MANAGED SWITCH
SOFTWARE MONITORING

CHAPTER
3

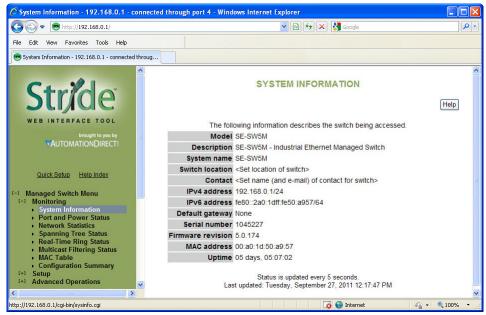## In This Chapter...

System Information

The System Information screen simply provides the information shown below. The screen is updated every five seconds.

Model: This field shows the model number of this particular switch. It is set by the factory and cannot be changed.

Description: This field displays more descriptive information about this particular switch model. It is also set by the factory and is not changeable. This data is available via SNMP as SYSTEM.SYSDESCR.0.

System Name: This field is configured by the user with the appropriate text for their application. It is configured in the "System Settings" tab under the Main Settings section. This field is also used as the hostname of the switch and, therefore, must contain only digits, dashes and letters. It is also available via SNMP as SYSTEM.SYSNAME.0.

Switch Location: This field is configured by the user with the appropriate text for their application. It is configured in the "System Settings" tab under the Main Settings section. This data is available via SNMP as SYSTEM.SYSLOCATION.0.

Contact: This field is configured by the user with the appropriate text for their application. It is configured in the "System Settings" tab under the Main Settings section. This data is available via SNMP as SYSTEM.SYSCONTACT.0.

IPv4 address: This field displays the current configured IPv4 address. IPv4 is the traditional 4 octet Internet Protocol address. An IPv4 address comprises 4 8-bit numbers separated by a period. Each number can be between 0 and 255 (some of the fields have more strict

limitations). The IPv4 address can be manually configured in the "System Settings" tab under the Main Settings section or the address can be set to be automatically retrieved using the DHCP protocol. If the address has been configured via DHCP, it will indicate this. This field also indicates the Subnet Mask by using the 'slash' notation that indicates the number of bits that are 1 in the mask. For example: A Subnet Mask of 255.255.0.0 would be indicated by a /16. A Subnet Mask of 255.255.255.0 would be indicated by a /24 and so on. The subnet mask is accessible via SNMP as RFC1213-MIB::IPADENT-NETMASK.<IPADDRESS> where <IPADDRESS> is the IP address of the switch (example: 192.168.0.1).

IPv6 address: This field displays the current configured IPv6 address. IPv6 is the newer standard of Internet Protocol addressing that greatly expands the number of addressing possibilities. Instead of the standard 4 x 8-bit address format that is used IPv4, IPv6 uses 8 fields of 16 bit values separated by colons. Each address display in hex format. If one particular fields contains a 0, a :: can be used. An IPv6 address can also be retrieved by DHCP. This field also uses the / designator for the subnet mask.

Default Gateway: This field contains the IP address of the router that this switch should send external packets to. This address can be assigned manually in the "System Settings" tab under the Main Settings section or can be retrieved automatically through DHCP. The default gateway is accessible via SNMP as RFC1213-MIB::IPROUTENEXTHOP.

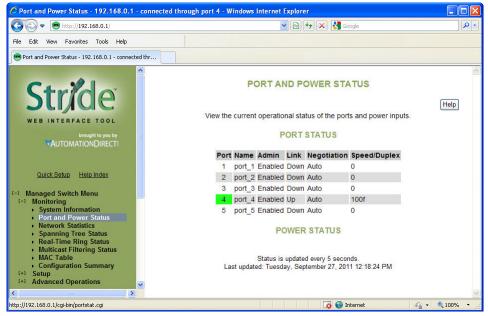**Serial Number:** This is the serial number assigned to this switch at the factory and cannot be changed.

Firmware revision: This is the current running firmware revision of this switch.

MAC address: This is the MAC address of this switch. It is configured at the factory and cannot be changed.

Uptime: This is the amount of time this switch has been running since power was applied. This data is available via SNMP as SYSTEM.SYSUPTIME.0.

