VSC6813

SMBStaX Software Product Specification
# Table of Contents

1 Product Overview ................................................................. 1
   1.1 Supported Switch Platforms ............................................... 1
   1.2 Terms and Abbreviations .................................................. 2
   1.3 Software Architecture .................................................... 3

2 Supported Features ............................................................. 5

3 Features and Platform Capacity .............................................. 11

4 System Requirements .......................................................... 13

5 Port and System Functionality ................................................ 15
   5.1 Port Functionality ............................................................ 15
   5.2 System Functionality ....................................................... 15

6 Firmware Upgrade ............................................................... 17

7 Port Control ....................................................................... 19
   7.1 VeriPHY Support ............................................................. 19
   7.2 PoE/PoE+ Support ............................................................ 19

8 Quality of Service (QoS) ......................................................... 21
   8.1 Policing ........................................................................ 21
   8.2 Scheduling and Shaping ..................................................... 21
   8.3 QCL Configuration ........................................................... 21
   8.4 WRED ........................................................................ 21
   8.5 Tag Remarking ............................................................... 21
   8.6 Ingress Port Classification ................................................ 22
   8.7 Queue Policers ............................................................... 22
   8.8 DSCP ......................................................................... 22

9 L2 Switching ....................................................................... 23
   9.1 VLAN ........................................................................... 23
   9.2 Generic VLAN Registration Protocol (GVRP) ......................... 24
   9.3 IEEE 802.3ad Link Aggregation ......................................... 24
   9.4 Bridge Protocol Data Unit (BPDU) Guard ............................ 25
   9.5 DHCP Snooping .............................................................. 25
   9.6 Universal Plug and Play (UPnP) ........................................ 26
   9.7 Storm Control ............................................................... 26
   9.8 MAC Table Configuration ................................................ 26
   9.9 Mirroring (SPAN/VSPAN and RSPAN) ......................... 26
   9.10 RMirror .................................................................. 27
   9.11 Spanning Tree .............................................................. 27
   9.12 Unidirectional Link Detection (UDLD) .............................. 27

10 L3 Switching .................................................................. 29
   10.1 IP Routing ................................................................. 29
   10.2 ICMPv6 ................................................................... 29
11 Security ................................................................. 31
11.1 802.1X and MAC-based Authentication ........................................... 31
11.2 Port Security .............................................................................. 31
11.3 Loop Protection ........................................................................ 32
11.4 Authentication Authorization Accounting (AAA) ......................... 33
11.5 Secure Access ............................................................................ 33
11.6 Users and Privilege Levels .............................................................. 33
11.7 Auth Method .............................................................................. 34
11.8 Access Control List (ACLs) ............................................................. 34
11.9 ARP Inspection/IP Source Guard ....................................................... 35

12 Stacking .................................................................................. 37
12.1 Stack Installation ........................................................................ 37
12.2 Stack Management ..................................................................... 37
12.3 Stack Split and Join ..................................................................... 37
12.4 Switch Addition - Mixed 24/48 GE Port Stacking ......................... 37
12.5 Switch Replacement ................................................................... 38

13 Robustness and Power Savings .................................................. 39
13.1 Robustness ............................................................................... 39
13.2 Green Ethernet .......................................................................... 39
13.3 VeriPHY ................................................................................... 40

14 Management ................................................................. 41
14.1 JSON-RPC ................................................................................. 41
14.2 Management Services ................................................................. 41
14.3 SNMP ....................................................................................... 44
14.4 RMON Statistics ....................................................................... 44
14.5 Internet Control Message Protocol (ICMP) ...................................... 45
14.6 SysLog ....................................................................................... 45
14.7 LLDP-MED ............................................................................... 45
14.8 802.1AB LLDP and CDP Aware ................................................... 47
14.9 IP Management, DNS, and DHCPv4/v6 ........................................ 48
14.10 DHCP Server ........................................................................... 48
14.11 DHCP Relay ............................................................................ 49
14.12 Management Requirements .......................................................... 49
14.13 Management Access Filtering ..................................................... 50
14.14 Thermal Protection ................................................................... 50
14.15 sFlow ....................................................................................... 50
14.16 Default Configuration ................................................................ 50
14.17 Configuration Upload/Download .................................................. 50
14.18 Port Statistics .......................................................................... 50
14.19 Network Time Protocol (NTP) ..................................................... 50
14.20 Loop Detection Restore to Default ............................................. 51
14.21 Dual Image .............................................................................. 51
14.22 Software Modules Supported by JSON-RPC ............................. 51

15 SNMP MIBs ............................................................................. 55
15.1 Private MIBs ............................................................................. 55
15.2 Standard MIBs .......................................................................... 56
16 List of Changes. ................................................................. 59
1 Product Overview

The SMBStaX turnkey software package is a fully managed L2 switch application for the small-medium enterprise (SME). This software package can be customized to support different port configurations with or without stacking. It is built on an Embedded Configurable Operating System (eCos) to ensure cost optimization without compromising efficiency. SMBStaX supports the following major capabilities.

- RedBoot boot loader
- Web or XMODEM update and dual boot support
- Up to 16 units in a stack
- Single point of management (SPOM)
- Shortest path forwarding (SPF)
- Slave units as backup masters
- 8 ms worst case master reelect across the stack

Management is done using a Web Graphical User Interface (GUI), Command Line Interface (CLI), Simple Network Management Protocol (SNMP), or Java Script Object Notation Remote Procedure Call (JSON-RPC) running on the internal MIPS24Kec CPU. SMBStaX is highly integrated with switch features such as QoS Control Lists (QCLs), Access Control Lists (ACLs), HW MAC table synchronization across the stack, and super priority management queue.

This document provides an overview of the switch and software features of SMBStaX 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.

1.1 Supported Switch Platforms

This software is supported on a series of Microsemi switches ranging from 10, 24 to 48 ports with Power over Ethernet (PoE) / non-PoE capabilities. The following table shows the supported switches.

<table>
<thead>
<tr>
<th>Switch</th>
<th>CPU</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VSC7414</td>
<td>MIPS 24Kec</td>
<td>SparX-III 8x1G + 2x2.5 G ports + 1 NPI*</td>
</tr>
<tr>
<td>VSC7424</td>
<td>MIPS 24Kec</td>
<td>SparX-III 10x1G Layer 2 switch</td>
</tr>
<tr>
<td>VSC7425</td>
<td>MIPS 24Kec</td>
<td>SparX-III 18x1G Layer 2 switch</td>
</tr>
<tr>
<td>VSC7426</td>
<td>MIPS 24Kec</td>
<td>SparX-III 24x1G Layer 2 switch</td>
</tr>
<tr>
<td>VSC7427</td>
<td>MIPS 24Kec</td>
<td>SparX-III 26x1G Layer 2 switch</td>
</tr>
<tr>
<td>VSC7431</td>
<td>MIPS 24Kec</td>
<td>E-StaX-III 24x1G + 2x12G stackable switch</td>
</tr>
<tr>
<td>VSC7432</td>
<td>MIPS 24Kec</td>
<td>E-StaX-III 24x1G + 2x10/12G stackable switch</td>
</tr>
<tr>
<td>VSC7434</td>
<td>MIPS 24Kec</td>
<td>E-StaX-III 24x1G + 4x10/12G stackable switch</td>
</tr>
<tr>
<td>VSC7442</td>
<td>500 MHz MIPS 24Kec</td>
<td>SparX-IV 52x1G Layer 2 / Layer 3 switch</td>
</tr>
</tbody>
</table>
1.2 Terms and Abbreviations

The following table provides the definitions of abbreviations used in this document.

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>AAA</td>
<td>Authentication Authorization Accounting</td>
</tr>
<tr>
<td>ACL</td>
<td>Access Control List</td>
</tr>
<tr>
<td>API</td>
<td>Application Programming Interface</td>
</tr>
<tr>
<td>BPDU</td>
<td>Bridge Protocol Data Unit</td>
</tr>
<tr>
<td>BSP</td>
<td>Board Support Package (specific OS running on specific CPU system)</td>
</tr>
<tr>
<td>CIST</td>
<td>Common and Internal Spanning Tree</td>
</tr>
<tr>
<td>CLI</td>
<td>Command Line Interface</td>
</tr>
<tr>
<td>EAPoL</td>
<td>Extensible Authentication Protocol (EAP) over LAN</td>
</tr>
<tr>
<td>eCos</td>
<td>Embedded Configurable Operating system</td>
</tr>
<tr>
<td>EEE</td>
<td>Energy-Efficient Ethernet</td>
</tr>
<tr>
<td>GUI</td>
<td>Graphical User Interface</td>
</tr>
<tr>
<td>GVRP</td>
<td>Generic VLAN Registration Protocol</td>
</tr>
<tr>
<td>ICMP</td>
<td>Internet Control Message Protocol</td>
</tr>
<tr>
<td>IGMP</td>
<td>Internet Group Management Protocol</td>
</tr>
<tr>
<td>IPMC</td>
<td>IP Multicast</td>
</tr>
<tr>
<td>LACP</td>
<td>Link Aggregation Control Protocol</td>
</tr>
<tr>
<td>LLDP</td>
<td>Link Layer Discovery Protocol</td>
</tr>
<tr>
<td>MLD</td>
<td>Multicast Listener Discovery</td>
</tr>
<tr>
<td>MVR</td>
<td>Multicast VLAN Registration</td>
</tr>
<tr>
<td>NAS</td>
<td>Network Access Server</td>
</tr>
<tr>
<td>NPI</td>
<td>Network Peripheral Interface</td>
</tr>
<tr>
<td>OS</td>
<td>Operating System</td>
</tr>
<tr>
<td>OUI</td>
<td>Organizationally Unique Identifier</td>
</tr>
<tr>
<td>PoE</td>
<td>Power Over Ethernet</td>
</tr>
<tr>
<td>QCL</td>
<td>QoS Control List</td>
</tr>
</tbody>
</table>
1.3 Software Architecture

The SMBStaX software provides standalone switch support. It consists of the following components.

- Operating system (eCos) for access to the hardware.
- API for a function library to control switches and PHYs.
- Control modules such as port control, MSTP, and 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, JSON-RPC, and SNMP for interfaces to the system based on the management API of the control modules.

