or disabled, use the command:

```
show epsr
```

and check the “Enhanced Recovery” field.

New in SNMP

This section describes enhancements to SNMP support as described in the *Simple Network Management Protocol (SNMP)* chapter in the *Software Reference for Version 2.9.1* for your router or switch.

For information about changes to the SNMP MIBs, see "New in SNMP MIB" on page 180.

SNMP trap delay (CR00021769)

Models This enhancement is supported on:

- AT-8948, x900-48
- AT-9900
- AT-9800
- AT-8800
- AT-8600
- AT-8700XL
- Rapier i, Rapier w
- AR44x, AR450S, AR415S
- AR725, AR745
- AR750S, AR770S

Module SNMP

Description A new command **set snmp trapdelay** has been added to allow SNMP traps to be queued for a specified time at start up.

By default, all SNMP traps are queued for 10 seconds following startup. This allows time for links to come up on the switch. However sometimes this is not enough time for other network protocols to converge and open up transmission paths to the SNMP management station.

The **set snmp trapdelay** command allows you configure a longer delay of up to 10 minutes on an SNMP trap. To change the delay, use the command:

```
SET SNMP TRapdelay=10..600
```

The default is 10 seconds.

This feature is similar to the syslog start-up delay feature ("Syslog start-up delay (CR00026520)" on page 177).

Link status trap delay (CR00022832)

Models This enhancement is supported on:

- AT-8948, x900-48
- AT-9900
- AT-9800
- AT-8800
- AT-8600
- AT-8700XL
- Rapier i, Rapier w
- AR44x, AR450S, AR415S
- AR725, AR745
- AR750S, AR770S

Module SNMP

Description The **set interface** command now has the parameter **trapdelay**, which allows you to delay the transmission of SNMP link status traps from 0 to 60 seconds. This is useful for situations where the SNMP link status traps need to wait for route tables to be updated or other protocols to process the link change event before being transmitted. The new command is:

```
set interface={ifIndex|interface} trapdelay=0..60
```

You cannot set a delay on a dynamic interface. The default is **0**.

The output of the **show interface=*interface*** command now displays the value for this parameter.

SNMP ASN.01 BER padding (CR00016523)

Models This enhancement is supported on:

- AT-8948, x900-48
- AT-9900
- AT-9800
- AT-8800
- AT-8600
- AT-8700XL
- Rapier i, Rapier w
- AR44x, AR450S, AR415S
- AR725, AR745
- AR750S, AR770S

Module SNMP

Description This enhancement enables you to specify whether SNMP adds 0x00 padding when the most significant 9 bits of an object's value are all 1, or whether the encoding follows the ASN.01 BER rule, which cuts off the most significant byte of 0xff. This setting has an impact on all integer type MIB objects, including 32 bit and 64 bit counter objects.

To add the padding, use the command:

```
set snmp asnberpadding={on|yes|true}
```

To use the ASN.01 BER rule, which is the default, use the command:

```
set snmp asnberpadding={off|no|false}
```

The following table lists examples.

Bits	Value (decimal)	Value (hex)	asnberpadding setting	Encoding
counter32	4289592837	0xFFADFE05	on	41 05 00 ff ad fe 05
			off	41 03 ad fe 05
counter64	18410715280977201498	0xFF800000ff80895A	on	46 09 00 ff 80 00 00 ff 80 89 5a
			off	46 07 80 00 00 ff 80 89 5a

To see whether or not padding is added, use the command:

```
show snmp
```

and check the new "ASN.01 BER Padding" field.

New in Logging Facility

This section describes enhancements to logging as described in the *Logging Facility* chapter in the *Software Reference for Version 2.9.1* for your router or switch.

Related enhancements include:

- "Log Eth link status change (CR00020171)" on page 47

Syslog start-up delay (CR00026520)

Models This enhancement is supported on:

- AT-8948, x900-48
- AT-9900
- AT-9800
- AT-8800
- AT-8600
- AT-8700XL
- Rapier i, Rapier w
- AR44x, AR450S, AR415S
- AR725, AR745
- AR750S, AR770S

Module Log

Description You can now specify a startup delay period, which has the effect of delaying the transmission of syslog messages. This allows for syslog servers that are connected via routing protocols (e.g. OSPF, BGP) that may take some time to negotiate network paths at startup. Previously, such log messages were lost because they are transmitted before the network path came up. This feature is similar to the SNMP trap delay feature ("SNMP trap delay (CR00021769)" on page 174).

- Syslog start-up delay can be configured for log output definitions created (or set) with a destination of **syslog** (e.g., create log out=1 dest=syslog server=172.20.133.1).
- Syslog start-up delay applies only to log messages generated at device startup and allows the transmission of syslog log messages generated during device startup to be delayed.

Use the new command **set log syslog delay** to specify the time to wait in seconds (**delay**) before sending log messages generated at device startup, and the number of messages to save (**messages**) for transmission when the delay period has expired. After the delay period, the saved log messages will be transmitted to the specified syslog server and normal syslog behaviour will resume.

Syntax

```
SET LOG SYSlog DELAY=<0-600> MESSages=<0-50>
```

Parameters **delay**: A delay time period (seconds). Syslog messages will not be transmitted from the device until the specified delay has expired.

messages: The number of log messages to be saved for transmission after the DELAY period has expired.

One or both of DELAY or MESSAGES parameters must be present on the command line. Setting DELAY to 0 disables the feature.

Aliases in script files (CR00016977)

Models This enhancement is supported on:

- AT-8948, x900-48
- AT-9900
- AT-9800
- AT-8800
- AT-8600
- AT-8700XL
- Rapier i, Rapier w
- AR44x, AR450S, AR415S
- AR725, AR745
- AR750S, AR770S

Module Script

Description This enhancement enables you to use aliases in commands in script files. The switch expands the aliases when it runs the script (except when it runs the script at start-up).

New in Terminal Server

This section describes new features and enhancements to Telnet, reverse Telnet session management as described in the *Terminal Server* chapter in the *Software Reference for Version 2.9.1* for your router or switch.

Reverse Telnet transparent mode (CR00027944)

Models This enhancement is supported on:

- AT-8800
- Rapier i, Rapier w
- AR44x, AR450S, AR415S
- AR725, AR745
- AR750S, AR770S

Module Telnet

Description A "transparent" mode has been added to reverse Telnet so that a completely transparent reverse Telnet connection can be made to a router asyn port. By default, the transparent mode is off. To enable it, use the new **transparent** parameter in the command:

```
SET RTELnet AUthentication={OFf|ON|NO|YEs|FAlse|TRue}
   TRANSParent={OFf|ON|NO|YEs|FAlse|TRue}
```

New in SNMP MIB

This section describes enhancements to the SNMP MIBs, as described in the *SNMP MIBs* appendix to the *Software Reference for Version 2.9.1* for your router or switch.

For information about changes to SNMP support on your switch or router, see "New in SNMP" on page 174.

AT SysInfo MIB support for memory OID (CR00024907)

Models This enhancement is supported on:

- AT-8948, x900-48
- AT-9900
- AT-9800
- AT-8800
- AT-8600
- AT-8700XL
- Rapier i, Rapier w
- AR44x, AR450S, AR415S
- AR725, AR745
- AR750S, AR770S

Module SNMP MIB

Description The AT SysInfo MIB now supports the memory (1.3.6.1.4.1.207.8.4.4.3.7) OID.

SNMP MIB enhancements for DHCP and Port Authentication (CR00025844)

Models This enhancement is supported on:

- AT-8948, x900-48
- AT-9900
- AT-9800
- AT-8800
- AT-8600
- AT-8700XL
- Rapier i, Rapier w
- AR44x, AR450S, AR415S
- AR725, AR745
- AR750S, AR770S

Module DHCP, portauth, SNMP MIBs

Description This software release introduces the following user interface and Simple Network Management Protocol (SNMP) Management Information Base (MIB) improvements:

The four main areas of enhancements include:

1. A Dynamic Host Configuration Protocol (DHCP) **MIB trap**, triggered on the IP address allocation of a DHCP range exceeding a specified threshold.

   This is achieved via:

   - a new parameter to set a threshold for DHCP pool address usage.
   - an SNMP MIB trap sent to a specified server/NMS to inform it that the DHCP range address pool is about to be exhausted, when the number of leased IP addresses exceed the threshold.

2. Host Name logging to Syslog

   Monitoring of the **hostname** parameter in the DHCP packet. A log message is sent to the syslog server when an IP address is leased. The log contains the following parameters:

   - MAC address of the DHCP Client
   - IP Address leased to the DHCP Client
   - Lease Time allocated to the DHCP Client
   - Port Number that the Client is connected on
   - Management IP Address of DHCP server
   - Name of DHCP Client

3. RADIUS Permit Mode (Authentication automatic invalidity function)

   In a customer's network there are any number of configured RADIUS servers, either IEEE802.1x or MAC Based. If the switch loses contact with ALL RADIUS servers, users are automatically authenticated, bypassing the normal authentication procedures.

   This is achieved via:

   - a new parameter that will enable/disable the automatic authentication functionality.

   When the **Radius Permit Mode** is enabled, the switch will indicate that the RADIUS permit mode is active and the log will contain the following parameters:

- Port Number that the supplicant is connected to
- User Name of the supplicant
- MAC address of the supplicant

4. Authentication-user Limit enhancement

   Currently the authentication-user limit is 480/unit and 320/port. This has been increased to 480/unit and 480/port.

Modified Commands

Selective command descriptions are shown, with changes shown in bold.

The following commands have been modified to implement the requested **DHCP** functionality. These modified commands will be available on ALL devices:

- set dhcp range
- show dhcp client
- show dhcp range

The following commands have been modified to implement the requested **authentication** functionality. These commands will only be available on the AT86 (Rapier) devices:

- enable portauth port
- set portauth port
- show portauth port

set dhcp range

Syntax

```
SET DHCP RANge=name [PRObe={ARP|ICMP}] }]
   [THREshold={ENABLED|DISABLED}] [UPperthreshold=0..100]
   [LOwerthreshold=0..100] [LOG={ENABLED|DISABLED}]
```

Description This command modifies the server's attributes.

The **probe** parameter specifies how the DHCP server checks whether an IP address is being used by other hosts. If **arp** is specified, the server sends ARP requests to determine if an address is in use. If ICMP is specified, the server sends ICMP Echo Requests (pings). The **default** is **icmp**.

Note that **arp** cannot be specified if the range includes a gateway (by specifying the gateway parameter when it was created), or if the network uses Proxy ARP.

The **threshold** parameter determines if an SNMP DHCP MIB trap is generated when the number of allocated IP addresses from a particular range pool exceeds a pre-defined threshold. The **default** setting for this parameter is disabled.

