Allen-Bradley

Stratix 8000 and Stratix 8300 Ethernet Managed Switches

Catalog Numbers 1783-MS06T, 1783-MS10T, 1783-RMS06T, 1783-RMS10T

Topic	Page
Enhancements	1
Corrected Anomalies	2
Known Anomalies	3
Application Notes	7
Additional Resources	7

About This Publication

These release notes provide hardware and software enhancements, anomalies, and other usage considerations for the Stratix 8000™ and Stratix 8300™ Ethernet Managed Switches, revision 6.001 [15.0(2)SEIES].

Enhancements

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

Table 1 - Enhancements with Revision 6.001 [15.0(2)SEIES]

Cat. No.	Description
1783-MS06T, 1783-MS10T, 1783-RMS06T, 1783-RMS10T	Support for IP version 6 (IPv6) multicast.
	Option to minimize boot up time with the boot fast command.
	Support for static routes on switch virtual interfaces (SVIs).
	Support for port security on EtherChannels.

Corrected Anomalies

This section describes corrected anomalies associated with this revision.

Table 2 - Anomalies with Revision 6.001 [15.0(2)SEIES]

Cat. No.	Description
1783-MS06T, 1783-MS10T, 1783-RMS06T, 1783-RMS10T	**CORRECTED:** IOS and IOS XE software contains a vulnerability that can allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition. An attacker could exploit this vulnerability by sending a crafted request to an affected device that has the DHCP version 6 (DHCPv6) server feature enabled, causing a reload. We have provided free software updates that address this vulnerability. This advisory is available at the following link: http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120926-dhcpv6
	CORRECTED: The archive download feature does not work if the nonvolatile memory contains an update directory. This situation is likely to occur if a previous download failed or was interrupted and the update directory is still left in the nonvolatile memory. The workaround is to delete the "update" directory in the flash memory before starting the archive download.
	CORRECTED: OSPF Version 3 (OSPF v3) neighbors can flap (broadcasting routing table updates that alternate between two different routes to a host) because of the way the switch handles IPv6 traffic destined for well-known IPv6 multicast addresses. There is no workaround.
	CORRECTED: Users connecting to the network through a device configured for Web proxy authentication may experience a Web authentication failure. There is no workaround. Use the clear tcp tcb command to release the HTTP Proxy Server process.
	CORRECTED: Using the dot1x default command on a port disables access control on the port and resets the values of the authentication host-mode and authentication timer reauthenticate commands to the default values. The workaround is to avoid using the dot1x default command and set various dot1x parameters individually. You can also reconfigure the parameters that were changed after you entered the dot1x default command.
	CORRECTED: When EnergyWise is disabled, the switch unexpectedly reloads and generates crash information. There is no workaround.
	CORRECTED: When using the switchport port-security maximum 1 vlan access command, if an IP phone with a personal computer connected to it is connected to an access port with port security, a security violation occurs on the interface. This type of message is displayed on the console: %PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred, caused by MAC address XXXX.XXXX.XXXX on port FastEthernet0/1. Here is a sample configuration: interface gigabitethernet 3/0/47 switchport access vlan 2 switchport mode access switchport voice vlan 3 switchport port-security maximum 2 switchport port-security maximum 1 vlan access switchport port-security maximum 1 vlan voice switchport port-security The workaround is to remove the line' switchport port-security maximum 1 vlan access'.
	CORRECTED: You can use Express Setup to enter the initial configuration of a switch. You enter the IP address and VLAN information. When you enter a different VLAN for the management and CIP interfaces and click submit, no error message is generated. If you then look at the Express Setup page, the CIP management VLAN is changed to the same VLAN ID as the management interface. If you enter the show vlan command at the CLI, the CIP VLAN was never created by the switch. The workaround is to edit the running configuration by using the CLI, and entering the vlan vlan-id command, where vlan-id is the CIP VLAN.
	CORRECTED: The switch does not correctly detect a loopback when the switch port on an authenticated IP phone is looped to a port configured and authenticated with dot1x security, even when bpduguard is configured on the interface. This situation can result in 100% CPU utilization and degraded switch performance. The workaround is to configure the interface with the authentication open command or to configure authentication mac-move permit on the switch.

Known Anomalies

This section describes known anomalies associated with this revision.

Table 3 - Known Anomalies with Revision 6.001 [15.0(2)SEIES]

Cat. No.	Description
1783-MS06T, 1783-MS10T, 1783-RMS06T, 1783-RMS10T	A static IP address can be removed when the previously acquired DHCP IP address lease expires. This problem occurs under these conditions: • When the switch is started up without a configuration (no config.text file in nonvolatile 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 MBps full-duplex or 100 MBps half-duplex can 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 MBps 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. 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 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, which 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.
	On a switch running both Resilient Ethernet Protocol (REP) and Bidirectional Forwarding Detection (BFD), when the REP link status layer (LSL) age-out value is less than 1 second, the REP link flaps if the BFD interface is shut down and then brought back up. The workaround is to use the rep lsl-age-out timer interface configuration command to configure the REP LSL age timer for more than 1000 ms (1 second).

Table 3 - Known Anomalies with Revision 6.001 [15.0(2)SEIES]

Cat. No.	Description
1783-MS06T, 1783-MS10T, 1783-RMS06T, 1783-RMS10T	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. If this happens, uneven traffic distribution will happen 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 the load-balance method as src-dst-ip. • For incrementing source-ip traffic, configure the load-balance method as src-ip. • For incrementing dest-ip traffic, configure the 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 either 2, 4, or 8, load distribution is optimal.
	When the rate of received DHCP requests exceeds 2000 packets per minute for a long time, the response time can 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.
	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. 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. It is not applied to packets that are forwarded through software. Hence, 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 is applicable 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.

