# Stratix 8000 Ethernet Managed Switches

Catalog Numbers 1783-MS06T, 1783-MS10T

## About This Publication

These release notes provide hardware and software enhancements, anomalies, and other usage considerations for the Stratix 8000 Ethernet Managed Switches, revision 3.001 [12.2(50)SE2].

**IMPORTANT** If you are using RSLogix 5000 software with the Stratix 8000 Add-on Profile (AOP), you must update the AOP to support this release of the switches. This release of the switches requires AOP revision number 3.001. This version of AOP is also backward compatible with releases 2 and 1 of the switches.

## Enhancements

This section describes the new and updated software features provided in this release.

| Enhancement | Description |
|---|---|
| DHCP | DHCP reserved-only option to allow users to allocate only reserved addresses in the Dynamic Host Configuration Protocol (DHCP) address pool. |
| IEEE 802.1 | Network Edge Access Topology (NEAT) with 802.1x switch supplicant, host authorization with CISP, and auto enablement to authenticate a switch outside a wiring closet as a suplicant to another switch. |
| | IEEE 802.1x with open access to allow a host to access the network before being authenticated. |
| | IEEE 802.1x authentication with downloadable ACLs and redirect URLs to allow per-user ACL downloads from a Cisco Secure ACS server to an authenticated switch. |

| Enhancement | Description |
|---|---|
| Authentication | Flexible-authentication sequencing to configure the order of the authentication methods that a port tries when authenticating a new host. |
| | Multiple-user authentication to allow more than one host to authenticate on an 802.1x-enabled port. |
| IP source guard | IP source guard restricts traffic on nonrouted interfaces by filtering traffic based on the DHCP snooping database and IP source bindings. |
| Dynamic ARP inspection | Dynamic ARP inspection to prevent malicious attacks on the switch by not relaying invalid ARP requests and responses to other ports in the same VLAN. |
| CPU monitoring | CPU utilization threshold trap monitors CPU utilization. |
| Embedded event manager | Support for Embedded Event Manager Version 2.4. |
| Profile enhancements | LLDP-MED network-policy profile time, length, value (TLV) for creating a profile for voice and voice-signalling by specifying the values for VLAN, class of service (CoS), differentiated services code point (DSCP), and tagging mode. |
| RADIUS server load balancing | RADIUS server load balancing to allow access and authentication requests to be distributed evenly across a server group. |
| Resilient Ethernet Protocol (REP) | Support for Resilient Ethernet Protocol (REP) for improved convergence times and network loop prevention without the use of spanning tree, including configuration of REP edge ports when the neighbor port is not REP-capable. |

## Corrected Anomalies

This section describes anomalies corrected in this release.

| Anomaly | Description |
|---|---|
| SSLVPN | SSLVPN service stops accepting any new SSLVPN connections due to a vulnerability in the processing of new TCP connections for SSLVPN services. If debug ip tcp transactions is enabled and this vulnerability is triggered, the user sees debug messages that indicate the connection queue limit has been reached. |
| CIP | This release addresses several issues regarding Common Industrial Protocol (CIP) compliance. |
| TCP | When a TCP packet with all flags set to zero (at the TCP level) is sent to a remote router, the remote (destination) router no longer returns an ACK/RST packet back to the source of the TCP segment. |
| Password | The switch now accepts an encrypted secret password. |
| Traffic | Traffic is now forwarded to the interfaces that are configured with static multicast MAC addresses after the switch is reloaded.<br><br>You cannot configure the static MAC address (unicast or multicast) entries on EtherChannel member interfaces, or add an interface into the EtherChannel if that interface is associated with a static MAC address entry. |
| Keepalive | When keepalive is disabled on an interface, the interface is no longer put in an error-disabled state when it receives keepalive packets. |
| Switched Port Analyzer | The Switched Port Analyzer (SPAN) destination port no longer detects IPv6 multicast packets from a VLAN that is not being monitored by SPAN. |
| Message log | This message no longer appears in the log during the system bootup on a switch that is running IOS 12.2(50)SE:<br><br>%COMMON_FIB-3-FIBIDBINCONS2 |
| PMD auto-negotiation advertised capability | The PMD auto-negotiation advertised capability is now correct on the gigabit ethernet switch ports. |