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

![Application Architecture](attachment:image.png)

### Table 2 • Terms and Abbreviations (continued)

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>RADIUS</td>
<td>Remote Authentication Dial In User Service</td>
</tr>
<tr>
<td>RSTP</td>
<td>Rapid Spanning Tree Protocol</td>
</tr>
<tr>
<td>SMB</td>
<td>Small and Medium Businesses</td>
</tr>
<tr>
<td>SME</td>
<td>Small and Medium Enterprises</td>
</tr>
<tr>
<td>SNMP</td>
<td>Simple Network Management Protocol</td>
</tr>
<tr>
<td>SSDP</td>
<td>Simple Service Discovery Protocol</td>
</tr>
<tr>
<td>SSM</td>
<td>Source-Specific Multicast</td>
</tr>
<tr>
<td>TLV</td>
<td>Type Length Value</td>
</tr>
<tr>
<td>UDLD</td>
<td>Unidirectional Link Detection</td>
</tr>
<tr>
<td>UPnP</td>
<td>Universal Plug and Play</td>
</tr>
<tr>
<td>VLAN</td>
<td>Virtual LAN</td>
</tr>
</tbody>
</table>
## 2 Supported Features

The following table shows the features supported by the SMBStaX software.

**Table 3 • Supported Features**

<table>
<thead>
<tr>
<th>Feature</th>
<th>SparX-III VSC7424-7</th>
<th>SparX-III VSC7414</th>
<th>E-StaX-III VSC7431/2/4</th>
<th>SparX-IV VSC7442/4/8</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>&quot;Port Control&quot;</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Port speed/duplex mode/flow control</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>Per priority pause</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Port frame size (Jumbo frames)</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>Port state (administrative status)</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>Port status (link monitoring)</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>Port statistics (MIB counters)</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>Port VeriPHY (cable diagnostics)</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>PoE/PoE+</td>
<td>•</td>
<td>•</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PoE/PoE+ with LLDP</td>
<td>•</td>
<td>•</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NPI port</td>
<td>•</td>
<td>•</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PCIe</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>On-the-fly SFP detection</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>UDLD</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td><strong>&quot;Quality of Service (QoS)&quot;</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Traffic classes (8 active priorities)</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>Port default priority</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>User priority</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>Input priority mapping</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>QoS control list (QCL mode)</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>Storm control for UC, MC and BC</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>Storm control for UC, BC and unknown</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td></td>
</tr>
<tr>
<td>Random Early Discard (RED)</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td><strong>Policers</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Port policers</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>Queue policers</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>Global/VCAP (ACL) policers</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>Port egress shaper</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>Queue egress shapers</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>DiffServ (RFC2474) remarking</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>Tag remarking</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>Supported Features (continued)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>------------------------------</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Feature</th>
<th>VSC6813</th>
<th>VSC6815</th>
<th>VSC6816</th>
<th>VSC6816-3</th>
<th>VSC6816-5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scheduler mode</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>&quot;L2 Switching&quot;</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IEEE-802.1D bridge</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Auto MAC address learning/aging</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MAC addresses – Static</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IEEE-802.1Q</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Virtual LAN</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Private VLAN – Static</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Port isolation – Static</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MAC based VLAN</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Protocol based VLAN</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IP subnet based VLAN</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>VLAN trunking</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>GARP VLAN registration – GVRP</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IEEE-802.1ad provider bridge (native or translated VLAN)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IEEE-802.1Q-2005</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Board Support Package (BSP)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Loop guard</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IEEE-802.3ad</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Link aggregation – Static</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Link aggregation – LACP</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>BPDU guard and restricted role</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>BPDU transparency/forwarding (customer specific)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Error disable recovery</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IGMPv2 snooping</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IGMPv3 snooping</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MLDv1 snooping</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MLDv2 snooping</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IGMP filtering profile</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IPMC throttling, filtering, leave proxy</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MVR</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MVR profile</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Voice VLAN</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DHCP snooping</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ARP inspection</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Port Mirroring</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Feature</td>
<td>Flow mirroring</td>
<td>Rhmirror</td>
<td>L3 Switching</td>
<td>Security</td>
<td>Stacking</td>
</tr>
<tr>
<td>--------------------------------------------------------------</td>
<td>---------------</td>
<td>----------</td>
<td>--------------</td>
<td>----------</td>
<td>----------</td>
</tr>
<tr>
<td>DHCP option 82 relay</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>UPNP</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>IPv4 Unicast: Static routing</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IPv4 Unicast: Static routing (hardware accelerated)</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IPv6 software Unicast routing</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IPv6 Unicast routing (hardware accelerated)</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Table 3 • Supported Features (continued)**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Flow mirroring</th>
<th>L3 Switching</th>
<th>Security</th>
<th>Stacking</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port-based 802.1X</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td></td>
</tr>
<tr>
<td>Single 802.1X</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td></td>
</tr>
<tr>
<td>Multiple 802.1X</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td></td>
</tr>
<tr>
<td>MAC-based authentication</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td></td>
</tr>
<tr>
<td>VLAN assignment</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td></td>
</tr>
<tr>
<td>QoS assignment</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td></td>
</tr>
<tr>
<td>Guest VLAN</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td></td>
</tr>
<tr>
<td>RADIUS authentication and authorization</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td></td>
</tr>
<tr>
<td>RADIUS accounting</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td></td>
</tr>
<tr>
<td>MAC address limit</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td></td>
</tr>
<tr>
<td>MAC freeze (customer specific)</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td></td>
</tr>
<tr>
<td>MAC spoofing (customer specific)</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td></td>
</tr>
<tr>
<td>IP MAC binding</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td></td>
</tr>
<tr>
<td>IP/MAC binding dynamic to static</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td></td>
</tr>
<tr>
<td>TACACS+ authentication and authorization</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td></td>
</tr>
<tr>
<td>TACACS+ command authorization</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td></td>
</tr>
<tr>
<td>TACACS+ accounting</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td></td>
</tr>
<tr>
<td>Web and CLI authentication</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td></td>
</tr>
<tr>
<td>Authorization (15 user levels)</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td></td>
</tr>
<tr>
<td>ACLs for filtering/policing/port copy</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td></td>
</tr>
<tr>
<td>IP source guard</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td></td>
</tr>
</tbody>
</table>

**"Stacking"**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Stacking</th>
</tr>
</thead>
<tbody>
<tr>
<td>Topology</td>
<td></td>
</tr>
<tr>
<td>Single Point of Management (SPOM)</td>
<td>•</td>
</tr>
<tr>
<td>Stacking Protocol using Routing Technology (SPROUT) – Shortest path forwarding</td>
<td>•</td>
</tr>
</tbody>
</table>
### Supported Features

<table>
<thead>
<tr>
<th>Feature</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Master reelection</td>
<td>•</td>
</tr>
<tr>
<td>Synchronization</td>
<td>•</td>
</tr>
<tr>
<td>NTPv4 Client</td>
<td>•</td>
</tr>
<tr>
<td>&quot;Robustness and Power Savings&quot;</td>
<td>•</td>
</tr>
<tr>
<td>Cold start</td>
<td>•</td>
</tr>
<tr>
<td>Cool start</td>
<td>•</td>
</tr>
</tbody>
</table>

#### Power Saving

<table>
<thead>
<tr>
<th>Feature</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>ActiPHY</td>
<td>•</td>
</tr>
<tr>
<td>PerfectReach</td>
<td>•</td>
</tr>
<tr>
<td>EEE power management</td>
<td>•</td>
</tr>
<tr>
<td>LED power management</td>
<td>•</td>
</tr>
<tr>
<td>Thermal protection</td>
<td>•</td>
</tr>
<tr>
<td>Adaptive fan control</td>
<td>•</td>
</tr>
</tbody>
</table>

#### Management

<table>
<thead>
<tr>
<th>Feature</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>JSON-RPC</td>
<td>•</td>
</tr>
<tr>
<td>JSON-RPC notifications</td>
<td>•</td>
</tr>
<tr>
<td>Stack IP address</td>
<td>•</td>
</tr>
<tr>
<td>Double VLAN tag management</td>
<td>•</td>
</tr>
<tr>
<td>DHCP client</td>
<td>•</td>
</tr>
<tr>
<td>DHCPv6 client</td>
<td>•</td>
</tr>
<tr>
<td>DHCP server</td>
<td>•</td>
</tr>
<tr>
<td>DNS client, proxy</td>
<td>•</td>
</tr>
<tr>
<td>HTTP server</td>
<td>•</td>
</tr>
<tr>
<td>Web with stack management</td>
<td>•</td>
</tr>
<tr>
<td>CLI - console port</td>
<td>•</td>
</tr>
<tr>
<td>CLI - telnet</td>
<td>•</td>
</tr>
<tr>
<td>CLI stack management</td>
<td>•</td>
</tr>
<tr>
<td>Industrial standard CLI</td>
<td>•</td>
</tr>
<tr>
<td>Industrial standard configuration</td>
<td>•</td>
</tr>
<tr>
<td>Industrial standard CLI debug commands</td>
<td>•</td>
</tr>
<tr>
<td>Management access filtering</td>
<td>•</td>
</tr>
<tr>
<td>HTTPS</td>
<td>•</td>
</tr>
<tr>
<td>SSHv2</td>
<td>•</td>
</tr>
<tr>
<td>IPv6 management</td>
<td>•</td>
</tr>
<tr>
<td>IPv6 ready logo PHASE2</td>
<td>•</td>
</tr>
<tr>
<td>RFC4884 (ICMPv6)</td>
<td>•</td>
</tr>
<tr>
<td>System syslog</td>
<td>•</td>
</tr>
</tbody>
</table>
### Table 3 • Supported Features (continued)

