Allen-Bradley

Stratix 8000 and Stratix 8300 Ethernet Managed Switches

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

About This Publication

These release notes provide hardware and software enhancements, anomalies, and other usage considerations for the Stratix 8000 and 8300 Ethernet Managed Switches, revision 4.002 [12.2(55)SE].

Enhancements

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

Enhancement	Description
CDP and LLDP	Exchanging location information with video end points for dynamic location-based content distribution from servers.
Auth-default ACL	Dynamic creation or attachment of an anti-auth default ACL on a port having no configured static ACL.
AAA guarantee-first	Enabling or disabling system accounting as the first record.
Supression	An option to supress verbose 802.1*x*, authentication manager, and MAC authentication bypass syslog messages.
NVRAM buffer	Ability to increase NVRAM buffer size for saving large configuration files.
ARP tracking probe	Enhancement to ARP tracking probe to specify a source IP address for a VLAN.
SFP modules	Support for 100EX SFP modules, version -02 (10-2262-02) or later.

Corrected Anomalies

This section describes anomalies corrected in this revision.

Anomaly	Description
Buffer space	The buffer space of a switch running TCP applications is full while the TCP sessions are in the TIME_WAIT state. Buffer space becomes available after the TCP session is closed.
Show interfaces privileged EXEC command	On a switch running version 12.2(46)SE, the output of the show interfaces privileged EXEC command shows 0 packets for port channel input and output rates. Reload the switch by entering the reload privileged EXEC command.
Switch failure	A switch that has at least one trunk port configured might fail when you configure more than 950 VLANS by using the vlan vlan-id global configuration command.
Switch stops on authentication	A switch running version 12.2(53)SE1 stops when IEEE 802.1*x* authentication is enabled. Apply a VLAN that the RADIUS server assigned to the switch.
ACL messages	After you apply an ACL, these messages appear: %IPACCESS-4-INVALIDACL: Invalid ACL field: Acl number is 0 %IPACCESS-4-INVALIDACL: Invalid ACL field: Acl type is 145
Client access	If the RADIUS authentication server is unavailable and inaccessible authentication bypass is enabled, the switch grants the client access to the network by putting the connected port in the critical-authentication state in the RADIUS-configured or the user-specified access VLAN. After the server is available, the client is not re-initalized and moved out of the critical VLAN.
Personal computer authentication	A personal computer in 802.1*x* or Multidomain Authentication (MDA) mode is connected to an IP phone and connected to a MDA-enabled switch port. After the personal computer and phone are authenticated on the port, the personal computer is down. The port does not automatically re-authenticate the personal computer.
Multidomain authentication	Multidomain authentication (MDA) with guest VLAN or MAC authentication bypass (MAB) as a fallback method is enabled on a switch running IOS revision 12.2(53)SE. When a non-802.1*x* client is connected to an IP phone and the phone is connected to a switch port, and shuts down and then restarts, the client MAC address status is dropped in the MAC address table. It takes 5 minutes for the client to access the network.
Error message	This error message is displayed after copying a configuration file to the running configuration file fails: %Error opening system:/running-config (No such file or directory) The output of the dir system:/ EXEC command also does not show a running configuration file. The workaround is to reload the switch.

Known Anomalies

This section describes known anomalies associated with this revision.

Anomaly	Description	Workaround
EtherChannel ports	When ports in an EtherChannel are linking up, the message EC-5-CANNOT_BUNDLE2 might appear. This condition is often self-correcting, indicated by the appearance of EC-5-COMPATIBLE message following the first message. On occasion, the issue does not self-correct, and the ports may remain unbundled.	Reload the switch or restore the EtherChannel bundle by shutting down and then enabling the member ports and the EtherChannel in this order: • Enter the shutdown interface configuration command on each member port. • Enter the shutdown command on the port-channel interface. • Enter the no shutdown command on each member port. • Enter the no shutdown command on the port-channel interface.
Cluster compatibility	You cannot create or manage switch clusters by using the Device Manager web interface.	To create switch clusters, use the command-line interface (CLI) or the network assistant (CNA): • We recommend configuring the most powerful switch in your cluster as the command switch. • If you manage the switch cluster by using the CNA, the switch with the latest operating software version should be the command switch. **Important:** Switch version 12.2(46)SEI and later are compatible only with CNA version 5.4 and later. • The standby switch must be the same type as the command switch. For example, if the command switch is a Stratix 8000 switch, all standby command switches must be Stratix 8000 switches.

