ExtremeSwitching 200 Series: Release Notes

Version V01.01.01

121188-00

Published May 2017

Legal Notice

Extreme Networks, Inc. reserves the right to make changes in specifications and other information contained in this document and its website without prior notice. The reader should in all cases consult representatives of Extreme Networks to determine whether any such changes have been made.

The hardware, firmware, software or any specifications described or referred to in this document are subject to change without notice.

Trademarks

Extreme Networks and the Extreme Networks logo are trademarks or registered trademarks of Extreme Networks, Inc. in the United States and/or other countries.

All other names (including any product names) mentioned in this document are the property of their respective owners and may be trademarks or registered trademarks of their respective companies/owners.

For additional information on Extreme Networks trademarks, please see:
www.extremenetworks.com/company/legal/trademarks

Software Licensing

Some software files have been licensed under certain open source or third-party licenses. End-user license agreements and open source declarations can be found at:
www.extremenetworks.com/support/policies/software-licensing

Support

For product support, phone the Global Technical Assistance Center (GTAC) at 1-800-998-2408 (toll-free in U.S. and Canada) or +1-408-579-2826. For the support phone number in other countries, visit: http://www.extremenetworks.com/support/contact/

For product documentation online, visit: https://www.extremenetworks.com/documentation/

Table of Contents

Preface

Providing Feedback to Us

We are always striving to improve our documentation and help you work better, so we want to hear from you! We welcome all feedback but especially want to know about:

- Content errors or confusing or conflicting information.
- Ideas for improvements to our documentation so you can find the information you need faster.
- Broken links or usability issues.

If you would like to provide feedback to the Extreme Networks Information Development team about this document, please contact us using our short online feedback form. You can also email us directly at internalinfodev@extremenetworks.com.

Getting Help

If you require assistance, contact Extreme Networks using one of the following methods:

- GTAC (Global Technical Assistance Center) for Immediate Support
  - Phone: 1-800-998-2408 (toll-free in U.S. and Canada) or +1 408-579-2826. For the support phone number in your country, visit: www.extremenetworks.com/support/contact
  - Email: support@extremenetworks.com. To expedite your message, enter the product name or model number in the subject line.
- GTAC Knowledge — Get on-demand and tested resolutions from the GTAC Knowledgebase, or create a help case if you need more guidance.
- The Hub — A forum for Extreme customers to connect with one another, get questions answered, share ideas and feedback, and get problems solved. This community is monitored by Extreme Networks employees, but is not intended to replace specific guidance from GTAC.
- Support Portal — Manage cases, downloads, service contracts, product licensing, and training and certifications.

Before contacting Extreme Networks for technical support, have the following information ready:

- Your Extreme Networks service contract number and/or serial numbers for all involved Extreme Networks products
- A description of the failure
- A description of any action(s) already taken to resolve the problem
- A description of your network environment (such as layout, cable type, other relevant environmental information)
- Network load at the time of trouble (if known)
- The device history (for example, if you have returned the device before, or if this is a recurring problem)
- Any related RMA (Return Material Authorization) numbers

Related Publications

200 Series Documentation

- *ExtremeSwitching 210 and 220 Series Switches: Hardware Installation Guide*
- *ExtremeSwitching 240 Series Switches: Hardware Installation Guide*
- *ExtremeSwitching 200 Series: Administration Guide*
- *ExtremeSwitching 200 Series: Command Reference Guide*

Other Documentation

- *Extreme Hardware/Software Compatibility and Recommendation Matrices*
- *Extreme Networks Pluggable Transceivers Installation Guide*
- *Environmental Guidelines for ExtremeSwitching Products*

Open Source Declarations

Some software files have been licensed under certain open source licenses. More information is available at: www.extremenetworks.com/support/policies/software-licensing

1 Software Features

This section lists the 200 Series software features supported for each operating platform.

Feature	Supported on Platform	
	220 Series	210 Series
802.1D	Yes	
802.1S	Yes	
802.1W	Yes	
802.1Q VLAN Tagging	Yes	
Private VLAN	Yes	
GARP/GVRP	Yes	
802.1p	Yes	
802.3x (Full Duplex & Flow Control)	Yes	
Asymmetric Flow Control	Yes	
RPVST / PVST	Yes	
802.1x	Yes	
Guest VLAN	Yes	
RADIUS-based VLAN assignment via.1x	Yes	
RADIUS-based filter ID assignment via .1x	Yes	
MAC-based .1x	Yes	
Supplicant	Yes	
MAC-based Authentication Bypass	Yes	
802.3ad – LAGs	Yes	
LACP	Yes	
Static LAGs	Yes	
Minimum active links features (LAGs)	Yes	
Storm Control	Yes	
Port Mirroring	Yes	
– Tx/Rx	Yes	
– Many to One Port Mirroring	Yes	
– LAGs supported as source ports	Yes	
– RSPAN	Yes	
RMON 1,2,3 & 9	Yes	
Static L2 Multicast Filtering	Yes	