| Anomaly | Description |
|---|---|
| Set TxPortFifo SRR Failed message | The Set TxPortFifo SRR Failed message no longer appears when you enter both the srr-queue bandwidth shape 200 0 2 200 and the priority-queue out interface configuration commands on the same interface. |
| Forwarding Information Base (FIB) | The switch no longer reloads when the Forwarding Information Base (FIB) adjacency table is added. |
| Unauthorized IP phone | An IP Phone connected to a switch no longer becomes unauthorized when it transitions from the data authorization domain to the voice authorization domain. |
| Switch port configured for IGMP snooping | A switch port configured for IGMP snooping no longer loses its group membership when the port receives a query that comes from an upstream device that is not configured for IGMP snooping. |
| SNMP polling for the ciscoCBQosMIB | A switch configured with class-based policies that are applied and active on at least one interface may no longer reload or display CPU hog messages during SNMP polling for the ciscoCBQosMIB. |
| MAC ID relearned | When you have entered the vlan dot1q tag native global configuration command to configure a switch to tag native VLAN frames on 802.1Q trunk ports, and you configure a new voice VLAN on an access port, the MAC ID of a connected PC is now correctly relearned. |
| Switch Virtual Interface (SVI) | When a Switch Virtual Interface (SVI) is configured as unnumbered and is pointing to a loopback interface, the switch no longer fails when the SVI receives a packet. |
| Voice traffic | When LLDP is enabled and a voice VLAN is configured, the L2 Priority and DSCP Value fields in the LLDP type, length, and value descriptions (TLVs) are now correctly marked to give the voice traffic the correct DSCP and Layer 2 priority. |
| Port authentication | Switch ports no longer attempt authentication at the interval configured for the port security timer instead of the configured IEEE 802.1x timer. |

## Known Anomalies

This section describes known anomalies associated with this release.

| Anomaly | Description | Workaround |
|---|---|---|
| Configuration timeout value | When you enter the boot host retry timeout global configuration command to specify the amount of time that the client should keep trying to download the configuration, and you do not enter a timeout value, the default value is zero. This should mean that the client keeps trying indefinitely. However, the client does not keep trying to download the configuration. | Always enter a non-zero value for the timeout value when you enter the boot host retry timeout timeout-value command. |
| CIP open connection failure | When an unsuccessful forward open request message is returned on the switch, the response does not contain the connection serial number, vendor ID, or vendor serial number information. Only the general and extended error codes are returned.<br><br>This problem applies only to unsuccessful forward open response messages. | Enable the CIP debug command to determine the cause of the forward open failure by reading the error codes from the console. |
| Domain name value | The show cip object tcp/ip interface privileged EXEC command displays an old value for the domain name after it has been unconfigured with the no ip domain-name global configuration command. | Ignore the domain name output of the show cip object tcp/ip interface privileged EXEC command. |
| Precision Time Protocol (PTP) | When you configure PTP in forward mode by entering the ptp mode forward global configuration command, the PTP page in the Device Manager web interface fails, due to a parser error. | There is no workaround. No PTP information is displayed when PTP is in forward mode. |
| Device Manager web interface legend | The Device Manager web interface legend incorrectly shows solid green for the Alarm and Setup status indicators in the Off state.<br><br>These status indicators in the Off state should be solid black (dark). | None |
| Redundant power supply failure | When one power supply in a redundant pair fails, a CIP query continues to show that both supplies are present and okay. | None |
| Unconnected MVR port | On switches running IOS Release 12.2(44)SE or 12.2(46)SE, when you enter the show mvr interface interface-id members privileged EXEC command to see status of an MVR port, an MVR member port that is not connected always shows as active. | Use the show mvr interface interface-id or the show mvr members privileged EXEC command. These command outputs show the correct status of an MVR port. |
| MVR VLAN | When you enter the mvr vlan vlan-id global configuration command to create an MVR VLAN and enable MVR on the switch by entering the mvr global configuration command, if you enter the show mvr interface interface-id members privileged EXEC command, the output shows the MVR groups on the interface.<br><br>If you enable MVR first and then create the MVR VLAN, the MVR groups are not displayed correctly. | None |