<table>
<thead>
<tr>
<th>Feature</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Software upload via web</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SNMP v1/v2c/v3 agent</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RMON (group 1, 2, 3, and 9)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RMON alarm and event (CLI, web)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SNMP multiple trap destinations</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IEEE-802.1AB-2005 Link Layer Discovery – LLDP</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TIA 1057 LLDP-MED</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cisco Discovery Filtering - CDP</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>sFlow</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Configuration download/upload - industrial standard</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Loop detection restore to default</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Symbolic register access</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Daylight saving</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SD/MMC card slot support</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### MIBs

| RFC 2674 VLAN MIB                                                      |   |   |   |   |   |
| RFC-802.1Q bridge MIB 2008                                            |   |   |   |   |   |
| RFC 2819 RMON (group 1, 2, 3, and 9)                                  |   |   |   |   |   |
| RFC 1213 MIB II                                                       |   |   |   |   |   |
| RFC 1215 TRAPS MIB                                                    |   |   |   |   |   |
| RFC 4188 bridge MIB                                                   |   |   |   |   |   |
| RFC 4292 IP forwarding table MIB                                      |   |   |   |   |   |
| RFC 4293 management information base for the Internet Protocol (IP)  |   |   |   |   |   |
| RFC 5519 multicast group membership discovery MIB                    |   |   |   |   |   |
| RFC 4668 RADIUS auth. client MIB                                      |   |   |   |   |   |
| RFC 4670 RADIUS accounting MIB                                        |   |   |   |   |   |
| RFC 3635 Ethernet-like MIB                                            |   |   |   |   |   |
| RFC 2863 interface group MIB using SMI v2                             |   |   |   |   |   |
| RFC 3636 802.3 MAU MIB                                                |   |   |   |   |   |
| RFC 4133 entity MIB version 3                                          |   |   |   |   |   |
| RFC 3411 SNMP management frameworks                                   |   |   |   |   |   |
| RFC 3414 user-based security model for SNMPv3                         |   |   |   |   |   |
| RFC 3415 view-based access control model for SNMP                     |   |   |   |   |   |
Table 3 • Supported Features (continued)

<table>
<thead>
<tr>
<th>RFC 2613 SMON MIB</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>RFC 2613 SMON – VLAN statistics</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>RFC 2613 SMON – PortCopy</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>IEEE 802.1 MSTP MIB</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>IEEE 802.1AB LLDP-MIB (LLDP MIB included in a clause of the STD)</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>IEEE 802.3ad (LACP MIB included in a clause of the STD)</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>IEEE 802.1X (PAE MIB included in a clause of the STD)</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>TIA 1057 LLDP-MED (MIB is part of the STD)</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>RFC 3621 LLDP-MED Power (POE) (No specific MIB for POE+ exists)</td>
<td>•</td>
<td></td>
</tr>
</tbody>
</table>

"Private MiBs"

<table>
<thead>
<tr>
<th>Private MIB framework</th>
<th>•</th>
<th>•</th>
</tr>
</thead>
<tbody>
<tr>
<td>Private MIB support</td>
<td>•</td>
<td>•</td>
</tr>
</tbody>
</table>
3 Features and Platform Capacity

The following table summarizes the features and platform capacity supported by the CE Services software. The capacity mentioned in many cases is hardware, not software, constrained.

**Table 4 • Features and Platform Capacity**

<table>
<thead>
<tr>
<th>Feature</th>
<th>SparX-III VSC7424-7</th>
<th>SparX-III VSC7414</th>
<th>E-StaX-III VSC7431/2/4</th>
<th>SparX-IV VSC7442/4/8</th>
</tr>
</thead>
<tbody>
<tr>
<td>Resilience and Availability</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IEEE 802.1s MSTP instances</td>
<td>8</td>
<td>8</td>
<td>8</td>
<td>8</td>
</tr>
<tr>
<td>IEEE 802.3ad LACP - Max LAGs</td>
<td>12</td>
<td>11</td>
<td>24 LAGs and 32 GLAGs</td>
<td>24 LAGs and 32 GLAGs</td>
</tr>
<tr>
<td>Traffic Control</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Port-based VLAN</td>
<td>4095</td>
<td>4095</td>
<td>4095</td>
<td>4095</td>
</tr>
<tr>
<td>Guest-VLAN</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Private VLAN</td>
<td>24</td>
<td>11</td>
<td>24</td>
<td>24</td>
</tr>
<tr>
<td>Voice VLAN</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>MAC table size</td>
<td>8k</td>
<td>32k</td>
<td>32k</td>
<td>32k</td>
</tr>
<tr>
<td>Storm control</td>
<td>1 – 1024 kpps in steps of $2^n$ where $n = 0..25$ (Global setting for Unicast, Multicast, and Broadcast)</td>
<td>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)</td>
<td>100 kbps – 10 Gbps (per port for Unicast (known/learned), Broadcast, and Unknown (flooded Unicast and Multicast))</td>
<td>25 kbps – 10 Gbps (per port for Unicast (known/learned), Broadcast, and Unknown (flooded Unicast and Multicast))</td>
</tr>
<tr>
<td>Jumbo frames supported</td>
<td>up to 9600</td>
<td>up to 10056</td>
<td>up to 10056</td>
<td>up to 10056</td>
</tr>
<tr>
<td>Security</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Port security aging</td>
<td>10 to 10000000s</td>
<td>10 to 10000000s</td>
<td>10 to 10000000s</td>
<td>10 to 10000000s</td>
</tr>
<tr>
<td>MAC address limit</td>
<td>1024</td>
<td>1024</td>
<td>1024</td>
<td>1024</td>
</tr>
<tr>
<td>Static MAC entries</td>
<td>64</td>
<td>64</td>
<td>64</td>
<td>64</td>
</tr>
</tbody>
</table>
### Table 4 • Features and Platform Capacity (continued)

<table>
<thead>
<tr>
<th>Feature</th>
<th>System 1</th>
<th>System 2</th>
<th>System 3</th>
<th>System 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>RADIUS authentication servers</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>TACACS+ authentication servers</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>RADIUS accounting servers</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>Telnet/SSH v2</td>
<td>4</td>
<td>4</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>Max ARP inspection</td>
<td>1K per system</td>
<td>1K per system</td>
<td>1K per system</td>
<td>1K per system</td>
</tr>
<tr>
<td>IPSG entries</td>
<td>Up to 256</td>
<td>Up to 512</td>
<td>Up to 512</td>
<td>Up to 512</td>
</tr>
<tr>
<td>Policy-based security filtering</td>
<td>512</td>
<td>512</td>
<td>512</td>
<td>512</td>
</tr>
<tr>
<td>Password length</td>
<td>32</td>
<td>32</td>
<td>32</td>
<td>32</td>
</tr>
<tr>
<td>Authorization user levels</td>
<td>15</td>
<td>15</td>
<td>15</td>
<td>15</td>
</tr>
<tr>
<td>ACE</td>
<td>256</td>
<td>512</td>
<td>512</td>
<td>512</td>
</tr>
<tr>
<td>Number of logged in users</td>
<td>20</td>
<td>20</td>
<td>20</td>
<td>20</td>
</tr>
</tbody>
</table>
4 System Requirements

SMBStaX software supports the port and hardware system requirements listed in the following tables.

**Table 5 • Port System Requirements**

<table>
<thead>
<tr>
<th>Requirement</th>
<th>SparX-III VSC7424-7</th>
<th>SparX-III VSC7414</th>
<th>E-StaX-III VSC7431/2/4</th>
<th>SparX-IV VSC7442/4/8</th>
</tr>
</thead>
<tbody>
<tr>
<td>LEDs per port</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>SFP+/SFP</td>
<td>SFP auto-detection</td>
<td>SFP auto-detection</td>
<td>SFP auto-detection / SFP+ manual</td>
<td>Both SFP/SFP+ auto-detection</td>
</tr>
<tr>
<td>Speed capability per 10/100M and Gigabit port</td>
<td>Supported</td>
<td>Supported</td>
<td>Supported</td>
<td>Supported</td>
</tr>
<tr>
<td>Duplex capability per 10/100M</td>
<td>Half/Full</td>
<td>Half/Full</td>
<td>Half/Full</td>
<td>Half/Full</td>
</tr>
<tr>
<td>Auto MDI/MDIX</td>
<td>Supported</td>
<td>Supported</td>
<td>Supported</td>
<td>Supported</td>
</tr>
<tr>
<td>Port packet forwarding rate</td>
<td>1488000 pps (1000 Mbps) (with 64 byte), 148800 pps (100 Mbps), and 14880 pps (10 Mbps)</td>
<td>1488000 pps (1000 Mbps) (with 64 byte), 148800 pps (100 Mbps), and 14880 pps (10 Mbps)</td>
<td>14880000 pps (10 Gbps), 1488000 pps (1000 Mbps) (with 64 byte), 148800 pps (100 Mbps), and 14880 pps (10 Mbps)</td>
<td></td>
</tr>
<tr>
<td>RJ45 connectors</td>
<td>Supported</td>
<td>Supported</td>
<td>Supported</td>
<td>Supported</td>
</tr>
<tr>
<td>Fiber slots</td>
<td>Supported</td>
<td>Supported</td>
<td>Supported</td>
<td>Supported</td>
</tr>
</tbody>
</table>

**Table 6 • Hardware System Requirements**

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alarm LED</td>
<td>Supported by hardware</td>
</tr>
<tr>
<td>CPU flash size</td>
<td>Supported by hardware</td>
</tr>
<tr>
<td>CPU memory type and size</td>
<td>Supported by hardware</td>
</tr>
<tr>
<td>EMC/safety requirement</td>
<td>Supported by hardware</td>
</tr>
<tr>
<td>Forwarding architecture</td>
<td>Supported by hardware</td>
</tr>
<tr>
<td>MAC address aging</td>
<td>Supported by hardware</td>
</tr>
<tr>
<td>MAC address entries</td>
<td>Supported by hardware</td>
</tr>
<tr>
<td>MAC buffer memory type and size</td>
<td>Supported by hardware</td>
</tr>
<tr>
<td>Management LED</td>
<td>Supported by hardware</td>
</tr>
<tr>
<td>Performance requirement</td>
<td>Supported by Hardware</td>
</tr>
<tr>
<td>Power LED</td>
<td>Supported by hardware</td>
</tr>
<tr>
<td>Reset button</td>
<td>Supported by hardware</td>
</tr>
<tr>
<td>Switch fabric capacity</td>
<td>Supported by hardware</td>
</tr>
</tbody>
</table>
### Table 6 • Hardware System Requirements (continued)

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>System DDR SDRAM</td>
<td>Supported by hardware</td>
</tr>
<tr>
<td>System LED</td>
<td>Supported by hardware</td>
</tr>
</tbody>
</table>
5 Port and System Functionality

SMBStaX software supports the following functionality.