Feature	Supported on Platform	
	220 Series	210 Series
MLD Snooping	Yes	
IGMP Snooping	Yes	
– Enable IGMP Snooping per VLAN	Yes	
– Snooping Querier	Yes	
Voice VLAN	Yes	
Protected Ports (Private Edge VLAN)	Yes	
802.1ab LLDP	Yes	
802.1ab LLDP-MED	Yes	
Static L2 Entries	Yes	
STP Root Guard	Yes	
BPDU Guard	Yes	
Dynamic ARP Inspection	Yes	
DHCP/DHCPv6 Client	Yes	
SHCP Snooping	Yes	
DHCP Client Option 60	Yes	No
DHCP L2 Relay (Option 82) per VLAN or per 802.1ad sub.	Yes	
Auto Install (DHCP Opt 55, 66, 67, 125 &150)	Yes	
sFLow	Yes	
GMRP	Yes	
Cable Test	Yes	
Outbound Telnet	Yes	
Syslog (RFC 3164)	Yes	
Port MAC Locking	Yes	
SNTP	Yes	
Denial of Service Protection (control plane)	Yes	
Denial of Service Protection (data plane)	Yes	
TACACS+	Yes	
Radius	Yes	
Management ACL	Yes	
Persistent log supported	Yes	
LAG Hashing	Yes	
ISDP	Yes	
STP Loop Guard	Yes	
Energy Efficient Ethernet	Yes	

Feature	Supported on Platform	
	220 Series	210 Series
UDLD	Yes	
802.1ak MMRP	Yes	
802.1ak MVRP	Yes	
MVR	Yes	
Routing		
Static Routing	Yes	
Port based Routing	Yes	
VLAN Routing	Yes	
– 802.3ad (LAG) for router ports	Yes	
RIPv2	Yes	No
Proxy ARP	Yes	
Multinetting	Yes	
ICMP redirect detection in hardware	Yes	
DNS Client	Yes	
DHCPv4/v6 Server	Yes	
Management Functionality		
Password Management	Yes	
CLI Commands logged to a syslog Server	Yes	
Web-based management	Yes	
Telnet	Yes	
IPv6 management	Yes	
SNMP v1/v2/v3	Yes	
SSH	Yes	
– SSH Session Configuration	Yes	
SSL / HTTPS	Yes	
File Transfer – HTTP, TFTP, FTP, SCP, SFTP	Yes	
CLI Scripting	Yes	
Text-based Configuration File	Yes	
HTTP download (firmware)	Yes	
QOS		
Access Control Lists	Yes	
– LS MAC ACLs	Yes	
– Ingress ACLs	Yes	
– Egress ACLs	Yes	No

Feature	Supported on Platform	
	220 Series	210 Series
– 802.3ad (LAG) for ACL assignment	Yes	
– Binding ACLs to VLANs	Yes	
– ACL Logging	Yes	
– Flow-based mirroring	Yes	
– Support for IPv6 fields	Yes	
Diffserv	Yes	
– Edge Node applicability	Yes	
– Interior Node applicability	Yes	
– 802.3ad (LAG) for service interface	Yes	
– Support for IPv6 fields	Yes	
– Egress	Yes	No
COS	Yes	
– 802.3ad (LAG) for COS configuration	Yes	
AutoVoIP	Yes	
– Protocol-based	Yes	
– OUI-based	Yes	
Stacking		
Support for stacked switches	Yes	No
Non-stop forwarding	Yes	No

2 Metrics

This section lists the supported limits, or maximum values, for 200 Series software features.

