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 2.001 (122-46.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 2.01.004. This version of AOP is also backward compatible with release 1 of the switches.

Enhancements

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

Enhancement	Description
Support for Precision Time Protocol (PTP)	PTP, as defined in the IEEE 1588 standard, synchronizes the real-time clocks of devices in a network with nanosecond accuracy.
Support for Smartport Macros	The switch, desktop, router, and wireless Smartport macros have been further optimized for industrial automation traffic.
CIP (Common Industrial Protocol) enhancements (the CIP revision has been incremented to 2.001 in this release)	• When CIP is enabled on the switch, you can specify the VLAN ID to be used as the CIP interface. • The Device Manager Web interface Express Setup page includes fields for IP address and mask for the CIP VLAN. • CIP indicates when the Compact Flash card is unplugged or not operating.
DHCP per port	DHCP per port allows the switch to assign IP addresses to end devices based on the physical port location of the device asking for its IP address.

Known Anomalies

This section describes known anomalies associated with this release.

Configuration

- A static IP address might be removed when the previously acquired DHCP IP address lease expires.

  This problem occurs under these conditions:

  - When the switch is booted up without a configuration (no config.text file in flash memory)
  - 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)
  - When an IP address is configured on VLAN 1 before the dynamic address lease assigned to VLAN 1 expires

  The workaround is to 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.

  The workaround is to configure the port for 10 Mb/s and half duplex, or to connect a hub or an unaffected 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

  The workaround is to enter the no switchport block unicast interface configuration command on that 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.

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. This condition adversely affects how the switch operates and could cause problems, such as STP convergence delay.

- 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:

  - Disable logging to the console.
  - Rate-limit logging messages to the console.
  - Remove the logging event spanning-tree interface configuration command from the interfaces.
- The far-end fault optional facility is not supported on the 1783-100FX SFP module.

  The workaround is to configure aggressive UDLD.

- 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. A value of zero should mean that the client keeps trying indefinitely. However, the client does not keep trying to download the configuration.

  The workaround is to always enter a non zero value for the timeout value when you enter the boot host retry timeout timeout-value command.

Ethernet

Traffic on EtherChannel ports is not perfectly load-balanced. Egress traffic on EtherChannel ports is distributed to member ports on load balance configuration and traffic characteristics like MAC or IP address. More than one traffic stream may map to the same member ports based on hashing results calculated by the ASIC.

If this happens, uneven traffic distribution will occur 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:

- For random source-ip and dest-ip traffic, configure load balance method as src-dst-ip.
- For incrementing source-ip traffic, configure load balance method as src-ip.
- For incrementing dest-ip traffic, configure load balance method as dst-ip.
- Configure the number of ports in the EtherChannel so that the number is equal to a power of 2 (that is. 2, 4, or 8).

  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 2, 4, or 8, load distribution is optimal.

CIP

- 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.

  This problem applies only to unsuccessful forward open response messages.

  The workaround is to enable the CIP debug command to determine the cause of the forward open failure.

- 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.

  The workaround is to ignore the domain name output of the show cip object tcp/ip interface privileged EXEC command.

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.

The workaround is to use rate limiting on DHCP traffic to prevent a denial of service attack from occurring.

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 breaks due to a parser error.

There is no workaround. No PTP information is displayed when PTP is in forward mode.

Multicasting

- If the number of multicast routes and Internet Group Management Protocol (IGMP) groups is 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.

  The workaround is to 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.

  IGMP filtering is not applied to packets that are forwarded through software. 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.

  There is no workaround.

- 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.

  - If the ALLOW_NEW_SOURCE record is before the BLOCK_OLD_SOURCE record, the switch removes the port from the group.
  - If the BLOCK_OLD_SOURCE record is before the ALLOW_NEW_SOURCE record, the switch adds the port to the group.

  There is no workaround.

- When IGMP snooping is disabled and you enter the switchport block multicast interface configuration command, IP multicast traffic is not blocked.

  The switchport block multicast interface configuration command applies only to non-IP multicast traffic.

  There is no workaround.

- Incomplete multicast traffic can be seen under either of these conditions:
  - You disable IP multicast routing or re-enable it globally on an interface.
  - A switch mroute table temporarily runs out of resources and recovers later.

  The workaround is to 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:

  - Cancel membership in the multicast group by using the no ip igmp join-group group-address interface configuration command on an SVI.
  - Disable IGMP snooping on the VLAN interface by using the no ip igmp snooping vlan vlan-id global configuration command.
- Entering the shutdown and the no shutdown interface configuration commands on the internal link can disrupt the PoE operation. 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 five minutes.