| Anomaly | Description | Workaround |
|---|---|---|
| Configuration | A static IP address might be removed when the previously acquired DHCP IP address lease expires.<br><br>This problem occurs under these conditions:<br><br>• When the switch is booted up without a configuration (no config.text file in flash memory).<br>• When the switch is connected to a DHCP server that is configured to give an address to it (the dynamic IP address is assigned to VLAN 1).<br>• When an IP address is configured on VLAN 1 before the dynamic address lease assigned to VLAN 1 expires. | Reconfigure the static IP address. |
| | When connected to some third-party devices that send early preambles, a switch port operating at 100 Mb/s full duplex or 100 Mb/s half duplex might bounce the line protocol up and down. The problem is observed only when the switch is receiving frames. | Configure the port for 10 Mb/s and half duplex or to connect a hub or a nonaffected device to the switch. |
| | When port security is enabled on an interface in restricted mode and the switchport block unicast interface command has been entered on that interface, MAC addresses are incorrectly forwarded when they should be blocked. | Enter the no switchport block unicast interface configuration command on the specific interface. |
| | A traceback error occurs if a crypto key is generated after an SSL client session. | There is no workaround. This is a cosmetic error and does not affect the functionality of the switch. |
| | When the logging event-spanning-tree interface configuration command is configured and logging to the console is enabled, a topology change might generate a large number of logging messages, causing high CPU utilization.<br><br>CPU utilization can increase with the number of spanning-tree instances and the number of interfaces configured with the logging event-spanning-tree interface configuration command.<br><br>This condition adversely affects how the switch operates and could cause problems such as STP convergence delay.<br><br>High CPU utilization can also occur with other conditions, such as when debug messages are logged at a high rate to the console. | Use one of these workarounds:<br><br>• Disable logging to the console.<br>• Rate-limit logging messages to the console.<br>• Remove the logging event spanning-tree interface configuration command from the interfaces. |

| Anomaly | Description | Workaround |
|---|---|---|
| EtherChannel | Traffic on EtherChannel ports is not perfectly load-balanced. Egress traffic on EtherChannel ports are distributed to member ports on load balance configuration and traffic characteristics like MAC or IP address. More than one traffic stream may map to same member ports based on hashing results calculated by the ASIC.<br><br>If this happens, traffic will be unevenly distributed on EtherChannel ports. | Changing the load balance distribution method or changing the number of ports in the EtherChannel can resolve this problem. Use any of these workarounds to improve EtherChannel load balancing:<br><br>• For random source-ip and dest-ip traffic, configure load balance method as src-dst-ip<br>• For Incrementing source-ip traffic, configure load balance method as src-ip<br>• For incrementing dest-ip traffic, configure load balance method as dst-ip<br>• Configure the number of ports in the EtherChannel so that the number is equal to a power of 2 (i.e. 2, 4, or 8)<br><br>For example, with load balance configured as dst-ip with 150 distinct incrementing destination IP addresses, and the number of ports in the EtherChannel set to either 2, 4, or 8, load distribution is optimal. |
| IP | When the rate of received DHCP requests exceeds 2,000 packets per minute for a long time, the response time might be slow when you are using the console. | Use rate limiting on DHCP traffic to prevent a denial of service attack. |
| Multicasting | If the number of multicast routes and Internet Group Management Protocol (IGMP) groups are more than the maximum number specified by the show sdm prefer global configuration command, the traffic received on unknown groups is flooded in the received VLAN even though the show ip igmp snooping multicast-table privileged EXEC command output shows otherwise. | Reduce the number of multicast routes and IGMP snooping groups to less than the maximum supported value. |
| | IGMP filtering is applied to packets that are forwarded through hardware. It is not applied to packets that are forwarded through software.<br><br>With multicast routing enabled, the first few packets are sent from a port even when IGMP filtering is set to deny those groups on that port. | None |