Feature	Maximum Value for Platform	
	220 Series	210 Series
Max source mirror ports in a session	Max on switch	
Max # of Management ACL Rules	64	
Max # of IP Helper Entries	512	
Max # of HTTP Sessions	3	
Max # of SSL/HTTPS Sessions	4	
Max # of configured users	6	
Max user name length	64	
Max password length	64	
Max # of IAS users	100	
Authentication Login list		
– Max Count	5	
– Max methods per list	4	
– Max name length	15	
Authentication Enable lists		
– Max Count	5	
– Max methods per list	4	
– Max name length	15	
Authentication HTTP lists		
– Max Count	1	
– Max methods per list	4	
– Max name length	15	
Authentication HTTPS lists		
– Max Count	1	
– Max methods per list	4	
– Max name length	15	
Authentication Dot1x lists		
– Max Count	1	
– Max methods per list	4	
– Max name length	15	

Feature	Maximum Value for Platform	
	220 Series	210 Series
Authentication exec lists		
– Max Count	5	
– Max methods per list	2	
– Max name length	15	
Accounting Commands lists		
– Max Count	5	
– Max methods per list	1	
– Max name length	15	
Login History	50	
Max units per Stack	4	NA
Max physical ports per stack	208	NA
Max # of remote Telnet connections	5	
Max # of remote SSH connections	2	
MAC Addresses	16K	
Max agetime (s)	1000000	
Max # of VLANs	1024	
Maximum VLAN ID	4093	
Number of 802.1p Traffic Classes (stk / non-stk)	7/8	8
Maximum multiple spanning tree instances	4	
(R)STP-PV Max VLANs/Max VLANs * Interfaces	8/2014	
Number of log messages buffered	200	
Static Filter Entries		
– Unicast MAC & source port	20	
– Multicast MAC & source port	20	
– Multicast MAC & destination port (only)	1024	
Maximum MFDC entries	1024	512
Jumbo Frame – Max size	9K	
Max number of DHCP Bindings	4K	8K
Max number of DHCP snooping static entries	1024	1024
Port MAX Locking		
– Dynamic address per port	600	
– Static addresses per port	20	
Radius		
– Max Authentication servers	16	

Feature	Maximum Value for Platform	
	220 Series	210 Series
– Max Accounting servers	16	
Number of Static Routes	64	60
Max # of DHCP Pools	8	
Total # of leases	128	
DNS Client		
– Concurrent request	16	
– Name server entries	8	
– Static host entries	64	
– Cache entries	128	
– Domain search list entries	32	
# Routing interfaces (including port/vlan)	15	
Static v4 ARP Entries	16	
# ACLs	100	
Maximum @ of configurable Rules per list	1023	
COS - # Configurable Queues per port	7	8
COS – Configurable Drop Precedence Levels	3	
Diffserv - # Queues	7	8
Diffserv – Max Rules per Class	13	
DIffserv – Max Instances per Policy	28	
Diffserv – Max attributes per Instance	3	
Diffserv – Max Service Interfaces	60	56
AutoVoIP Number of simultaneous voice calls	20	
Voice VLAN Number of devices	64	

3 Operational Characteristics and Known Issues

The following sections list operational characteristics and known issues associated with the 200 Series software.

200 Series Base System

1. S2xx-179575, S2xx-179447. The 200 Series software cannot read SFP diagnostic information.
2. S2xx-181872. If the deployment traffic scenario contains only jumbo frames, then the minimum bandwidth settings will be inaccurate by 20%.
3. ExtremeCloud support in this release is limited to image and connector upgrades only.
4. Adding a default route to the routing function may disrupt connectivity to the service port in a device running Linux. The Linux networking stack will use the first entry in its routing table that matches a particular address.

   Multiple default routes will result in behavior that is dependent on the order in which those routes appear in the routing table.
5. The 200 Series software assigns a MAC address to the service port as follows: base MAC address + 1.
6. Devices with Ethernet service ports are generally supported with network drivers included as part of the standard Linux kernel sources. Some of these drivers choose to log status changes to the system console. Such console messages (generally referring to “eth0”) can be safely ignored.
7. S2xx-35136: It is possible to obtain neighbor table related messages on the console if the kernel IPv6 neighbor table is exceeded.

