VSC6819

WebStaX Software Product Specification

Product Overview

The WebStaX turnkey software package is a fully managed L2 switch application for the small and medium-sized enterprise (SME). This software package can be customized to support different port configurations. It is built on Linux to ensure cost optimization without compromising efficiency. WebStaX supports the following major capabilities.

- RedBoot bootloader
- U-boot bootloader
- Web or XMODEM update

Management is done using a web graphical user interface (GUI), command line interface (CLI), JavaScript Object Notation-Remote Procedure Call (JSON-RPC), or Simple Network Management Protocol (SNMP) running on the internal MIPS24Kec CPU. WebStaX is highly integrated with switch features such as QoS control lists (QCLs), access control lists (ACLs), and super priority management queue.

This document provides an overview of the switch and software features of the WebStaX software and lays the basis for further specifications. The supported configuration details including parameters and limitations are beyond the scope of this document. The module specific requirement specifications and configuration guides may be referred to for obtaining these details.

Supported Switch Platforms

This software is supported on a series of Microchip switches with 12, 26, or 57 ports with Power over Ethernet (PoE)/ non-PoE capabilities. The following table shows the supported switches.

Table 1. Supported Switches

Switch	Description
VSC7410	6-port SGMII Gigabit Ethernet Switch with VeriTime™ and Gigabit Ethernet PHYs
VSC7414	11-port layer 2 SGMII Gigabit Ethernet Enterprise Switch with VeriTime™
VSC7415	6-Port SGMII Gigabit Ethernet Switch with VeriTime™, Integrated DPLL, and Gigabit Ethernet PHYs
VSC7416	6-port Carrier Ethernet Switch Engine with ViSAA™, VeriTime™, and MPLS/MPLS-TP
VSC7418	11-port Carrier Ethernet Switch Engine with ViSAA™, VeriTime™, and MPLS/MPLS-TP
VSC7423	7-port, layer 2 Gigabit Ethernet Switch with VeriTime™, 5 Integrated Copper PHYs, and Embedded 32-bit CPU
VSC7424	10-port layer 2 Gigabit Ethernet Switch with 8 Fully Integrated Copper PHYs and Embedded 416-MHz CPU
VSC7425	18-port layer 2 Gigabit Ethernet Switch with 12 Fully Integrated Copper PHYs and Embedded 416-MHz CPU

.....continued	
Switch	**Description**
VSC7426	24-port layer 2 Gigabit Ethernet Switch with 12 Fully Integrated Copper PHYs and Embedded 416-MHz CPU
VSC7427	26-port layer 2 Gigabit Ethernet Switch with 12 Fully Integrated Copper PHYs and Embedded 416-MHz CPU
VSC7428	11-port Carrier Ethernet Switch Engine with ViSAA™, VeriTime™, and PHYs
VSC7429	26-port Carrier Ethernet Switch with ViSAA™, VeriTime™, and 12 Fully Integrated Copper PHYs
VSC7430	6-port Carrier Ethernet Switch with ViSAA™, VeriTime™, and Gigabit Ethernet PHYs
VSC7435	6-port Carrier Ethernet Switch with ViSAA™, VeriTime™, and Integrated DPLLs and Gigabit Ethernet PHYs
VSC7436	10-port Carrier Ethernet Switch with ViSAA™, VeriTime™, and Integrated Gigabit Ethernet PHYs
VSC7437	8-port Carrier Ethernet Switch with ViSAA™, VeriTime™, and Integrated DPLLs and Gigabit Ethernet PHYs
VSC7438	14-port Carrier Ethernet Switch with ViSAA™, VeriTime™, MPLS-TP, and L3 Routing
VSC7440	10-port L2/L3 Enterprise Gigabit Ethernet Switch with 10 Gbps Links
VSC7442	52-port L2/L3 Enterprise and Industrial Ethernet Switch
VSC7444	26-port L2/L3 Enterprise Gigabit Ethernet Switch with 10 Gbps Links
VSC7448	52-port L2/L3 Enterprise Gigabit Ethernet Switch with 10 Gbps Links
VSC7449	6-port SGMII Gigabit Ethernet Switch with VeriTime™ and Gigabit Ethernet PHYs
VSC7464	11-port layer 2 SGMII Gigabit Ethernet Enterprise Switch with VeriTime™
VSC7468	6-port Carrier Ethernet Switch Engine with ViSAA™, VeriTime™, and MPLS/MPLS-TP
VSC7513	8-port L2 Gigabit Ethernet Switch
VSC7514	10-port L2 Gigabit Ethernet Switch
VSC7546	29-port L2/L3 Industrial Gigabit Ethernet Switches
VSC7549	53-port L2/L3 Industrial Gigabit Ethernet Switches
VSC7552	57-port L2/L3 Industrial Gigabit Ethernet Switches
VSC7556	57-port L2/L3 Industrial Gigabit Ethernet Switches
VSC7558	57-port L2/L3 Industrial Gigabit Ethernet Switches
VSC7546TSN	29-port L2/L3 Industrial Gigabit Ethernet Switches
VSC7549TSN	53-port L2/L3 Industrial Gigabit Ethernet Switches
VSC7552TSN	57-port L2/L3 Industrial Gigabit Ethernet Switches
VSC7556TSN	57-port L2/L3 Industrial Gigabit Ethernet Switches
VSC7558TSN	57-port L2/L3 Industrial Gigabit Ethernet Switches

The following table lists the supported 1G PHYs.

Table 2. Supported 1G PHYs

PHY	Description
VSC8211	Single-port 10/100/1000BASE-T PHY and 1000BASE-X PHY with SGMII, SerDes, GMII, MII, TBI, RGMII/RTBI MAC Interfaces
VSC8221	Single-port 10/100/1000BASE-T PHY with 1.25 Gbps SerDes/SGMII for SFPs/GBICs
VSC8501	Single-port GbE Copper PHY with Synchronous Ethernet and RGMII/GMII Interface
VSC8502	Dual-port GbE Copper PHY with Synchronous Ethernet and RGMII/GMII Interface
VSC8504	Quad-port 10/100/1000BASE-T PHY with Synchronous Ethernet and QSGMII/SGMII MAC
VSC8512	12-port 10/100/1000BASE-T PHY with SGMII and QSGMII MAC Interface
VSC8514	Quad-port Gigabit Copper EEE PHY with QSGMII MAC-to-PHY Interface
VSC8522	12-port 10/100/1000BASE-T PHY with QSGMII MAC Interface
VSC8552	Dual-port RGMII/SGMII/QSGMII Dual Media PHY with EEE Support
VSC8562	Dual-port 10/100/1000BASE-T PHY with Synchronous Ethernet, Intellisec™, and QSGMII/SGMII MAC
VSC8564	Dual-port 10/100/1000BASE-T PHY with Synchronous Ethernet, MACsec, and QSGMII/SGMII MAC
VSC8572	Dual-port 10/100/1000BASE-T PHY with VeriTime™, Synchronous Ethernet, and RGMII/SGMII MAC
VSC8574	Quad-port Dual Media QSGMII/SGMII GbE PHY with VeriTime™
VSC8575	Quad-port 10/100/1000BASE-T PHY with Synchronous Ethernet, VeriTime™, and QSGMII/SGMII MAC
VSC8582	Dual-port Dual Media QSGMII/SGMII GbE PHY with Intellisec™ and VeriTime™
VSC8584	Quad-port Dual Media QSGMII/SGMII GbE PHY with Intellisec™ and VeriTime™

The following table lists the supported 10G PHYs.

Table 3. Supported 10G PHYs

PHY	Description
VSC8254	Dual Channel 1G/10GBASE-KR to SFI Ethernet LAN/WAN PHY with VeriTime™ and Intellisec™
VSC8256	Quad Channel 1G/10GBASE-KR to SFI Ethernet Repeater
VSC8257	Quad Channel 1G/10GBASE-KR to SFI Ethernet WIS PHY with VeriTime™ and Intellisec™
VSC8258	Quad Channel 1G/10GBASE-KR to SFI Ethernet WIS PHY with VeriTime™ and Intellisec™
VSC8489	Dual-port WAN/LAN/Backplane RXAUI/XAUI to SFP+/KR 10 GbE PHY
VSC8490	Dual-port WAN/LAN/Backplane RXAUI/XAUI to SFP+/KR 10 GbE PHY with Intellisec™ and VeriTime™
VSC8491	WAN/LAN/Backplane RXAUI/XAUI to SFP+/KR 10 GbE PHY with Intellisec™ and VeriTime™

Software Architecture

The WebStaX software provides support for standalone switches. It consists of the following components.

- Operating system (Linux) for access to the hardware.
- Application programming interface (API) for a function library to control switches and PHYs.
- Control modules, such as port control, Spanning Tree Protocol (STP), and Virtual LAN (VLAN)—to implement product features and protocols. These modules may include threads and provide a management API for configuration and monitoring.
- Management modules, such as CLI, web, and SNMP—for interfaces to the system based on the management API of the control modules.

The following illustration shows the architecture of the Microchip managed application software and a few control and management modules.

Figure 1. Application Architecture

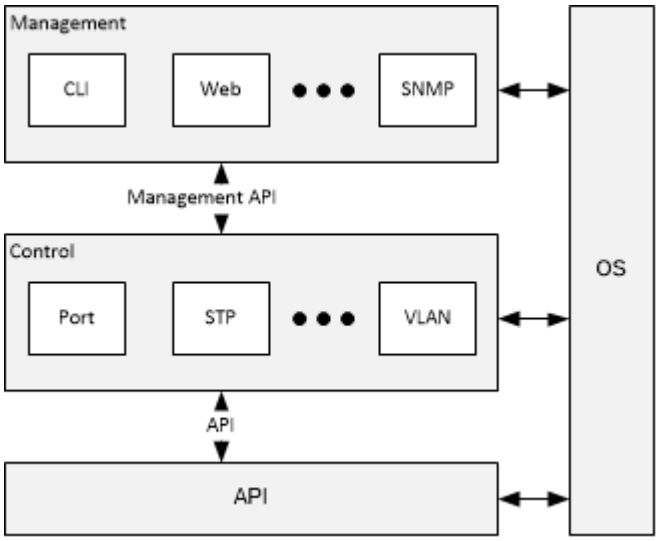

Table of Contents

Product Overview....1
1. Supported Switch Platforms....1
2. Software Architecture....3

1. Supported Features....7
1.1. BSP and API....7
1.2. Port Control....7
1.3. Quality of Service....8
1.4. L2 Switching....9
1.5. L3 and Routing....10
1.6. Security....11
1.7. Robustness and Power Savings....12
1.8. Customization Framework....12
1.9. Management....13
1.10. SNMP MIBs....14

2. Features and Platform Capacity....16

3. System Requirements....19

4. Port and System Capabilities....21
4.1. PortCapability....21
4.2. System Capability....21

5. Firmware Upgrade....22

6. Port Control....23
6.1. SFP Detection....23
6.2. VeriPHY Support....23
6.3. PoE/PoE+ Support....23
6.4. NPI Port....23
6.5. PCIe....23
6.6. POE/POE+ with LLDP....23

7. Quality of Services (QoS)....24
7.1. Port Policers....24
7.2. Scheduling and Shaping....24
7.3. QoS Control List (QCL) Configuration....24
7.4. Weighted Random Early Detection (WRED)....24
7.5. Ingress Port Classification....24
7.6. Global Storm Control....25

8. L2 Switching....26
8.1. Virtual LAN....26
8.2. IEEE 802.3ad Link Aggregation....26
8.3. MAC Table Configuration....27
8.4. Mirroring (SPAN/VSPAN and RSPAN)....27
8.5. Spanning Tree....28

8.6. Loop Guard 28
8.7. Internet Group Management Protocol (IGMP)v2 Snooping 28

9. L3 and Routing 29

10. Security 30
10.1. 802.1X and MAC-Based Authentication 30
10.2. Port Security 31
10.3. Authentication, Authorization, and Accounting (AAA) 31
10.4. Secure Access 31
10.5. Authentication and Authorization Methods 31
10.6. Access Control List (ACLs) 32

11. Robustness and Power Savings 33
11.1. Robustness 33
11.2. Power Savings 33

12. Management 35
12.1. Management Services 35
12.2. SNMP 37
12.3. Internet Control Message Protocol 38
12.4. SysLog 38
12.5. IP Management 38
12.6. Console 38
12.7. System Management 38
12.8. Management Access Filtering 39
12.9. Default Configuration 39
12.10. Configuration Upload/Download 39
12.11. Loop Detection Restore to Default 39
12.12. Symbolic Register Access 39
12.13. SD/MMC Card Slot 39
12.14. 802.1AB LLDP and CDP Aware 39

13. SNMP MIBs 41

14. Revision History 42

The Microchip Website 46

Product Change Notification Service 46

Customer Support 46

Microchip Devices Code Protection Feature 46

Legal Notice 46

Trademarks 47

Quality Management System 47

Worldwide Sales and Service 48

1. Supported Features

The following sections describe the features of each module in the SMBStaX software.