Anomaly	Description	Workaround
Configuration	A static IP address might be removed when the previously acquired DHCP IP address lease expires. This anomaly occurs when the following occurs: • The switch is powered up without a configuration.txt file in switch memory. • The switch is connected to a DHCP server configured to supply an address to the switch (they dynamic IP address is assigned to VLAN 1). • An IP address is configured on VLAN1 before the dynamic address lease assigned to it expires.	Reconfigure the static IP address.
	When the switch is receiving frames, and is connected to some third-party devices that send early preambles, a switch port operating at 100 MBps full- or half-duplex may 'bounce' the line protocol up and down.	Configure the port for 10 MBps, half-duplex, or connect a hub or a non-affected 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 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 switch functionality.
	The far-end fault optional facility is not supported on the GLC-GE-100FX SFP module.	Configure aggressive UDLD.
	When you enter the boot host-retry timeout global configuration command to specify the amount of time the client should try 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.	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 restarted.	Use the rep lsl-age-out timer interface configuration command to configure the REP LSL age timer for more than 1000 ms (1 second).
Ethernet	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 addresses. 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 occurs on EtherChannel ports.	Changing the load balance distribution method or changing the number of ports in the EtherChannel can resolve this anomaly. 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 (for example, 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.
IP	When the rate of received DHCP requests exceeds 2000 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 from occurring.

Anomaly	Description	Workaround
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. 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 IG MP 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 only applicable 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.	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 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.

Anomaly	Description	Workaround
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.	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 might 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 might 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.
SPAN and RSPAN	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.	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 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 status indicator blinks amber, and the frames are not counted on the interface statistics.	There is no workaround.
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. 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.
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.

Application Notes

You cannot create and manage switch clusters through the device manager. To create and manage switch clusters, use the CLI or Cisco Network Assistant.

We recommend this browser setting to speed up the time needed to display the device manager from the Microsoft Internet Explorer browser.

From the Microsoft Internet Explorer browser, perform the following steps.

1. From the Tools menu, choose Internet Options.
2. Click Settings in the 'Temporary Internet files' area.
3. From the Settings dialog box, choose Automatically.
4. Click OK.
5. Click OK to exit the Internet Options dialog box.

   The HTTP server interface must be enabled to display the device manager. By default, the HTTP server is enabled on the switch. Use the show running-config privileged EXEC command to see if the HTTP server is enabled or disabled.

Beginning in privileged EXEC mode, follow these steps to configure the HTTP server interface.

Step	Command	Purpose
1	configure terminal	Enter Global Configuration mode.
2	ip http authentication {aaa | enable | local}	Configure the HTTP server interface for the type of authentication that you want to use: • aaa—Enable the authentication, authorization, and accounting feature. You must enter the aaa new-model interface configuration command for the aaa keyword to appear. • enable—Enable password, which is the default method of HTTP server user authentication, is used. • local—Local user database, as defined on the Cisco router or access server, is used.
3	end	Return to privileged EXEC mode.
4	show running-config	Verify your entries.

The Device Manager web interface uses the HTTP protocol (the default is port 80) and the default method of authentication (the enable password) to communicate with the switch through any of its Ethernet ports and to allow switch management from a standard web browser.

Use care when changing the switch IP information. If you change the HTTP port, you must include the new port number when you enter the IP address in the browser Location or Address f**ield** (for example, http://10.1.126.45:184 where 184 is the new HTTP port number). You should write down the port number through which you are connected.

If you are not using the default method of authentication (the enable password), you need to configure the HTTP server interface with the method of authentication used on the switch.

Beginning in privileged EXEC mode, follow these steps to configure the HTTP server interface.

Step	Command	Purpose
1	configure terminal	Enter Global Configuration mode.
2	ip http authentication {enable | local | tacacs}	Configure the HTTP server interface for the type of authentication that you want to use: • enable—Enable password, which is the default method of HTTP server user authentication, is used. • local—Local user database, as defined on the Cisco router or access server, is used. • tacacs—TACACS server is used.
3	end	Return to privileged EXEC mode.
4	show running-config	Verify your entries.

Default Password

With revision 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.

Additional Resources

These documents contain additional information concerning related Rockwell Automation products.

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.
Product Certifications website, http://www.ab.com	Provides declarations of conformity, certificates, and other certification details.

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

Allen-Bradley, Rockwell Software, Rockwell Automation, Stratix 8000, Stratix 8300, and TechConnect are trademarks of Rockwell Automation, Inc.

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

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-RN002D-EN-P - September 2010

Supersedes Publication 1783-RN002C-EN-E - December 2009

Copyright © 2010 Rockwell Automation, Inc. All rights reserved. Printed in the U.S.A.