Switching

1. 200 Series software implements IEEE 802.1s running in IEEE 802.1w-compatibility mode, rather than the IEEE 802.1w protocol itself. As such, ANVL RSTP test suites are not supported. ANVL MSTP Test cases are supported.
2. S2xx-30109. Dynamically learned VLANs are not always flushed when GVRP is disabled globally.
3. S2xx-75340. LLDP MED application should not allow configuration of location and inventory transmit TLVs as the underlying application is not present. The switch allows configuring transmission of these location and inventory TLVs even though the underlying application to support location and inventory are not supported. There is no operational impact from this setting, although these TLVs will not be transmitted.
4. S2xx-91249. For Denial of Service ICMP command, 200 Series adds 8 bytes to the value configured by the user, to accommodate the ICMP header size.
5. S2xx-98290. The IP address for a configured trap receiver host name gets resolved at configuration time and is then stored as a resolved address. When configuring through the web interface, if the DNS resolution fails at this time then a null (for example, 0.0.0.0) address is stored.
6. S2xx-98517. The DiffServ policy name received from the RADIUS server as a filter-id attribute in the RADIUS accept message fails to apply on the authorized port when the port control mode is “Auto” (i.e., port-based dot1x mode).
7. S2xx-98879. Automatic configurations (for example, vlan ingressfilter, vlan acceptframe, vlan participation, etc.) done by dot1AD commands can be overwritten by the administrator, but upon save and reload those overwritten commands might not be retained.
8. S2xx-104194. If an SNMP set is used to set the download image name to Image1, and then a get upload image name is performed, the name returned is the download image name. This is due to using a single variable in the application. No upload/download functionality is impacted; it is only a display issue.
9. S2xx-108568. When the network port is connected to stacking member unit, ping reply takes up to 40 ms to 50 ms.
10. S2xx-110640, S2xx-116224. When there are large numbers of MSTP instances and large numbers of connected ports to another switch and auto edge (auto portfast) is enabled, there is a chance of small loop when one of the switches reboots causing traffic disruption and NSF failover takes up to 5 seconds.
11. S2xx-112703. Occasionally, when dot1x is enabled on a port and a VLAN participates in this dot1x enabled unauthorized port, the port egresses the traffic on that VLAN.
12. S2xx-124582. Unable to register voice device MAC address when Voice VLAN authentication is enabled with IP phones supporting ISDP. When Voice VLAN authentication is enabled with VoIP phones supporting ISDP, and MAB is enabled with a Guest VLAN timer of 10 seconds, the port is kept in the held state for 10 seconds by dot1x and, after the timer expires, DUT treats the VoIP device as a dot1x unaware client and authenticates the port using MAB. The entire process takes more than 10 seconds to complete and, once the port is authorized, DUT then waits for VoIP queries from the phone to add the device to Voice VLAN. But, when ISDP is enabled, the VoIP phone sends only 8 or 9 VoIP queries and is not sending them periodically. So after the port is authorized, we are not receiving any queries and the device is not added to Voice VLAN. A workaround for this problem is to configure the Guest VLAN timer to less than 5 seconds when ISDP is enabled.
13. S2xx-129490. SNMP walk is not successful while doing walk on root port. The complete SNMP walk on agentConfigGroup or any higher node (for example, fastPathSwitching node or the root node) is successful all the times through MG-SOFT SNMP browser. When the same is performed using Net-

SNMP, the timeout interval must be set to 2 or more seconds. Otherwise it says, Timed out and SNMP walk operation is not successful.

14 S2xx-149479, S2xx-103674. When RADIUS or Syslog uses a DNS host name for configuring server entries, they are unaware of changes in the DNS cache host mapping. When a RADIUS or Syslog server entry is added, the DNS host address is resolved and is persistent until the server entry times out; therefore, the RADIUS or Syslog application attempts to send the packet to the RADIUS or Syslog server configured on the switch.

15 S2xx-158505. When maximum MSTP instances are configured and a large number of ports are connected to another switch, continuous log messages are observed and the switch becomes nonresponsive.

16 S2xx-158745. The `clear config` command maintains the previous Ethernet counters after a `clear counters all` command.

17 S2xx-171812. Dropping unregistered multicast data and flooding of unregistered multicast data only to mrouter ports is not supported for port based MGMD snooping.

18 S2xx-183177. User/administrator cannot remove a physical port from the LAG if the admin key configured on LAG interface is different from the physical port's admin key.

19 The PVSTP/PVRSTP feature has issues handling a large number of BPDUs by virtue of the number of interfaces participating in VLANs that are PVSTP/PVRSTP enabled. The failure scenarios include, but are not limited to:

- Unexpected topology changes in xSTP.
- Very long times for convergence.
- Message delivery failures in stacking.
- (Very stressful conditions only) System reboots and crashes.

The present solution scales reasonably well up to a cumulative total of around 200 [interface, VLAN] tuples participating in PVSTP/PVRSTP, beyond which system behavior is unpredictable.

20 S2xx-205769. The RA packet counters are per rule and are incremented whenever a packet matches the rule (rather than when an action corresponding to a matching rule is taken). Hence, there is a possibility that the counters get incremented even when the action corresponding to the RAGUARD rule was not taken. It is not recommended to attach conflicting ACL rules on the interface on which RAGUARD is configured.