1.1 BSP and API

The following table lists the features supported by the Board Support Package (BSP) and API module.

Table 1-1. BSP and API: Supported Features

Feature	Luton26 VSC7423 VSC7424 VSC7425 VSC7426 VSC7427 VSC7428 VSC7429	Jaguar-2 VSC7438 VSC7442 VSC7444 VSC7448 VSC7449 VSC7464 VSC7468	Serval-T VSC7410 VSC7415 VSC7430 VSC7435 VSC7436 VSC7437 VSC7440	Ocelot VSC7513 VSC7514	SparX-5 VSC7546 VSC7549 VSC7552 VSC7556 VSC7558
Internal CPU	•	•	•	•	•
External CPU	—	—	—	—	•
64-bit CPU Architecture	—	—	—	—	•
API and application split	•	•	•	•	•
MESA layer	•	•	•	•	•
MEBA layer	•	•	•	•	•
U-Boot	•	•	•	•	•
U-Boot network support	•	•	•	•	•
32MB NOR FLASH only option	•	•	•	•	—
64MB NOR FLASH only option	•	•	•	•	—

1.2 Port Control

The following table lists the features supported by the port control module. For more information, see 6. Port Control.

Table 1-2. Port Control: Supported Features

Feature	Luton26 VSC7423 VSC7424 VSC7425 VSC7426 VSC7427 VSC7428 VSC7429	Jaguar-2 VSC7438 VSC7442 VSC7444 VSC7448 VSC7449 VSC7464 VSC7468	Serval-T VSC7410 VSC7415 VSC7430 VSC7435 VSC7436 VSC7437 VSC7440	Ocelot VSC7513 VSC7514	SparX-5 VSC7546 VSC7549 VSC7552 VSC7556 VSC7558
Port speed/duplex mode/flow control	•	•	•	•	•
Aquantia 2.5G PHY Gen2	•	•	•	•	•
Aquantia 2.5G PHY Gen3	•	•	•	•	•
Aquantia 5G PHY Gen3	—	•	—	—	—
Aquantia 10G PHY Gen2	—	•	•	—	•
802.1Qbb per priority flow control	—	•	•	•	•
Port frame size (jumbo frames)	•	•	•	•	•
Port state (administrative status)	•	•	•	•	•
Port status (link monitoring)	•	•	•	•	•
Port statistics (MIB counters)	•	•	•	•	•
Port VeriPHY (cable diagnostics)	•	•	•	•	•
PoE/PoE+ with PD69200 support (external controller)	•	•	•	•	—
PoE/PoE+ with Link Layer Discovery Protocol (LLDP)	•	•	•	•	—
PoE IEEE802.3bt w/o LLDP (external controller)	•	•	•	•	—
NPI port	•	•	•	•	•
PCIe	—	•	•	•	•
On-the-fly SFP detection	•	•	•	•	•
IEEE 802.3ap 10G-KR	—	—	—	—	•
IEEE 802.3ap 25G-KR	—	—	—	—	•

1.3 Quality of Service

The following table lists the features supported by the quality of service (QoS) module. For more information, see 7. Quality of Services (QoS).

Table 1-3. QoS: Supported Features

Feature	Luton26 VSC7423 VSC7424 VSC7425 VSC7426 VSC7427 VSC7428 VSC7429	Jaguar-2 VSC7438 VSC7442 VSC7444 VSC7448 VSC7449 VSC7464 VSC7468	Serval-T VSC7410 VSC7415 VSC7430 VSC7435 VSC7436 VSC7437 VSC7440	Ocelot VSC7513 VSC7514	SparX-5 VSC7546 VSC7549 VSC7552 VSC7556 VSC7558
Traffic classes (8 active priorities)	•	•	•	•	•
Port default priority	•	•	•	•	•
User priority	•	•	•	•	•
QoS control list (QCL mode)	•	•	•	•	•
Global storm control for UC, MC, and BC	•	•	•	•	•
Random early discard (RED)	—	•	•	•	•
Port policers	•	•	•	•	•
Global/VCAP (ACL) policers	•	•	•	•	•
Port egress shaper	•	•	•	•	•
Queue egress shapers	•	•	•	•	•
Scheduler mode	•	•	•	•	•

1.4 L2 Switching

The following table lists the features supported by the L2 Switching module. For more information, see 8. L2 Switching.

Table 1-4. L2 Switching: Supported Features

Feature	Luton26 VSC7423 VSC7424 VSC7425 VSC7426 VSC7427 VSC7428 VSC7429	Jaguar-2 VSC7438 VSC7442 VSC7444 VSC7448 VSC7449 VSC7464 VSC7468	Serval-T VSC7410 VSC7415 VSC7430 VSC7435 VSC7436 VSC7437 VSC7440	Ocelot VSC7513 VSC7514	SparX-5 VSC7546 VSC7549 VSC7552 VSC7556 VSC7558
IEEE 802.1D Bridge					
Auto MAC address learning/aging	•	•	•	•	•

.....continued

Feature	Luton26 VSC7423 VSC7424 VSC7425 VSC7426 VSC7427 VSC7428 VSC7429	Jaguar-2 VSC7438 VSC7442 VSC7444 VSC7448 VSC7449 VSC7464 VSC7468	Serval-T VSC7410 VSC7415 VSC7430 VSC7435 VSC7436 VSC7437 VSC7440	Ocelot VSC7513 VSC7514	SparX-5 VSC7546 VSC7549 VSC7552 VSC7556 VSC7558
MAC addresses—static	•	•	•	•	•
IEEE 802.1Q					
Virtual LAN	•	•	•	•	•
Private VLAN—static	•	•	•	•	•
Port isolation—static	•	•	•	•	•
VLAN trunking	•	•	•	•	•
IEEE 802.1ad provider bridge (native or translated VLAN)	•	•	•	•	•
Rapid Spanning Tree Protocol (RSTP), STP	•	•	•	•	•
Loop guard	•	•	•	•	•
IEEE 802.3ad					
Link aggregation—static	•	•	•	•	•
Link aggregation—Link Aggregation Control Protocol (LACP)	•	•	•	•	•
AGGR/LACP user interface alignment with Industry standard	•	•	•	•	•
UNI LAG (LACP) 1:1 active/standby	•	•	•	•	•
LACP revertive/non-revertive	•	•	•	•	•
LACP loop free operation	•	•	•	•	•
IGMPv2 snooping	•	•	•	•	•
Port mirroring	•	•	•	•	•

1.5 L3 and Routing

The following table lists the features supported by the L3 Routing module. For more information, see 9. L3 and Routing.

Table 1-5. L3 and Routing: Supported Features

Feature	Luton26 VSC7423 VSC7428 VSC7429	Jaguar-2 VSC7438 VSC7442 VSC7444 VSC7448 VSC7449 VSC7464 VSC7468	Serval-T VSC7410 VSC7415 VSC7430 VSC7435 VSC7436 VSC7437 VSC7440	Ocelot VSC7513 VSC7514	SparX-5 VSC7546 VSC7549 VSC7552 VSC7556 VSC7558
Software-based IPv4 L3 static routing with Linux Kernel integration	•	—	—	•	—
Hardware-based IPv4 L3 static routing with Linux Kernel integration	—	•	•	—	•
RFC2992 (ECMP) support for HW based L3 static routing	—	•	•	—	•
RFC-1812 L3 checking (version, IHL, checksum, and so on)	•	•	•	•	•

1.6 Security

The following table lists the features supported by the security module. For more information, see 10. Security.

Table 1-6. Security: Supported Features

Feature	Luton26 VSC7423 VSC7424 VSC7425 VSC7426 VSC7427 VSC7428 VSC7429	Jaguar-2 VSC7438 VSC7442 VSC7444 VSC7448 VSC7449 VSC7464 VSC7468	Serval-T VSC7410 VSC7415 VSC7430 VSC7435 VSC7436 VSC7437 VSC7440	Ocelot VSC7513 VSC7514	SparX-5 VSC7546 VSC7549 VSC7552 VSC7556 VSC7558
Port-based 802.1X	•	•	•	•	•
MAC-based authentication	•	•	•	•	•
Remote authentication dial In user service (RADIUS) authentication and authorization	•	•	•	•	•
MAC Address Limit	•	•	•	•	•
Persistent MAC learning	•	•	•	•	•
Web and CLI authentication	•	•	•	•	•

.....continued					
Feature	**Luton26** **VSC7423** **VSC7424** **VSC7425** **VSC7426** **VSC7427** **VSC7428** **VSC7429**	**Jaguar-2** **VSC7438** **VSC7442** **VSC7444** **VSC7448** **VSC7449** **VSC7464** **VSC7468**	**Serval-T** **VSC7410** **VSC7415** **VSC7430** **VSC7435** **VSC7436** **VSC7437** **VSC7440**	**Ocelot** **VSC7513** **VSC7514**	**SparX-5** **VSC7546** **VSC7549** **VSC7552** **VSC7556** **VSC7558**
ACLs for filtering/policing/port copy	•	•	•	•	•
Secure FTP client	•	•	•	•	•

1.7 Robustness and Power Savings

The following table lists the features supported by the robustness and power savings module. For more information, see 11. Robustness and Power Savings.

Table 1-7. Robustness and Power Savings: Supported Features

Feature	**Luton26** **VSC7423** **VSC7424** **VSC7425** **VSC7426** **VSC7427** **VSC7428** **VSC7429**	**Jaguar-2** **VSC7438** **VSC7442** **VSC7444** **VSC7448** **VSC7449** **VSC7464** **VSC7468**	**Serval-T** **VSC7410** **VSC7415** **VSC7430** **VSC7435** **VSC7436** **VSC7437** **VSC7440**	**Ocelot** **VSC7513** **VSC7514**	**SparX-5** **VSC7546** **VSC7549** **VSC7552** **VSC7556** **VSC7558**
Cold start	•	•	•	•	•
Cool start	•	•	•	•	•
ActiPHY	•	•	•	•	•
PerfectReach	•	•	•	•	•
Energy-Efficient Ethernet (EEE) power management	•	•	•	•	•
LED power management	•	•	—	—	•
Thermal protection	•	•	•	•	•
Adaptive fan control	•	•	•	—	•

1.8 Customization Framework

The following table lists the features supported by the customization framework module.