The **upperthreshold** parameter specifies at what percentage of utilised client addresses the SNMP MIB trap should be generated. The **default** is 80% of IP addresses allocated from a particular range pool. The upper threshold value must be equal to or greater than the lower and vice-versa.

The **lowerthreshold** parameter specifies at what percentage of utilised client addresses that the threshold breach is considered to have cleared itself. No trap

will be generated to indicate that the condition has been cleared. The **show dhcp range** command will display the threshold status. The **default** is 75% of IP addresses allocated from a particular range pool.

The **log** parameter specifies whether or not to enable logging of the DHCP clients login. This may generate a lot of log messages depending on refresh timers and clients. The **default** setting for this parameter is enabled.

Example To set the range **office** to use ARP packets to probe IP addresses, an upper threshold of 70% and a lower threshold of 65%, use the command:

```
set dhcp range=office pro=arp thre=ena up=70 lo=65 log=dis
```

Related commands
add dhcp range
create dhcp range
delete dhcp range
destroy dhcp range

show dhcp client

Syntax `SHow DHCP CLIEnt[=ipaddress] [RANge=name] [DETail]`

Description This command displays information about the currently defined range client entries.

If the **range** parameter is specified, then the clients in the specified range are displayed.

If an **IP** address is specified on the **client** parameter, then information for that IP address is displayed.

If the **detail** option is supplied then extra information about the clients is displayed.

Parameter details are contained in Table 49 on page 184.

Details of the show command are shown in Figure on page 183 and Figure on page 184.

Figure 32: Example output from the **show dhcp client** command

```
DHCP Client Entries
IP Address      ClientId          State   Type   Expiry
-------------------------------------------------------------------
202.36.163.14   00-00-c0-00-00-01 unused  static never
202.36.163.20   08-00-5a-a1-02-3f inuse   auto   never
202.36.163.23                     unused  auto   never
202.36.163.28   00-40-10-02-e8-a3 inuse   auto   never
192.168.100.92  00-00-c0-c9-c6-21 inuse   dyn    19-Jun-1997 12:30:51
192.168.100.93                    unused  dyn
192.168.100.118                   reclaim dyn
```

Figure 33: Example output from the **show dhcp client detail** command

```
DHCP Client Entries
IP Address      ClientId          State   Type   Expiry
                Host Name
-------------------------------------------------------------------
202.36.163.14   00-00-c0-00-00-01 unused  static never

202.36.163.20   08-00-5a-a1-02-3f inuse   auto   never

202.36.163.23                     unused  auto   never

202.36.163.28   00-40-10-02-e8-a3 inuse   auto   never

192.168.100.92  00-00-c0-c9-c6-21 inuse   dyn    19-Jun-1997 12:30:51
                DHCP Client
192.168.100.93                    unused  dyn

192.168.100.118                   reclaim dyn
```

Table 49: Parameters in output of the **show dhcp client** command

Parameter	Meaning
Show DHCP CLIENT	
IP Address	IP address from the range of available IP addresses.
ClientId	Hardware address of the client, if any, that has been assigned the IP address.
State	State of the IP address: ■ Unused - not currently in use and is available for assignment ■ Inuse - currently assigned to a client ■ Reclaim - currently being reclaimed
Expiry	Date for dynamically allocated IP addresses.
Hostname	The host name of the client as supplied in the DHCP Request message. Note that by default the Hostname of the client comes from the system name (**set sys name**) and as such has a possible length of 255 characters on the client machine. We have restricted the length of the name we record to 64 characters.

Examples To display detailed information about the clients in a range named **remote**, use the command:

```
sh dhcp clie ran=remote det
```

Related commands
show dhcp
show dhcp policy
show dhcp range

show dhcp range

Syntax `SHow DHCP RANge[=name]`

Description The format of this command is unchanged. The command output has been enhanced to display detailed threshold and **client usage** information.

The details of the new display information are detailed in Table 50 on page 185.

Examples of the new output are detailed in Figure on page 188.

Table 50: Parameters in output of the **show dhcp range** command

Parameter	Meaning
Show DHCP RANGE - "CLIENT INFORMATION"	
Number In Range	The number of clients configured for this range.
Number Allocated	The number of clients actually allocated from this range and in the **inuse** state.
Percentage Allocated	The percentage of **inuse** clients against the clients configured. Note that this is only the **inuse** clients, not the **reclaim** or **unused** clients.
Logging Status	The logging of client connections may be enabled or disabled on a per range basis. This field will display the logging status for this particular range and will display enabled or disabled.
Show DHCP RANGE - "SNMP MIB THRESHOLD INFORMATION"	
Status	This field will display the status of the threshold functionality - enabled or disabled. This will determine if the SNMP DHCP MIB trap is raised when the IP address allocation upper limit threshold has been exceeded.
Upper Limit	The upper client allocation threshold for **Percentage Allocated**. When this limit is exceeded the device will generate an SNMP DHCP MIB trap.
Lower Limit	The lower client allocation threshold for **Percentage Allocated**. This is the value at which the threshold exceed condition is considered to be cleared. It is to stop any hysteresis in the system where the number of clients hover around the upper threshold and generate multiple traps as it rises above and drops below the threshold. Note that there is no SNMP MIB trap generated when the condition is cleared.
SNMP MIB Trap Status	When the **Percentage Allocated** exceeds the **Upper Limit** an SNMP DHCP MIB trap will be generated. This field will then display RAISED. When the **Percentage Allocated** drops below the **Lower Limit** the condition is declared to be cleared and the field will display LOWERED. No SNMP DHCP MIB trap will be generated when the condition is cleared.

Figure 34: Example output from the **show dhcp range** command

```
Manager DHCP Server> sh dhcp range=range2

Name: range2
  Policy ..................... centrecom
  Probe Type ................. ICMP
  Start Address .............. 192.168.2.100
  End Address ................ 192.168.2.104
  Reclaim status ............. Stopped
  Used Address(es) ........... 192.168.2.101
  Free Address(es) ........... 192.168.2.100   192.168.2.102
                               192.168.2.103   192.168.2.104
  Reclaiming Address(es) ..... none
  In DHCP Messages ........... 268
  In Discover Messages ....... 1
  In Request Messages ........ 267
  In Decline Messages ........ 0
  In Release Messages ........ 0
  Out DHCP Messages .......... 268
  Out Offer Messages ......... 1
  Out Ack Messages ........... 267
  Out Nak Messages ........... 0
  In BOOTP Messages .......... 0
  Out BOOTP Messages ......... 0

Client Information:
  Addresses In Range ......... 5
  Addresses Allocated ........ 1
  Percentage Allocated........ 20
  Logging Status ............. ENABLED

SNMP Threshold Information:
  Status ..................... ENABLED
  Upper Limit........ ........ 19
  Lower Limit................. 10
  SNMP MIB Trap Status........ RAISED
```

enable and set portauth port

Syntax

```
ENAble PORTAuth[=8021x] POrt={ALL|switch-port}
   TYpe=Authenticator
   CONTrol={AUTHorised|AUTO|UNauthorised}] [MAXReq=1..10]
   [MODe={MUlti|SIngle}] [PIGgyback={TRue|FAlse}]
   [QUIETperiod=0..65535] [REAUTHENAbled={TRue|FAlse}]
   [REAUTHMax=1..10] [REAUTHPeriod=1..86400]
   [SERVERTimeout=1..60] [SUPPTimeout=1..60]
   [TXperiod=1..65535] [GUEstvlan={1..4094|vlan-name|NONe}]
   [SECurevlan={ON|OFF}]
   [VLANAssignment={ENAbled|DIsabled}]
   [MIBReset={ENAbled|DIsabled}]
   [TRap={SUCcess|FAILure|BOTh|NONe}]
   [AUTOAuthenticate={TRUE|FALSE}]

SET PORTAuth[=8021x] POrt={ALL|switch-port}
   TYpe=AUthenticator
   [CONTrol={AUTHorised|AUTO|UNauthorised}] [MAXReq=1..10]
   [MODe={MUlti|SIngle}][PIGgyback={TRue|FAlse}]
   [QUIETperiod=0..65535][REAUTHENAbled={TRue|FAlse}]
   [REAUTHMax=1..10][REAUTHPeriod=1..86400]
   [SERVERTimeout=1..60][SUPPTimeout=1..60]
   [TXperiod=1..65535] [GUEstvlan={1..4094|vlan-name|NONe}]
   [SECurevlan={ON|OFF}]
   [VLANAssignment={ENAbled|DIsabled}]
   [MIBReset={ENAbled|DIsabled}]
   [TRap={SUCcess|FAILure|BOTh|NONe}]
   [AUTOAuthenticate={TRUE|FALSE}]

ENAble PORTAuth=MACbased POrt={ALL|switch-port}
   [CONTrol={AUTHorised|UNauthorised|AUTO}]
   [REAUTHENAbled={TRue|FAlse}] [REAUTHPeriod=1..86400]
   [QUIETperiod=0..65535] [SECurevlan={ON|OFF}]
   [VLANAssignment={ENAbled|DIsabled}]
   [MIBReset={ENAbled|DIsabled}]
   [TRap={SUCcess|FAILure|BOTh|NONe}]
   [AUTOAuthenticate={TRUE|FALSE}]

SET PORTAuth=MACbased POrt={ALL|switch-port}
   [CONTrol={AUTHorised|UNauthorised|AUTO}]
   [REAUTHENAbled={TRue|FAlse}] [REAUTHPeriod=1..86400]
   [QUIETperiod=0..65535] [SECurevlan={ON|OFF}]
   [VLANAssignment={ENAbled|DIsabled}]
   [MIBReset={ENAbled|DIsabled}]
   TRap={SUCcess|FAILure|BOTh|NONe}]
   [AUTOAuthenticate={TRUE|FALSE}]
```

Description

The **enable portauth** and **set portauth** commands have been amended to incorporate a new automatic authentication value—**AUTOAuthenticate**.

Ordinarily, a user attempts to gain authorisation to join a network by passing certain criteria via an authenticating switch to a RADIUS authentication server. When the RADIUS server is unavailable then all supplicants will be unable to connect to the network as this is deemed a failure to authenticate by the authenticating switch.

Multiple RADIUS servers can be configured (ADD RADIUS). When communication with all RADIUS servers (1-n) is lost then this command will provide the opportunity for the customer to automatically authenticate all users requesting access to the network. The **default** value of this field is FALSE.

SECURITY NOTE: this command exposes the customer to a high degree of vulnerability. When the RADIUS servers return to operational status the clients automatically authenticated will remain authenticated.

Note that there is functionality in the **portauth** (**set portatuh reauthenable** and **reauthperiod**) that will re-authenticate users after a certain timeout period. This functionality is disabled by default and it is recommended that this functionality is enabled in conjunction with the automatic authentication functionality.