Port and Power Status

The current status of each port and the Power and Ok terminal status can be viewed in this section.

Port Status: The status for each port can be viewed in this section. Some of the information shown for the ports is configured through the "Port Settings" tab of the Main Settings section. If the negotiation settings have been set to Auto, this tab will show what settings were negotiated between the switch and the attached device. On this page, the color highlighting the port number indicates the speed:

<div align="center">

Yellow = 10 Mbps

Green = 100 Mbps

Red = 1000 Mbps

</div>

Power Status: There are 2 power input terminals for the input 24VDC. This tab will show which terminals have power. This tab will also show if the criteria for enabling the OK output is true or false. The configuration for this output is configured in the "Alarm (OK) Output" tab of the Monitoring Settings section.

Network Statistics

The Network Statistics display can be a very useful diagnostic tool for indication of the type of traffic and packets that the switch is receiving.

RMON Statistics: RMON stands for "Remote Monitoring" statistics and includes the following:

- **Drop Events** = The number of packets that have been dropped by the switch because of a lack of resources and/or large queues.

- **Octets** = The number of data 8-bit units received into this port.

- **Packets** = The number of Ethernet packets received into this port.

- **Broadcast packets** = The number of broadcast packets received into this port.

- **Multicast packets** = The number of multicast packets received into this port.

- **CRC Align errors** = The number of Ethernet packets received into this port with an invalid CRC.

- **Undersize packets** = The number of Ethernet packets received into this port that were less than 64 bytes in size but contained a valid CRC (64 bytes is the minimum required in Ethernet).

- **Oversize packets** = The number of Ethernet packets received into this port that were greater than 1536 bytes in size but contained a valid CRC (1536 is the maximum size allowed in Ethernet).

- **Fragments** = The number of Ethernet packets received into this port that were less than 64 bytes in size and did not contain a valid CRC.

- **Jabbers** = The number of Ethernet packets received into this port that were greater than 1536 bytes in size and did not contain a valid CRC.

- **Collisions** = The number of collisions detected on this port.

- **64-octet Packets** = The number of Ethernet packets received into this port that were 64 bytes in length.

- **65 – 127-octet Packets** = The number of Ethernet packets received into this port that were between 65 and 127 bytes in length.

- **128 – 255-octet Packets** = The number of Ethernet packets received into this port that were between 128 and 255 bytes in length.

- **256 – 511-octet Packets** = The number of Ethernet packets received into this port that were between 256 and 511 bytes in length.

- **512 – 1023-octet Packets** = The number of Ethernet packets received into this port that were between 512 and 1023 bytes in length.

- **1024 – 1518-octet Packets** = The number of Ethernet packets received into this port that were between 1024 and 1518 bytes in length.

NETWORK STATISTICS

[Help]

Monitor the various counters and problem indicators maintained by the switch.

Port [port_1 ▾] **Statistics** [Ether-like statistics ▾]

#	Stat	Current	Change
1	Alignment Errors	0	0
2	FCS Errors	0	0
3	Single Collision Frames	0	0
4	Multiple Collision Frames	0	0
5	SQE Test Errors	0	0
6	Deferred Transmissions	0	0
7	Late Collisions	0	0
8	Excessive Collisions	0	0
9	Internal Mac Transmit Errors	0	0
10	Carrier Sense Errors	0	0
11	Frame Too Longs	0	0
12	Internal Mac Receive Errors	0	0
13	Symbol Errors	0	0

Status is updated every 5 seconds.
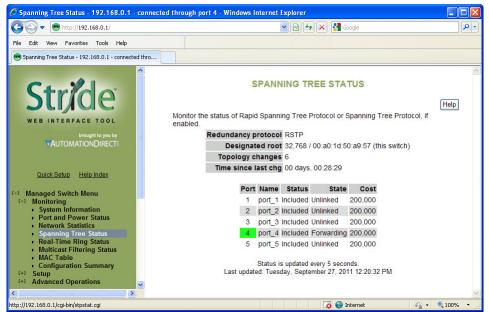Last updated: Tuesday, September 27, 2011 11:38:04 AM

Ether-like statistics: The Ether-like statistics provide information on possible hardware, electrical and/or noise problems on the network.