Table 1-8. Customization Framework: Supported Features

Feature	Luton26 VSC7423 VSC7424 VSC7425 VSC7426 VSC7427 VSC7428 VSC7429	Jaguar-2 VSC7438 VSC7442 VSC7444 VSC7448 VSC7449 VSC7464 VSC7468	Serval-T VSC7410 VSC7415 VSC7430 VSC7435 VSC7436 VSC7437 VSC7440	Ocelot VSC7513 VSC7514	SparX-5 VSC7546 VSC7549 VSC7552 VSC7556 VSC7558
Separate BSP and application	•	•	•	•	•
Append or change a binary image	•	•	•	•	•
IPC JSON-RPC socket (with notification support)	•	•	•	•	•
Overwrite default startup configuration	•	•	•	•	•
Boot and initialization of third-party daemons	•	•	•	•	•
Configuration to disable certain built-in features	•	•	•	•	•
Microchip Ethernet board API (MEBA)	•	•	•	•	•

1.9 Management

The following table lists the features supported by the management module. For more information, see 12. Management.

Table 1-9. Management: Supported Features

Feature	Luton26 VSC7423 VSC7424 VSC7425 VSC7426 VSC7427 VSC7428 VSC7429	Jaguar-2 VSC7438 VSC7442 VSC7444 VSC7448 VSC7449 VSC7464 VSC7468	Serval-T VSC7410 VSC7415 VSC7430 VSC7435 VSC7436 VSC7437 VSC7440	Ocelot VSC7513 VSC7514	SparX-5 VSC7546 VSC7549 VSC7552 VSC7556 VSC7558
JSON-RPC	•	•	•	•	•
RFC 2131 DHCP client	•	•	•	•	•
IPv4/IPv6 ping	•	•	•	•	•
IPv4/IPv6 traceroute	•	•	•	•	•

.....continued					
Feature	**Luton26** **VSC7423** **VSC7424** **VSC7425** **VSC7426** **VSC7427** **VSC7428** **VSC7429**	**Jaguar-2** **VSC7438** **VSC7442** **VSC7444** **VSC7448** **VSC7449** **VSC7464** **VSC7468**	**Serval-T** **VSC7410** **VSC7415** **VSC7430** **VSC7435** **VSC7436** **VSC7437** **VSC7440**	**Ocelot** **VSC7513** **VSC7514**	**SparX-5** **VSC7546** **VSC7549** **VSC7552** **VSC7556** **VSC7558**
HTTP server	•	•	•	•	•
CLI—console port	•	•	•	•	•
Industrial standard CLI	•	•	•	•	•
Industrial standard configuration	•	•	•	•	•
Industrial standard CLI debug commands	•	•	•	•	•
Port description CLI	•	•	•	•	•
Management access filtering	•	•	•	•	•
HTTPS	•	•	•	•	•
System syslog	•	•	•	•	•
Software upload through web	•	•	•	•	•
SNMP v1/v2c/v3 agent[1]	•	•	•	•	•
IEEE 802.1AB-2005 link layer discovery—LLDP	•	•	•	•	•
FTP client	•	•	•	•	•
Configuration download/upload—industrial standard	•	•	•	•	•
Loop detection restore to default	•	•	•	•	•
Symbolic register access	•	•	•	•	•

Note:

1. It does not support SNMPv1 trap.

1.10 SNMP MIBs

The following table lists the features supported by the SNMP MIBs module. For more information, see #unique_22.

Table 1-10. SNMP MIBs: Supported Features

Feature	Luton26 VSC7423 VSC7424 VSC7425 VSC7426 VSC7427 VSC7428 VSC7429	Jaguar-2 VSC7438 VSC7442 VSC7444 VSC7448 VSC7449 VSC7464 VSC7468	Serval-T VSC7410 VSC7415 VSC7430 VSC7435 VSC7436 VSC7437 VSC7440	Ocelot VSC7513 VSC7514	SparX-5 VSC7546 VSC7549 VSC7552 VSC7556 VSC7558
RFC 1213 MIB II	•	•	•	•	•
RFC 1215 TRAPS MIB	•	•	•	•	•
RFC 4188 bridge MIB	•	•	•	•	•
RFC 3635 Ethernet-like MIB	•	•	•	•	•
RFC 3411 SNMP management frameworks	•	•	•	•	•
IEEE 802.1 MSTP MIB	•	•	•	•	•
IEEE 802.1AB LLDP-MIB (LLDP MIB included in a clause of the STD)	•	•	•	•	•
RFC 3621 LLDP-MED power (PoE) (no specific MIB for PoE+ exists)	•	•	•	•	—

2. Features and Platform Capacity

The following table lists the features and platform capacity supported by the WebStaX software. The capacity mentioned can either be software or hardware constrained, depending on the case.

Table 2-1. Features and Platform Capacity

Feature	SparX-III and Caracal VSC7423 VSC7424 VSC7425 VSC7426 VSC7427 VSC7428 VSC7429	SparX-IV and Jaguar-2 VSC7438 VSC7442 VSC7444 VSC7448 VSC7449 VSC7464 VSC7468	SparX-IV and Serval-T VSC7410 VSC7415 VSC7430 VSC7435 VSC7436 VSC7437 VSC7440	Ocelot VSC7513 VSC7514	SparX-5 VSC7546 VSC7549 VSC7552 VSC7556 VSC7558
Resilience and Availability					
IEEE 802.3ad LACP: Max LAGs	3 LAGs in VSC7423 5 LAGs in VSC7424/7428 9 LAGs in VSC7425 12 LAGs in VSC7426 13 LAGs in VSC7427	7 LAGs in VSC7438 26 LAGs in VSC7442/48/49/68 13 LAGs in VSC7444/64	3 LAGs in SC7410/15, VSC7430/35 5 LAGs in VSC7436, VSC7440 4 LAGs in VSC7437	4 LAGs in VSC7513 5 LAGs in VSC7514	35 LAGs in VSC7546 37 LAGs in VSC7549, VSC7552, VSC7556, VSC7558
Traffic Control					
Port-based VLAN	4095	4095	4095	4095	4095
Private VLAN	7 in VSC7423 10 in VSC7424/7428 18 in VSC7425 24 in VSC7426 26 in VSC7427	14 in VSC7438 52 in VSC7442/48/49/68 26 in VSC7444/64	6 in VSC7410/15, VSC7430/35 10 in VSC7436, VSC7440 8 in VSC7437	8 in VSC7513 10 in VSC7514	9

.....continued

Feature	SparX-III and Caracal VSC7423 VSC7424 VSC7425 VSC7426 VSC7427 VSC7428 VSC7429	SparX-IV and Jaguar-2 VSC7438 VSC7442 VSC7444 VSC7448 VSC7449 VSC7464 VSC7468	SparX-IV and Serval-T VSC7410 VSC7415 VSC7430 VSC7435 VSC7436 VSC7437 VSC7440	Ocelot VSC7513 VSC7514	SparX-5 VSC7546 VSC7549 VSC7552 VSC7556 VSC7558
MAC table size 8K	8K	32K	8K in VSC7410/15/30/35 16K in VSC7436/37/40	4K	32K
Storm control	1, 2, 4, 8, 16, 32, 64, 128, 256, 512, 1000, 2000, 4000, 8000, 16000, 32000, 64000, 128000, 256000, 512000,or 1024000 kpps (global setting for Unicast, Multicast, and Broadcast)	25 kbps –10 Gbps (per port for Unicast [(known/ learned), Broadcast, and Unknown (flooded Unicast and Multicast)]	25 kbps –10 Gbps [per port for Unicast (known/ learned), Broadcast, and Unknown (flooded Unicast and Multicast)]	25 kbps –10 Gbps [per port for Unicast (known/ learned), Broadcast, and Unknown (flooded Unicast and Multicast)]	10 kbps – 13128 mbps
Jumbo frames supported	Up to 9600	Up to 10240	Up to 10240	Up to 10240	10240
Security					
Static MAC entries supported	64	64	64	64	64
RADIUS authentication servers	5	5	5	5	5
RADIUS accounting servers	5	5	5	5	5
Policy-based security filtering	512	512	512	512	512

.....continued

Feature	SparX-III and Caracal VSC7423 VSC7424 VSC7425 VSC7426 VSC7427 VSC7428 VSC7429	SparX-IV and Jaguar-2 VSC7438 VSC7442 VSC7444 VSC7448 VSC7449 VSC7464 VSC7468	SparX-IV and Serval-T VSC7410 VSC7415 VSC7430 VSC7435 VSC7436 VSC7437 VSC7440	Ocelot VSC7513 VSC7514	SparX-5 VSC7546 VSC7549 VSC7552 VSC7556 VSC7558
Password length	32	32	32	32	32
ACE	256	512	512	512	512
Number of logged in users	20	20	20	20	20

3. System Requirements

The following table lists the port system requirements supported by the WebStaX software.

Table 3-1. Port System Requirements

Feature	SparX-III and Caracal VSC7423 VSC7424 VSC7425 VSC7426 VSC7427 VSC7428 VSC7429	SparX-IV and Jaguar-2 VSC7438 VSC7442 VSC7444 VSC7448 VSC7449 VSC7464 VSC7468	SparX-IV and Serval-T VSC7410 VSC7415 VSC7430 VSC7435 VSC7436 VSC7437 VSC7440	Ocelot VSC7513 VSC7514	SparX-5 VSC7546 VSC7549 VSC7552 VSC7556 VSC7558
LEDs per port	1	1	1	1	1
SFP+/SFP	SFP only supported	Both SFP/SFP+ supported	Both SFP/SFP + supported	Both SFP/SFP+ supported	Both SFP/SFP + supported
Speed capability per 10/100M and Gigabit port	Supported	Supported	Supported	Supported	Supported
Duplex capability per 10/100M	Half/full	Half/full	Half/full	Half/full	Half/full
Auto MDI/MDIX	Supported	Supported	Supported	Supported	Supported
Port packet forwarding rate	1488000 pps (1000 Mbps with 64 bytes) 148800 pps (100 Mbps) 14880 pps (10Mbps)	14880000 pps (10 Gbps) 1488000 pps (1000 Mbps with 64 bytes) 148800 pps (100 Mbps) 14880 pps (10 Mbps)	14880000 pps (10 Gbps) 1488000 pps (1000 Mbps with 64 bytes) 148800 pps (100 Mbps) 14880 pps (10 Mbps)	14880000 pps (10 Gbps) 1488000 pps (1000 Mbps with 64 bytes) 148800 pps (100 Mbps) 14880 pps (10 Mbps)	14880000 pps (10 Gbps) 1488000 pps (1000 Mbps with 64 bytes) 148800 pps (100 Mbps) 14880 pps (10 Mbps)
RJ45 connectors	Supported	Supported	Supported	Supported	Supported
Fiber slots	Supported	Supported	Supported	Supported	Supported

The following table lists the hardware system requirements supported by the WebStaX software.