The **autoauthenticate** parameter refers exclusively to the authentication switch and will have no effect on the supplicant.

show portauth port

Syntax `SHow PORTAuth[={8021x|MACbased}] POrt={ALL|port-name}`

Description The format of the **show portauth port** command output will be altered to display the AUTOAuthentication status. This is shown in Figure 35 on page 188.

Figure 35: Example output from the **show portauth port** command

```
Manager PAE Auth> sh portauth port=9

Portauth Port Information - 802.1X Based Configuration
---------------------------------------------------------------
Interface: port9
  PAE Type............................. Authenticator

          Authenticator PAE State....... AUTHENTICATING
          Port Status................... unauthorised
          Backend Authenticator State... RESPONSE
          AuthControlPortControl........ Auto
          quietPeriod................... 60
          txPeriod...................... 30
          suppTimeout................... 30
          serverTimeout................. 30
          maxReq........................ 2
          reAuthMax..................... 2
          reAuthPeriod.................. 3600
          reAuthEnabled................. False
          piggyBack..................... True
          keyTransmissionEnabled........ False (not supported)
          adminControlledDirections..... Both (not supported)
          guestVlan..................... None (VLAN ID=0)
          trap.......................... None
          vlanAssignment................ Enabled
          Auto Authenticate............. True
```

Log Message Descriptions

No new logs will be generated by these enhancements. However, existing logs will be updated:

Module	DHCP
Type	LOG_TYPE_DHCP, 27, "DHCP"
SubType	LOG_STY_DHCP_BIND, 1
Severity	LOG_SEV_INFO

Description The existing DHCP log has been updated to reflect the addition of the MAC address, the lease period, the port, the serverId and the client hosts name. The enhanced log has this output:

```
05 15:55:33 3 DHCP DHCP  00001 mac=00-00-cd-1d-9e-b3, ip=192.168.2.101
                                lease=60, port=2, serverId=192.168.2.1,
                               host=DHCP Client
```

Reference field: None

String Format
"mac=%E, ip=%I, lease=%u, port=%p, serverId=%I, host=%s"

Parameters

%I The IP address of the server

%E The MAC address of the server

%p The port number

%s The clients host name.

Routine(s) logged from:

dhcpmain.c: **dhcpLogEvent**

Recommended action: No action is required.

Name	PORTAUTH_LOG_MACBASED_AUTHSUCCESS
Module	DHCP
Type	LOG_TYPE_DHCP, 27, "DHCP"
SubType	LOG_STY_DHCP_BIND, 1
Severity	LOG_SEV_INFO

Description The existing DHCP log has been updated to reflect the addition of a new reason. The enhanced log has this output:

```
05 12:10:24 3 PORT PORTA MACB  Auth Success : Port=port9 User=john
                                 MAC=00-00-cd-05-da-80 PreAuthVLAN=default
                            PostAuthVLAN=default Reason=Auto Auth
```

Reference field: None

String Format

"Auth Success : Port=%w MAC=%E PreAuthVLAN=%s PostAuthVLAN=%s Reason=%s"

Parameters

%w The port as a string "portxx" where xx is the port number.

%I The IP address of the server

%E The MAC address of the server

%s The vlan settings or the success reason. The "reason" field has been enhanced to display the value "Auto Auth" when communication has been lost with the RADIUS server and a timeout has occurred and the "AUTO AUTHENTICATE" field has been set for the range - "SET DHCP RANGE=rangeX AUTOA=TRUE".

Routine(s) logged from:

pamacstate.c: **portAuthMacAuthPaeStateMachineUpdate**

Recommended action

This log indicates that the communication between the switch and the RADIUS server has been lost. There will be additional logs indicating this loss but investigation of this log would be prudent.

Name	PORTAUTH_LOG_AUTHSUCCESS
Module	PORTAUTH
Type	LOG_TYPE_PORTAUTH, 64, "PORTA"
SubType	LOG_STY_PORTAUTH_AUTH, 2, "AUTH
Severity	LOG_SEV_INFO

Description

The existing DHCP log has been updated to reflect the addition of a new reason. The enhanced log has this output:

```
05 12:10:24 3 PORT PORTA AUTH  Auth Success : Port=port9 User=john
                               MAC=00-00-cd-05-da-80 PreAuthVLAN=default
                               PostAuthVLAN=default Reason=Auto Auth
```

Reference field: None

String Format
"Auth Success : Port=%w User=%s MAC=%E PreAuthVLAN=%s PostAuthVLAN=%s Reason=%s"

Parameters

%w The port as a string "portxx" where xx is the port number.

%I The IP address of the server

%E The MAC address of the server

%s The vlan settings or the success reason. The **reason** field has been enhanced to display the value **Auto Auth** when communication has been lost with the RADIUS server and a timeout has occurred and the AUTO AUTHENTICATE field has been set for the range - SET DHCP RANGE=rangeX AUTOA=TRUE.

Routine(s) logged from:

pamain.c: **portAuthAuthSuccessNotify**

Recommended action This log indicates that the communication between the switch and the RADIUS server has been lost. There will be additional logs indicating this loss but investigation of this log would be prudent.

DHCP SNMP MIB TRAPS

The ATL Enterprise MIB will be updated to reflect two new SNMP MIB Traps.

The first trap, dhcpRangeExceededThresholdTrap, will be generated when the number of clients allocated from the range exceed the upper threshold value.

The contents of this SNMP Trap are detailed in Table 51 on page 191.

The MIB definition is detailed in Figure on page 192.

A screen dump of the MIB console is detailed in Figure 37 on page 192.

The second trap, dhcpRangeExceededThresholdClearTrap, will be generated when the number of clients allocated from the range fall below the lower threshold value.

This trap will utilise the same parameters as detailed in Table 51.

The MIB definition is detailed in Figure on page 193.

A screen dump of the MIB console is detailed in Figure 39 on page 193.

Note that the AT-DHCP.MIB file will require updating in the customers configuration to fully interpret the new trap information.

Table 51: SNMP MIB Parameters for the threshold exceeded and cleared traps

Parameter	Meaning
sysUpTime	The duration the system has been in operation.
snmpTrapOID	The Object Identifier (OID) of the trap – dhcpRangeExceededThresholdTrap
dhcpRangeExhaustedInterface	The interface upon which the range resides.
dhcpRangeExceededRange	The name of the DHCP range.
dhcpRangeExceededClients	The number of clients statically allocated to the DHCP range.
dhcpRangeExceededRemaining	The number of DHCP clients that are still available to be allocated.
dhcpRangeExceededPercentage	The current percentage of DHCP clients that are allocated.

Figure 36: SNMP MIB Properties for dhcpRangeExceededThresholdTrap

```
Name:dhcpRangeExceededThresholdTrap

Type:NOTIFICATION-TYPE

OID:1.3.6.1.4.1.207.8.4.4.4.70.0.2
Full Path:
iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).alliedTelesis(207).mi
bObject(8).brouterMib(4).atRouter(4).modules(4).dhcp(70).dhcpTraps(0).dhcpRangeE
xceededThresholdTrap(2)

Module:AT-DHCP-MIB
Parent:dhcpTraps
Prev sibling:dhcpRangeExhaustedTrap

Status:current
Objects:1: dhcpRangeExhaustedInterface
        2: dhcpRangeExceededRange
        3: dhcpRangeExceededClients
        4: dhcpRangeExceededRemaining
        5: dhcpRangeExceededPercentage

Description: This trap is generated when a DHCP client makes a request for an IP
address and a pre-defined usage threshold has been exceeded.
The IP addresses will continue to be allocated until the range is exhausted.
```

Figure 37: SNMP MIB Screen Dump for **dhcpRangeExceededThresholdTrap** (Trap #19)