21 S2xx-235436. The user can configure duplicate rules for Management ACAL. The duplicate rules have the same behavior and have no functional impact.

22 S2xx-237397. If the MAC limit is set by the user while continuously sending the traffic, MAC addresses learned are more than the configured limit, due to simultaneous Flushing and Learning operations. It is recommended to stop traffic while configuring the MAC-address limit in VLAN MAC Locking.

23 S2xx-12425. The 1519–1522 frame counter is incremented only for VLAN-tagged frames. Untagged frames with that size increment the >1522 counter.

24 S2xx-25949. When DoS is configured, IP packets with the More Fragments bit are not honored.

25 S2xx-25966. For Maximum ICMP packet size Denial of Service (DoS) prevention, Maximum ICMP packet size parameter refers to the ICMP payload size and not the total packet size.

26 S2xx-25971. For Minimum TCP header size DoS prevention, although 200 Series UI specifies to enter the minimum TCP header size, you must enter the minimum TCP payload size. Also, the TCP Fragment Mode DoS feature must be enabled for the Minimum TCP header DoS prevention feature to work.

27 S2xx-27237. MAC addresses can take longer than the age time to age from the hardware MAC table. If the age time is not being changed, it can take up to twice the age time to delete the MAC address. If the age time is changed, it can take up to three times the age time to delete the MAC address.

28 S2xx-27537. In order for jumbo frames to be switched, the Maximum Transmission Unit (MTU) needs to be set on the ingress port as well as on the port that the packet egresses from.

29 S2xx-45367. For short cables, the length reported using cable diagnostics may not be accurate.

30 S2xx-149918. Untagged multicast traffic with reserved MAC addresses 01:80:c2:00:00:14 to 01:80:c2:00:00:15 as destination addresses are not forwarded.

31 S2xx-151777. UDLD frames are not dropped by deny any MAC ACL applied in an outbound direction.

32 S2xx-158985. Unicast Packets Received counter value is not incrementing properly upon receiving unicast traffic with random frame size.

33 MAC address entries may not be inserted in or removed from the CPU's copy of the forwarding database after being learned on the underlying hardware. This is most likely to occur under heavy periods of learning or aging. This does not affect the normal operation of the switch.

34 With storm control enabled on an interface, the threshold (number of packets per second) is calculated on the basis of the speed of the port and the configured threshold level. The threshold is based on an average packet size of 512 bytes.

35 The maximum number of MAC addresses supported by the hardware is offered but not guaranteed. The total number of MAC addresses that can be learned is dependent upon how the VLAN/MAC keys are hashed. The hardware table is broken up into buckets. Once a bucket's entries are used, any other VLAN/MAC keys that hash to that same bucket are not learned. Additionally, L2 multicast and L3 interfaces consume MAC addresses.

36 If you enable port security on a port that is connected to another bridge, you must add the MAC address of the connected interface to the list of entries allowed. Create the static MAC address entry by using the `port security mac-address mac addr vlanid command`. This will ensure that control frames like BPDUs and LAC PDUs from the partner device will not be dropped if the dynamic limit for PML is reached.

37 For port mirroring, in case of unknown DAs and broadcasts egressing the multiple mirrored ports, only one copy of the packet will be seen on the probe, even though the same packet goes out the multiple mirrored ports.

38 S2xx-175112. Ping does not function properly when SNAP encapsulation is enabled on an interface.

39 S2xx-188631. An incorrect short reach status of Inactive might be reported even if auto short reach is enabled on the port and a cable shorter than 10 meters is connected.

40 S2xx-231691. Duplicate IGMP protocol packets are switched. This has a low impact on downstream switches since the traffic rate is usually very low.

Switching SNMP

1 MIB II object ifSpeed does not list LAG ports.

2 The following MIB objects are labeled Not Supported:

   a RFC 1493 Bridge MIB: dot1dTpLearnedEntryDiscards, dot1dStatic Table

   b RFC 1643 Ethernet MIB: dot3Coll Table

   c RFC 2233 Interfaces MIB: ifCounterDiscontinuityTime, ifStackTable, ifRcvAddressTable, ifMIBObjects Group

   d RFC 2674 VLAN MIB: dot1dPortGmrpTable, dot1qFdb Table, dot1qTpFdbTable, dot1qTpGroupTable, dot1qForwardAllTable, dot1qForwardUnregisteredTable,

dot1qStaticUnicastTable, dot1qStaticMulticastTable, dot1qConstraintSetDefault, dot1qConstraintTypeDefault, dot1qPortGvrpFailedRegistrations, dot1qPortGvrpLastPduOrigin, dot1qLearningConstraintsTable

3 In the private MIB, the object agentLagSummaryName cannot be set.
4 Set and Get operations on object dot3adAggPortActorAdminState occurs in reverse order.
5 Cannot change the snmpTargetAddrRowStatus from notInService(2) and notReady(3) states to active(1) state.
6 Deleting entry in snmpNotifyFilterProfileTable and snmpNotifyFilterTable is successful when FilterProfileStoreType is set to permanent(4), and readOnly(5).
7 The VLAN port option AdmitUntaggedOnly is missing in SNMP.