Table 3-2. Hardware System Requirements

Requirement	Support
Power LED	Supported by hardware
System LED	Supported by hardware
Management LED	Supported by hardware

.....continued

Requirement	Support
Alarm LED	Supported by hardware
Switch fabric capacity	Supported by hardware
Forwarding architecture	Supported by hardware
MAC address entries	Supported by hardware
MAC address aging	Supported by hardware
MAC buffer memory type and size	Supported by hardware
CPU flash size	Supported by hardware
CPU memory type and size	Supported by hardware
System DDR SDRAM	Supported by hardware
Reset button	Supported by hardware
EMC/safety requirement	Supported by hardware
Performance requirement	Supported by hardware

4. Port and System Capabilities

The following sections describe the port and system capabilities supported by the WebStaX software.

4.1 PortCapability

The ports are equipped with the following capabilities.

- All copper ports can be configured as full-duplex or half-duplex.
- Copper ports operating at 10/100 Mbps support auto-sensing and auto-negotiation.
- Full-duplex, auto-sensing, and auto-negotiation are supported on 1000 Mbps ports.
- Full-duplex flow control is supported according to the IEEE 802.3x standard.
- Half-duplex flow control is supported using collision-based backpressure.
- LEDs for all the ports are driven by the SGPIO and shift registers.
- Different port-based configurations are supported on all available ports. For more information, see 1. Supported Features.

4.2 System Capability

The 6- to 52-port turnkey switch platform model switches can be supported using the WebStaX software with wire speed layer 2 Gigabit/Fast Ethernet switches, with an option to additionally support the PoE functionality with partner vendors.

The turnkey switch software runs on Linux. The following system-wide operations are supported:

- Store-and-forward forwarding architecture.
- Configurable MAC address aging support (300 seconds default timeout value).
- Port packet-forwarding rates of 1488095 pps (1000 Mbps), 148810 pps (100 Mbps), and 14880 pps (10 Mbps).
- 128-MB system DDR SDRAM is recommended for a typical 24- to 48-port switch.
- 16-MB flash size is recommended for a typical 24- to 48-port switch.
- NOR-only, flash-based hardware designs are supported. NOR flash size of 64 MB is supported.

5. Firmware Upgrade

The WebStaX firmware, which controls the switch, can be updated using one of the following methods. The turnkey switch software runs on Linux. The following system-wide operations are supported:

- Web, using the HTTP protocol
- CLI, using the TFTP client on the switch

The software image selection information includes the following:

- Image—the file name of the firmware image
- Version—the version of the firmware image
- Date—the date when the firmware was produced

After the software image is uploaded from the web interface, a web page announces that the firmware update is initiated. After about a minute, the firmware is updated and the switch restarts. While the firmware is being updated, web access appears to be defunct. The front LED flashes green/off with a frequency of 10 Hz while the firmware update is in progress.

Note:
Do not restart or power off the device at this time or the switch may fail to function.

6. Port Control

The following sections describe the port control features supported by the WebStaX software.

6.1 SFP Detection

The WebStaX software detects SFP at run time.

6.2 VeriPHY Support

VeriPHY is supported on the WebStaX software for running cable diagnostics to find cable shorts/opens and to determine cable length.

6.3 PoE/PoE+ Support

The WebStaX software provides PoE/PoE+ support to comply with the IEEE 802.3at and IEEE 802.3af standards for enabling the supply of up to 30 W per port and up to the total power budget.

6.4 NPI Port

The WebStaX software supports the NPI port to manage the switch core. Any front port can be configured as an NPI port through which frames can be injected from and extracted to an external CPU.

6.5 PCIe

The PCIe interface allows a back-to-back connection with an external CPU. The external CPU has read/write access to device registers and can burst frame-data in (injection) and out (extraction) through memory-mapped injection/extraction registers.

6.6 POE/POE+ with LLDP

The WebStaX software allows automatic power configuration if the link partner supports PoE. When LLDP is enabled, the information about the power usage of the PD is available, and then the switch can comply with or ignore this information.

7. Quality of Services (QoS)

The following sections describe the rich QoS features supported by the WebStaX software.

7.1 Port Policers

The QoS ingress port policers are configurable per port and are disabled by default. The software allows disable/enable flow control on the port policer. Flow control is disabled by default. If flow control is enabled and the port is in flow control mode, then pause frames are sent instead of discarding frames.

7.2 Scheduling and Shaping

Each egress port implements a scheduler that controls eight queues, one queue (priority) per QoS class. The scheduler mode can be set to strict priority or weighted (modified-DWRR). Strict priority is selected by default. It is possible to specify the weight for each of the queues (0–5).

Each egress port also implements a port shaper and a shaper per queue. The software allows disabling/enabling the port and queue shaper as part of egress shaping. The port shaper and queue shaper are disabled by default.

It is possible to specify the maximum bit rate in kbps or mbps.

7.3 QoS Control List (QCL) Configuration

QoS classification based on basic classification can be overruled by an intelligent classifier called QCL.

The QCL consists of QCE entries where each entry is configured with keys and actions. The keys specify which part of the frames must be matched and the actions specify the applied classification parameters.

When a frame is received on a port, the list of QCEs is searched for a match. If the frame matches the configured keys, the actions are applied and the search is terminated.

The QCL configuration is a table of QCEs containing QoS control entries that classify to a specific QoS class on specific traffic objects. A QoS class can be associated with a particular QCE ID.

7.4 Weighted Random Early Detection (WRED)

While the random early detection (RED) settings are configurable for queues 0–5, WRED is configurable to either disable/enable, and is disabled by default.

The minimum and maximum percentage of the queue fill level or drop probability can be configured before WRED starts discarding frames.

By specifying a different RED configuration for the queues (QoS classes), it is possible to obtain the WRED operation between queues.

7.5 Ingress Port Classification

Classification is the first step for implementing QoS. There is a one-to-one mapping between QoS class, queue, and priority. The QoS class is represented by numbers; higher numbers correspond to higher priority.

The features supported are as follows:

- Port default priority (QoS class)
- Port default priority (DP level)
- Port default PCP
- Port default DEI
- DSCP mapping to QoS class and DP level

- DSCP classification (DiffServ)
- Advanced QoS classification

7.6 Global Storm Control

Global storm control on the WebStaX software is done as per the system globally on SparX-III and SparX-IV-based switches. Storm rate control configuration for unicast frames, broadcast frames, and multicast frames are supported and can be configured in pps on SparX-III switches. Storm control is disabled by default.

8. L2 Switching

The following sections describe the rich L2 switching features supported by the WebStaX software.

8.1 Virtual LAN

The WebStaX software supports the IEEE 802.1Q standard virtual LAN (VLAN). The default configuration is as follows:

- All ports are VLAN-aware.
- All ports are members of VLAN 1.
- The switch management interface is on VLAN 1. All ports have a Port VLAN ID (PVID) of 1.
- A port can be configured to one of the following three modes.
  - Access
  - Trunk
  - Hybrid
- By default, all ports are in Access mode and are normally used to connect to end stations. Access ports have the following characteristics.
  - Member of exactly one VLAN, the Port VLAN (Access VLAN), which by default is 1.
  - Accepts untagged and C-tagged frames.
  - Discards all frames that are not classified to the Access VLAN.
  - On egress all frames classified to the Access VLAN are transmitted untagged. Others (dynamically added VLANs) are transmitted tagged.
- The PVID is set to 1 by default.
- Ingress filtering is always enabled.

Trunk ports can carry traffic on multiple VLANs simultaneously, and are normally used to connect to other switches. Trunk ports have the following characteristics.

- By default, a trunk port is a member of all VLANs (1–4095). This may be limited by the use of allowed VLANs.
- If frames are classified to a VLAN that the port is not a member of, they are discarded.
- By default, all frames classified to the Port VLAN (also known as Native VLAN) get tagged on egress. Frames classified to the Port VLAN do not get C-tagged on egress.
- Egress tagging can be changed to tag all frames, in which case only tagged frames are accepted on ingress.

Hybrid ports resemble trunk ports in many ways, but provide the following additional port configuration features.

- Can be configured to be VLAN tag unaware, C-tag aware, S-tag aware, or S-custom-tag aware.
- Ingress filtering can be controlled.
- Ingress acceptance of frames and configuration of egress tagging can be configured independently.

8.1.1 Private VLAN, Port Isolation

In a private VLAN, communication between isolated ports in that private VLAN is not permitted.

Private VLANs are based on the source port mask, and there are no connections to VLANs. This means that VLAN IDs and private VLAN IDs can be identical.

8.2 IEEE 802.3ad Link Aggregation

A link aggregation is a collection of one or more full duplex (FDX) Ethernet links. These links when combined together form a Link Aggregation Group (LAG), such that the networking device can treat it as if it were a single link. The traffic distribution is based on a hash calculation of fields in the frame:

- Source MAC address—can be used to calculate the destination port for the frame. By default, the source MAC address is enabled.

- Destination MAC address—can be used to calculate the destination port for the frame. By default, the destination MAC address is disabled.
- IP address—can be used to calculate the destination port for the frame. By default, the IP address is enabled.
- TCP/UDP port number—can be used to calculate the destination port for the frame. By default, the TCP/UDP port number is enabled.

An aggregation can be configured statically or dynamically through the Link Aggregation Control Protocol (LACP).

8.2.1 Auto MAC Address Learning/Aging

Learning is done automatically as soon as a frame with unknown SMAC is received. Dynamic entries are removed from the MAC table after a configured aging time (in seconds), if frames with learned MAC address are not received within aging period.

8.2.2 MAC Addresses–Static

Statically-added MAC entries are not subjected to aging.

8.2.3 Static

Static aggregations can be configured through the CLI or the web interface. A static LAG interface does not require a partner system to be able to aggregate its member ports. In Static mode, the member ports do not transmit LACPDUs.

8.2.4 Link Aggregation Control Protocol (LACP)

The LACP exchanges LACPDUs with an LACP partner and forms an aggregation automatically. The LACP can be enabled or disabled on the switch port. The LACP will form an aggregation when two or more ports are connected to the same partner.

The key value can be configured to a user-defined value or set to auto to calculate based on the link speed in accordance with IEEE 802.3ad standard.

The role for the LACP port configuration can be selected as either active to transmit LACP packets each second, or passive to wait for an LACP packet from a partner.

8.3 MAC Table Configuration

MAC learning configuration can be configured per port.

- Auto—learning is done automatically as soon as a frame with unknown Static MAC (SMAC) is received.
- Disable—no learning is done.
- Secure—only SMAC entries are learned, all other frames are dropped.

The static entries can be configured in the MAC table for forwarding. The user can enable/disable MAC learning per VLAN. VLAN learning is enabled by default.

MAC aging is configurable to age out the learned entries.

MAC learning cannot be administered on each individual aggregation group.

8.4 Mirroring (SPAN/VSPAN and RSPAN)

The WebStaX software allows selected traffic to be copied, or mirrored, to a mirror port where a frame analyzer can be attached to analyze the frame flow. By default, mirror monitors all traffic, including multicast and bridge PDUs.

The software will support many-to-one port mirroring. The destination port is located on the local switch in the case of Mirror. The switch can support VLAN-based mirroring.

Note:
The mirroring session either have ports or VLANs as sources, but not both.

8.5 Spanning Tree

The WebStaX software supports the Spanning Tree versions IEEE 802.1 Spanning Tree Protocol (STP) and 802.1w Rapid STP (RSTP). The desired version is configurable and the RSTP is selected by default.