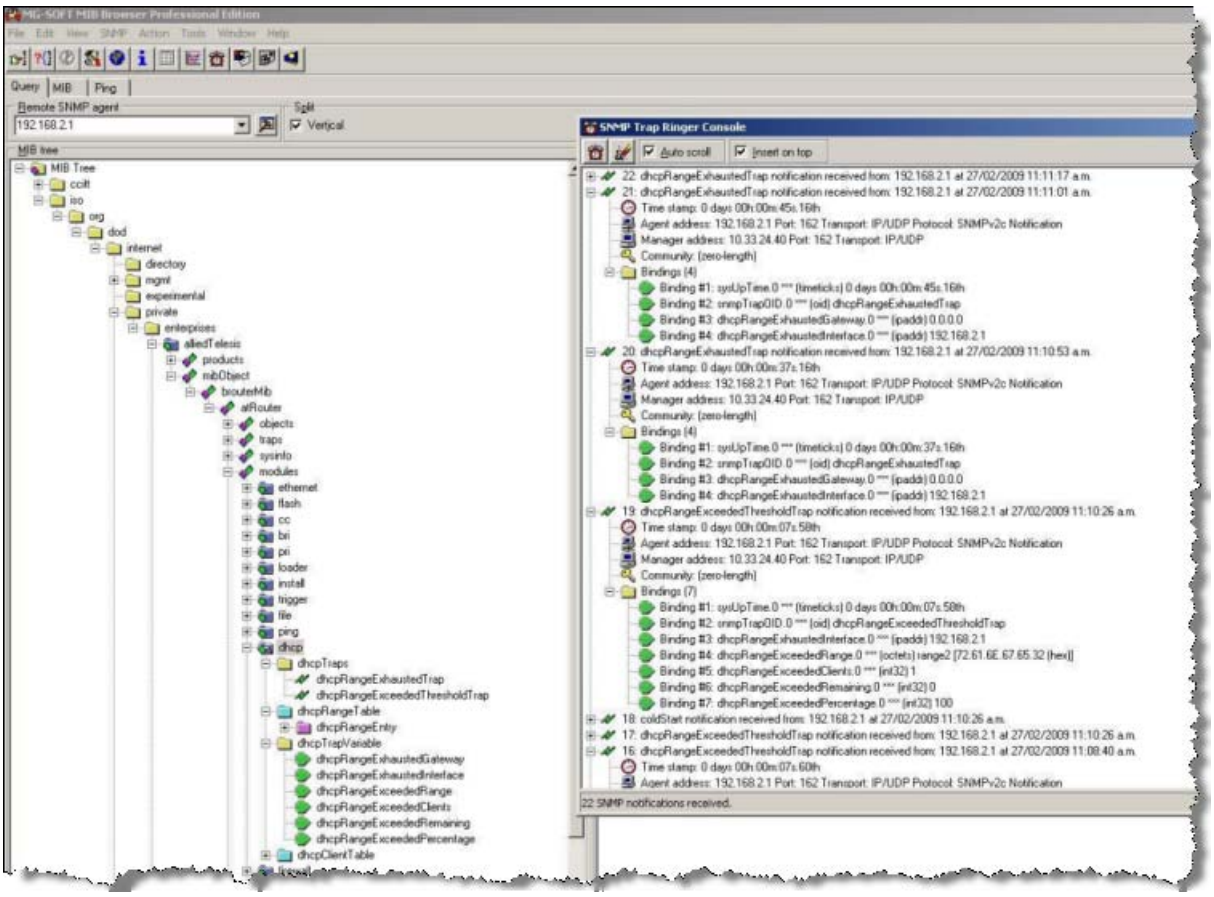
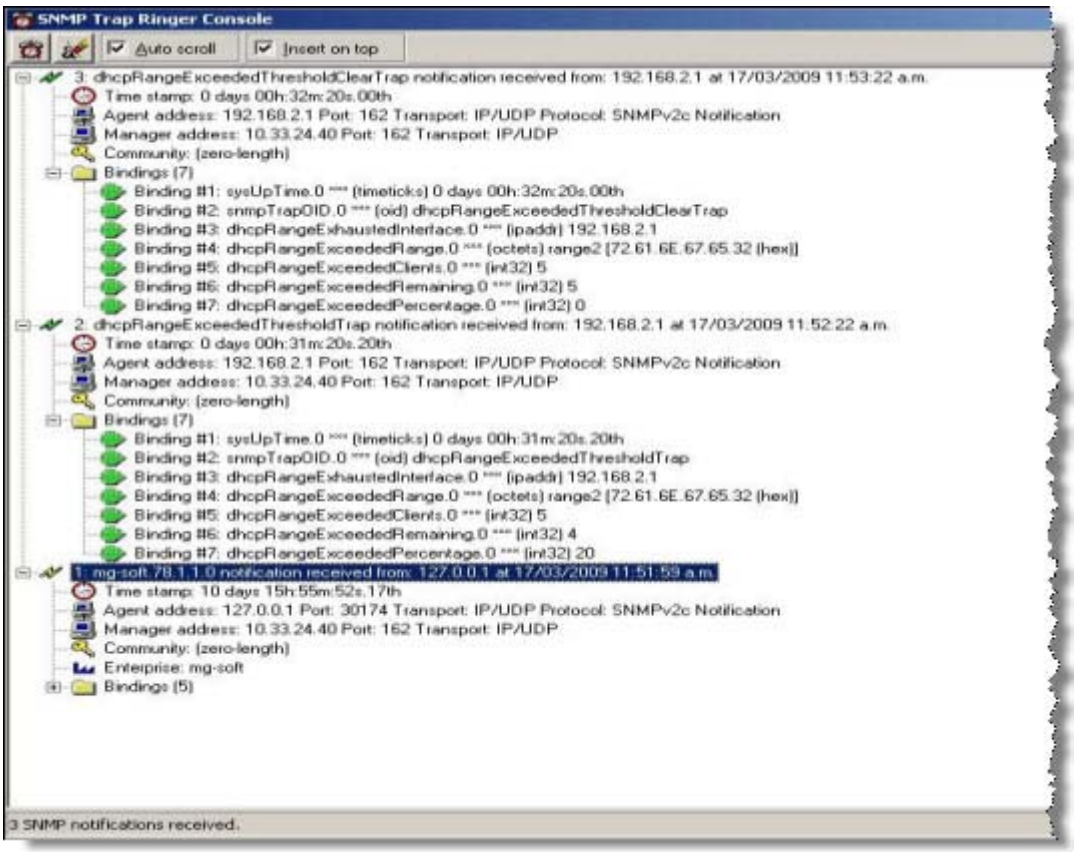


Figure 38: SNMP MIB Properties for dhcpRangeExceededThresholdClearTrap

```
Name:dhcpRangeExceededThresholdClearTrap

Type:NOTIFICATION-TYPE

OID:1.3.6.1.4.1.207.8.4.4.4.70.0.3
Full path:
iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).alliedTelesis(207).mi
bObject(8).brouterMib(4).atRouter(4).modules(4).dhcp(70).dhcpTraps(0).dhcpRangeE
xceededThresholdClearTrap(3)

Module:AT-DHCP-MIB
Parent:dhcpTraps
Prev sibling:dhcpRangeExceededThresholdTrap

Status:current
Objects:1: dhcpRangeExhaustedInterface
        2: dhcpRangeExceededRange
        3: dhcpRangeExceededClients
        4: dhcpRangeExceededRemaining
        5: dhcpRangeExceededPercentage

Description: This trap is generated when the number of allocated clients in a
designated range falls below a pre-defined usage threshold
```

Figure 39: SNMP MIB Screen Dump for dhcpRangeExceededThresholdClearTrap (Trap #3)



IGMP Group MIB (CR00018418)

Models This enhancement is supported on:

- AT-8948, x900-48
- AT-9900
- AT-9800
- AT-8800
- AT-8600
- AT-8700XL
- Rapier i, Rapier w
- AR44x, AR450S, AR415S
- AR725, AR745
- AR750S, AR770S

Module IGMP, MIB

Description 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.

Backing up the configuration with SNMP (CR00016221)

Models This enhancement is supported on:

- AT-8948, x900-48
- AT-9900
- AT-9800
- AT-8800
- AT-8600
- AT-8700XL
- Rapier i, Rapier w
- AR44x, AR450S, AR415S
- AR725, AR745
- AR750S, AR770S

Module Load, MIBs

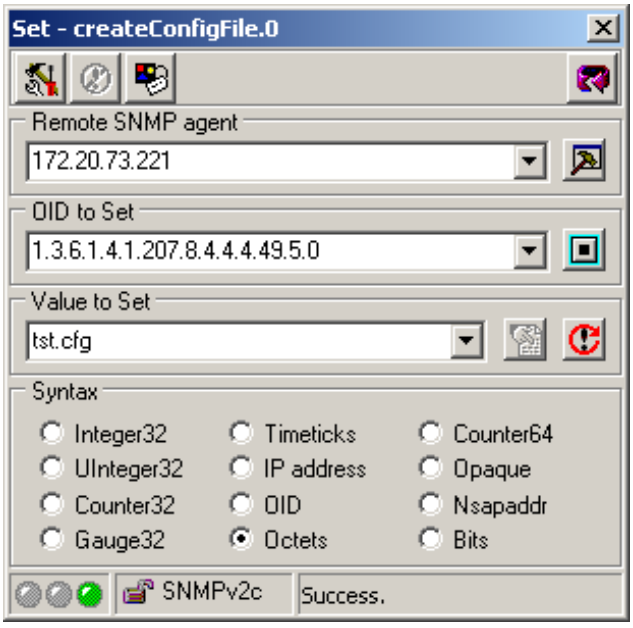
Description With this enhancement, you can use SNMP to:

- 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.

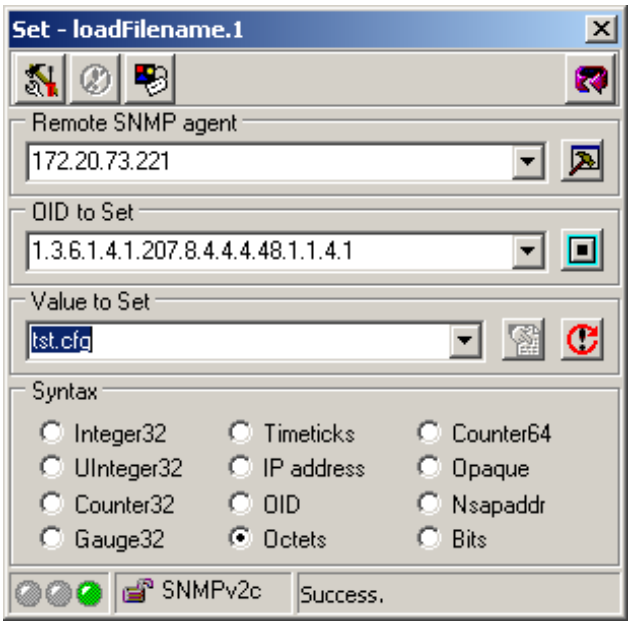
1. Save the configuration

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



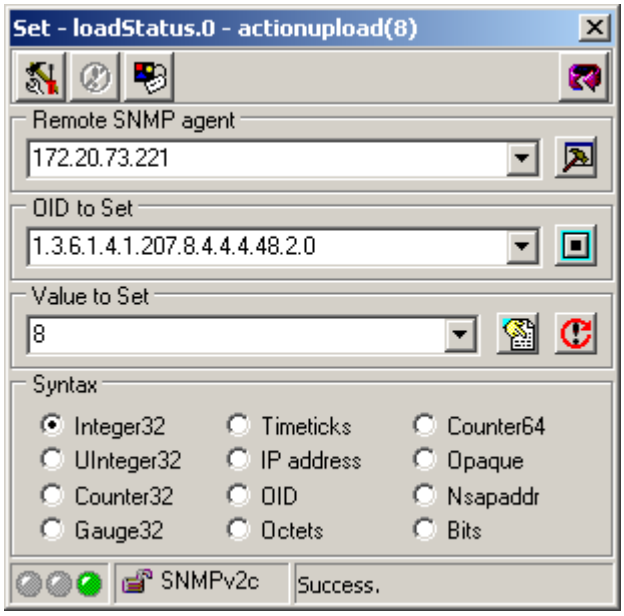
2. Set the load parameters

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.



Resolved Issues

in 2.9.2 Software Maintenance Versions

This software maintenance version includes the resolved issues in the following tables. In the tables, for each product series:

- "Y" in a column indicates that the resolution is available in for that product series.
- "-" in a column indicates that the issue did not apply to that product series.

The issues addressed in this maintenance version 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.