Stacking

1 S2xx-23724. When a new unit is added to the stack, traffic on existing units may be temporarily interrupted.
2 S2xx-41344, S2xx-46247. Moving management while the switch is operational in a network may take several minutes.
3 S2xx-45684. When the user renumbers the management unit, the text configuration is applied.
4 S2xx-45934. When a stack is reloaded, Link aggregation groups may become unstable for a short interval during boot up.
5 S2xx-60197. When reloading multiple units in the stack, it is recommended to either reload all units or reload one unit at a time and wait for it to join the stack before reloading other units.
6 S2xx-72545. When the stacking link between units is oversubscribed, the traffic is handled through weighted round-robin scheduling. Queues 0–6 on stacking links always operate in weighted round robin mode (or weighted deficit round robin mode where supported).

   The consequence of this is that traffic that traverses stack links is scheduled according to the weights of the stack link. An example scenario where this behavior may be visible is when traffic is received on port 1 on unit 1 at a rate of 10 Gbps and is forwarded to port 3 on unit 2. This traffic has a priority of zero. Traffic is received on port 2 on unit 1 at a rate of 10 Gbps and is forwarded to port 3 on unit 2. This traffic has a priority of 6. Port 3 on unit 2 operates at 10 Gbps. The system is configured such that priority 0 maps to queue 0 and priority 6 maps to queue 6. Additionally, the system is configured such that queue 6 operates in strict priority mode.

   Given this scenario, you might expect that only priority 6 traffic will be observed on unit 2, port 3. However, traffic from both priorities 0 and 6 will be observed on this port. This is because the stack link schedules queues 0 and 6 as weighted round robin. Therefore traffic from both priorities arrives on unit 2. Since port 3 operates at 10 Gbps, traffic from both priorities is egressed because there is less than 10 Gbps of priority 6 traffic received at unit 2.
7 S2xx-77849. Invalid user queue configurations can lead to stack instability. The Series 200 switches send PDUs on queues 5 and 6 (stacking builds) or 6 and 7 (non-stacking builds). The user configuration must ensure that these queues can always be serviced by the scheduler. Otherwise these queues may get backed up and the system may get into a situation where the CPU cannot send any packets (either to front panel ports or to other CPUs in the stack). In this condition the stack may get detached and network protocols may not behave properly.

As an example, consider a configuration where queue 4 is set to operate in strict priority. Given this configuration, the administrator should also set queues 5 and 6 to operate in strict priority to guarantee that the CPU can send PDUs in a timely manner.

8 S2xx-158470. When CPU is flooded with control packets on an 8 unit stack, a code download fails. More traffic is generated on CPU queue 7 and the CPU is not able to handle this rate causing packet drops on queue 7 because of which a code download fails. This may also cause the stack to fall apart.

QoS

1 ACL operational characteristics:
   - A single ACL is limited to the number of user-configurable rules supported by the platform. Multiple L2 and L3 ACLs can be applied to the same interface, as long as the total number of combined rules fit within the platform-specific limit.

2 CoS Queuing operational characteristics:
   - Egress CoS minimum bandwidth guarantees on a LAG assume equal traffic distribution across all members.
   - Egress port rate shaping on LAGs assume equal traffic distribution across all members.
   - The actual guaranteed minimum bandwidth allocation might differ slightly from the configured value. The deviation varies depending on the average frame size.
   - The upper limit on the guaranteed minimum bandwidth for a single queue is 68%.
   - S2xx-27778. IP Precedence to priority mapping is not supported.
   - S2xx-27783. In Trust IP-DSCP mode, the DSCP table maps to 802.1p priority directly. This means that tagged IP packets mapped via the DSCP table will be marked with a new 802.1p priority upon egress, as well as being assigned the specific CoS queue. In a stacking package, queue 7 is reserved for stacking CPU-to-CPU traffic.