The RSTP portion of the module conforms to IEEE 802.1D-2004. IEEE 802.1s supports 16 instances. The STP port configurations are allowed as per the physical port or aggregated port and priority configurations.

Port error recovery is supported to control whether a port in the error-disabled state automatically will be enabled after a certain time.

8.6 Loop Guard

Loops inside a network are very costly because they consume resources and lower network performance. Detecting loops manually can become cumbersome and tasking. Loop protection can be enabled or disabled on a port, or system-wide.

If loop protection is enabled, it sends packets to a reserved layer 2 multicast destination address on all the ports on which the feature is enabled. Transmission of the packet can be disabled on selected ports, even when loop protection is on. If a packet is received by the switch with matching multicast destination address, the source MAC in the packet is compared with its own MAC. If the MAC does not match, the packet is forwarded to all ports that are member of the same VLAN, except to the port from which it came in, treating it similar to a data packet. If the feature is enabled and source MAC matches its own MAC, the port on which the packet is received will be shut down, logged, or both actions taken depending upon the action configured.

If the feature is disabled, the packet will be dropped silently. The following matching criteria are used.

- DA= determined on customer requirement, AND
- SA= first 5 bytes of switch SA, AND
- Ether Type= 9003, AND

Loop protection is disabled by default, with an option to either enable globally on all the ports or individually on each port of the switch including the trunks (static only). Loop protection will coexist with the (M)STP protocol being enabled on the same physical ports. Loop protection will not affect the ports that (M)STP has put in non-forwarding state.

The following sections describe the rich L3 switching features supported by the WebStaX software.

8.7 Internet Group Management Protocol (IGMP)v2 Snooping

IGMP snooping can be configured system-wide including unregistered IP Multicast (IPMC) flooding, Source-Specific Multicast (SSM) range, proxy, and leave proxy. Per VLAN configuration is also supported for configuring IGMP snooping. The maximum IGMP interfaces refer to the maximum IP interfaces.

9. L3 and Routing

L3 routing is to select path and forward traffic to the nexthop based on the routing table. L3 routing includes hardware routing and software routing. Software routing is supported by the WebStaX software and hardware routing is supported by the VCAP LPM table. If the switch has no LPM table then it only uses software routing.

Only manually configured routing entries are supported, that is, static routes.

10. Security

The following sections describe the security features supported by the WebStaX software.

10.1 802.1X and MAC-Based Authentication

The IEEE 802.1X standard defines a port-based access control procedure that prevents unauthorized access to a network by requiring users to first submit credentials for authentication. One or more central servers, the backend servers, determine whether the user is allowed access the network.

Unlike port-based 802.1X, MAC-based authentication is not a standard, but merely a best-practices method adopted by the industry. In a MAC-based authentication, users are called clients, and the switch acts as a supplicant on behalf of clients. The initial frame (any kind of frame) sent by a client is snooped by the switch, which in turn uses the client's MAC address as both username and password in the subsequent Extensible Authentication Protocol (EAP) exchange with the Remote Authentication Dial In User Service (RADIUS) server.

The 6-byte MAC address is converted to a string in the following form: xx-xx-xx-xx-xx-xx. That is, a dash (-) is used as separator between the lower-case hexadecimal digits. The switch only supports the MD5- Challenge authentication method, so the RADIUS server must be configured accordingly. When authentication is complete, the RADIUS server sends a success or failure indication, which in turn causes the switch to open up or block traffic for that particular client, using the port security module. The frames from the client are then forwarded to the switch. There are no EAP over LAN (EAPOL) frames involved in this authentication, and therefore, MAC-based authentication has nothing to do with the 802.1X standard.

The advantage of MAC-based authentication over 802.1 X-based authentication is that the clients do not need special supplicant software to authenticate. The disadvantage is that MAC addresses can be spoofed by equipment whose MAC address is a valid RADIUS user that can be used by anyone. The maximum number of clients that can be attached to a port can be limited using the Port Security Limit Control functionality.

In a port-based 802.1X authentication, once a supplicant is successfully authenticated on a port, the whole port is opened for network traffic. This allows other clients connected to the port (for instance through a hub) to piggyback on the successfully authenticated client and get network access even though they really are not authenticated. To overcome this security breach, use the Single 802.1X variant.

Multi 802.1X is not an IEEE standard, but a variant that features many of the same characteristics. In Multi 802.1X, one or more supplicants can get authenticated on the same port at the same time. Each supplicant is authenticated individually and secured in the MAC table using the port security module. In Multi 802.1X, it is not possible to use the multicast BPDU MAC address as destination MAC address for EAPOL frames sent from the switch toward the supplicant because that causes all supplicants attached to the port to reply to requests sent from the switch. Instead, the switch uses the supplicant's MAC address, which is obtained from the first EAPOL Start or EAPOL Response Identity frame sent by the supplicant. An exception to this is when no supplicants are attached. In this case, the switch sends EAPOL Request Identity frames using the BPDU multicast MAC address as destination to wake up any supplicants that might be on the port.

The maximum number of supplicants that can be attached to a port can be limited using the Port Security Limit Control functionality.

When RADIUS-assigned QoS/VLANs are enabled globally and on a given port, the switch reacts to the QoS Class/ VLAN information carried in the RADIUS Access-Accept packet transmitted by the RADIUS server when a supplicant is successfully authenticated. If QoS information is present and valid, traffic received on the supplicant's port will be classified to the given QoS class in the case of RADIUSassigned QoS. Conversely, if VLAN ID is present and valid, the port's Port VLAN ID will be changed to this VLAN ID, the port will be set to be a member of that VLAN ID, and the port will be forced into VLAN

Unaware mode. Once assigned, all traffic arriving on the port will be classified and switched on the RADIUS-assigned VLAN ID. RADIUS-assigned VLANs based on a VLAN name are also supported.

If (re-)authentication fails, or the RADIUS Access-Accept packet no longer carries a QoS class/VLAN ID, or it's invalid, or the supplicant is otherwise no longer present on the port, the port's QoS class in the case of RADIUS-assigned QoS, and VLAN in the case of RADIUS-assigned VLAN, are immediately reverted to the original values (which may be changed by the administrator in the meanwhile without affecting the RADIUS-assigned).

This RADIUS-assigned QoS or VLAN option is only available for single-client modes, namely Port-based 802.1X.

10.2 Port Security

Port security enables configuration of the port security limit control system and port settings. It is possible to configure the port security limit aging per system.

Limit control enables limiting the number of users on a given port. A user is identified by a MAC address and VLAN ID. If limit control is enabled on a port, the limit specifies the maximum number of users on the port. If this number is exceeded, an appropriate action can be taken.

The switch is configured with a total number of MAC addresses, which all ports draw when a new MAC address is seen on a port security-enabled port. Because all ports draw from the same pool, it may happen that a configured maximum cannot be granted, if the remaining ports have already used all available MAC addresses.

10.3 Authentication, Authorization, and Accounting (AAA)

The AAA allows the common server configuration including the Timeout, Retransmit, Secret key, NAS IP address, NAS identifier, and Dead time parameters. WebStaX software supports the configuration of the RADIUS servers.

The RADIUS servers use the UDP protocol, which is unreliable by design. In order to cope with lost frames, the timeout interval is divided into three sub-intervals of equal length. If a reply is not received within the sub-interval, the request is transmitted again. This algorithm causes the RADIUS server to be queried up to three times before it is considered dead. The RADIUS authentication servers are used both by the NAS module and to authorize access to the switch's management interface.

The dead time, which can be set to a number between 0–3600 seconds, is the period during which the switch does not send new requests to a server that has failed to respond to a previous request. This stops the switch from continually trying to contact a server that it has already determined as dead. Setting the dead time to a value greater than zero enables this feature, but only if more than one server has been configured.

10.4 Secure Access

The following table lists the options available for Secure Access.

Table 10-1. Secure Access Options

Method	Description
SSL/HTTPs	Enable or disable.
HTTPs auto redirect	A redirect web browser to HTTPS option available when HTTPS mode is enabled.

10.5 Authentication and Authorization Methods

The following authentication and authorization methods are available.

10.5.1 Authentication Method

This method allows configuration of how users are authenticated when they log into the switch from one of the management client interfaces. The following configuration is allowed on the following management client types..

- Console
- SSH
- Web

Methods that involve remote servers are timed out if the remote servers are offline. In this case, the next method is tried. Each method is tried from left to right (when entered in the CLI) and continues until a method either approves or rejects a user. If a remote server is used for primary authentication, it is recommended to configure secondary

authentication as local. This enables the management client to log in using the local user database if none of the configured authentication servers are alive.

10.6 Access Control List (ACLs)

The ACL consists of a table of ACEs containing access control entries that specify individual users or groups permitted access to specific traffic objects such as a process or a program. The ACE parameters vary according to the frame type selected.

Each accessible traffic object contains an identifier to its ACL. The ACE action determine whether there are specific traffic object access rights.

ACL implementations can be quite complex, for example, when the ACEs are prioritized for the various situations. In networking, ACL refers to a list of service ports or network services that are available on a host or server, each with a list of hosts or servers permitted to use the service. ACLs can generally be configured to control inbound traffic, and in this context, they are similar to firewalls.

There are three rich configurable sections associated with the manual ACL configuration.

The ACL configuration shows the ACEs in a prioritized way, highest (top) to lowest (bottom). An ingress frame will only get a hit on one ACE even though there are more matching ACEs. The first matching ACE will take action (permit/deny) on that frame and a counter associated with that ACE is incremented. An ACE can be associated with any combination of ingress port(s) and policy (value/mask pair). If an ACE policy is created then that policy can be associated with a group of ports as part of the ACL port configuration. There are a number of parameters that can be configured with an ACE.

The ACL ports configuration is used as the default port rule. A policy can contain more than one ACE and it can be assigned on many ports. This is useful to group ports to obey the same traffic rules. Traffic policy is created under the ACL configuration. The following traffic properties can be set for each ingress port.

- Action
- Rate limiter
- Port redirect
- Mirror
- Logging
- Shutdown

The management interface allows the port action that is used to determine whether forwarding is permitted (Permit) or denied (Deny) on the port. The default action is Permit.

The default port rule is hit when the ingress frame from a specific port doesn't match any existing ACE. In that case a counter associated with that port is incremented. There can be 16 different ACL rate limiters. A rate limiter ID may be assigned to the ACE(s) or ingress port(s).

An ACE consists of several parameters. These parameters vary according to the frame type selected. The ingress port needs to be selected for the ACE, and then the frame type. Different parameter options are displayed depending on the frame type selected. The supported frame types include the following:

- Any
- Configurable Ethernet type
- IPv4
- IPv6

MAC-based filtering and IP protocol-based filtering can be achieved with configurations based on the selection of appropriate frame types.

11. Robustness and Power Savings

The following sections describe the robustness and power savings (green Ethernet) features supported by the WebStaX software.

11.1 Robustness

The following section introduces a robustness feature.

11.1.1 Cold and Cool Restart

The software defines and supports the following restart types.

- Cold—power cycle induced reset of the switch.
- Cool—software initiated reset of the switch (with traffic disruption).

11.2 Power Savings

The following sections introduce the power saving features.

11.2.1 Energy-Efficient Ethernet (EEE) Support

The EEE is a power saving option that reduces the power usage when there is low traffic utilization (or no traffic). EEE support allows the user to inspect and configure the current EEE port settings.