| Anomaly | Description | Workaround |
|---|---|---|
| Multicasting | If an IGMP report packet has two multicast group records, the switch removes or adds interfaces depending on the order of the records in the packet:<br><br>If the ALLOW_NEW_SOURCE record is before the BLOCK_OLD_SOURCE record, the switch removes the port from the group.<br><br>If the BLOCK_OLD_SOURCE record is before the ALLOW_NEW_SOURCE record, the switch adds the port to the group. | None |
| | When IGMP snooping is disabled and you enter the switchport block multicast interface configuration command, IP multicast traffic is not blocked.<br><br>The switchport block multicast interface configuration command is only applicable to non-IP multicast traffic. | None |
| | Incomplete multicast traffic can be seen under either of these conditions:<br><br>You disable IP multicast routing or re-enable it globally on an interface.<br><br>A switch mroute table temporarily runs out of resources and recovers later. | Enter the clear ip mroute privileged EXEC command on the interface. |
| | After you configure a switch to join a multicast group by entering the ip igmp join-group *group-address* interface configuration command, the switch does not receive join packets from the client, and the switch port connected to the client is removed from the IGMP snooping forwarding table. | Use one of these workarounds:<br><br>Cancel membership in the multicast group by using the no ip igmp join-group group-address interface configuration command on an SVI.<br><br>Disable IGMP snooping on the VLAN interface by using the no ip igmp snooping vlan vlan-id global configuration command. |
| IP Phone | Entering the shutdown and the no shutdown interface configuration commands on the internal link can disrupt the PoE operation.<br><br>If a new IP phone is added while the internal link is in shutdown state, the IP phone does not get inline power if the internal link is brought up within 5 minutes. | Enter the shutdown and the no shutdown interface configuration commands on the Fast Ethernet interface of a new IP phone that is attached to the service module port after the internal link is brought up. |
| QoS | Some switch queues are disabled if the buffer size or threshold level is set too low with the mls qos queue-set output global configuration command.<br><br>The ratio of buffer size to threshold level should be greater than 10 to avoid disabling the queue. | Choose compatible buffer sizes and threshold levels. |

| Anomaly | Description | Workaround |
|---|---|---|
| QoS | When auto-QoS is enabled on the switch, priority queuing is not enabled. Instead, the switch uses shaped round robin (SRR) as the queuing mechanism.<br><br>The auto-QoS feature is designed on each platform based on the feature set and hardware limitations, and the queuing mechanism supported on each platform might be different. | None |
| SPAN and RSPAN | Discovery Protocol (CDP), VLAN Trunking Protocol (VTP), and Port Aggregation Protocol (PAgP) packets received from a SPAN source are not sent to the destination interfaces of a local SPAN session. | Use the monitor session session_number destination {interface interface-id encapsulation replicate} global configuration command for local SPAN. |
| Trunking | The switch treats frames received with mixed encapsulation (IEEE 802.1Q and Inter-Switch Link [ISL]) as frames with FCS errors, increments the error counters, and the port LED blinks amber.<br><br>This happens when an ISL-unaware device receives an ISL-encapsulated packet and forwards the frame to an IEEE 802.1Q trunk interface. | None |
| | IP traffic with IP options set is sometimes leaked on a trunk port.<br><br>For example, a trunk port is a member of an IP multicast group in VLAN X but is not a member in VLAN Y. If VLAN Y is the output interface for the multicast route entry assigned to the multicast group and an interface in VLAN Y belongs to the same multicast group, the IP-option traffic received on an input VLAN interface other than one in VLAN Y is sent on the trunk port in VLAN Y. This happens because the trunk port is forwarding in VLAN Y, even though the port has no group membership in VLAN Y. | None |
| | For trunk ports or access ports configured with IEEE 802.1Q tagging, inconsistent statistics might appear in the show interfaces counters privileged EXEC command output.<br><br>Valid IEEE 802.1Q frames of 64 to 66 bytes are correctly forwarded even though the port status indicator blinks amber, and the frames are not counted on the interface statistics. | None |
| VLAN | If the number of VLANs times the number of trunk ports exceeds the recommended limit of 13,000, the switch can fail. | Reduce the number of VLANs or trunks. |
| | When line rate traffic is passing through a dynamic port, and you enter the switchport access vlan dynamic interface configuration command for a range of ports, the VLANs might not be assigned correctly.<br><br>One or more VLANs with a null ID appears in the MAC address table instead. | Enter the switchport access vlan dynamic interface configuration command separately on each port. |

| Anomaly | Description | Workaround |
|---|---|---|
| Device Manager web interface | When you are prompted to accept the security certificate and you click No, you see a blank screen, and the Device Manager web interface does not launch. | Click Yes when you are prompted to accept the certificate. |
| | When you successfully upgrade an image by using the Device Manager web interface and click No when prompted to reload the image, the Device Manager web interface becomes unusable. | Manually reload the switch. |
| Saving changes made with CIP | When changes are made to the switch configuration by using the CIP interface, the changes are applied only to the running configuration. The changes will not be retained in non-volatile storage unless a Save service is mde to the vendor-specific Switch Parameter Object.<br><br>If you made changes by using the RSLogix 5000 software AOP, this issue will not occur, since the Save serivce is issued automatically by the tool. | If you made configuration changes by using CIP and did not use RSLogix 5000 software, issue the Save Configuration Data service (0x16) to the Switch Parameter Object (0x35F), instance 1. |

## Default Password

With release 3.001 and later, you must enter the default password 'switch' the first time you launch Express Setup. Once you launch Express Setup, you will be prompted to change the default password.