The workaround is to 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. The ratio of buffer size to threshold level should be greater than 10 to avoid disabling the queue.

  The workaround is to choose compatible buffer sizes and threshold levels.

- 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.

  The auto-QoS feature is designed on each platform based on the feature set and hardware limitations. The queuing mechanism supported on each platform might be different.

  There is no workaround.

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. The workaround is to 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 status indicator blinks amber.

  This happens when an ISL-unaware device receives an ISL-encapsulated packet and forwards the frame to an IEEE 802.1Q trunk interface.

  There is no workaround.

- IP traffic with IP options set is sometimes leaked on a trunk port. 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 occurs because the trunk port is forwarding in VLAN Y, even though the port has no group membership in VLAN Y.

  There is no workaround.

- 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.

  Valid IEEE 802.1Q frames of 64…66 bytes are correctly forwarded even though the port LED blinks amber, and the frames are not counted on the interface statistics.

  There is no workaround.

VLAN

- If the number of VLANs multiplied by the number of trunk ports exceeds the recommended limit of 13,000, the switch can fail.

  The workaround is to 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. One or more VLANs with a null ID appears in the MAC address table instead.

  The workaround is to enter the switchport access vlan dynamic interface configuration command separately on each port.

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.

  The workaround is to click Yes when you are prompted to accept the certificate.

- When you successfully upgrade an image by using Device Manager Web interface and click No when prompted to reload the image, the Device Manager Web interface becomes unusable.

  The workaround is to manually reload the switch.

- The Device Manager Web interface legend incorrectly shows solid green for the Alarm and Setup status indicators in the Off state. The correct color of these status indicators in the Off state is solid black (dark).

  There is no workaround.

Corrected Anomalies

- Traceback messages such as these no longer appear when a large number of IEEE 802.1x supplicants repeatedly try to log in and log out.

```
Jan 3 17:54:32 L3A3 307: Jan 3 18:04:13.459: %SM-4-BADEVENT:
Event 'eapReq' is invalid for the current state
'auth_bend_idle': dot1x_auth_bend Fa9
Jan 3 17:54:32 L3A3 308: -Traceback= B37A84 18DAB0 2FF6C0 2FF260
8F2B64 8E912C Jan 3 19:06:13 L3A3 309: Jan 3 19:15:54.720:
%SM-4-BADEVENT: Event 'eapReq_no_reAuthMax' is invalid for the
current ate 'auth_restart': dot1x_auth Fa4
```

- When IEEE 802.1x is globally disabled on the switch by using the no dot1x system-auth-control global configuration command, interface level IEEE 802.1x configuration commands, including the dot1x timeout and dot1x mac-auth-bypass commands, are now available.

  The configuration file used for the configuration replacement feature no longer requires the character string end\n at the end of the file.

- A switch configured for Link Layer Discovery Protocol (LLDP) now correctly reports the enabled switch capabilities in the LLDP type, length, and value (TLV) attributes. System capabilities appear correctly, and the enabled capabilities are now identified if the switch is configured only as a Layer 2 switch.
- When two switches are connected with both copper and fiber connections on the same port, and a 1783-100FX SFP module is connected to the switch, when you change the media-type from SFP to copper, the copper link now comes up correctly.
- When configuring a switch management VLAN to be another VLAN during Express Setup, the computer no longer loses the network connection to the switch if the computer remains connected to the same port.
- When a diagnostic or port mirroring role is defined on an interface and you change it to another port role, the port role icon in Device Manager Web interface is now correct.
- If you remove the secure MAC address from an interface through CIP, the switchport port-security violation restrict CLI configuration no longer remains on the interface.
- In a Multi Domain Authentication (MDA) setup with per-virtual port error-disable configured, when authenticated data and voice clients on the member switch port are dynamically assigned to VLANs and a second data client causes a security violation, only the data virtual port is error-disabled. The voice virtual port is no longer error-disabled at the same time.
- When the switch IP address is successfully changed via CIP, the expected successful CIP response is now returned. When changing the domain name or switch host name, odd-length strings with the required padding are no longer rejected by the switch.

- When an IEEE 802.1x client is directly connected to an interface configured for 802.1x multi-domain with no IP phone attached, the interface is initially assigned to the guest VLAN. Once the 802.1x supplicant allows access to the guest VLAN and an EAPOL packet is detected, the interface now correctly reverts to an unauthorized state, and IEEE 802.1x authentication restarts.

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.
Stratix 8000 Ethernet Managed Switches Release Notes, publication 1783-RN002	Lists enhancements and anomalies associated with the software release.
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 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-RN002A-EN-E - January 2009 PN-39577

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