EEE works by powering down circuits when there is no traffic. When a port gets data to be transmitted all circuits are powered up. The time it takes to power up the circuits is named wakeup time. The default wakeup time is 17 ms for 1 Gbit links and 30 ms for other link speeds. EEE devices must agree upon the value of the wakeup time to make sure that both the receiving and transmitting devices have all circuits powered up when traffic is transmitted. The devices can exchange information about device wakeup times using the LLDP protocol.

EEE works for ports in auto-negotiation mode, where the port is negotiated to either 1G or 100 megabits full duplex mode.

11.2.2 LED Power Reduction Support

The WebStaX software supports the LED power reduction feature.

The LED power consumption can be reduced by lowering the intensity of LEDs. LEDs can be dimmed or turned off. LED intensity can be set for 24 one-hour periods in a day and can be configured from 0% to 100% in 10% increments for each period.

A network administrator may want to have full LED intensity during the maintenance period. Therefore it is possible to specify that the LEDs will use full intensity for a specific period of time.

Maintenance time is the number of seconds (10 to 65535, 10 being default) that the LEDs will have full intensity after either a port has changed link state or the LED button has been pressed.

11.2.3 Fan Information

The WebStaX software supports the following fan controls.

- Maximum temperature—temperature at which the fan runs at full speed.
- Turn on temperature—temperature at which the fan runs at the lowest possible speed.

11.2.4 ActiPHY

ActiPHY works by lowering the power for a port when there is no link. The port is power up for short moment in order to determine if cable is inserted.

11.2.5 PerfectReach

Perfect reach determines the cable length and lowers power consumption at ports with short cables.

11.2.6 Thermal Protection

Powering down ports if the temperature becomes high.

12. Management

The following sections describe the management features supported by the SMBStaX software.

12.1 Management Services

The WebStaX software provides the network administrator with a set of comprehensive management functions. The network administrator has a choice of the following easy-to-use management methods.

- CLI Interface
- Web-based
- Simple Network Management Protocol (SNMP)
- JSON-RPC

Management interfaces of the turnkey switch solutions are branded to comply with platform changes and the customer recommended standards as desired.

12.1.1 Industry Standard CLI Model

The CLI interface of the WebStaX software is an Industry Standard CLI model and consists of different configuration commands structure with an ability to configure and view the configuration using the Serial Console, Telnet (on port 23), or SSH access.

The Industry Standard CLI model includes the following features.

- Command history (by pressing the up arrow, the history of commands is available to the user).
- Command-line editing.
- VT100 compatible CLI terminal.
- Command groups based on command types.
- Configuration commands for configuring features and available options of the device.
- Show commands for displaying switch configuration, statistics, and other information.
- Copy commands for transferring or saving the software images for upgrade/downgrade, configuration files to and from the switch.
- Help for groups and specific commands.
- Shortcut key options. For example, the full command syntax support can be viewed for each possible command using the Ctrl+Q shortcut.

```
(config-if-vlan)# ip^Qip address
{{ <ipv4_addr> <ipv4_netmask> } | { dhcp [ fallback <ipv4_addr> < ipv4_netmask>
[ timeout <uint> ] ] } }
ip igmp snooping
ip igmp snooping compatibility { auto | v1 | v2 | v3 }
ip igmp snooping last-member-query-interval <0-31744>
ip igmp snooping priority <0-7>
ip igmp snooping querier { election | address <ipv4_ucast> }
ip igmp snooping query-interval <1-31744>
ip igmp snooping query-max-response-time <0-31744>
ip igmp snooping robustness-variable <1-255>
ip igmp snooping unsolicited-report-interval <0-31744>
```

- Context-sensitive help. Click '?' button for a list of valid possible parameters, with descriptions.
- Auto completion. Press <tab> key by partially typing the keyword. The rest of the keyword will be entered automatically.
- Ctrl+C option to break the display
- Modes for commands. Each command can belong to one or more modes. The commands in a particular mode can be made invisible in any other mode. The interface also allows wildcard support.

```
(config)# interface *
(config-if)#
```

If multiple sessions are concurrently in the same sub mode with same parameters, then 'no' form of commands will not work and will display a warning message.

- Privilege. A set of privilege attributes may be assigned to each command based on the level configured. A command cannot be accessed or executed if the logged in user does not have sufficient privilege.

12.1.1.1 User EXEC Mode

The User EXEC mode is the initial mode available for the users with insufficient privileges. The User EXEC mode contains a limited set of commands. The command prompt shown at this level is: `WebStaX>`.

12.1.1.2 Privileged EXEC Mode

The administrator/user must enter the privileged EXEC mode in order to have access to the full command suite. The privileged EXEC mode requires password authentication using an `enable` command, if set. The command prompt shown at this level is: WebStaX#

It is also possible to have runtime configurable privilege levels per command.

- Keyword abbreviations—any keyword can be accepted just by typing an unambiguous prefix (for example, “sh” for “show”).

```
WebStaX# sh ip route
0.0.0.0/0 via VLAN1:10.9.61.1 <UP GATEWAY HW_RT>
10.9.61.0/24 via VLAN1 <UP HW_RT>
127.0.0.1/32 via OS:lo:127.0.0.1 <UP HOST>
224.0.0.0/4 via OS:lo:127.0.0.1 <UP>
```

- Error checking—before executing a command, the CLI checks whether the current mode is still valid, user has sufficient privileges, and valid range of parameter(s) among others. The user is alerted to the error by displaying a caret under the offending word along with an error message.

```
WebStaX(config)# clock summer-time PDT date 14
^
% Invalid word detected at '^' marker
```

  Every configuration command has a no form to negate or set its default. In general, the no form is used to reverse the action of a command or reset a value back to the default. For example, the `no ip routing configuration` command reverses the ip routing of an interface.

- `do` command support—this will allow the users to execute the commands from the configuration mode.

```
(config)# do show vlan
VLAN Name Interface
---- ---- ---------
1 default Gi 1/1-9 2.5G 1/1-2
```

- Platform debug command support—this allows the users to obtain technical support by entering and running a debug command in this field.

12.1.2 Industry Standard Configuration Support

The WebStaX software supports an industry standard configuration (ICFG) where commands are stored in a text format.

The switch stores its configuration in a number of text files in CLI format. The files are either virtual (RAM-based), or stored in flash on the switch.

There are three system files:

- `running-config`—a virtual file that represents the currently active configuration on the switch. This file is volatile.
- `startup-config`—the startup configuration for the switch, read at boot time.
- `default-config`—a read-only file with vendor-specific configuration. This file is read when the system is restored to default settings. This is a per-build customizable file that does not require C source code changes.

It is also possible to store up to four files and apply them to `running-config`, thereby switching configuration. The maximum number of files in the configuration file is limited to a compressed size not exceeding 1 MB. The configuration can be dynamically viewed by issuing the `show running-config` command.

This current running configuration may be copied to the startup configuration using the copy command. ICFG may be edited and populated on multiple other switches using any standard text editor offline.

It is possible to upload a file from the web browser to all the files on the switch, `except default- config`, which is read-only. If the destination is `running-config`, the file will be applied to the switch configuration. This can be done in two ways:

- Replace mode—the current configuration is fully replaced with the configuration in the uploaded file.
- Merge mode—the uploaded file is merged with `running-config`.

If the file system is full, (that is, contains the three system files mentioned previously along with other files), it is not possible to create new files. An existing file must be overwritten or another deleted first.

It is possible to activate any of the configuration files present on the switch, except `running-config`, which represents the currently active configuration. This will initiate the process of completely replacing the existing configuration with that of the selected file.

It is possible to delete any of the writable files stored in flash, including `startup-config`. If this is done and the switch is rebooted without a prior Save operation, it effectively resets the switch to default configuration.

12.1.3 Web

The web-based software management method allows the network administrator to configure, manage, view, and control the switches remotely. The web-based management method also provides help pages for assisting the switch administrator in understanding the usage.

The supported web browsers are as follows:

- Internet Explorer 8.0 and above
- Firefox 30 and above
- Google Chrome 30 and above
- Safari S5
- Opera 11

The WebStaX software also supports a copy-all feature for selecting all the available ports. The web configuration is divided into different trees for the following tasks.

- Configuration of the features
- Monitoring of the configured features using the Auto-Refresh option
- Running supported diagnostics
- Maintenance of the related features

12.2 SNMP

The WebStaX software provides rich SNMP system configuration features with support for SNMPv1, SNMPv2c, and SNMPv3. SNMPv3 configuration facilitates creation of users without authentication and privacy.

SNMPv1 is supported as best effort, that is, 64-bit counters are included, they are left blank. SNMPv1 traps are not supported. This is because the implementation of SNMPv1 traps is very different from v2/v3 where the traps fit the OID scheme.

SNMPv3 User, Group, View, and Access configuration is also supported including authentication and privacy protocols/passwords. The SNMPv3 configuration allows creation of users without authentication and privacy.

By default, only MD5 and DES are supported for SNMPv3. To add support for sha and aes, openssl must be added to the brsdk.

SNMP configuration is supported with an option to specify the allowed network addresses restricted for read-only and read-write privileges.

12.3 Internet Control Message Protocol

Internet Control Message Protocol (ICMP) based ping is supported on these switches. By default, five ICMP packets are transmitted to the configured IP address, and the sequence numbers and round trip times are displayed upon the receipt of a reply. The payload size is set to 56 and is configurable from 2–1452. The number of ICMP packets sent is also configurable in a range from 1–60. The ping interval of the ICMP packet can be set from 0 seconds to 30 seconds.

- Ping—is a tool that checks the connectivity to a remote Internet Protocol (IP) host. It can also calculate the round-trip delay time for the complete route to the host. Both IPv4 and IPv6 are supported.
- Traceroute—is a tool that can determine the route an Internet Protocol (IP) packet takes from the source host to the remote destination host and also calculate the round-trip delay time for each hop of the route. Both IPv4 and IPv6 are supported. The timeout value can be configured from 1–86400 seconds while the default value is three seconds. Source address can be mentioned by using saddr option. The number of probes (range is 1–60) can be specified per hop with 3 as the default value. The number of hops (starting TTL) can be specified from 1–30 with 1 as the default value. The maximum number of hops can be configured from 1–255 with 30 as the default value. It can also be specified whether to use ICMP instead of UDP for IPv4 option.

12.4 SysLog

Syslog is a method to collect messages from devices to a server running a Syslog daemon. Logging to a central Syslog server helps in aggregation of logs and alerts. The WebStaX software can send the log messages to a configured Syslog server running on UDP port 512.

Some of the supported Syslog events are as follows:

- Port link up and down
- Port security limit control reach but the action is none
- Switch boot up

The total RAM buffer size of Syslog is 10 MB. Generally, the most recent 20,000 entries can be reserved, although each message length varies.

12.5 IP Management

The WebStaX software IP stack can be configured to act either as a host or a router. In Host mode, IP traffic between interfaces will not be routed. In Router mode, traffic is routed between all interfaces using Unicast routing.

The system can be configured with zero or more IP interfaces. Each IP interface is associated with a VLAN, and the VLAN represents the IP broadcast domain. Each IP interface may be configured with an IPv4 address. The DHCP (IPv4) client can be enabled to automatically obtain an IPv4 address from a DHCP server.