- **Alignment Errors** = These errors are more indicative of receiving the improper number of bits. These errors are a good indication of noise and/or electrical problems. Check the wiring and routing of cables in the event that many of these errors are seen.

- **FCS Errors** = This is the error that results from an incorrect CRC calculation. These errors along with the Alignment Errors indicate noise and/or electrical problems. Check the wiring and routing of cables in the event that many of these errors are seen.

- **Single Collision Frames** = This error occurs when only 1 collision occurs and the sending device is able to send the packet on the subsequent attempt.

- **Multiple Collision Frames** = This error occurs when collisions occur on more than 1 attempt to send a packet from a device.

- **SQE Test Errors** = The Signal Quality Error test verifies that the collision detection circuit is working correctly. If the device does not detect the SQE test, this causes an error.

- **Deferred Transmissions** = A deferred transmission occurs when the device detects a carrier signal (a device is already transmitting).

- **Late Collisions** = In some situations, a collision is not detected until after the Ethernet device has started transmitting the packet. This is called a Late Collision. A Late Collision is more specifically defined as a collision that is detected 51.2 microseconds after the device has started sending on a 10BASE-T network and 5.12 microseconds on a 100BASE-T network. Late collisions are usually caused by improper network configurations, compliance issues between devices, incorrect cabling and/or fault Network Interface Cards.

- **Excessive Collisions** = As part of the CSMA/CD mechanism, an Ethernet device will attempt to re-transmit a frame 16 times if a collision is detected. If the device is unsuccessful after 16 times, it will give up and that frame will not be transmitted.

- **Internal MAC Transmit Errors** = This error occurs when frames fail to be transmitted correctly due to an internal MAC sub-layer transmit error.

- **Carrier Sense Errors** = This error occurs when the carrier sense is lost during a transmission from the Ethernet device. The error only increments once during the transmission even if the carrier sense is lost and regained multiple times during that transmission.

- **Frame Too Long** = This error occurs when a frame is encountered that exceeds the maximum frame size.

- **Internal MAC Receive Errors** = This error occurs when frames fail to be received correctly due to an internal MAC sub-layer receive error.

- **Symbol Errors** = These errors occur when the device could not correctly decode a symbol that has been received. This is usually indicative of bad cabling and/or electrical noise problems. A symbol is a waveform change on the wire that may contain 1 or many bits of information.

Spanning Tree Status

This section shows the current status of the Spanning Tree redundancy feature of the switch. For more information on the particular details of the Spanning Tree features of the switch, refer to the "Spanning Tree Settings" section under the "Redundancy Settings" section of this document.

On this page, the color highlighting the port number indicates the speed:

Yellow = 10 Mbps

Green = 100 Mbps

Red = 1000 Mbps

Redundancy protocol: This is the protocol that the switch has been configured for. The selections available are Spanning Tree Protocol, Rapid Spanning Tree Protocol or None.

Designated root: This field specifies which device is the Root switch and what the Bridge ID of that switch is along with the MAC ID.

Topology changes: This counter tracks the number of times that the topology has changed on the network layout. There are a number of things that can cause the topology to change. If the link is lost on a port that is forwarding and the switch has to change its path, this will cause a topology change. If a Topology Change Notice is received by the switch from some other switch, the counter will also increment.

Time since last chg: Informs how long it has been since the last topology change occurred.

Port: The number of the port. This corresponds to the labels on the switch.

Name: The user configured name of the port.

Status: The configured state of the port in the STP protocol (included or excluded). An included port is part of the managed network. An excluded port will not be used as part of the managed network. For example, a single uplink from a managed network of factory devices to a business network would be configured to be excluded from STP use. A pair of ports configured for Real-Time Ring should be excluded from Spanning Tree.

State: The STP/RSTP state of the port:

STP:

- **Blocking** = A port in this state does not participate in frame relay (pass frames received to other locations). Once a port is in this state, it prevents frame duplication caused by multiple paths in an active topology.

- **Listening** = A port in this state is about to participate in frame relay, but is not involved in any relay of frames (no frames will be forwarded). The reason for not entering frame relay immediately is to ensure that there are no temporary loops introduced when the network topology is changing. During this state, the switch will disable all learning states on its ports to prevent the race conditions when ports are changing roles and the forwarding process will discard all frames and not submit any frames for transmission. Meanwhile BPDUs (Configuration Messages - Bridge Protocol Data Units) can still be received and forwarded to keep the algorithm running.