5.1 Port Functionality

The ports of Caracal, Serval, and Jaguar-1 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 “Supported Features” on page 5.

Interface capabilities details can be viewed by executing the `show interface capabilities` command in the CLI interface.

5.2 System Functionality

The 8 to 48 port turnkey switch platform model switches can be supported using the SMBStaX 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 the Embedded Configurable Operating System (eCOS v3.0). The following system-wide operations are supported:

- Store-and-forward forwarding architecture.
- 8K MAC table entries on the Caracal/Serval-based switch models and 32K MAC table entries on the Jaguar-1 based switches.
- 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 Mbytes system DDR SDRAM is recommended for a typical 24 to 48 port switch.
- 16 Mbytes flash size is recommended for a typical 24 to 48 port switch.
- IP routing is supported on Jaguar-1 in hardware and is supported in software on the Caracal/Serval family.

The following table shows some of the other features across the switch family.

<table>
<thead>
<tr>
<th>Feature</th>
<th>SparX-III VSC7424-7</th>
<th>SparX-III VSC7414</th>
<th>E-StaX-III VSC7431/2/4</th>
<th>SparX-IV VSC7442/4/8</th>
</tr>
</thead>
<tbody>
<tr>
<td>Integrated shared memory</td>
<td>0.5 MB - 1 MB</td>
<td>8 Mbit</td>
<td>4 MByte</td>
<td>4 MByte</td>
</tr>
<tr>
<td>MAC table</td>
<td>8K</td>
<td>8K</td>
<td>32K</td>
<td>32K</td>
</tr>
<tr>
<td>Embedded processor</td>
<td>416 MHz</td>
<td>416 MHz</td>
<td>416 MHz</td>
<td>416 MHz</td>
</tr>
<tr>
<td>Power</td>
<td>4.5 W (8 port)</td>
<td>2.5 W (VSC741x)</td>
<td>2.5 W</td>
<td>5 W (24 port)</td>
</tr>
</tbody>
</table>
6 Firmware Upgrade

The SMBStaX firmware controlling the switch can be updated using one of the following methods.
- 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.

**Warning**  Do not restart or power off the device at this time or the switch may fail to function.
7 Port Control

SMBStaX software supports the following Port Control features.

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

7.2 PoE/PoE+ Support
The SMBStaX software provides PoE/PoE+ support on the Caracal and Serval (except VSC741x) and the Jaguar-1 and Jaguar-2 switch based solutions to comply with the IEEE802.3at and IEEE802.3af standards of enabling the supply of up to 30 W per port and up to the total power budget.

- Texas Instruments Slus787
- SiliconLabs Si3452
8 Quality of Service (QoS)

SMBStaX software provides support for the following rich Quality of Service (QoS) features.

8.1 Policing

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.

8.2 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 through 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 kbits per second or Mbits per second. The use of excess bandwidth for a queue is configurable and is disabled by default.

The software also has the QoS leaky bucket egress shapers support per queue (0-7) as well as per port.

8.3 QCL Configuration

QoS classification based on basic classification can be overruled by an intelligent classifier called QoS Control List (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.

8.4 WRED

While the random early detection (RED) settings are configurable for queues 0 to 5, weighted RED (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.

8.5 Tag Remarking

Tag remarking determines how an egress frame is edited before transmission. This includes the remarking of PCP and DEI values in tagged frames.
When adding a VLAN tag, the software allows specifying a mode where the PCP and DEI values are taken from Classified, Mapped, or Default. Classified is the default.

The QoS class DEI, DP Level to PCP, can also be mapped for QoS egress tag remarking per port when the classification is set to Mapped.

### 8.6 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

### 8.7 Queue Policers

The Queue policers are configurable per queue and are disabled by default.

### 8.8 DSCP

SMBStaX software allows disabling/enabling port DSCP remarking, which is disabled by default. Port DSCP remarking is possible for both IPv4 and IPv6.

In addition to the ingress DSCP remarking done by the analyzer, the rewriter supports egress DSCP remarking of IP (IPv4 & IPv6) frames where the actual change is made to the DSCP field in frame.

The remarking can be configured as enable/disable per egress port. It is also possible to enable/disable DSCP remapping on the egress port and to use the translated DSCP value for DSCP remarking.

DSCP remapping is disabled by default. If DSCP remarking is enabled, the new DSCP value in a transmitted frame is either from the analyzer (basic classification or advanced classification based on TCAM), or from the DSCP remapped on egress. The following configuration options are available if DSCP remapping is enabled.

1. Get the DSCP value from the analyzer (ingress classification) and always remap based on global remap table. This is done independently of the value of the drop precedence level.
2. Get DSCP value from the analyzer and remap based on drop precedence level and remap table.

DSCP remarking is not possible for frames where PTP time stamps are also generated. It is automatically disabled in such cases. It is possible to configure per DSCP (0 - 63) value for each QoS class and set the DPL. The per DSCP value parameters are configurable for DSCP translation. The software allows mapping QoS class and DPL to DSCP value on SMBStaX software.
9  L2 Switching

The SMBStaX software supports the following rich L2 switching features.

9.1  VLAN

Voice LAN (VLAN) is configured specially for voice traffic. Adding the ports with voice devices attached to VLAN to perform QoS-related configuration for voice data, ensures the transmission priority of voice traffic and voice quality. Individual options allow the port to participate in a VLAN using the port security feature. A configurable port discovery protocol will also be available to detect voice devices attached to port using the Port Discovery Protocol. This discovery can be done either based on an Organizationally Unique Identifier (OUI) or Link Layer Discovery Protocol (LLDP) or both.

SMBStaX software supports the IEEE 802.1Q standard VLANs. 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
9.1.1 Guest VLAN

A guest VLAN is a special VLAN, typically with limited network access, on which 802.1X-unaware clients are placed after a network administrator-defined timeout.

When a guest VLAN is enabled globally and on a given port, the switch considers moving the port into the guest VLAN.

This option is only available for Extensible Authentication Protocol (EAP) over LAN (EAPOL) based modes such as Port-based 802.1X, Single 802.1X, and Multi 802.1X.

9.1.2 Private VLAN

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.

The PVLAN ID is only configurable on SparX-III, SparX-IV, and E-StaX-III 24 port switches.

The private VLAN feature is unavailable on the Dual E-StaX-III and SparX-IV-based switch models.

9.1.3 MAC-based, Protocol-based, and IP Subnet-based VLAN

A MAC-based VLAN enables mapping a specific MAC address to a specific VLAN.

A Protocol-based VLAN enables mapping to a VLAN whose frame type may be one of the following.

- Ethernet - Valid values for etype ranges from 0x0600-0xffff
- SNAP - Valid value in this case also is comprised of two sub-values.
  - Organizationally Unique Identifier (OUI)
  - Protocol ID (PID): If the OUI is hexadecimal 000000, the PID is the Ethernet type (EtherType) field value for the protocol running on top of SNAP. If the OUI is an OUI for a particular organization, the PID is a value assigned by that organization to the protocol running on top of SNAP.
- LLC - Valid value in this case is comprised of two sub-values.
  - DSAP: 1-byte long string (0x00-0xff)
  - SSAP: 1-byte long string (0x00-0xff)

The precedence of these VLANs is that the MAC-based VLAN is preferred over the protocol-based VLAN, and protocol-based VLAN is preferred over port-based VLAN.

9.2 Generic VLAN Registration Protocol (GVRP)

GVRP is a method of registering on VLANs. Though this has been superseded by MVRP as described in IEEE802.1Q-2011, it is still of interest due to legacy systems with which it can interoperate.

GVRP is a method of dynamically telling a bridge port that there are devices for a particular VLAN on that port. A host can announce (register) that it wants to be part of a particular VLAN. It can de-register when it does not want to be part of a certain VLAN anymore. It then becomes the responsibility of GVRP to propagate this information in the network, so that a given VLAN gets proper connectivity.

9.3 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  The 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**  The destination MAC address can be used to calculate the destination port for the frame. By default, the destination MAC Address is disabled.

• **IP Address**  The IP address can be used to calculate the destination port for the frame. By default, the IP Address is enabled.

• **TCP/UDP Port Number**  The 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 via the Link Aggregation Control Protocol (LACP).

### 9.3.1 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.

### 9.3.2 Link Aggregation Control Protocol (LACP)

The LACP exchanges LACPDUs with an LACP partner and forms an aggregation automatically. LACP can be enabled or disabled on the switch port. 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.

### 9.4 Bridge Protocol Data Unit (BPDU) Guard

This is provided as part of the Spanning Tree Protocol (STP) configuration settings. The BPDU guard is a control that specifies whether a port explicitly configured as Edge will disable itself upon reception of a BPDU. The port will enter the error-disabled state, and will be removed from active topology.

The Common and Internal Spanning Tree (CIST) port setting for the BPDU Guard is not subject to Edge status dependency. For restricted role, CIST port setting may also be seen as a security measure.

### 9.4.1 BPDU Filtering

BPDU filtering is a control that specifies whether a port explicitly configured as Edge will transmit and receive BPDUs. This is also provided as part of the STP configuration settings.

### 9.5 DHCP Snooping

DHCP snooping is used to block intruders on the untrusted ports of the switch device when it tries to intervene by injecting a bogus DHCP (for IPv4) reply packet to a legitimate conversation between the DHCP (IPv4) client and server.

DHCP snooping is a series of techniques applied to ensure the security of an existing DHCP infrastructure. When DHCP servers allocate IP addresses to clients on the LAN, DHCP snooping can be configured on LAN switches to harden the security on the LAN to allow only clients with specific IP/MAC addresses to have access to the network.

DHCP snooping ensures IP integrity on a Layer 2 switched domain by allowing only a white-list of IP addresses to access the network. The white-list is configured at the switch port level, and the DHCP server manages access control.