3 DiffServ operational characteristics:
   - ACL lists and DiffServ policies cannot coexist on the same interface. However, it is possible for DiffServ to emulate ACL functions using the policy attribute drop.
   - For policing policies on LAGs, the meters are allocated on a per-unit basis and all ports on a unit update the meter. However, the meters cannot be shared across units in a stack or in back-to-back configurations. In these cases, the metered rate will be maintained separately per unit.
   - Policing policies can be color-aware based upon IP Precedence or IP DSCP only.
   - For policing statistics, all non-conforming traffic is counted as in-discarded-packets even if the nonconforming action is not set to discard.
   - DSCP and IP precedence can be marked for both policing conforming traffic and non-conforming traffic.
   - S2xx-29181. Policing rate is configurable in increments of 64 Kbps. If the specified value is not an integral multiple of 64, it is rounded down to the immediately lower multiple of 64.
   - S2xx-126438. When configuring Traffic Class Groups (TCGs), the user must assign queues to TCGs in order from lowest TCG to highest TCG. When only TCG0 and TCG2 are used, and TCG1 is added later, all queues must first be assigned to TCG0, then all three TCGs may be configured in

order. If queues are moved from one TCG to another TCG, the TCG is considered unused and the ordering requirement applies.

- S2xx-206662. After issuing the clear counters all command, congestion drops, but the counter does not get cleared. Users need to compare the previous reported values with the current values to determine the delta.

QoS (DiffServ) Configuration

1. DiffServ configuration is intended for use only with IP packets.
2. The optional `match not` command in Class-Map Config mode, when specified, is used to negate the class match condition. This parameter is not supported for the class-map (for example, reference class) match condition.
3. The IP DSCP, IP Precedence, and IP TOS (with mask) class match conditions are alternative methods to specify classification based on the contents of the IP Service Type (TOS) octet in the IP packet header:
   - IP DSCP compares the high-order six bits of the IP Service Type octet and ignores the remaining bits, or
   - IP Precedence compares the high-order three bits of the IP Service Type octet and ignores the remaining bits, or
   - The IP TOS (with mask) is intended for use as a free-form match specification of the IP Service Type octet.
4. A class of type all or any may reference at most one other class, but it must be of the same class type. Class referencing is not supported for class type ACL. Class references may be chained, but the total number of class match conditions in a chain is limited to twice the maximum number of rules normally allowed for a single class (actual value is platform specific).
5. The Service Table Operational Status denotes the current up/down state of the DiffServ operation on the directional service interface. For the DiffServ Operational Status to be up, all of the following conditions must be true:
   - A policy is successfully attached to the service interface in the appropriate direction.
   - The policy contains one or more policy-class instances (it need not have policy attributes defined when best-effort service is desired).
   - Each policy-class instance refers to a valid class.
   - A valid class consists of at least one class match condition.
   - Each class match condition is supported by the policy type (direction) based on platform features and limitations.
   - All MIB table rows representing each of the preceding items must have a row status of active (of particular importance when using SNMP).
   - The port must be up, administratively enabled, and generally able to forward traffic.
6. S2xx-79708. The bucket count for EFP meters is only modified when bytes are actually egressed on the port. If the conforming action is drop, the conforming packets are not transmitted, and the bucket counter is not changed. Therefore, all packets end up being treated as conforming packets and are discarded in this configuration.

QoS (DiffServ) SNMP

1. The following items pertain to the DiffServ standard MIB support (RFC 3289):

- This MIB is supported as read-only. All SNMP configurations for DiffServ are handled through a private MIB (FASTPATH-QOS-DIFFSERV-PRIVATE-MIB).
- The object diffServAlgDropQThreshold is not supported and always reads 16384 (for example, 16 KB).
- The IP Multifield Classification Table (diffServMultiFieldClfrTable) is not used. Instead, an Auxiliary Multifield Classification Table (agentDiffServAuxMfClfrTable) is defined in a Broadcom extension to the standard MIB (FASTPATH-QOS-DIFFSERV-EXTENSIONS-MIB) and is used for all DiffServ classifier definitions. This extension's MIB is also supported as read-only.

2 Regarding the DiffServ private MIB: If a platform only supports Service Table actions for all interfaces in a particular direction (that is, does not allow individual <slot.port> specification), then any SNMP set operation performed on an individual object instance in the agentDiffServServiceTable is automatically applied to all supported DiffServ service interface instances in that direction.