A fallback optional mechanism is also provided in the case of IPv4 so that the user can enter time period in seconds to obtain a DHCP address. After this lease expires, a configured IPv4 address will be used as the IPv4 interface address.The DHCP query process can be re-initiated on a VLAN.

12.6 Console

The WebStaX software uses the serial console to support the CLI for out of band management, debugging, and software upgrades.

12.7 System Management

The WebStaX software can be supported in band through any of the front panel ports.

It is possible to create a separate dedicated configurable Management VLAN corresponding to a port for managing the system. The system can be managed through SSH, SNMP, and web interfaces from this Management VLAN. However, there is no specific service port available on the device.

12.8 Management Access Filtering

It is possible to restrict access to the switch by specifying the IP address of the VLAN. The HTTP/HTTPs, SNMP, and Telnet/SSH interfaces can be restricted with this feature. The maximum number of management access filter entries allowed is 16.

If the application's type matches any one of the access management entries, it will allow access to the switch. The access management statistics can also be viewed.

12.9 Default Configuration

The user can also reset the configuration of the switch using the web interface. Only the IP configuration is retained after resetting to factory defaults. The new configuration is available immediately, which means that no restart is necessary.

12.10 Configuration Upload/Download

The switch software allows saving, viewing, or loading the switch configuration. For more information, see 12.1.2 Industry Standard Configuration Support.

12.11 Loop Detection Restore to Default

Restoring factory default can also be performed by making a physical loopback between port 1 and port 2 within the first minute from switch reboot. In the first minute after boot, loopback packets is transmitted at port 1.

If a loopback packet is received at port 2, the switch restores to default.

12.12 Symbolic Register Access

Switch core registers can be accessed through system read and write operations.

12.13 SD/MMC Card Slot

SD-MMC support has been added to the following:

- Serval1 reference (not redboot)
- Serval1 Network Interface Device (NID) (not redboot)
- Serval2 NID (both redboot and application)

SD-MMC can be used it for storing performance monitoring, EVC counter, MEP data for Persisting measurements (24H). With the availability of SD/MMC and a new set of redboot commands, an SD card can be inserted in the socket on a Serval1 REF or NID board. The SD card must be FAT-formatted.

12.14 802.1AB LLDP and CDP Aware

Link Layer Discovery Protocol (LLDP) is a protocol used to help network administrators managing the network and maintaining an accurate network topology. LLDP capable devices discover each other by periodically advertising their presence and configuration parameters through messages called Type Length Value (TLV) fields to neighbor devices.

The LLDP can operate in three modes:

- Transmit only mode—the device only transmits configuration parameters.
- Receive-only mode—the device can only receive configuration parameters (from neighbor device).
- Transmit and receive mode—the device can both transmit and receive configuration parameters.

It is possible to enable/disable the Rx and Tx parts separately. The LLDP standard consists of a set of mandatory TLVs and a set of optional TLVs. The mandatory TLVs, optional basic TLVs are supported. None of the IEEE 802.1 Organizationally Specific TLVs are supported.

13. SNMP MIBs

The WebStaX supports the following comprehensive set of private and standard MIBs. The SNMPv3 is supported and is backward compatible with SNMPv2c and SNMP v1. The MIB information can be viewed with the configured community name. For more information, see SNMP, page 40. The following CLI commands can be used to display the supported MIBs and view the ifIndex mapping.

```
# show snmp mib context
BRIDGE-MIB :
- dot1dBase (.1.3.6.1.2.1.17.1)
- dot1dTp (.1.3.6.1.2.1.17.4)
Dot3-OAM-MIB :
- dot3OamMIB (.1.3.6.1.2.1.158)
ENTITY-MIB :
- entityMIBObjects (.1.3.6.1.2.1.47.1)
EtherLike-MIB :
- transmission (.1.3.6.1.2.1.10)
IEEE8021-BRIDGE-MIB
:
# show snmp mib ifmib ifIndex
```

Table 13-1. ifIndex Descriptions

ifIndex	ifDescr	Interface
1	VLAN 1	VLAN 1
1000001	Switch 1–port 1	GigabitEthernet 1/1
1000002	Switch 1–port 2	GigabitEthernet 1/2
1000003	Switch 1–port 3	GigabitEthernet 1/3
1000004	Switch 1–port 4	GigabitEthernet 1/4
1000005	Switch 1–port 5	GigabitEthernet 1/5
1000006	Switch 1–port 6	GigabitEthernet 1/6
1000007	Switch 1–port 7	GigabitEthernet 1/7
1000008	Switch 1–port 8	GigabitEthernet 1/8
1000009	Switch 1–port 9	2.5 GigabitEthernet 1/1
10000010	Switch 1–port 10	2.5 GigabitEthernet 1/2
10000011	Switch 1–port 11	GigabitEthernet 1/9

14. Revision History

Revision	Date	Description
B	February 2021	Revision B was published in February 2021 to align with the Linux application software release 202012. The following is a summary of changes in revision B of this document. • The BSP and API: Supported Features table was updated. For more information, see Table 1-1. • The Port Control: Supported Features table was updated. For more information, see Table 1-2. • The QoS: Supported Features table was updated. For more information, see Table 1-3. • The L2 Switching: Supported Features table was updated. For more information, see Table 1-4. • The L3 and Routing: Supported Features table was updated. For more information, see Table 1-5. • The Security: Supported Features table was updated. For more information, see Table 1-6. • The Robustness and Power Savings: Supported Features table was updated. For more information, see Table 1-7. • The Customization Framework: Supported Features table was updated. For more information, see Table 1-8. • The Management: Supported Features table was updated. For more information, see Table 1-9. • The SNMP MIBs: Supported Features table was updated. For more information, see Table 1-10. • The Features and Platform Capacity table was updated. For more information, see Table 2-1. • The Features and Platform Capacity table was updated. For more information, see Table 3-1. • The SNMP section was updated. For more information, see 12.2 SNMP.

.....continued

Revision	Date	Description
A	June 2020	Revision A was published in June 2020 to align with the Linux application software release 2020.3.0. The following is a summary of changes in revision A of this document. • The document was migrated to Microchip template. • The document number was updated from VPPD-04313 to DS30010227A. • The Supported Switches table was updated. For more information, see Table 1. • The BSP and API: Supported Features table was updated. For more information, see Table 1-1. • The Port Control: Supported Features table was updated. For more information, see Table 1-2. • The QoS: Supported Features table was updated. For more information, see Table 1-3. • The L2 Switching: Supported Features table was updated. For more information, see Table 1-4. • The L3 and Routing: Supported Features table was updated. For more information, see Table 1-5. • The Security: Supported Features table was updated. For more information, see Table 1-6. • The Robustness and Power Savings: Supported Features table was updated. For more information, see Table 1-7. • The Customization Framework: Supported Features table was updated. For more information, see Table 1-8. • The Management: Supported Features table was updated. For more information, see Table 1-9. • The SNMP MIBs: Supported Features table was updated. For more information, see Table 1-10. • The Features and Platform Capacity table was updated. For more information, see Table 2-1. • The Features and Platform Capacity table was updated. For more information, see Table 3-1.
1.8	June 2019	Revision 1.8 was published in June 2019 to align with the Linux application software release 2019.6.0. In this version, only the release information was updated.
1.7	June 2019	Revision 1.7 was published in June 2019 to align with the Linux application software release 4.8. The following is a summary of changes in revision 1.7 of this document. • The Port Control: Supported Features table was updated. For more information, see Table 1-2. • The L3 and Routing: Supported Features table was added. For more information, see 1.5 L3 and Routing. • The Security: Supported Features table was updated. For more information, see Table 1-6. • The L3 and Routing section was added. For more information, see 9. L3 and Routing.

.....continued

Revision	Date	Description
1.6	January 2019	Revision 1.6 was published in January 2019 to align with the Linux application software release 4.7. The following is a summary of changes in revision 1.6 of this document. • The BSP and API: Supported Features table was updated. For more information, see Table 1-1. • The Port Control: Supported Features table was updated. For more information, see Table 1-2. • The QoS: Supported Features table was updated. For more information, see Table 1-3. • The L2 Switching: Supported Features table was updated. For more information, see Table 1-4. • The Security: Supported Features table was updated. For more information, see Table 1-6. • The Robustness and Power Savings: Supported Features table was updated. For more information, see Table 1-7. • The Customization Framework: Supported Features table was updated. For more information, see Table 1-8. • The Management: Supported Features table was updated. For more information, see Table 1-9. • The SNMP MIBs: Supported Features table was updated. For more information, see Table 1-10.
1.5	October 2018	Revision 1.5 was published in October 2018 to align with the Linux application software release 4.6. The following is a summary of changes in revision 1.5 of this document. • The Port Control: Supported Features table was updated. For more information, see Table 1-2. • The QoS: Supported Features table was updated. For more information, see Table 1-3. • The Security: Supported Features table was updated. For more information, see Table 1-6. • The Robustness and Power Savings: Supported Features table was updated. For more information, see Table 1-7. • The Customization Framework: Supported Features table was updated. For more information, see Table 1-8. • The Management: Supported Features table was updated. For more information, see Table 1-9. • The SNMP MIBs: Supported Features table was updated. For more information, see Table 1-10. • Removed the VLAN Translation is removed from the L2 Switching chapter. • The Cold and Cool Restart section was updated. For more information, see 11.1.1 Cold and Cool Restart. • Removed the Port Statistics section from the Management chapter. • Removed the Software Functions Supported by JSON RPC section from the Management chapter. • Removed the Private MIB and the Standard MIB sections from the SNMP MIBs chapter.

.....continued

Revision	Date	Description
1.4	July 2018	Revision 1.4 was published in July 2018 to align with the Linux application software release 4.5. The following is a summary of changes in revision 1.4 of this document. • The System Capability section was added. For more information, see 4.2 System Capability. • The list of features in the Port Control: Supported Features table was updated with three more features. For more information, see 1.2 Port Control.
1.3	April 2018	Revision 1.3 was published in April 2018 to align with the Linux application software release 4.4. The following is a summary of changes in revision 1.3 of this document. • The System Capability section was added. For more information, see 4.2 System Capability. • The VLAN Translation section was added. For more information, see #unique_90. • The Internet Control Message Protocol section was added. For more information, see 12.3 Internet Control Message Protocol.
1.2	January 2018	Revision 1.2 was published in January 2018 to align with the Linux application software release 4.3. The following is a summary of changes in revision 1.2 of this document. • The list of supported switches in the Supported Switches table was updated with the details of VSC7415. For more information, see #unique_91. • The header rows of all the tables in Supported Features section were updated. For more information, see #unique_92. • The list of features in the Port Control: Supported Features table was updated with three more features. For more information, see 1.2 Port Control. • The list of features in the L2 Switching: Supported Features table was updated with four more features. For more information, see 1.4 L2 Switching.
1.1	June 2017	Revision 1.1 was published in June 2017 to align with the Linux application software release 4.1. The following is a summary of changes in revision 1.1 of this document. • The list of supported switches was updated to reflect available devices. For more information, see #unique_91. • The list of supported features was updated to reflect the SparX-IV, Serval-T, and Ocelot devices. For more information, see #unique_92. • The list of features and platform capacity was updated to reflect the SparX-IV, Serval-T, and Ocelot devices. For more information, see 2. Features and Platform Capacity. • The list of port system requirements was updated to reflect the SparX-IV, Serval-T, and Ocelot devices. For more information, see 3. System Requirements.
1.0	November 2016	Revision 1.0 was published in November 2016 to align with the Linux application software release 4.0. It was the first publication of this document.