Only specific IP addresses with specific MAC addresses on specific ports may access the IP network.
DHCP snooping also stops attackers from adding their own DHCP servers to the network. An attacker-controlled DHCP server could cause malfunction of the network or even control it. The port role can be set as Trusted or Untrusted in order to protect it.

### 9.6 Universal Plug and Play (UPnP)

The addressing, discovery, and description parts of UPnP-client protocol are implemented in the device. It is used to help the network administrator in managing the network. The purpose of UPnP in the device is similar to LLDP. However, UPnP is a layer-4 protocol that allows UPnP-clients to be located on a different subnet with UPnP-control points.

In the implementation, the switch sends SSDP messages periodically at the interval one-half of the advertising duration minus 30 seconds.

When the UPnP mode is enabled, two ACEs are added automatically to trap UPnP related packets to CPU. The ACEs are automatically removed when the mode is disabled.

### 9.7 Storm Control

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

On the E-StaX-III switch models, storm control is configured per port. Storm rate control configuration for unicast frames, broadcast frames, and a storm rate control configuration for unknown (flooded) frames can be configured in kbps, Mbps, fps, and kfps on the E-StaX-III-based switches.

Storm control is disabled by default.

### 9.8 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.

### 9.9 Mirroring (SPAN/VSPAN and RSPAN)

SMBStaX 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-1' 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 will have either ports or VLANs as sources, but not both.
9.10 **RMirror**

RMirror is an extension to mirror that allows for mirroring traffic from one switch to a port on another switch. RMirror is more flexible than Mirror. When a host wants to send traffic to a remote Host connected to a different switch, the first switch will copy the traffic to a dedicated RMirror VLAN, which will cause the traffic to be flooded to ports that are members of that VLAN. The administrator can use a sniffer to analyze network traffic on remote switches.

RMirror does not support BPDU monitoring, but rather supports IGMP packet monitoring when IGMP snooping is disabled on the RMirror VLAN.

All hardware error packets are discarded at the source port, so they are not copied to the destination port.

9.11 **Spanning Tree**

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

The RSTP portion of the module conforms to IEEE 802.1D-2004 and the MSTP portion of the module conforms to IEEE 802.1Q-2005.

IEEE 802.1s supports 16 instances.

The STP MSTI and CIST port configurations are allowed per physical port or aggregated port, as also STP MSTI bridge instance mapping 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.

9.12 **Unidirectional Link Detection (UDLD)**

UDLD is used to determine the link's physical status and detect a unidirectional link.

A UDLD packet is sent to the port it links to for each device and for each port. The packet contains sender's identity information (device and port), and expected receiver identity information (device and port). Each port checks that the UDLD packets it receives contain the identifiers of its own device and port.

The UDLD implementation conforms to the RFC5171.

**Note**  
RFC5171 is unclear about timers as well as messaging sequences. It is assumed that initially probe messages will be exchanged in every one second, and once link status is detected, probe messages will be exchanged depending on message time interval (by default 7 sec).

Time interval Type Length Value (TLV), Message interval TLV, and Sequence interval TLV are not fully supported due to insufficient information in this RFC.

Detection will start once the UDLD enabled port gets new device ID and port ID pair. If a port is detected as unidirectional or loopback link, the port will be shut down if mode is Aggressive. In Normal mode, the port will not be shut down.

Port will be reopened once UDLD is disabled/enabled on that port.
10 L3 Switching

SMBStaX software provides support for the following rich L3 switching features.

10.1 IP Routing

SMBStaX software static routing provides the ability to route IPv4 and IPv6 frames between different VLANs. These VLANs may exist on different ports.

It should be noted that hardware has no L3 data plane, but control plane routing is supported in software on Caracal/Serval. However, Jaguar and Jaguar 2 have the hardware support for routing. There is a provision in the software API to assign at least two router legs to a given VLAN.

When an IP interface is configured, the corresponding interface route will be installed in the routing table. In addition, the device administrator can install static routes in the routing table.

10.1.1 VLAN IP Interface Configuration

The IP stack can be configured to act either as a host or a router. The VLAN IP interface can be configured with IPv4/IPv6 parameters for assigning an IP address corresponding to a VLAN.

- **Host Mode**  Traffic between interfaces will not be routed, and auto-configuration starts automatically when each IPv6 interface starts operation (for example, triggered by link-up or creation).
- **Router Mode**  Traffic is routed between all interfaces.

10.1.2 Static IP Route Configuration

The static IPv4 route can also be configured with a valid destination IPv4/IPv6 address/mask, gateway, and a next hop VLAN. Support is available for the link-local address used as the next hop for IPv6 static routes.

10.2 ICMPv6

ICMPv6-based ping is supported on these switches. Five ICMPv6 packets are transmitted to the configured IP address, and the sequence number and roundtrip time are displayed upon reception of a reply. The ping size is set to 56 and is configurable from 1 to 1452.
11 Security

SMBStaX software supports the following security features.

11.1 802.1X 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 piggy-back 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.

Single 802.1X is not an IEEE standard, but features many of the same characteristics as port-based 802.1X. In Single 802.1X, a maximum of one supplicant can get authenticated on the port at a time. Normal EAPOL frames are used in the communication between the supplicant and the switch. If more than one supplicant is connected to a port, the one that comes first when the port's link comes up will be the first one considered. If that supplicant does not provide valid credentials within a certain amount of time, another supplicant will get a chance. Once a supplicant is successfully authenticated, only that supplicant will be allowed access. This is the most secure of all the supported modes. In this mode, the Port Security module is used to secure a supplicant's MAC address once successfully authenticated.

Multi 802.1X, like Single 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 RADIUS-assigned 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.

- Port-based 802.1X
- Single 802.1X

11.2 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, one of the following actions is taken.

- None
- Syslog
- Shutdown
- Syslog and Shutdown

The switch is configured with a total number of MAC addresses from 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.

11.3 Loop Protection

Loops inside a network are very costly because they consume resources and lower network performance. Detecting loops manually can be very 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 layer2 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 co-exist 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.

11.4 Authentication Authorization Accounting (AAA)

AAA allows the common server configuration including the Timeout, Retransmit, Secret Key, Network Access Server (NAS) IP Address, NAS IPv6 Address, NAS Identifier, and Dead Time parameters. SMBStaX software supports the configuration of the RADIUS and TACACS+ servers. SMBStaX software also supports TACACS+ authentication, authorization, and accounting from the CLI, Web, and SNMP interfaces.

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.

Dead time, which can be set to a number between 0 and 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 0 (zero) enables this feature, but only if more than one server has been configured.

Authorization is for authorizing users to access the management interfaces of the switch.

RADIUS authentication servers are used both by the NAS module and to authorize access to the switch’s management interface. The RADIUS accounting servers are only used by the NAS module.

TACACS+ is an access control network protocol for routers, network access servers, and other networked computing devices.

11.5 Secure Access

The following options are available for Secure Access.

<table>
<thead>
<tr>
<th>Table 8 • Secure Access Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Method</td>
</tr>
<tr>
<td>SSH</td>
</tr>
<tr>
<td>SSL/HTTPS</td>
</tr>
<tr>
<td>HTTPS Auto redirect</td>
</tr>
</tbody>
</table>

Note: SSL and HTTPs are not supported in the non-crypto version of the software.

11.6 Users and Privilege Levels

Multiple users can be created on the switch identified by the username and privilege level.

The privilege level of the user allowed range is 1 to 15. A privilege level value of 15 enables access to all groups and grants full control of the device. User privilege should be the same or greater than the privilege level for the group. By default, privilege level 5 provides read-only access and privilege level 10 provides read-write access for most groups. Privilege level 15 is needed for system maintenance tasks.
such as software upload and factory default restore. Generally, privilege level 15 is used for an administrator account, privilege level 10 for a standard user account, and privilege level 5 for a guest account.

The name identifying the privilege group is called the Group name. In most cases, a privilege level group consists of a single module (for example, LACP, RSTP, or QoS), but a few of them contains more than one.

Each group has an authorization privilege level configurable between 1 to 15 for the following sub-groups.

- Configuration read-only
- Configuration/execute read-write
- Status/statistics read-only
- Status/statistics read-write (for example, for clearing of statistics).

Group privilege levels are used only in the Web interface. The CLI privilege level works on each individual command. User privilege should be same or greater than the privilege level for the group.

### 11.7 Auth Method

#### 11.7.1 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 all the four management client types.

- Console
- Telnet
- 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 will enable the management client to log in using the local user database if none of the configured authentication servers are alive.

#### 11.7.2 Command Authorization Method Configuration

This configuration allows the administrator to limit the CLI commands available to the user from the different management clients, Console, Telnet, and SSH. It is possible to set the privilege level and authorize configuration commands. An authorization method can be configured either to TACACS+ or disable.

#### 11.7.3 Accounting Method Configuration

This configuration allows the administrator to configure command and Exec (login) accounting of the user from the different management clients, Console, Telnet, and SSH. It is possible to set the privilege level and enable exec (login) accounting. The accounting method can be configured either to TACACS+ or disable.

### 11.8 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 privileges 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 to assign a policy ID to an ingress port. 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.

An ACE will only apply if the frame gets past the ACE matching without getting matched. 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
- ARP
- IPv4
- IPv6

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

## 11.9 ARP Inspection/IP Source Guard

ARP Inspection is a security feature. Several types of attacks can be launched against a host or devices connected to Layer 2 networks by poisoning the ARP caches. This feature is used to block such attacks. Only valid ARP requests and responses can go through the switch device.

IP source guard is a security feature used to restrict IP traffic on DHCP snooping untrusted ports by filtering traffic based on the DHCP snooping table or manually configured IP source bindings. It helps prevent IP spoofing attacks when a host tries to spoof and use the IP address of another host.

It is possible to translate all dynamic entries to static entries for both ARP inspection and dynamic ARP inspection.
It is also possible to add a new entry to the static ARP inspection table and/or IP source guard by specifying the Port, VLAN ID, MAC address, and IP address for the new entry.
12 Stacking

SMBStaX SW has been designed to support stackable switching on the E-StaX-III-based switches. The following stacking scenarios describe some requirements used for the software architecture.