Issues Resolved in 292-07

Software Maintenance Version 292-07 includes the issues resolved in the following tables:

No Level 1 Issues

Level 2

CR	Module	Level	Description	AR44x/AR450S/AR415S	AR7x5	AR750S / AR770S	Rapier i	Rapier w	AT-8800	AT-8600	AT-8700XL	AT-8948 / x900-48	AT-9900	AT-9800
CR00034495	**ISAKMP**	**2**	Previously, when a Windows VPN host using IKE v1 wished to remain connected for longer than 8 hours, the connection sometimes dropped before this time because Windows IKE v1 does not renegotiate the ISAKMP SA, and child SAs, such as an IPSec SA, are normally not allowed to exist if the parent is removed by the host (by an ISAKMP Delete Informational exchange). This issue has been resolved. ISAKMP in AlliedWare can now detect a Windows PC operating in this mode and will allow this IPSec SA to exist until it is renegotiated.	Y	Y	Y	Y	Y	Y	–	–	–	–	–

CR	Module	Level	Description	AR44x/AR450S/AR415S	AR7x5	AR750S / AR770S	Rapier i	Rapier w	AT-8800	AT-8600	AT-8700XL	AT-8948 / x900-48	AT-9900	AT-9800
CR00034753	**ISAKMP**	**2**	Previously, when an IPSec secure connection was configured in transport mode, such as for L2TP over IPSec VPN connections, and an IPSec Security Association is rekeyed by the initiator (VPN host), then during the transition from old to new Security Association, packets were sometimes lost and as a result, a connection may have been attempted from the Responder side. This issue has been resolved.	Y	Y	Y	Y	Y	Y	–	–	–	–	–
CR00034862	**RIP**	**2**	Previously, when using RIP, some routes were deemed unusable (set to metric 16) when the route was actually still available. This issue has been resolved.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR00034934	**L2 Switching**	**2**	Previously, using the **set swi buffer** command on an AR750S sometime resulted in a system reboot. This issue has been resolved.	–	–	Y	–	–	–	–	–	–	–	–
CR00034972	**IPsec**	**2**	Previously, when an old IPSec SA was deleted by an IPsec delete message after IPSec SA's rekey, an associated route, created by a route template was sometimes also deleted. This issue has been resolved.	Y	Y	Y	Y	Y	Y	Y	–	–	–	–

Level 3

CR	Module	Level	Description	AR44x/AR450S/AR415S	AR7x5	AR750S / AR770S	Rapier i	Rapier w	AT-8800	AT-8600	AT-8700XL	AT-8948 / x900-48	AT-9900	AT-9800
CR00033273	**IPv6**	**3**	Previously, a unique link local IPv6 unicast address beginning with FC or FD (as defined in RFC4193) could not be assigned to an interface. This issue has been resolved.	Y	Y	Y	Y	Y	Y	–	–	Y	Y	Y
CR00034382	**Ping**	**3**	Previously, an ICMP packet with an ICMP checksum of all zeroes would result in the packet being dropped. This issue has been resolved.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR00034546	**IPv6**	**3**	Previously, if the IPv6 address configured to specify an IPv6 over IPv4 tunnel was a link local address but was different from the automatically generated link local address, the tunnel selection in IPv6 routing sometimes failed, causing some packets to be lost. This issue has been resolved.	Y	Y	Y	Y	Y	Y	–	–	Y	Y	Y
CR00034839	**ARP**	**3**	Previously, if a supplicant was authorised using MAC-based port authentication on a port and then connected to a different port without disconnecting the first port (e.g., if the host is connected to a intermediate device), then the process of removing the duplicate ARP entry from the original port caused other entries to be removed. This issue has been resolved.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y

Level 4

CR	Module	Level	Description	AR44x/AR450S/AR415S	AR7x5	AR750S / AR770S	Rapier i	Rapier w	AT-8800	AT-8600	AT-8700XL	AT-8948 / x900-48	AT-9900	AT-9800
CR00033711	**PKI**	**4**	Previously, it was possible to specify **pki** as an unnecessary optional parameter in the **set pki** command: `set pki pki` This issue has been resolved—the extra **pki** is no longer an option for this command.	Y	Y	Y	Y	Y	Y	–	–	–	–	–

Issues Resolved in 292-06

Software Maintenance Version 292-06 includes the issues resolved in the following tables:

No Level 1 Issues

Level 2

CR	Module	Level	Description	AR44x/AR450S/AR415S	AR7x5	AR750S / AR770S	Rapier i	Rapier w	AT-8800	AT-8600	AT-8700XL	AT-8948 / x900-48	AT-9900	AT-9800
CR00033710	**L2 Switching**	**2**	Under network loop conditions, when using subnet-based VLANs it was possible for static FDB entries to be removed from the FDB. This issue has been resolved.	–	–	–	–	–	–	–	–	Y	Y	Y

Level 3

CR	Module	Level	Description	AR44x/AR450S/AR415S	AR7x5	AR750S / AR770S	Rapier i	Rapier w	AT-8800	AT-8600	AT-8700XL	AT-8948 / x900-48	AT-9900	AT-9800
CR00034357	**PIM-SM v4**	**3**	Previously, if the rendezvous point (RP) in use by a PIM sparse mode route became unreachable for an extended period of time and no other RP was available, the routes may not have recovered correctly when the RP became reachable again. This issue has been resolved.	–	–	–	Y	Y	Y	Y	–	Y	Y	Y
CR00034376	**PPPoE**	**3**	Previously it was not possible to set the **padtunknown** parameter on a PPP template. Because of this, the behaviour defaulted to not sending a PADT in response to a PPPoE frame with an unknown session ID. This issue has been resolved by supporting the **padtunknown** parameter on PPP templates. See "PPPOE Ignore Unknown Session (CR00032988 & CR00034376)" on page 52	Y	Y	Y	Y	Y	Y	–	–	Y	Y	Y
CR00034410	**L2TP**	**3**	If a Layer 2 Tunnelling Protocol connection request (L2TP SCCRQ) was received while a connection from the same remote peer and port was already being established, then a STOPCCN would be sent in reply to the second request. This resulted in the first connection being unable to be established. This issue has been resolved. Now the second SCCPRQ is recognized as a retransmission and is ignored, allowing the connection in progress to proceed.	Y	Y	Y	Y	Y	Y	–	–	Y	Y	Y

Issues Resolved in 292-05

Software Maintenance Version 292-05 includes the issues resolved in the following tables:

No Level 1 Issues

Level 2

CR	Module	Level	Description	AR44x/AR450S/AR415S	AR7x5	AR750S / AR770S	Rapier i	Rapier w	AT-8800	AT-8600	AT-8700XL	AT-8948 / x900-48	AT-9900	AT-9800
CR00033210	**IPSec**	**2**	When using a route template with IPSec, the route associated with a policy bundle may have beeen incorrectly deleted or retained, depending on the situation. This was due to the template route being deleted when the latest SA was deleted by the **delete payload** message from the peer. This issue has been resolved.	Y	Y	Y	Y	–	Y	–	–	–	–	–
CR00034075	**ETH**	**2**	Previously, a ping via another interface from a remote host to an IP address associated with a disabled Ethernet port on an **AR770** could result in a system reboot. This issue has been resolved.	–	–	Y	–	–	–	–	–	–	–	–

CR	Module	Level	Description	AR44x/AR450S/AR415S	AR7x5	AR750S / AR770S	Rapier i	Rapier w	AT-8800	AT-8600	AT-8700XL	AT-8948 / x900-48	AT-9900	AT-9800
CR00034117	**Link Aggregation RSTP**	**2**	It was possible for the STP port state of an aggregated port to be different from the STP port state of the aggregator Master port. This issue has been resolved.	–	–	–	Y	Y	Y	Y	Y	Y	Y	Y
CR00030778	**SQoS**	**2**	When the ethernet port speed is set to 10M, there is an SQoS performance hit when mainly low-priority traffic is available. A new parameter has been added to the **set eth** command called **SQoSmaxqlen**, that allows the user to tweak the SQoS maximum queue length to suit the type of network traffic. SQoSmaxqlen can be set within the range of 1kB to 12.5kB, and it has been found that 10.15kB provides the optimum balance between performance and latency for higher priority traffic.	–	–	–	–	–	–	–	–	–	–	–

Level 3

CR	Module	Level	Description	AR44x/AR450S/AR415S	AR7x5	AR750S / AR770S	Rapier i	Rapier w	AT-8800	AT-8600	AT-8700XL	AT-8948 / x900-48	AT-9900	AT-9800
CR00032639	**IPSec**	**3**	Previously, some VPN hosts (such as Android phones) using L2TP over IPSec in transport mode which specify port 0 during IPSec negotiation and have port numbers dynamically allocated using NAT-T, were incorrectly handled and could result in connection failure if more than one remote device was connecting. All other ports were handled appropriately, but specifically port 0 was not treated as a dynamic port. This issue has been resolved.	Y	Y	Y	Y	–	Y	–	–	–	–	–
CR00033201	**OSPFv2**	**3**	In OSPF, when alternate routes existed to an AS boundary router, the AS Summary LSA generated by the Area Border Router when one of the paths changed may have been incorrect until the next refresh of the AS Summary LSA. This could lead to temporary incorrect routing or perceived slow updates into the backbone area by the ABR. This has been corrected so the AS Summary LSA is correct and updated immediately at the backbone.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR00033844	**ISAKMP**	**3**	When ISAKMP detected an unexpected address or dynamic port change in an established session, the counter msgRxBadPortIpChange would increment. However, this action also would also result in a slow memory leak. The memory leak has been rectified.	Y	Y	Y	Y	–	Y	–	–	–	–	–

CR	Module	Level	Description	AR44x/AR450S/AR415S	AR7x5	AR750S / AR770S	Rapier i	Rapier w	AT-8800	AT-8600	AT-8700XL	AT-8948 / x900-48	AT-9900	AT-9800
CR00034078	**SNMP MIB Support**	**3**	When querying the status of the 2nd PSU via SNMP, the details of the 1st PSU may be returned instead. OID information: PSU bay 2 of fanAndPsPsuFan MIB(OID:.1.3.6.1.4.1.207.8.4.4.3.1.11.1.4.2) This issue has been resolved.	–	–	–	–	–	–	–	–	Y	–	–
CR00034079	**IPSec ISAKMP**	**3**	If the router is configured as a responder with **peer=any**, using a single policy for ISAKMP, then connections from behind a remote NA(P)T device are all established with the same peer address and policy (port numbers are unique). In this case, checks to determine if a new connection is a rekey of a previous ISAKMP SA were invalid because this distinction cannot be made conclusively and would lead to activity counters being counted incorrectly. When the ISAKMP policy is configured with **rekey=true**, this could lead to the router being unable to properly distinguish the SA's to the remote clients behind the remote NA(P)T device. These issues have been resolved.	Y	Y	Y	Y	–	Y	–	–	–	–	–

CR	Module	Level	Description	AR44x/AR450S/AR415S	AR7x5	AR750S / AR770S	Rapier i	Rapier w	AT-8800	AT-8600	AT-8700XL	AT-8948 / x900-48	AT-9900	AT-9800
CR00034097	**IPSec ISAKMP**	**3**	The ISAKMP **rekey** option is used to allow compatibility with VPN devices which ignore negotiation of a connection expiry value that is lower at the responder side than the initiator. The **rekey** option is only valid when the router is configured as a responder using **peer=any** in the policy configuration. When the policy is created, the check for rekey option was correct, however, it was possible to change the configuration to a value other than peer=any once the rekey option was set true. This would result in an invalid configuration. This issue has been resolved.	Y	Y	Y	Y	–	Y	–	–	–	–	–

Issues Resolved in 292-04

Software Maintenance Version 292-04 includes the issues resolved in the following tables:

No Level 1 Issues

Level 2

CR	Module	Level	Description	AR44x/AR450S/AR415S	AR7x5	AR750S / AR770S	Rapier i	Rapier w	AT-8800	AT-8600	AT-8700XL	AT-8948 / x900-48	AT-9900	AT-9800
CR00032336	**MSTP**	**2**	There was an MSTP issue that meant that transitory inter-regional loops could occur in VLANs assigned to an MSTI when a region experienced a change in CIST regional root. This issue has been resolved.	–	–	–	Y	Y	Y	Y	Y	Y	Y	Y
CR00032372	**PIM-SM v4**	**2**	In certain addressing schemes it was possible for the multicast hardware table and its software shadow to become out of sync, eventually resulting in multicast data stream loss. This was only possible if the VLAN ID and multicast group address were the same for two entries but those two entries' source addresses were more than 128.0.0.0 IP addresses apart. This issue has been resolved.	–	–	–	Y	Y	Y	Y	–	Y	Y	Y

CR	Module	Level	Description	AR44x/AR450S/AR415S	AR7x5	AR750S / AR770S	Rapier i	Rapier w	AT-8800	AT-8600	AT-8700XL	AT-8948 / x900-48	AT-9900	AT-9800
CR00032910	**OSPF**	**2**	With MD5 authentication enabled on OSPF interfaces, there was a possibility that sending OSPF packets may have occasionally resulted in a system reboot in the case when larger LSUs (associated with large OSPF area routing domains) were being flooded to a neighbour. This issue has been resolved.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR00032930	**IPSEC ISAKMP**	**2**	When IPSec Security Authorisations (SAs) were set to timeout and renegotiate in multiples of time of the ISAKMP SAs, then it was possible for a new IPSec SA to be established over the older expiring ISAKMP SA. In this case, when the older ISAKMP SA was deleted when it expired, it also removed the IPSEC SA. However, if a newer ISAKMP SA had already been renegotiated, then the IPSEC SA should have been switched to the new one and the IPSEC SA should have been unaffected by the expiration of the old ISAKMP SA. This has been corrected to maintain the IPSEC SA as long as there is a valid and active ISAKMP SA negotiated.	Y	Y	Y	Y	–	Y	–	–	–	–	–
CR00033045	**BGP**	**2**	If in BGP, a peer sends an update message very soon after (or included with) the first keepalive message, then there was a possibility that the update message was not processed, resulting in routes contained in the update message not appearing in the route table. This issue has been resolved.	Y	Y	Y	Y	Y	Y	–	–	Y	Y	Y

CR	Module	Level	Description	AR44x/AR450S/AR415S	AR7x5	AR750S / AR770S	Rapier i	Rapier w	AT-8800	AT-8600	AT-8700XL	AT-8948 / x900-48	AT-9900	AT-9800
CR00033101	**OSPFv2**	**2**	On devices with slower network connections running OSPF with a relatively large number of LSAs (4000+) being stored, if there was an event which triggered a large number of those LSAs to be deleted, only to be reinstated by the reversal of this event, then on rare occasions it was possible for a system reboot to occur. This issue has been resolved.	Y	Y	-	-	-	-	-	Y	-	-	-
CR00033522	**OSPFv2**	**2**	Previously, when a large number of static interfaces were exported as External LSAs in an OSPF network and MD5 authentication was used, it was possible for packets to become lost and for neighbour relationships to stay in 'loading' state whenever a large number of LSAs had to be updated simultaneously. For example, if one end resets OSPF or a device is restarted. Under normal operations this has a low likelihood of occurring. The system typically recovered on its own if the number of LSAs to update decreases. This issue has been resolved.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR00030778	**SQOS**	**2**	When the Ethernet port speed is set to 10M, there is an SQoS performance hit when mainly low-priority traffic is available. A new parameter has been added to the **SET ETH** command called **SQOSmaxqlen**, that allows the user to tweak the SQoS maximum queue length to suit the type of network traffic. **SQOSmaxqlen** can be set within the range of 1kB to 12.5kB, and it has been found that 10.15kB provides the optimum balance between performance and latency for higher priority traffic.	–	–	–	–	–	–	–	–	–	–	–

Level 3

CR	Module	Level	Description	AR44x/AR450S/AR415S	AR7x5	AR750S / AR770S	Rapier i	Rapier w	AT-8800	AT-8600	AT-8700XL	AT-8948 / x900-48	AT-9900	AT-9800
CR00030494	**IGMP Snooping**	**3**	Previously, on x8900 and x900 switches, control protocols using registered multicast (MC) addresses (e.g. RIPm OSPF) were throttled along with all other MC UDP traffic if **igmpmaxudp** was set greater than 0 (default is 100). This issue has been resolved so that control protocols are now unaffected by the throttling mechanism.	–	–	–	–	–	–	–	–	Y	Y	–

Level 4

CR	Module	Level	Description	AR44x/AR450S/AR415S	AR7x5	AR750S / AR770S	Rapier i	Rapier w	AT-8800	AT-8600	AT-8700XL	AT-8948 / x900-48	AT-9900	AT-9800
CR00033023	**IPSec**	**4**	In IPSec, when a local configuration had many IPSec policies with peer=DYNAMIC or peer=ANY, then 'initial contact' notification from the IPSec initiator may have incorrectly triggered DNS lookups with a null DNS name, producing a log message: "Unable to resolve empty name to IP address;lookup required to match isakmp/IPsec policy" There was no service impact, but unnecessary log messages may have resulted for each affected IPSec policy. This issue has been resolved.	Y	Y	Y	Y	–	Y	–	–	–	–	–

Issues Resolved in 292-03

Software Maintenance Version 292-03 includes the issues resolved in the following tables.

No Level 1 Issues

Level 2

CR	Module	Level	Description	AR44x/AR450S/AR415S	AR7x5	AR750S / AR770S	Rapier i	Rapier w	AT-8800	AT-8600	AT-8700XL	AT-8948 / x900-48	AT-9900	AT-9800
CR00032515	**OSPFv2**	**2**	In an OSPF network where there are two paths to the same subnet, if the path with the lowest cost becomes unreachable under conditions other than an interface failure (for example the port is disabled), then is restored, a summary LSA at the Area Border Router (ABR) will not always regenerate the summary Link State Advertisment (LSA), thus leaving no route to this subnet in the backbone network. This issue has been resolved and ensures the summary Link State Advertisement is generated.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR00032727	**IPSec**	**2**	On an IPSec connection, if the IPSec SA expiry on the initiating client end is set higher than on the responding side, then an unexpected reboot could occur on the responding side. This issue has been resolved.	Y	Y	Y	Y	Y	Y	–	–	–	–	–

CR	Module	Level	Description	AR44x/AR450S/AR415S	AR7x5	AR750S / AR770S	Rapier i	Rapier w	AT-8800	AT-8600	AT-8700XL	AT-8948 / x900-48	AT-9900	AT-9800
CR00032701	**BGPv4**	**2**	If a routemap for route importation is added to BGP using the command line and the routemap is configured to exclude previously imported routes, then BGP will not perform the exclude operation on those routes. This issue has been resolved.	Y	Y	Y	Y	Y	Y	Y	–	–	Y	Y
CR00032813	**ISAKMP**	**2**	Previously, if several ISAKMP peers attached to a router were started at the same time, a small number of them would lose the route created by the route template, and could not be re-negotiated. This issue has been resolved.	Y	Y	Y	Y	Y	Y	–	–	–	–	–

Level 3

CR	Module	Level	Description	AR44x/AR450S/AR415S	AR7x5	AR750S / AR770S	Rapier i	Rapier w	AT-8800	AT-8600	AT-8700XL	AT-8948 / x900-48	AT-9900	AT-9800
CR00032365	**Reverse Telnet**	**3**	Previously a Windows Telnet connection to rtelnet closed with Ctrl-D could block other rtelnet connections for the next two minutes. This issue has been resolved.	Y	Y	Y	Y	Y	Y	–	–	–	–	–

CR	Module	Level	Description	AR44x/AR450S/AR415S	AR7x5	AR750S / AR770S	Rapier i	Rapier w	AT-8800	AT-8600	AT-8700XL	AT-8948 / x900-48	AT-9900	AT-9800
CR00032467	**TCP**	**3**	If two ends of a TCP connection are closed at the same time - for example, when BGP peers simultaneously lose connectivity, with data remaining still to be sent, then if the TCP connection is restored before t he original TCP connection has timed out, TCP's attempt to deliver the last remaining packets from the original TCP connection and then close that connection may result in some unnecessary retransmissions. There is no impact on the ability of TCP to eventually close the connection or to reconnect. This issue has been resolved and ensures no unnecessary transmissions occur as a result of the original TCP connection drop.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y

Level 4

CR	Module	Level	Description	AR44x/AR450S/AR415S	AR7x5	AR750S / AR770S	Rapier i	Rapier w	AT-8800	AT-8600	AT-8700XL	AT-8948 / x900-48	AT-9900	AT-9800
CR00032768	**PPP**	**4**	If a PPP interface description field was not set or if the field was eliminated using the command 'set ppp desc=" " ', then when the ppp interface configuration is displayed or the ppp interface limits displayed using the show commands then invalid characters were displayed in place of the empty description name. This issue has been resolved.	Y	Y	Y	Y	Y	Y	Y	–	–	Y	Y

Issues Resolved in 292-02

Software Maintenance Version 292-02 includes the issues resolved in the following tables.