## CNA Comptibility

Cisco Network Assistant (CNA), version 5.4 and later is compatible with release 3.001 and earlier of the switches.

CNA 5.4 does not support the following Smartport roles:

- Desktop for Automation
- Switch for Automation
- Router for Automation
- Phone for Automation
- Wireless for Automation

Using the new Smartport roles will cause CNA errors.

## Additional Resources

These documents contain additional information concerning related Rockwell Automation products.

| Resource | Description |
|---|---|
| Stratix 8000 Ethernet Managed Switches Installation Instructions, publication 1783-IN005 | Describes how to get started installing and configuring the switch. |
| Stratix 8000 Ethernet Managed Switches Hardware User Manual, publication 1783-UM002 | Provides detailed information on installing and using your switches. |
| Stratix 8000 Ethernet Managed Switches Software User Manual, publication 1783-UM003 | Provides detailed information on configuring and managing your switches. |
| Industrial Automation Wiring and Grounding Guidelines, publication 1770-4.1 | Provides general guidelines for installing a Rockwell Automation industrial system. |
| Product Certifications website, http://www.ab.com | Provides declarations of conformity, certificates, and other certification details. |

You can view or download publications at http://literature.rockwellautomation.com. To order paper copies of technical documentation, contact your local Rockwell Automation distributor or sales representative.

# Rockwell Automation Support

Rockwell Automation provides technical information on the Web to assist you in using its products. At http://support.rockwellautomation.com, you can find technical manuals, a knowledge base of FAQs, technical and application notes, sample code and links to software service packs, and a MySupport feature that you can customize to make the best use of these tools.

For an additional level of technical phone support for installation, configuration, and troubleshooting, we offer TechConnect support programs. For more information, contact your local distributor or Rockwell Automation representative, or visit http://support.rockwellautomation.com.

## Installation Assistance

If you experience a problem within the first 24 hours of installation, please review the information that's contained in this manual. You can also contact a special Customer Support number for initial help in getting your product up and running.

| | |
|---|---|
| United States | 1.440.646.3434<br>Monday – Friday, 8 a.m. – 5 p.m. EST |
| Outside United States | Please contact your local Rockwell Automation representative for any technical support issues. |

## New Product Satisfaction Return

Rockwell Automation tests all of its products to ensure that they are fully operational when shipped from the manufacturing facility. However, if your product is not functioning and needs to be returned, follow these procedures.

| | |
|---|---|
| United States | Contact your distributor. You must provide a Customer Support case number (call the phone number above to obtain one) to your distributor in order to complete the return process. |
| Outside United States | Please contact your local Rockwell Automation representative for the return procedure. |

Allen-Bradley, Rockwell Automation, Stratix, and TechConnect are trademarks of Rockwell Automation, Inc.

Trademarks not belonging to Rockwell Automation are property of their respective companies.

**www.rockwellautomation.com**

**Power, Control and Information Solutions Headquarters**

Americas: Rockwell Automation, 1201 South Second Street, Milwaukee, WI 53204-2496 USA, Tel: (1) 414.382.2000, Fax: (1) 414.382.4444
Europe/Middle East/Africa: Rockwell Automation, Vorstlaan/Boulevard du Souverain 36, 1170 Brussels, Belgium, Tel: (32) 2 663 0600, Fax: (32) 2 663 0640
Asia Pacific: Rockwell Automation, Level 14, Core F, Cyberport 3, 100 Cyberport Road, Hong Kong, Tel: (852) 2887 4788, Fax: (852) 2508 1846

Publication 1783-RN002B-EN-E - May 2009 PN-36092

Copyright © 2009 Rockwell Automation, Inc. All rights reserved. Printed in the U.S.A.