Table 3 - Known Anomalies with Revision 6.001 [15.0(2)SEIES]

Cat. No.	Description
1783-MS06T, 1783-MS10T, 1783-RMS06T, 1783-RMS10T	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.
	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 levelmust 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, and the queuing mechanism supported on each platform can be different. There is no workaround.
	If you configure a large number of input interface VLANs in a class map, a traceback message similar to this can appear: 01:01:32: %BIT-4-OUTOFRANGE: bit 1321 is not in the expected range of 0 to 1024 There is no impact to switch functionality. There is no workaround.
	Cisco 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.
	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 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 can 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 status indicator blinks amber, and the frames are not counted on the interface statistics. There is no workaround.

Table 3 - Known Anomalies with Revision 6.001 [15.0(2)SEIES]

Cat. No.	Description
1783-MS06T, 1783-MS10T, 1783-RMS06T, 1783-RMS10T	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 may 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.
	If the number of VLANs times 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 many VLANs are configured on the switch, high CPU utilization occurs when many links are flapping at the same time. The workaround is to remove unnecessary VLANs to reduce CPU utilization when many links are flapping at the same time.
	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 the 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 maximum number of VPN routing and forwarding (VRF) instances that can be configured is 25 instead of 26. There is no workaround.
	When an attempt is made to view the web pages of a switch, the initial request for a password by the Device Manager Web interface is an unsecure connection. After the password is accepted, the next dialog box asks if a secure connection is desired. The workaround is to manually establish a secure connection to the switch.
	The password must be entered twice before it is accepted in Express Setup, if redirected from another site. There is no workaround.
	The vendor specific attribute PortLogSyncIntervalCfg is a struct with a UINT type member variable called PortLogSyncInterval. The specified range of valid values for PortLogSyncInterval is from -1…6. A value of -1 cannot be assigned to the PortLogSyncInterval variable. There is no workaround.
	After the switch powers up, a connected device does not receive Gratuitous ARP (GARP) packets from the switch. The workaround is to perform one of the following actions: • Clear the ARP cache on the connected device. • Use the switchport nonegotiate command on the port to which the device is connected. • Ping from the switch to the connected device.
	When a master switch in a switch stack reloads or loses power and rejoins the stack as a member switch (Switch A), traffic from Switch A to the destination is lost. The workaround is to ping the destination from Switch A.
	When you attempt to reconfigure a flow monitor on an interface, errors occur. The workaround is to use the no flow monitor command in interface configuration mode and then configure flow monitor on the interface again.
	When the switch reverts from a floating static route to a static route, packets are lost. The workaround is to set static ARP.

Application Notes

Observe these guidelines when using the Device Manager Web interface.

- You cannot create and manage switch clusters through the Device Manager Web interface. To create and manage switch clusters, use the command-line interface (CLI) or the Network Assistant application.

  When creating a switch cluster or adding a switch to a cluster, follow these guidelines:

  – When you create a switch cluster, we recommend configuring the highest-end switch in your cluster as the command switch.
  – If you are managing the cluster through Network Assistant, the switch with the latest software must be the command switch.
  – The standby command switch must be the same type as the command switch. For example, if the command switch is a Stratix 8300 switch, all standby command switches must be Stratix 8300 switches.

- We recommend this browser setting to speed up the time needed to display the Device Manager Web interface from the Microsoft Internet Explorer browser.

  Follow these steps in the Microsoft Internet Explorer browser.

  1. Choose Tools >Internet Options.
  2. Click Settings in the Temporary Internet files area.
  3. From the Settings window, choose Automatically.
  4. Click OK.
  5. Click OK to exit the Internet Options window.

Additional Resources

These documents contain additional information concerning related products from Rockwell Automation.

Resource	Description
Stratix 8000 and Stratix 8300 Ethernet Managed Switches Installation Instructions, publication 1783-IN005	Describes how to get started installing and configuring the switch.
Stratix 8000 and Stratix 8300 Ethernet Managed Switches 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.

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

Rockwell Automation Support

Rockwell Automation provides technical information on the Web to assist you in using its products. At http://www.rockwellautomation.com/support, you can find technical manuals, 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. You can also visit our Knowledgebase at http://www.rockwellautomation.com/knowledgebase for FAQs, technical information, support chat and forums, software updates, and to sign up for product notification updates.

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

Installation Assistance

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

United States or Canada	1.440.646.3434
Outside United States or Canada	Use the Worldwide Locator at http://www.rockwellautomation.com/support/americas/phone_en.html, or contact your local Rockwell Automation representative.

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 to complete the return process.
Outside United States	Please contact your local Rockwell Automation representative for the return procedure.

Documentation Feedback

Your comments will help us serve your documentation needs better. If you have any suggestions on how to improve this document, complete this form, publication RA-DU002, available at http://www.rockwellautomation.com/literature/.

Rockwell Otomasyon Ticaret A.Ş., Kar Plaza İş Merkezi E Blok Kat:6 34752 İçerenköy, İstanbul, Tel: +90 (216) 5698400

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 NV, Pegasus Park, De Kleetlaan 12a, 1831 Diegem, 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-RN002F-EN-P - December 2012
Supersedes Publication 1783-RN002E-EN-P - August 2011