12.1 Stack Installation

The initial setup of the switch stack - that provides a plug-and-play experience - requires the following steps:

1. The E-StaX-III 24 and 48 port-based stackable switches are connected and powered on. The software automatically elects a master switch, which assigns a unique switch IDs to all switches. Within a managed stack, one master switch (or just master) must be elected. Any switch not being master is a slave switch (or just slave).
2. The master is indicated using a master LED. The user can connect to the switch preferred as master and force any other member switch to become the master.
3. The default IP address to the stack is configured as desired by the customer.

12.2 Stack Management

After installation, the stack can be managed using Web GUI on the stack IP address. The following management options are possible:

- Configuration: Setup of ports, VLANs, QoS, LAG etc. The master switch controls the configuration of all switches in the stack.
- Monitoring: State and statistics monitoring. The master switch has the state of centralized protocol state machines and may collect statistics from slave switches.
- Diagnostics: Ping and VeriPHY tools are available.
- Maintenance: Various special functions can be used for the stack:
  - Reset the stack.
  - Set factory default configuration for the stack.
  - Perform software upgrade of the stack.

12.3 Stack Split and Join

Various events may cause the stack to be split in two (or more) stacks, which will begin to operate independently. When the stack is re-established, it must resume operation using the original master. A stack split may be caused by the following events:

- One or more stack cables are disconnected.
- One or more switches are powered off.
- One or more switches are booted, for example, due to firmware upgrade.

12.4 Switch Addition - Mixed 24/48 GE Port Stacking

The stack may be extended with a switch, which has not previously been a member of the stack. For example:

- A completely new 24 or 48 port-based E-StaX-III-based stackable switch is added.
- A slave 24 or 48 port-based E-StaX-III based-stackable switch from another stack is added.
- A master 24 or 48 port-based E-StaX-III based-stackable switch from another stack is added.
All switches in the stack must have the same software version. If two neighboring switches have different software versions, then an LED on the two switches will blink to indicate the problem. Stacking connectivity will not be established between the two switches.

When a switch is added to the stack, a Switch ID is automatically assigned to the switch. The automatic SID assignment can be modified by choosing a different Switch ID on the Stack Configuration page. This method allows Switch IDs to be assigned so that it is easier for the user to remember the ID of each switch.

The Switch IDs of two switches can be swapped by simply interchanging the values in the Switch ID configuration. Changing Switch IDs does not result in any interruption of the stack operation.

To ensure that the new switch does not accidentally become the master, it must be powered on at least 30 seconds after the stack’s master is elected. Alternatively, the user may explicitly specify that the new switch cannot become master by configuring the master priority before adding it to the stack.

### 12.5 Switch Replacement

One of the switches in the stack may be replaced, for example because it has a defect. It may be one of these cases:

- The master switch is replaced.
- A slave switch is replaced.

When a switch is removed from the stack, the configuration for the switch is preserved, and the switch still appears on the Stack Configuration page. If the configuration of the switch is not to be transferred to another switch, then the configuration may be deleted by choosing Delete, followed by Save.
13 Robustness and Power Savings

The SMBStaX software supports the following features for robustness and power savings (Green Ethernet).

13.1 Robustness

13.1.1 Cold and Cool Restart
All Caracal, Serval-1, and Jaguar-1 turnkey solutions support cold restart as well as cool restart.

13.1.2 Reset Button
SMBStaX software supports the addition of a Reset button, generally accessible on the front panel of a switch. This button acts as a reset when pressed for more than 1 second. The switch automatically reboots and reloads its factory default configuration upon restart.

13.1.3 Console
SMBStaX software uses the serial console to support the CLI interface for configuration.

13.1.4 CPU Load
The system running processes and CPU load information can be viewed using the `show process load` command.

13.2 Green Ethernet

13.2.1 Energy-Efficient Ethernet (EEE) Support
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 μs for 1Gbit links and 30 μs 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 Mbit full duplex mode.

13.2.2 LED Power Reduction Support
SMBStaX software supports the LED power reduction feature.

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 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.

13.2.3 Fan Information
SMBStaX 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.

13.3 VeriPHY
VeriPHY is supported for running cable diagnostics.
14 Management

The SMBStaX software supports the following management features.

14.1 JSON-RPC

JSON-RPC is a protocol that allows making remote procedure calls. The messages exchanged in JSON-RPC are JSON encoded data structures. The JSON-RPC protocol has two roles - that of a server and a client. The client initiates the communication by sending a request to the server, and the server processes the request and sends back a response.

SMBStaX software includes a JSON-RPC server, and in order to use it, a JSON-RPC client. JSON-RPC provides a high-level interface that is the functional equivalent of CLI or SNMP with the following additional properties:

- Machine, and human friendly interface.
- Reliable connections orientated communication provided by the TCP and HTTP message encapsulation.
- RPC orientated protocol, which fits into most programming languages.
- Can be implemented in practically any language and needs only a very limited foot-print in terms of program memory and data memory.

For more information about the JSON-RPC specification, see http://json-rpc.org/. For information about the general JSON specification, see http://json.org.

For details on the software modules supported by JSON-RPC, see "Software Modules Supported by JSON-RPC" on page 51.

Note: JSON-RPC is not an end user interface intended for human interaction; it is a high level machine friendly interface. Because of this, the intended audience of this document is developers who are already familiar with the JSON-RPC technology. It is recommended that users not already familiar with JSON or JSON-RPC read the short and well written official standards.

14.1.1 JSON-RPC Notifications

JSON-RPC includes support for unsolicited notifications, that is, asynchronous events generated on the server and sent to the client. This allows the client to react on events when they happen, without the need for polling. When an event occurs, the JSON-RPC notification service takes the initiative to send a request to the configured notification receiver. In network terminology, this makes the notification receiver the server and the device that implements the notification service the client.

This means that when supporting both normal JSON-RPC service and notifications, the target acts as both a server and a client. Likewise for the user of the service, a client is used to access the normal JSON-RPC service, and a server is needed to receive the notification events.

As the current implementation uses http as the message exchange protocol, the client needs an http client to post the requests and an http server to receive the notifications. Only http (and not https) is currently supported for JSON-RPC notifications.

14.2 Management Services

SMBStaX 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.

14.2.1 Industry Standard CLI Model

The CLI interface of the SMBStaX 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. Clicking Up arrow presents the history of commands.
• 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.

14.2.1.1 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:

SMBStaX>
14.2.1.2 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: SMBStaX#

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").

```
SMBStaX# 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 0S: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.