No Level 1 Issues

Level 2

CR	Module	Level	Description	AR44x/AR450S/AR415S	AR7x5	AR750S / AR770S	Rapier i	Rapier w	AT-8800	AT-8600	AT-8700XL	AT-8948 / x900-48	AT-9900	AT-9800
CR00032472	**PIM-SM**	**2**	Previously, if there was a dynamic change of unicast route towards the RPF source referenced by PIM sparse mode, a system reboot could occur. This issue has been resolved.	Y	Y	Y	Y	Y	Y	Y	–	Y	Y	Y

Level 3

CR	Module	Level	Description	AR44x/AR450S/AR415S	AR7x5	AR750S / AR770S	Rapier i	Rapier w	AT-8800	AT-8600	AT-8700XL	AT-8948 / x900-48	AT-9900	AT-9800
CR00029800	**OSPFv2**	**3**	Previously, when OSPF interfaces were defined as non-broadcast, then under certain circumstances, the OSPF Link State Update (LSU) packets were sent as multicast instead of unicast. This issue has been resolved.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR00030816	**ISAKMP**	**3**	Previously, on very rare occasions, a system reboot could occur when ISAKMP tried to send a Notify message. This issue has been resolved.	Y	Y	Y	Y	Y	Y	–	–	–	–	–
CR00032024	**SFP**	**3**	Previously, aggregate trunk groups set up on an AT-8648 over the uplinks ports using the SFP sockets would not pass traffic. This issue has been resolved.	–	–	–	–	–	–	Y	–	–	–	–
CR00032119	**ISAKMP** **IPsec**	**3**	Previously, if IPsec/ISAKMP configuration used an IP address to describe the peer address (instead of using unresolved DNS addresses), then when IPsec was disabled, ISAKMP Informational packets with the delete payloads may have been sent to the wrong peer. This issue has been resolved.	Y	Y	Y	Y	Y	Y	–	–	–	–	–
CR00032259	**IPsec** **Route template**	**3**	Previously, when an IPsec bundle expired, it would remove the route template route entry associated with the IPsec bundle if no traffic was present, even if the bundle had been updated. This has been resolved to ensure the route is retained during IPsec update.	Y	Y	Y	Y	Y	Y	–	–	–	–	–

CR	Module	Level	Description	AR44x/AR450S/AR415S	AR7x5	AR750S / AR770S	Rapier i	Rapier w	AT-8800	AT-8600	AT-8700XL	AT-8948 / x900-48	AT-9900	AT-9800
CR00032388	**BGP**	**3**	Previously, in BGP, when a routemap with more than one entry was applied as an outgoing routemap to a BGP peer across different prefixes, then parameters which were to be to set by the routemap may not have been correctly applied. This issue has been resolved.	Y	Y	Y	Y	Y	Y	–	–	Y	Y	Y
CR00032401	**LDF**	**3**	Previously, if LDF packets were sent with an 802.1Q tag in their header, and the 802.1p value in that tag as non-zero, then the LDF packet was incorrectly processed when received. This caused the LDF feature to fail to detect Layer-2 loops. This issue has been resolved.	–	–	–	Y	Y	Y	Y	Y	–	–	–
CR00032494	**DHCP snooping**	**3**	Previously, when using DHCP snooping and BOOTP relay, DHCP packets were dropped before being processed by BOOTP relay. This resulted in DHCP clients failing to receive a DHCP allocated IP address. This issue has been resolved.	–	–	–	Y	Y	Y	Y	Y	–	–	–

Issues Resolved in 292-01

Software Maintenance Version 292-01 includes the issues resolved since 291-23 in the following tables.

No Level 1 Issues

Level 2

CR	Module	Level	Description	AR44x/AR450S/AR415S	AR7x5	AR750S / AR770S	Rapier i	Rapier w	AT-8800	AT-8600	AT-8700XL	AT-8948 / x900-48	AT-9900	AT-9800
CR00028315	**Firewall**	**2**	Previously, under sustained high rates of TCP SYN traffic arriving at the firewall public interface (for example an extended TCP Syn attack), Firewall TCP handling could become unstable, which eventually may have resulted in a system reboot. This issue has been resolved. The Firewall now withstands high rates of TCP SYN traffic for extended periods of time.	Y	Y	Y	Y	Y	Y	–	–	–	–	Y

CR	Module	Level	Description	AR44x/AR450S/AR415S	AR7x5	AR750S / AR770S	Rapier i	Rapier w	AT-8800	AT-8600	AT-8700XL	AT-8948 / x900-48	AT-9900	AT-9800
CR00029716	**IPsec**	**2**	Previously, the following issues prevented interoperation with some other vendors' equipment when they were configured with a transform equivalent to data protected by tunneled ESP with a tunneled authenticated header (AH) (e.g., crypto ipsec transform-set ex1 ah-sha-hmac esp-des esp-sha-hmac), which is the equivalent to an AlliedWare bundle specification of 'ESP and AH'. ■ AlliedWare did not accept IPsec transforms of ESP and AH when presented in an order different (though technically equivalent) to the way in which the AlliedWare devices store the same set of transforms. This issue has been resolved. ■ For improved compatibility, AlliedWare now supplies IPsec Transforms selected in the same order that the far end has sent them to the AlliedWare device (as long as the AlliedWare and peer device transforms match), rather than the order in which AlliedWare stores the transforms. ■ The combination of ESP and AH tunneling protocols produced two outer headers in the IP packet, which could affect interoperability with some vendors' equipment. This was the case for both IPv4 and IPv6.This issue has been resolved. Now, packets contain a single AH outer header followed by the ESP encrypted packet.	Y	Y	Y	Y	Y	Y	–	–	–	–	–
CR00029754	**IPsec**	**2**	Previously, an IPSec Security Association could not be established in ISAKMP aggressive mode when the peer was configured to use Fully Qualified Domain Name (FQDN) user id. This issue has been resolved.	Y	Y	Y	Y	Y	Y	–	–	–	–	–

CR	Module	Level	Description	AR44x/AR450S/AR415S	AR7x5	AR750S / AR770S	Rapier i	Rapier w	AT-8800	AT-8600	AT-8700XL	AT-8948 / x900-48	AT-9900	AT-9800
CR00030433	**SQoS ETH**	**2**	Previously, if an AR750S Eth port operating at speed 10Mbps under high traffic loading was reset (**reset eth** command), the port would sometimes incorrectly requeue packets when data transmission was controlled by a software QoS policy. This could result in an unnecessary buildup of the ethernet transmission queue and subsequent data loss. This issue has been resolved. The ethernet transmission queue is now appropriately cleared.	–	–	Y	–	–	–	–	–	–	–	–
CR00030736	**Firewall**	**2**	Previously, when the firewall was enabled, a specialised TCP DoS attack could occasionally overwhelm the firewall event queue, and result in a system reboot. This issue has been resolved.	Y	Y	Y	Y	Y	Y	–	–	–	–	Y
CR00031372	**IPv4 multicast**	**2**	Previously, routed multicast data would not flow correctly when the upstream interface was a VLAN and the downstream interface was a non-VLAN interface, resulting in unnecessary multicast data loss. This issue has been resolved.	Y	Y	Y	Y	Y	–	–	–	–	–	–

CR	Module	Level	Description	AR44x/AR450S/AR415S	AR7x5	AR750S / AR770S	Rapier i	Rapier w	AT-8800	AT-8600	AT-8700XL	AT-8948 / x900-48	AT-9900	AT-9800
CR00029713	**Firewall**	**2**	Previously, if a firewall private interface could only be identified after a NAT rule was applied on a public interface policy (for instance, if neither interface NAT nor load balancing were configured that reference the private interface), then the firewall sometimes set the internal destination interface incorrectly (though it routed the packet correctly). This could affect the source interface for packets which the firewall generated on behalf of the host (for example, for TCP sessions). If policy-based routing was configured, this issue resulted in incorrect routing of the packet because the source interface no longer matched the policy filter. This issue has been resolved.	Y	Y	Y	Y	Y	Y	–	–	–	–	Y
CR00029632	**ETH**	**2**	When an ETH interface on an AR750S was reset, or the speed of the ETH interface on an AR415S was set, the interface would very occasionally stop receiving packets successfully. Sometimes this would also happen when the ETH interface speed was forced to 10Mbps or 100Mbps and the cable was quickly removed and reinserted twice. These issues have been resolved.	Y	Y	Y	–	–	–	–	–	–	–	–
CR00031526	**PKI**	**2**	Previously, if a PKI certificate's serial number had a leading zero, it could not be revoked by adding a corresponding certificate revokation list (CRL). This could allow an IPsec VPN connection to be formed with a neighbour using a revoked PKI certificate instead of being blocked. This issue has been resolved. Note, if the CRL is subsequently deleted, the certificate will remain untrusted until a reboot occurs.	Y	Y	Y	Y	Y	Y	–	–	–	–	–

CR	Module	Level	Description	AR44x/AR450S/AR415S	AR7x5	AR750S / AR770S	Rapier i	Rapier w	AT-8800	AT-8600	AT-8700XL	AT-8948 / x900-48	AT-9900	AT-9800
CR00031765	**DVMRP IGMP**	**2**	Previously, if a multicast client joined a group where the client's interface was the same interface as the multicast soure, and DVMRP was used on the same interface, then the client was not added to receive the multicast stream. This issue has been resolved.	Y	Y	Y	Y	Y	Y	–	–	Y	Y	Y
CR00029328	**DHCP**	**2**	A user-defined DHCP option that used a predefined DHCP option number would append a blank space ASCII character to a string-type value. The extraneous blank space has now been eliminated. This issue has been resolved.	–	–	–	Y	Y	Y	Y	Y	Y	–	–
CR00029532	**Firewall**	**2**	Previously, when adding dynamic interfaces to a firewall policy using the **add firewall policy interface** command, the **trustprivate** parameter could be entered, but had no effect on the configuration of behaviour of the firewall. This issue has been resolved. For a description of the **trustprivate** parameter for dynamic and static interfaces, see "Security enhancement for untrusted private firewall interfaces (CR00029643)" on page 133.	Y	Y	Y	Y	Y	Y	–	–	–	–	Y
CR00029818	**L2 switching**	**2**	Previously, deleting a port from a tagged VLAN would inadvertently delete the port from all VLANs of which it was a tagged member.	–	–	–	–	–	–	–	–	Y	Y	Y

CR	Module	Level	Description	AR44x/AR450S/AR415S	AR7x5	AR750S / AR770S	Rapier i	Rapier w	AT-8800	AT-8600	AT-8700XL	AT-8948 / x900-48	AT-9900	AT-9800
CR00029884	**IGMP**	**2**	Previously, when IGMP snooping was disabled, local IGMP member(s) might not have received a multicast stream if the same interface received a multicast routing protocol which was interpreted by the switch as a signal to stop sending traffic on the interface, such as DVMRP prune, PIM leave etc. This issue has been resolved.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR00029088	**IPv6**	**2**	Previously, if the device was experiencing heavy IPv6 traffic over a secure connection (for example using protocol=ESP) it may have suffered a system reboot. This issue has been resolved.	Y	Y	Y	Y	Y	Y	Y	–	–	Y	Y
CR00029804	**L2 switching**	**2**	Previously, when a frame was padded to the Ethernet minimum of 64 bytes it could have been padded with up to 3 bytes more. This was standard-compliant, but some vendor equipment rejects packets that are padded more than is strictly necessary. This issue has been resolved. Ethernet frames are now sent with minimum padding.	Y	–	–	–	–	–	–	–	–	–	–

CR	Module	Level	Description	AR44x/AR450S/AR415S	AR7x5	AR750S / AR770S	Rapier i	Rapier w	AT-8800	AT-8600	AT-8700XL	AT-8948 / x900-48	AT-9900	AT-9800
CR00029808	**Port Authentication STP**	**2**	When STP in rapid mode has a port which is disabled by command (because it is also configured for MAC-based port authorisation), then two packets were required to complete MAC-based port authorisation instead of one. This may have introduced a delay when supplicants were connecting, such as in the case where the first packet from the supplicant is a DHCP discover, which is only rebroadcast periodically in the absence of a response. This issue has been resolved. Now, the first DHCP discover packet received from the Supplicant triggers immediate MAC-based authentication and all subsequent packets are correctly forwarded when the Supplicant is authorised without delay.	–	–	–	Y	Y	Y	Y	Y	–	–	–
CR00030019	**OSPF**	**2**	In an OSPF configuration with many dial-on-demand interfaces (PPP over ISDN) as well as neighbour relationships via VLAN interfaces, the PPP interface status was not being set correctly and the neighbour relationships over the VLAN were not forming after a restart. A work around is to manually disable the VLAN interface and then re enable it. This update has corrected this fault and neighbour formation should proceed automatically after a restart. This issue has been resolved.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y