Routing

1 Source IP address checking is not performed for packets routed in hardware. For IP packets sent to the CPU for forwarding, the source IP address is checked and those packets containing a net-directed broadcast or any value 224.0.0.0 or higher (including the limited broadcast) address are silently discarded.

2 S2xx-32084. The DHCP server supports no more than 16 static address mappings.

3 S2xx-32087. The DHCP Server gives priority to the IP address requested by the client over a manually configured IP address.

4 S2xx-80714. If DHCP server is enabled, after the reload cycle, the client renews its IP address along with lease time. This lease time has to be saved to the configuration data for next reload cycle. Therefore, the user sees prompt to save the data on reload command.

5 S2xx-87339. In a stacking environment, when the system has a large startup configuration to apply, OSPF adjacencies may be lost temporarily.

6 S2xx-108571. DHCPv6 Client does not send a Release message upon disabling the routing interface. The user does not have any impact with this behavior, but the server reserves the address for this client until the binding entries get timed out.

7 S2xx-154991. While the system boots up, a couple of link flaps are observed on fiber ports. Because of this, the routing interface is suppressed after reload, even though the restart-penalty is less than suppress threshold.

8 S2xx-172759. Any Control Traffic with a match on "match term" in a route-map that is applied on an interface is affected if the action specified through "set terms" routes that traffic differently. This is because if the route-map specified "set term" to policy route packet to a different next-hop, then things such as "neighbor-ship not getting formed" will occur.

9 S2xx-172866. When an ACL rule contains a rate-limit action or any action that requires metering in hardware, that particular ACL is not a candidate to be included in route-map statement as match condition. This is because, for each route-map statement, we add counters. As meters and counters are mutually exclusive in hardware, applying a route-map with such ACL in a match condition results in a failure.

10 S2xx-173871. An IP assigned from the DHCP server is not fully removed after disabling and enabling DHCP on the routing management port.

11 S2xx-185220. When using the CLI, the configured client identifier cannot be seen in the `show ip dhcp pool configuration all` command output. The `show running-config` command shows the configured client identifier value.

12 S2xx-222483. When traceroute is initiated with large packet sizes, some of the fragments may get dropped due to ICMP rate limiting.

Security

1 A dot1x port that is up and authenticated may not return to the authenticated state after a switch reboot when spanning tree is enabled. The recommended workaround is to set the RADIUS server timeout to 15 seconds or higher.

2 When enabling SSH on a system that does not have the private keys, the CLI will be unresponsive while creating the RSA and DSA private keys. There is no indication on the CLI that the keys are being generated. The amount of time that the system remains unresponsive is system dependent.

3 For SSL/TLS, the device will not generate its own certificates, and no default certificates are present. In order to use SSL/TLS, certificates must be obtained (in PEM format) from a certificate granting authority (commercial or otherwise) and downloaded to the device. Tools for establishing a certificate granting authority are not provided with 200 Series software.

4 S2xx-30014. SSL access to certain interface configuration pages in a stacking environment may respond to Refresh or Submit with a Page not found error. The size of the buffer used for SSL reads may need to be increased to meet specific system needs.

5 S2xx-151600. When the login authentication method is configured as enable or line to authenticate users using the enable or line password, then the user name is not required. The “User:” prompt is not displayed for console and telnet users; however, SSH users are still prompted to provide user details.

Web User Interface

The following operational characteristics and known issues pertain to the 200 Series web user interface.

1 S2xx-83053. Service port LED on the web page is found to be highlighted even when nothing is connected to it.

2 S2xx-181207. When enabling or disabling HTTP and HTTPS from the administrative web interface, it is possible that an error message will be displayed on the user’s web browser. This error message results from the momentary restart of the web server on the device. To work around this issue, simply acknowledge the error message (click **OK**) and reload the web page.

3 S2xx-206594. An HTTP/HTTPS session is disconnected when sending a disconnect message using Dynamic Authorization. Instead of an appropriate pop-up message indicating the session was forcefully disconnected, the message indicates that the session timed out.

4 S2xx-225640. The web interface does not support the distribution of code image to all stack members using a single request. If using the web interface, individual stack members must be selected explicitly.

5 S2xx-232629. Unable to set non-default authentication list from web. User configured Authentication lists can be created via the web, but assigning various terminal types (Console, Telnet, SSH) fail. As a workaround, please use the associated CLI commands.

CLI (Command-Line Interface)

1 S2xx-218328. While entering certain modes via the CLI, the Help prompt inadvertently provides information on commands that may not be available. For example, while configuring a physical interface, the `autostate` command is listed, but is actually applicable for VLAN routing interfaces only.