```
SMBStaX(config)# clock summer-time PDT date 14
^%
```

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 will allow the users to obtain technical support by entering and running a debug command in this field.

14.2.2 Industry Standard Configuration Support

The SMBStaX 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.

### 14.2.3 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 SMBStaX 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:

1. Configuration of the features
2. Monitoring of the configured features using the Auto-Refresh option
3. Running supported diagnostics
4. Maintenance of the related features

### 14.3 SNMP

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

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.

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

#### 14.3.1 Multiple SNMP Trap Destinations

SMBStaX software provides SNMP configuration features with support for multiple trap destinations on SNMPv1, SNMPv2c, and SNMPv3. SNMPv2c and SNMPv3 also support Inform mode.

### 14.4 RMON Statistics

The following RMON1 statistics with corresponding configuration support is available.

- History
14.5 Internet Control Message Protocol (ICMP)

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

14.6 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. SMBStaX 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
- IP source guard table is full
- IP source guard table reaches the port limitation
- IP source guard port limitation changes, should delete entry
- Switch boot up
- SNMP authentication failure

The Syslog RAM buffer supports the display of a maximum of 21622 of the most recent entries.

14.7 LLDP-MED

It is possible to configure SMBStaX software either as a Link Layer Discovery Protocol (LLDP) end-point device or connectivity device.

The default is to act as an end-point device.

LLDP-MED is an extension of IEEE 802.1ab and is supported for the following:

- Fast Repeat Count

Rapid startup and emergency call service location identification discovery of endpoints is a critically important aspect of VoIP systems in general. In addition, it is best to advertise only those pieces of information that are specifically relevant to particular endpoint types. For example, advertise only the voice network policy to permitted voice-capable devices. This is advised in order to conserve the limited LLDPDU space and also to reduce security and system integrity issues that can come with inappropriate knowledge of the network policy.

With this in mind, LLDP-MED defines an LLDP-MED fast start interaction between the protocol and the application layers on top of the protocol to achieve these related properties. Initially, a network connectivity device will only transmit LLDP TLVs in an LLDPDU. Only after an LLDP-MED endpoint device is detected, will an LLDP-MED capable network connectivity device start to advertise LLDP-MED TLVs in outgoing LLDPDUs on the associated port. The LLDP-MED application will temporarily speed up the transmission of the LLDPDU to start within a second, when a new LLDP-MED neighbor has been detected in order to share LLDP-MED information as fast as possible with new neighbors.

Because there is a risk of an LLDP frame being lost during transmission between neighbors, it is recommended to repeat the fast start transmission multiple times to increase the possibility of the neighbors receiving the LLDP frame. With fast start repeat count, it is possible to specify the number of times the fast start transmission will be repeated. The recommended value is four times, given that four
LLDP frames with a 1 second interval will be transmitted, when an LLDP frame with new information is received.

It should be noted that LLDP-MED and the LLDP-MED fast start mechanism is only intended to run on links between LLDP-MED network connectivity devices and endpoint devices, and as such does not apply to links between LAN infrastructure elements, including network connectivity devices, or other types of links.

- Coordinates location
- Civic address location
- Emergency call service
- Network policies

Network policy discovery enables the efficient discovery and diagnosis of mismatch issues with the VLAN configuration, along with the associated Layer 2 and Layer 3 attributes, which apply for a set of specific protocol applications on that port. Improper network policy configurations are a very significant issue in VoIP environments that frequently result in voice quality degradation or loss of service. Policies are only intended for use with applications that have specific ‘real-time’ network policy requirements, such as interactive voice and/or video services. The network policy attributes advertised are as follows:

- Layer 2 VLAN ID (IEEE 802.1Q-2003)
- Layer 2 priority value (IEEE 802.1D-2004)
- Layer 3 Diffserv code point (DSCP) value (IETF RFC 2474)

This network policy is potentially advertised and associated with multiple sets of application types supported on a given port. The application types specifically addressed are as follows:

- Voice
- Guest voice
- Softphone voice
- Video conferencing
- Streaming video
- Control/Signaling (conditionally support a separate network policy for the preceding media types)

A large network may support multiple VoIP policies across the entire organization, and different policies per application type. LLDP-MED allows multiple policies to be advertised per port, each corresponding to a different application type. Different ports on the same network connectivity device may advertise different sets of policies, based on the authenticated user identity or port configuration.

It should be noted that LLDP-MED is not intended to run on links other than between network connectivity devices and endpoints, and therefore does not need to advertise the multitude of network policies that frequently run on an aggregated link interior to the LAN.

Intended uses of the application types are as follows:

- **Voice** Used by dedicated IP telephony handsets and other similar appliances supporting interactive voice services. These devices are typically deployed on a separate VLAN for ease of deployment and enhanced security by isolation from data applications.

- **Voice Signaling (conditional)** Used in network topologies that require a different policy for the voice signaling than for the voice media. This application type should not be advertised if the same network policies apply as those advertised in the Voice application policy.

- **Guest Voice** Supports a separate limited feature-set voice service for guest users and visitors with their own IP telephony handsets and other similar appliances supporting interactive voice services.

- **Guest Voice Signaling (conditional)** Used in network topologies that require a different policy for the guest voice signaling than for the guest voice media. This application type should not be advertised if the same network policies apply as those advertised in the Guest Voice application policy.

- **Softphone Voice** Used by softphone applications on typical data centric devices, such as PCs or laptops. This class of endpoints frequently does not support multiple VLANs, if at all, and are
typically configured to use an untagged VLAN or a single tagged data specific VLAN. When a network policy is defined for use with an untagged VLAN, the L2 priority field is ignored and only the DSCP value has relevance.

- **Video Conferencing** Used by dedicated video conferencing equipment and other similar appliances supporting real-time interactive video/audio services.
- **Streaming Video** Used by broadcast or multicast-based video content distribution and other similar applications supporting streaming video services that require specific network policy treatment. Video applications relying on TCP with buffering would not be an intended use of this application type.
- **Video Signaling (conditional)** Used in network topologies that require a separate policy for the video signaling than for the video media. This application type should not be advertised if the same network policies apply as those advertised in the video conferencing application policy.

### 14.8 802.1AB 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 via messages called Type Length Value (TLV) fields to neighbor devices.

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.

#### 14.8.1 CDP Awareness

CDP awareness is disabled by default. The CDP operation is restricted to decoding incoming CDP frames. The switch does not transmit CDP frames. CDP frames are only decoded if LLDP is enabled on the port.

Only CDP TLVs that can be mapped to a corresponding field in the LLDP neighbors' table are decoded. All other TLVs are discarded. Unrecognized CDP TLVs and discarded CDP frames are not shown in the LLDP statistics.

CDP TLVs are mapped onto LLDP neighbors' table as follows:

- **Device ID** is mapped to the LLDP Chassis ID field.
- **Address** is mapped to the LLDP Management Address field. The CDP address TLV can contain multiple addresses, but only the first address is shown in the LLDP neighbors' table.
- **Port ID** is mapped to the LLDP Port ID field.
- **Version and Platform** is mapped to the LLDP System Description field.
- Both the CDP and LLDP support system capabilities, but the CDP capabilities cover capabilities that are not part of the LLDP. These capabilities are shown as others in the LLDP neighbor's table.

If all ports have CDP awareness disabled, the switch forwards CDP frames received from neighbor devices. If at least one port has CDP awareness enabled all CDP frames are terminated by the switch.
When CDP awareness on a port is disabled, the CDP information is not removed immediately, but gets removed when the hold time is exceeded.

14.9 IP Management, DNS, and DHCPv4/v6

The SMBStaX 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 and/or IPv6 address.

By default, all management interfaces are available on all configured IP interfaces. If this is not desirable, then management access filtering must be configured. For more information, see "Access Control List (ACLs)" on page 34.

The IP address, IP Mask, IP Gateway, and the Next hop VLAN (in the case of IPv6 only) can be configured along with an assigned VLAN. For more information, see "VLAN IP Interface Configuration" on page 29.

The DHCP (IPv4 and/or IPv6) client can be enabled to automatically obtain an IPv4 or IPv6 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.

The Rapid-Commit option is available when a DHCPv6 client is used. If this option is enabled, the DHCPv6 client terminates the waiting process as soon as a Reply message with a Rapid Commit option is received. The IP (both v4 and v6) address of the DNS server can be provided as part of the IP configuration.

There is also an option to select the DNS proxy where the DUT relays DNS requests to the current configured DNS server on DUT, and replies as a DNS resolver to the client device on the network when enabled.

14.10 DHCP Server

DHCP provides a framework for passing configuration information to hosts on a TCP/IP network and is based on the Bootstrap protocol (BOOTP). It adds the capability of automatic allocation of reusable network addresses and additional configuration options.

DHCP consists of two components: a protocol for delivering host-specific configuration parameters from a DHCP server to a host and a mechanism for allocation of network addresses to hosts. It is a client-server model where the DHCP client is the Internet host to obtain configuration parameters such as network address. The DHCP server is the Internet host that allocates network address and returns configuration parameters to the client.

The SMBStaX software conforms to the RFC2131 implementation.
14.11 DHCP Relay

The following configuration parameters are available for configuring the DHCP relay.

Table 9 • DHCP Relay Configuration Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Allowed Range</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Relay Mode</td>
<td>Enabled/Disabled</td>
<td>Disabled</td>
</tr>
<tr>
<td>Relay Server Address</td>
<td>IP Address</td>
<td>None</td>
</tr>
<tr>
<td>Relay Information Mode</td>
<td>Enabled/Disabled</td>
<td>Disabled</td>
</tr>
<tr>
<td>Relay Information Policy</td>
<td>Replace, Keep, Drop</td>
<td>Keep</td>
</tr>
</tbody>
</table>

Relay Information mode enables or disables the DHCP option 82 operation. When DHCP Relay Information mode operation is enabled, the agent inserts specific information (option 82) into a DHCP message when forwarding to DHCP server and removes it from a DHCP message when transferring to DHCP client.

The first four characters represent the VLAN ID, the fifth and sixth characters are the module ID (in standalone device it always equals 0, in stackable device it means switch ID), and the last two characters are the port number.

14.12 Management Requirements

14.12.1 Console

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

14.12.2 System Management

The SMBSstaX 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 Telnet, SSH, SNMP, RMON, and Web interfaces from this Management VLAN. However, there is no specific service port available on the device.

14.12.3 Crash File Support

The SMBSstaX software support has a provision to capture the crash file when the system has crashed. This is stored in the Flash and can be managed using the CLI interface to support the following operations.

- List the files on the Flash using the `dir` command
- Read the file using the `more` command
- Delete the file using the `del` command
- Transfer the crash file to a remote server via TFTP using the `copy` command
14.13 **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 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.

14.14 **Thermal Protection**

Thermal protection is used to protect the chip from getting overheated. SMBStaX software supports thermal protection. This allows users to inspect and configure the current setting for controlling thermal protection.

When the temperature exceeds the configured thermal protection temperature, the ports will be turned off. It is possible to assign ports with different priorities. Each priority can be given a temperature at which the assigned ports will be turned off.

14.15 **sFlow**

sFlow is an industry standard technology for monitoring switched networks through random sampling of packets on switch ports and time-based sampling of port counters. The sampled packets and counters (referred to as flow samples and counter samples, respectively) are sent as sFlow UDP datagrams to a central network traffic monitoring server. This central server is called an sFlow receiver or sFlow collector. Additional information can be found at http://sflow.org.

14.16 **Default Configuration**

The user can also reset the configuration of the switch via Web, CLI, or SNMP. Only the IP configuration is retained after resetting to factory defaults. The new configuration is available immediately, which means that no restart is necessary.

14.17 **Configuration Upload/Download**

The switch software allows saving, viewing, or loading the switch configuration. XML configuration upload/download has been obsoleted by the industry standard configuration. For more information, see "Industry Standard Configuration Support" on page 43.

14.18 **Port Statistics**

SMBStaX software supports detailed port related statistics and system information related configuration. It is possible to view the detailed QoS related statistics using SMBStaX software.

14.19 **Network Time Protocol (NTP)**

NTP is widely used to synchronize system clocks among a set of distributed time servers and clients. NTP is disabled by default. The implemented NTP version is 4.

The NTP IPv4 or IPv6 address can be configured and a maximum of five servers are supported. Daylight saving time can also be supported to automatically adjust the Time offset.
14.20 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 will be transmitted at port 1.

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

14.21 Dual Image

SMBStaX software supports the provision for a dual software image. It also provides software image selection information for the active and alternate (backup) firmware images in the device to enable reverting to the alternate image if desired.

If the alternate image is active (as a result of corruption of the primary image or by manual intervention), uploading a new firmware image to the device will automatically use the primary image slot and activate this image.

The software image selection information includes the following:

- **Image** The flash index name of the firmware image
- **Version** The version of the firmware image
- **Date** The date where the firmware was produced

14.22 Software Modules Supported by JSON-RPC

This section lists the software modules that are supported by JSON-RPC.

14.22.1 Port Control

- Port Speed/Duplex Mode/Flow Ctrl
- Per Priority Pause
- Port Frame Size (Jumbo frames)
- Port State (administrative status)
- Port Status (link monitoring)
- Port Statistics (MIB counters)
- Port VeriPHY (cable diagnostics)
- DDMI
- UDLD

14.22.2 QoS

- Traffic Classes (8 active priorities)
- Port Default Priority
- User Priority
- Input priority mapping
- QoS Control List (QCL Mode)
- Storm Control for UC, MC and BC
- Random Early Discard (RED)
- Policers
- Port policers
- Service policing including BW profile
- Queue policers
• Global/VCAP (ACL) policers
• Queue egress shapers
• DiffServ (RFC2474) remarking
• Tag remarking
• Scheduler mode
• H-QoS
• H-QoS scheduling
• Per ASP and EVC Queuing and scheduling, (Per Service Queuing)
• H-QoS scheduling for microwave backhaul

14.22.3 L2 Switching

• IEEE-802.1D Bridge
• Auto MAC addr. Learning/Ageing
• MAC Addresses – Static
• IEEE-802.1Q
• Virtual LAN
• VLAN translation
• Private VLAN – Static
• MAC-based VLAN
• Protocol-based VLAN
• IP subnet-based VLAN
• VLAN Trunking
• GARP VLAN registration – GVRP
• IEEE-802.1ad Provider Bridge (Native or Translated VLAN)
• EVC Classification of L3 Flows (SIP, SIP, IP Prot, SPort, DPort)
• Service enabled PB [JPS]
• E-LINE (EPL, EVPL)
• MPLS/MPLS-TP
• EoMPLS LER (PWE)
• LSR
• P2MP
• MPLS-TP: E-LINE (EPL, EVPL)
• MPLS-TP: E-TREE (EP-TREE, EVP-TREE)
• MPLS-TP: E-LAN (H-VPLS, EP-LAN, EVP-LAN)
• MPLS-TP: LSR E-LINE (EPL, EVPL)
• L2CP Tunneling
• IEEE-802.1Q-2005
• BSP
• Rapid Spanning tree – RSTP, STP
• Loop Guard
• IEEE-802.3ad
• Link Aggregation – Static
• Link Aggregation – LACP
• IGMPv2 snooping
• IGMPv3 snooping
• MLDv1 snooping
• MLDv2 snooping
• IGMP filtering profile
• MVR
• DHCP snooping
• ARP inspection

14.22.4 L3 Switching
• DHCP option 82 relay
• UPNP
• IPv4 Unicast: Static routing
• IPv4 Unicast: Static routing (hardware accelerated)
• IPv6 software Unicast Routing
• IPv6 Unicast Routing (hardware accelerated)

14.22.5 Security
• RADIUS Accounting
• TACACS+
• TACACS+ Accounting
• Web & CLI Authentication
• Authorization (15 user levels)
• ACLs for filtering/policing/port copy

14.22.6 Synchronization
• 1588v2 PTP with two step clock
• 1588v2 PTP with one step clock
• Peer-to-peer transparent clock
• End-to-end transparent clock
• Boundary Clock
• Redundant masters and multiple timing domains
• ITU filtering
• PTP over IPv4
• Unicast/Multicast
• Transparent Clock over Microwave
• TC internal Master/Slave w. PDV filtering and no modulation or latency feedback from modems
• TC internal Master/Slave w. reduced PDV filtering and modem provides feedback on modulation or latency
• G.781 compliant clock selection algorithm for the platform as a PTP slave
• Combined SyncE & 1588
• 3rd Part servo algorithm integration
• NTPv4 Client

14.22.7 Robustness
• Cold start
• Cool start
14.22.8 Power Saving

- ActiPHY
- PerfectReach
- EEE Power Management
- LED Power Management
- Thermal Protection
- Adaptive Fan Control

14.22.9 Management

- DHCP Client
- DHCPv6 Client
- DHCP Server
- DNS client, proxy
- Industrial Standard Configuration
- Management access filtering
- HTTPS
- SSHv2
- System Syslog
- IEEE802.1AB-2005 Link Layer Discovery – LLDP
- TIA 1057 LLDP-MED
- Configuration Download/Upload - Industrial Standard
- Daylight Saving
SMBStaX supports the following comprehensive set of private and standard MIBs.

SNMPv3 is supported and is backward compatible with SNMPv2c and SNMP v1. The MIB information can be viewed with the Community name configured. For more information, see "SNMP" on page 44.

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 (.1.3.6.1.2.1.47.1)
IEEE8021-BRIDGE-MIB :
  # show snmp mib ifmib ifIndex
```