CR	Module	Level	Description	AR44x/AR450S/AR415S	AR7x5	AR750S / AR770S	Rapier i	Rapier w	AT-8800	AT-8600	AT-8700XL	AT-8948 / x900-48	AT-9900	AT-9800
CR00029632	**ETH**	**2**	When an ETH interface on an AR750S was reset, or the speed of the ETH interface on an AR415S was set, the interface would very occasionally stop receiving packets successfully. Sometimes this would also happen when the ETH interface speed was forced to 10Mbps or 100Mbps and the cable was quickly removed and re-inserted twice. These issues have been resolved.	Y	Y	Y	–	–	–	–	–	–	–	–
CR00030395	**ETH**	**2**	When an ETH interface on an AR750S or AR415S was forced to 10Mbps with the command SET ETH=n SPEED=10MFULL or SET ETH=n SPEED=10MHALF then very occasionally when the link came up, packet exchange with the link partner would fail until the link was taken down and back up again. This issue has been resolved.	Y	Y	Y	–	–	–	–	–	–	–	–
CR00028680	**Telnet Firewall**	**2**	Established TELNET sessions were discontinued if the firewall public interface cable was removed. This issue has been resolved. This solution ensures that the TELNET session is properly cleared down.	Y	Y	Y	Y	Y	Y	–	–	–	–	Y

Level 3

CR	Module	Level	Description	AR44x/AR450S/AR415S	AR7x5	AR750S / AR770S	Rapier i	Rapier w	AT-8800	AT-8600	AT-8700XL	AT-8948 / x900-48	AT-9900	AT-9800
CR00021170	**IP**	**3**	Previously, if a static ARP entry was added to the switch (**add ip arp** command) while the IP feature was disabled (**disable ip** command, disabled by default), a system reboot could occasionally occur. This issue has been resolved.	–	–	–	Y	Y	Y	Y	–	–	–	–
CR00031537	**SWI**	**3**	Previously, if a DoS defence was enabled (**enable dosdefence port** command) for a port range that included a mirror port (**set switch mirror** command), a system reboot could occur. This issue has been resolved.	–	–	–	–	–	–	Y	–	–	–	–
CR00030284	**IPsec**	**3**	When a secure connection's integrity is protected using the ISAKMP Heartbeat method, on failure, an ISAKMP Delete Notification is sent to the peer. Previously, on processing a received Delete Notification, it was possible for only the ISAKMP Security Association (SA) to be removed, leaving the IPSec SA active but isolated and no longer protected by the Heartbeat mechanism. This issue has been resolved. Receipt of an ISAKMP SA Delete Notification will now remove both ISAKMP and related IPsec SAs.	Y	Y	Y	Y	Y	Y	–	–	–	–	–

CR	Module	Level	Description	AR44x/AR450S/AR415S	AR7x5	AR750S / AR770S	Rapier i	Rapier w	AT-8800	AT-8600	AT-8700XL	AT-8948 / x900-48	AT-9900	AT-9800
CR00030428	**BGPv4**	**3**	Previously, if a BGP update message containing an unknown BGP attribute (with the extended length flag set) was received from a BGP peer—and the actual attribute length was less than 255, this resulted in a malformed BGP update being sent to a subsequent BGP peer that contained an improper length field value. This could result in the BGP connection going down. This issue has been resolved.	Y	Y	Y	Y	Y	Y	–	–	Y	Y	Y
CR00030482	**SQoS**	**3**	Previously, when software QoS weight scheduling was set to deficit weighted round robin (DWRR) and there was high traffic loading, occasionally, packets queued by SQOS for transmission were dropped, resulting in low level data loss. This issue has been resolved.	Y	Y	Y	Y	Y	–	–	–	–	–	–
CR00030834	**System**	**3**	Previously, when creating a configuration file in flash memory from the running configuration (**create config** command), on rare occasions writing the config file to flash memory could fail. This issue has been resolved.	Y	Y	Y	–	–	–	–	–	–	–	–

CR	Module	Level	Description	AR44x/AR450S/AR415S	AR7x5	AR750S / AR770S	Rapier i	Rapier w	AT-8800	AT-8600	AT-8700XL	AT-8948 / x900-48	AT-9900	AT-9800
CR00031199	**Firewall**	**3**	Previously, if a firewall rule was automatically deleted from a policy as a result of deleting a list (because the list was the only entry in the rule—**delete firewall policy list** command), adding the same rule to the policy again (**add firewall policy rule** command) resulted in an error indicating that the rule already existed. Also, previously the same list file name could be added to the same rule more than once (**add firewall policy rule** command). This issue has been resolved— adding the same list file name to a rule more than once results in an error indicating that an identical rule already exists. These issues have been resolved.	Y	Y	Y	Y	Y	Y	–	–	–	–	Y
CR00031388	**BGPv4**	**3**	When network interfaces were disconnected and reconnected repeatedly, causing BGP sessions via those interfaces to drop and recover, many BGP routing table updates occurred. Previously, the frequent addition and deletion of large numbers of BGP routes could result in low level memory loss over a period of many months if a route map that matched those BGP route table entries was also configured. This issue has been resolved.	Y	Y	Y	Y	Y	Y	–	–	Y	Y	Y

CR	Module	Level	Description	AR44x/AR450S/AR415S	AR7x5	AR750S / AR770S	Rapier i	Rapier w	AT-8800	AT-8600	AT-8700XL	AT-8948 / x900-48	AT-9900	AT-9800
CR00032163	**PPP**	**3**	Previously, when the AlliedWare device was interoperating with a PPP peer from another vendor, an endless PPP CDP Control Protocol negotiation loop could occur if the PPP peers had mismatched PPP CDP configuration. For example, this could happen if the CDP configuration option was enabled on the AlliedWare device and disabled on the PPP peer device. Only the PPP CDP control protocol negotiation was affected; the PPP link opened successfully. Either of the following commands could be used on the AlliedWare device to avoid this situation by ensuring that the CDP configuration option configured on the AllieWare device matched the PPP peer device: `disable lldp cdp` `disable lldp cdp interface=<ppp-instance>` The software has been enhanced. Now, the PPP CDP control protocol restart procedure is automatically disabled, preventing the possibility of a PPP CDP-CP negotiation loop from occurring, even if the PPP CDP configurations in each PPP peer device do not match. Note: AlliedWare supports the reception and processing of CDP advertisements, but does not generate CDP advertisements of its own.	Y	Y	Y	Y	Y	Y	–	–	Y	Y	Y
CR00029717	**Secure Shell**	**3**	A non-standard SSHv1.5 client could cause the AlliedWare SSH server to read an incorrect frame length, particularly if the Client ID string was greater than 50 characters. This issue has been resolved and the device now supports a Client ID string up to 1584 characters in length. Also, when a device was operating as an SSH client, the Client ID string included the word "Server". This has been changed to be "Client".	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y

CR	Module	Level	Description	AR44x/AR450S/AR415S	AR7x5	AR750S / AR770S	Rapier i	Rapier w	AT-8800	AT-8600	AT-8700XL	AT-8948 / x900-48	AT-9900	AT-9800
CR00028694	**Firewall**	**3**	Previously, all empty RTSP (Real Time Streaming Protocol) messages (continuation commands) embedded in Ethernet frames were expected to terminate with a sequence of characters consisting of 2 CRLF pairs (i.e. CRLF CRLF). The device firewall now accepts RTSP continuation messages that are terminated with a single CRLF pair (i.e. CRLF). Thus, an RTSP message consisting of only CRLF will now be accepted by the firewall.	Y	Y	Y	Y	Y	Y	–	–	–	–	Y
CR00030240	**Port Auth**	**3**	Previously, if a supplicant was authorised using MAC-based port authentication on a port and then connected to a different port without disconnecting the first port (if the interface was connected to a intermediate device for example), then the supplicant was not automatically disconnected from the previous port after being authorised on the new port. This issue has been resolved.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CR00030006	**QoS**	**3**	When a SQoS controlled ETH interface egress was oversubscribed with frames containing fragmented IP packets the output queue length of the interface appeared to grow unboundedly. This was because when SQoS limited its egress queue by discarding a frame it would take care to discard any the other frames that made up a fragmented IP packet. However, when it discarded more than one frame at a time it still only decremented the ETH queue length by one. This led to a queue length that increased over time as increments were not balanced by decrements. This discrepancy could lead to the ETH interface being reset due to the queue length not being zero at a time when all queued frames had been transmitted. This transmit queue length issue has been resolved.	Y	Y	Y	–	–	–	–	–	–	–	–

CR	Module	Level	Description	AR44x/AR450S/AR415S	AR7x5	AR750S / AR770S	Rapier i	Rapier w	AT-8800	AT-8600	AT-8700XL	AT-8948 / x900-48	AT-9900	AT-9800
CR00030139	**Switching**	**3**	Previously, when an AR770S switch port was disabled any entries for that port remained in the forwarding database. Now when the port is disabled any FDB entries associated with that port are immediately deleted.	–	–	Y	–	–	–	–	–	–	–	–
CR00030339	**HW Filter**	**3**	Previously, packets that should have been dropped by the switch hardware filters may still have reached the CPU. This issue has been resolved.	–	–	–	Y	Y	Y	Y	Y	–	–	–

Level 4

CR	Module	Level	Description	AR44x/AR450S/AR415S	AR7x5	AR750S / AR770S	Rapier i	Rapier w	AT-8800	AT-8600	AT-8700XL	AT-8948 / x900-48	AT-9900	AT-9800
CR00030116	**ETH**	**4**	Previously, if an Eth port on an AR770S router was physically disabled (**disable eth**=0 **link**=**disable** command) and then re-enabled while the link was down (e.g. no cable was plugged in), the Eth State in the **show eth**=0 **state** command output was not updated. This issue has been resolved.	–	–	Y	–	–	–	–	–	–	–	–
CR00029769	**IPv4**	**4**	After a **create conf**, and a subsequent config reload via a router reboot, the **set community= aa:xx** parameter in the **add ip routemap** command (as displayed in the **show config dyn=ip** command output) changed to a single integer value that had no relationship to the original colon separated command value entered into the CLI. This issue has been resolved so that the Community Value will display exactly as entered into the CLI via the **show config dyn=ip** command output.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y