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, release 4.001 [12.2(52)SE].

Enhancements

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

Enhancement	Description
IP source guard	Support for IP source guard.
Change of Authorization (CoA)	When a change in policy for a user or group occurs, administrators can reinitialize authentication and apply new policies.
IEEE 802.1x user distribution	Allows deployments for multiple VLANs (for a group of users) to improve network scalability.
VLAN multi-authentication	When a port is configured for multiple authentication and an AAA server is unavailable, the port is placed in a critical VLAN to permit access to critical resources.
Customizable Web authentication enhancement	Allows the creation of user-defined login, success, failure, and expire Web pages for local Web authentication.
Network Edge Access Topology (NEAT)	Changes the port host mode and applies a standard port configuration on the authenticator switch port.
VLAN-ID based MAC authentication	Uses the combined VLAN and MAC address information for user authentication. Prevents network access from unauthorized VLANs.
MAC move	Allows hosts to move across ports within the same switch without restrictions. With MAC move, the switch treats the reappearance of the same MAC address on a different port as a new MAC address.
Support for 3DES and AES with version 3 of Simple Network Management Protocol (SNMPv)3	Support for the 168-bit Triple Data Encryption Standard (3DES) and the 128-bit, 192-bit, and 256-bit Advanced Encryption Standard (AES) encryption algorithms to SNMPv3.
DHCP	Including a hostname in the Option 12 field of DHCPDISCOVER packets sends identical configuration files with the DHCP protocol.
DHCP snooping	Enhanced to support the selection of a fixed string-based format for the circuit-id sub-option of the Option 82 DHCP field.
LLPD-MED	Increased support for LLPD-MED by allowing the switch to grant power to the power device (PD), based on the power policy TLV request.

Enhancement	Description
VTP version 3	Includes support for configuring extended range VLANs (VLANs 1006 to 4094) in any VTP mode, enhanced authentication (hidden or secret passwords), propagation of other databases in addition to VTP, VTP primary and secondary servers, and the option to turn VTP on or off by port.
CIP	Enhancement to the Common Industrial Protocol (CIP) that adds the ability to configure DHCP parameters with CIP.
Supported MIBs	Support for the LLPD-MED MIB and the CISCO-ADMISSION-POLICY-MIB.

Corrected Anomalies

This section describes anomalies corrected in this release.

Anomaly	Description
Forward Open request	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 anomaly applies only to unsuccessful forward open response messages.
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.
Precision Time Protocol (PTP) error	When you configure PTP in forward mode by entering the PTP mode forward global configuration command, the PTP page in device manager breaks due to a parser error.
Alarm and Setup status indicators in Device Manager Web interface	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).
Redundant power supply failure	When one power supply connected to the switch in a redundant pair fails, a CIP query continues to show that both supplies are present and okay.
MVR port status	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.
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. However, if you enable MVR first and then create the MVR VLAN, the MVR groups are not displayed correctly.
QoS	When VLAN-based quality of service (QoS) is enabled and then disabled on an interface by entering the mls qos vlan-based interface configuration command followed by the no version of the command, the port policy is not applied properly and could result in undefined behavior for packets matching the port policy.
VLAN tagging	If you enable 802.1Q native VLAN tagging by entering the vlan dot1q tag native global configuration command and then change the native VLAN ID on an ingress trunk port by entering the switchport trunk native vlan vlan-id interface command, untagged traffic is forwarded instead of being dropped.
Memory leaking and shutdown	If you repeatedly enter the show tech-support privileged EXEC command, the switch might leak memory and, in some cases, shut down.
Unexpected reloading	The switch unexpectedly reloads when copying a configuration file from a remote server or from flash memory containing logging file flash.
Login banner	When you have configured a login banner by entering the banner login c message c global configuration command and the switch reloads, the output of banner is missing a carriage return, making the format incorrect.
Link to SFP module	The link between a switch with a 100BaseFX-FE small form-factor pluggable (SFP) module and a connected device remains up when one of the fiber cables is removed.
Remote neighbor updating	When remote neighbors change, the LLDP MIB does not properly update the remote neighbors.

Known Anomalies

This section describes known anomalies associated with this release.

Anomaly	Description	Workaround
Loss of static IP address	A static IP address might be removed when the previously acquired DHCP IP address lease expires. This anomaly occurs when: • the switch is booted up without a configuration (no config.text file in flash memory). • 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). • an IP address is configured on VLAN 1 before the dynamic address lease assigned to VLAN 1 expires.	Reconfigure the static IP address.
Line protocol	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 anomaly occurs only when the switch is receiving frames.	Configure the port for 10 Mb/s and half duplex or to connect a hub or an unaffected device to the switch.
Port security	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.
Traceback error	A traceback error occurs if a crypto key is generated after an SSL client session.	None.
High CPU utilization	When the logging event-spanning-tree interface configuration command is configured and logging into 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 issues 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.
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, which should mean that the client keeps trying indefinitely. However, the client does not keep trying to download the configuration.	Enter a non-zero value for the timeout value when you enter the boot host retry timeout timeout-value command.
REP link status layer (LSL) age-out value	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 s, the REP link flaps if the BFD interface is shut down and then brought back up.	Use the rep lsl-age-out timer interface configuration command to configure the REP LSL age timer for more than 1000 ms (1 s).

Anomaly	Description	Workaround
Traffic on EtherChannel ports	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 same member ports based on hashing results calculated by the ASIC. This causes 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 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.
DHCP requests received rate	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 from occurring.
Multicasting and IGMP snooping routes	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	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.	None.
IGMP report packet	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.	None.
IGMP snooping	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.	None.

Anomaly	Description	Workaround
Incomplete multicast traffic	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.
Configuring switch for a multicast group	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
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.	None.
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.	None.
	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.	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. 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.

Anomaly	Description	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.
Web authentication	When you configure an ACL and enter the access-group interface configuration command to apply it to an interface for web authentication, the output from the show epm session ip-address or show ip access_list interface interface-id privileged EXEC command does not show any web authentication filter ID.	None.
Port channel input and output rates	On a switch running IOS release 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.
IP phone network connectivity	On switches running IOS release 12.2(50)SE3 running MAC authentication bypass with multidomain authentication (MDA), IP phones connected to a port might not be able to regain network connectivity in the VOICE domain if the session times out and all RADIUS servers are unreachable.	None.

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 Compatibility

Cisco Network Assistant (CNA), version 5.5 is compatible with release 4.001 and earlier of the switches.

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 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.

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, 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://www.rockwellautomation.com/support.

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

Allen-Bradley, Rockwell Automation, Rockwell Software, Stratix 8000 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-RN002C-EN-E - December 2009
Supersedes Publication 1783-RN002B-EN-E - May 2009
Copyright © 2009 Rockwell Automation, Inc. All rights reserved. Printed in the U.S.A.