<table>
<thead>
<tr>
<th>ifIndex</th>
<th>ifDescr</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>VLAN 1</td>
<td>vlan 1</td>
</tr>
<tr>
<td>1000001</td>
<td>Switch 1 - Port 1</td>
<td>GigabitEthernet 1/1</td>
</tr>
<tr>
<td>1000002</td>
<td>Switch 1 - Port 2</td>
<td>GigabitEthernet 1/2</td>
</tr>
<tr>
<td>1000003</td>
<td>Switch 1 - Port 3</td>
<td>GigabitEthernet 1/3</td>
</tr>
<tr>
<td>1000004</td>
<td>Switch 1 - Port 4</td>
<td>GigabitEthernet 1/4</td>
</tr>
<tr>
<td>1000005</td>
<td>Switch 1 - Port 5</td>
<td>GigabitEthernet 1/5</td>
</tr>
<tr>
<td>1000006</td>
<td>Switch 1 - Port 6</td>
<td>GigabitEthernet 1/6</td>
</tr>
<tr>
<td>1000007</td>
<td>Switch 1 - Port 7</td>
<td>GigabitEthernet 1/7</td>
</tr>
<tr>
<td>1000008</td>
<td>Switch 1 - Port 8</td>
<td>GigabitEthernet 1/8</td>
</tr>
<tr>
<td>1000009</td>
<td>Switch 1 - Port 9</td>
<td>2.5GigabitEthernet 1/1</td>
</tr>
<tr>
<td>1000010</td>
<td>Switch 1 - Port 10</td>
<td>2.5GigabitEthernet 1/2</td>
</tr>
<tr>
<td>1000011</td>
<td>Switch 1 - Port 11</td>
<td>GigabitEthernet 1/9</td>
</tr>
</tbody>
</table>

15.1 Private MIBs

The following private MIBs are supported.

- VTSS-ACCESS-MANAGEMENT-MIB
- VTSS-ACL-MIB
- VTSS-AGGR-MIB
- VTSS-ARP-INSPECTION-MIB
- VTSS-AUTH-MIB
- VTSS-DAYLIGHT-SAVING-MIB
SNMP MIBs

- VTSS-DDMI-MIB
- VTSS-DHCP-RELAY-MIB
- VTSS-DHCP-SERVER-MIB
- VTSS-DHCP-SNOOPING-MIB
- VTSS-DHCP6-CLIENT-MIB
- VTSS-DNS-MIB
- VTSS-EEE-MIB
- VTSS-FAN-MIB
- VTSS-FIRMWARE-MIB
- VTSS-HTTPS-MIB
- VTSS-ICFG-MIB
- VTSS-IP-MIB
- VTSS-IPMC-MVR-MIB
- VTSS-IPMC-PROFILE-MIB
- VTSS-IPMC-SNOOPING-MIB
- VTSS-LACP-MIB
- VTSS-LED-POWER-REDUCTION-MIB
- VTSS-LLDPMED-MIB
- VTSS-LOOP-PROTECTION-MIB
- VTSS-MAC-MIB
- VTSS-MSTP-MIB
- VTSS-NTP-MIB
- VTSS-PORT-MIB
- VTSS-PORT-POWER-SAVINGS-MIB
- VTSS-PRIVILEGE-MIB
- VTSS-PVLAN-MIB
- VTSS-QOS-MIB
- VTSS-RMIRROR-MIB
- VTSS-SMI
- VTSS-SNTP-MIB
- VTSS-SSH-MIB
- VTSS-SYSLOG-MIB
- VTSS-SYSUTIL-MIB
- VTSS-TC
- VTSS-THERMAL-PROTECTION-MIB
- VTSS-UDLD-MIB
- VTSS-UPNP-MIB
- VTSS-USERS-MIB
- VTSS-VCL-MIB
- VTSS-VLAN-MIB

15.2 Standard MIBs

The following standard MIBs are supported.

- BRIDGE-MIB
- DIFFSERV-DSCP-TC
• ENTITY-MIB
• EtherLike-MIB
• IANA-ADDRESS-FAMILY-NUMBERS-MIB
• IANAifType-MIB
• IEEE8021-MSTP-MIB
• IEEE8021-PAE-MIB
• IEEE8021-Q-BRIDGE-MIB
• IEEE8021-TC-MIB
• IEEE8023-LAG-MIB
• IF-MIB
• IGMP-STD-MIB
• INET-ADDRESS-MIB
• IP-FORWARD-MIB
• IP-MIB
• IPATM-IPMC-MIB
• LLDP-EXT-MED-MIB
• LLDP-MIB
• MAU-MIB
• MGMD-MIB
• POWER-ETHERNET-MIB
• Q-BRIDGE-MIB
• RADIUS-ACC-CLIENT-MIB
• RADIUS-AUTH-CLIENT-MIB
• RFC1213-MIB
• RMON-MIB
• RMON2-MIB
• SFLOW-MIB
• SMON-MIB
• SNMP-FRAMEWORK-MIB
• SNMP-MPD-MIB
• SNMP-USER-BASED-SM-MIB
• SNMP-VIEW-BASED-ACM-MIB
• SNMPv2-CONF
• SNMPv2-MIB
• SNMPv2-PDU
• SNMPv2-SMI
• SNMPv2-TC
16 List of Changes

The following changes were implemented in this document. The changes are listed by revision, starting with the most current publication.

<table>
<thead>
<tr>
<th>Date</th>
<th>Revision</th>
<th>Changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>July 2015</td>
<td>1.0</td>
<td>This was the first publication of the document. All examples and descriptions are valid for the API release version 4.64m.</td>
</tr>
</tbody>
</table>
Microsemi Corporation (Nasdaq: MSCC) offers a comprehensive portfolio of semiconductor and system solutions for communications, defense & security, aerospace and industrial markets. Products include high-performance and radiation-hardened analog mixed-signal integrated circuits, FPGAs, SoCs and ASICs; power management products; timing and synchronization devices and precise time solutions, setting the world's standard for time; voice processing devices; RF solutions; discrete components; security technologies and scalable anti-tamper products; Ethernet solutions; Power-over-Ethernet ICs and midspans; as well as custom design capabilities and services. Microsemi is headquartered in Aliso Viejo, Calif., and has approximately 3,600 employees globally. Learn more at www.microsemi.com.