The Microchip Website

Microchip provides online support via our website at www.microchip.com/. This website is used to make files and information easily available to customers. Some of the content available includes:

- **Product Support** – Data sheets and errata, application notes and sample programs, design resources, user's guides and hardware support documents, latest software releases and archived software
- **General Technical Support** – Frequently Asked Questions (FAQs), technical support requests, online discussion groups, Microchip design partner program member listing
- **Business of Microchip** – Product selector and ordering guides, latest Microchip press releases, listing of seminars and events, listings of Microchip sales offices, distributors and factory representatives

Product Change Notification Service

Microchip's product change notification service helps keep customers current on Microchip products. Subscribers will receive email notification whenever there are changes, updates, revisions or errata related to a specified product family or development tool of interest.

To register, go to www.microchip.com/pcn and follow the registration instructions.

Customer Support

Users of Microchip products can receive assistance through several channels:

- Distributor or Representative
- Local Sales Office
- Embedded Solutions Engineer (ESE)
- Technical Support

Customers should contact their distributor, representative or ESE for support. Local sales offices are also available to help customers. A listing of sales offices and locations is included in this document.

Technical support is available through the website at: www.microchip.com/support

Microchip Devices Code Protection Feature

Note the following details of the code protection feature on Microchip devices:

- Microchip products meet the specification contained in their particular Microchip Data Sheet.
- Microchip believes that its family of products is one of the most secure families of its kind on the market today, when used in the intended manner and under normal conditions.
- There are dishonest and possibly illegal methods used to breach the code protection feature. All of these methods, to our knowledge, require using the Microchip products in a manner outside the operating specifications contained in Microchip's Data Sheets. Most likely, the person doing so is engaged in theft of intellectual property.
- Microchip is willing to work with the customer who is concerned about the integrity of their code.
- Neither Microchip nor any other semiconductor manufacturer can guarantee the security of their code. Code protection does not mean that we are guaranteeing the product as "unbreakable."

Code protection is constantly evolving. We at Microchip are committed to continuously improving the code protection features of our products. Attempts to break Microchip's code protection feature may be a violation of the Digital Millennium Copyright Act. If such acts allow unauthorized access to your software or other copyrighted work, you may have a right to sue for relief under that Act.

Legal Notice

Information contained in this publication regarding device applications and the like is provided only for your convenience and may be superseded by updates. It is your responsibility to ensure that your application meets with

your specifications. MICROCHIP MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WHETHER EXPRESS OR IMPLIED, WRITTEN OR ORAL, STATUTORY OR OTHERWISE, RELATED TO THE INFORMATION, INCLUDING BUT NOT LIMITED TO ITS CONDITION, QUALITY, PERFORMANCE, MERCHANTABILITY OR FITNESS FOR PURPOSE. Microchip disclaims all liability arising from this information and its use. Use of Microchip devices in life support and/or safety applications is entirely at the buyer's risk, and the buyer agrees to defend, indemnify and hold harmless Microchip from any and all damages, claims, suits, or expenses resulting from such use. No licenses are conveyed, implicitly or otherwise, under any Microchip intellectual property rights unless otherwise stated.

Trademarks

The Microchip name and logo, the Microchip logo, Adaptec, AnyRate, AVR, AVR logo, AVR Freaks, BesTime, BitCloud, chipKIT, chipKIT logo, CryptoMemory, CryptoRF, dsPIC, FlashFlex, flexPWR, HELDO, IGLOO, JukeBlox, KeeLoq, Kleer, LANCheck, LinkMD, maXStylus, maXTouch, MediaLB, megaAVR, Microsemi, Microsemi logo, MOST, MOST logo, MPLAB, OptoLyzer, PackeTime, PIC, picoPower, PICSTART, PIC32 logo, PolarFire, Prochip Designer, QTouch, SAM-BA, SenGenuity, SpyNIC, SST, SST Logo, SuperFlash, Symmetricom, SyncServer, Tachyon, TempTrackr, TimeSource, tinyAVR, UNI/O, Vectron, and XMEGA are registered trademarks of Microchip Technology Incorporated in the U.S.A. and other countries.

APT, ClockWorks, The Embedded Control Solutions Company, EtherSynch, FlashTec, Hyper Speed Control, HyperLight Load, IntelliMOS, Libero, motorBench, mTouch, Powermite 3, Precision Edge, ProASIC, ProASIC Plus, ProASIC Plus logo, Quiet-Wire, SmartFusion, SyncWorld, Temux, TimeCesium, TimeHub, TimePictra, TimeProvider, Vite, WinPath, and ZL are registered trademarks of Microchip Technology Incorporated in the U.S.A.

Adjacent Key Suppression, AKS, Analog-for-the-Digital Age, Any Capacitor, AnyIn, AnyOut, BlueSky, BodyCom, CodeGuard, CryptoAuthentication, CryptoAutomotive, CryptoCompanion, CryptoController, dsPICDEM, dsPICDEM.net, Dynamic Average Matching, DAM, ECAN, EtherGREEN, In-Circuit Serial Programming, ICSP, INICnet, Inter-Chip Connectivity, JitterBlocker, KleerNet, KleerNet logo, memBrain, Mindi, MiWi, MPASM, MPF, MPLAB Certified logo, MPLIB, MPLINK, MultiTRAK, NetDetach, Omniscient Code Generation, PICDEM, PICDEM.net, PICkit, PICtail, PowerSmart, PureSilicon, QMatrix, REAL ICE, Ripple Blocker, SAM-ICE, Serial Quad I/O, SMART-I.S., SQI, SuperSwitcher, SuperSwitcher II, Total Endurance, TSHARC, USBCheck, VariSense, ViewSpan, WiperLock, Wireless DNA, and ZENA are trademarks of Microchip Technology Incorporated in the U.S.A. and other countries.

SQTP is a service mark of Microchip Technology Incorporated in the U.S.A.

The Adaptec logo, Frequency on Demand, Silicon Storage Technology, and Symmcom are registered trademarks of Microchip Technology Inc. in other countries.

GestIC is a registered trademark of Microchip Technology Germany II GmbH & Co. KG, a subsidiary of Microchip Technology Inc., in other countries.

All other trademarks mentioned herein are property of their respective companies.

ISBN: 978-1-5224-7594-1

Quality Management System

For information regarding Microchip's Quality Management Systems, please visit www.microchip.com/quality.

Worldwide Sales and Service

AMERICAS	ASIA/PACIFIC	ASIA/PACIFIC	EUROPE
Corporate Office 2355 West Chandler Blvd. Chandler, AZ 85224-6199 Tel: 480-792-7200 Fax: 480-792-7277 Technical Support: www.microchip.com/support Web Address: www.microchip.com **Atlanta** Duluth, GA Tel: 678-957-9614 Fax: 678-957-1455 **Austin, TX** Tel: 512-257-3370 **Boston** Westborough, MA Tel: 774-760-0087 Fax: 774-760-0088 **Chicago** Itasca, IL Tel: 630-285-0071 Fax: 630-285-0075 **Dallas** Addison, TX Tel: 972-818-7423 Fax: 972-818-2924 **Detroit** Novi, MI Tel: 248-848-4000 **Houston, TX** Tel: 281-894-5983 **Indianapolis** Noblesville, IN Tel: 317-773-8323 Fax: 317-773-5453 Tel: 317-536-2380 **Los Angeles** Mission Viejo, CA Tel: 949-462-9523 Fax: 949-462-9608 Tel: 951-273-7800 **Raleigh, NC** Tel: 919-844-7510 **New York, NY** Tel: 631-435-6000 **San Jose, CA** Tel: 408-735-9110 Tel: 408-436-4270 **Canada - Toronto** Tel: 905-695-1980 Fax: 905-695-2078	**Australia - Sydney** Tel: 61-2-9868-6733 **China - Beijing** Tel: 86-10-8569-7000 **China - Chengdu** Tel: 86-28-8665-5511 **China - Chongqing** Tel: 86-23-8980-9588 **China - Dongguan** Tel: 86-769-8702-9880 **China - Guangzhou** Tel: 86-20-8755-8029 **China - Hangzhou** Tel: 86-571-8792-8115 **China - Hong Kong SAR** Tel: 852-2943-5100 **China - Nanjing** Tel: 86-25-8473-2460 **China - Qingdao** Tel: 86-532-8502-7355 **China - Shanghai** Tel: 86-21-3326-8000 **China - Shenyang** Tel: 86-24-2334-2829 **China - Shenzhen** Tel: 86-755-8864-2200 **China - Suzhou** Tel: 86-186-6233-1526 **China - Wuhan** Tel: 86-27-5980-5300 **China - Xian** Tel: 86-29-8833-7252 **China - Xiamen** Tel: 86-592-2388138 **China - Zhuhai** Tel: 86-756-3210040	**India - Bangalore** Tel: 91-80-3090-4444 **India - New Delhi** Tel: 91-11-4160-8631 **India - Pune** Tel: 91-20-4121-0141 **Japan - Osaka** Tel: 81-6-6152-7160 **Japan - Tokyo** Tel: 81-3-6880- 3770 **Korea - Daegu** Tel: 82-53-744-4301 **Korea - Seoul** Tel: 82-2-554-7200 **Malaysia - Kuala Lumpur** Tel: 60-3-7651-7906 **Malaysia - Penang** Tel: 60-4-227-8870 **Philippines - Manila** Tel: 63-2-634-9065 **Singapore** Tel: 65-6334-8870 **Taiwan - Hsin Chu** Tel: 886-3-577-8366 **Taiwan - Kaohsiung** Tel: 886-7-213-7830 **Taiwan - Taipei** Tel: 886-2-2508-8600 **Thailand - Bangkok** Tel: 66-2-694-1351 **Vietnam - Ho Chi Minh** Tel: 84-28-5448-2100	**Austria - Wels** Tel: 43-7242-2244-39 Fax: 43-7242-2244-393 **Denmark - Copenhagen** Tel: 45-4485-5910 Fax: 45-4485-2829 **Finland - Espoo** Tel: 358-9-4520-820 **France - Paris** Tel: 33-1-69-53-63-20 Fax: 33-1-69-30-90-79 **Germany - Garching** Tel: 49-8931-9700 **Germany - Haan** Tel: 49-2129-3766400 **Germany - Heilbronn** Tel: 49-7131-72400 **Germany - Karlsruhe** Tel: 49-721-625370 **Germany - Munich** Tel: 49-89-627-144-0 Fax: 49-89-627-144-44 **Germany - Rosenheim** Tel: 49-8031-354-560 **Israel - Ra'anana** Tel: 972-9-744-7705 **Italy - Milan** Tel: 39-0331-742611 Fax: 39-0331-466781 **Italy - Padova** Tel: 39-049-7625286 **Netherlands - Drunen** Tel: 31-416-690399 Fax: 31-416-690340 **Norway - Trondheim** Tel: 47-72884388 **Poland - Warsaw** Tel: 48-22-3325737 **Romania - Bucharest** Tel: 40-21-407-87-50 **Spain - Madrid** Tel: 34-91-708-08-90 Fax: 34-91-708-08-91 **Sweden - Gothenberg** Tel: 46-31-704-60-40 **Sweden - Stockholm** Tel: 46-8-5090-4654 **UK - Wokingham** Tel: 44-118-921-5800 Fax: 44-118-921-5820