- **Learning** = A port in this state is about to participate in frame relay, but it is not involved in any relay of frames. Frame relays are not performed to prevent the creation of temporary loops during the active topology of a changing bridged LAN. In addition, the forwarding process will discard all frames and not submit any frames for transmission. The reason for enabling learning is to acquire information prior to any frame relay activities. Information gathered will be used and placed in the filtering database (MAC table) to reduce the number of frames being unnecessarily relayed.

- **Forwarding** = A port in the forwarding state is currently participating in frame relay. BPDUs will include the forwarding port in the computation of the active topology. BPDUs received are processed according to the Spanning Tree algorithm and transmitted based on the hello time or BPDU information received.
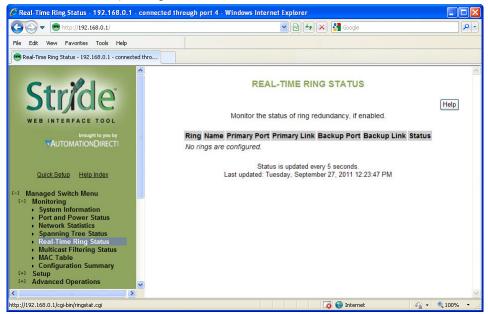
RSTP:

- **Discarding** = In this state, station location information is not added to the Filtering Database (MAC table) because any changes in port role will make the Filtering Database information inaccurate.

- **Learning** = In this state, information is being added to the Filtering Database under the assumption that the port role is not changing. Gathering information before frame relay (forwarding state) will reduce the number of frames sent out when entering the forwarding state.

- **Forwarding** = Frames will be forwarded to and from the particular port that is in the forwarding state. In addition, during the forwarding state, the learning process is still incorporating station information into the Filtering database.

Cost: The cost of using this port to reach other parts of the managed network. The cost is used in calculating the best path from the switch to the root bridge. The lower the cost, the more likely that the path will be used. See the configuration section for Spanning Tree settings for more detail.

Real-Time Ring Status

Each ring that is configured is assigned a number and can be given a name. For more information on the Real-Time Ring feature, refer to the "Real-Time Ring Settings" section under the "Redundancy Settings" section of this document.
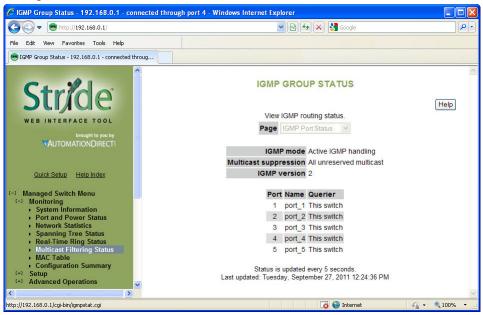

On this page, green hightlight on the ring number indicates the ring is complete, red indicates the ring is broken. On the Port, green indicates both ends of the link are connected and communicating. Red indicates on side of the link is not connected or communicating. For each ring configured a Primary port is assigned and a Backup port (if the Primary port is disrupted). The Ring Status page shows the status of the Primary port, its Link status, the status of the Backup port and its Link status.

The Status field indicates whether the Ring is complete or if there is a break in the Ring. If the Ring is broken at the switch being monitored, it will indicate "Local". If the Ring is broken at another switch, it will indicate "Remote".

Multicast Filtering Status

This section shows the current IGMP Multicast Filtering Status. For more information on the particular details of the Multicast Filtering features of the switch, refer to the "Multicast Filtering (IGMP)" section of this document.

IGMP Port Status:

- **IGMP mode:** Displays the configured mode of IGMP handling. The three choices are: IGMP disabled, Passive IGMP handling and Active IGMP handling. The specific details of each mode are discussed in more detail in the "Multicast Filtering (IGMP)" configuration section.

- **Multicast suppression:** Displays the configured mode of Multicast suppression. The three choices are: None, IP multicast groups and All unreserved multicast. The specific details of each mode are discussed in more detail in the "Multicast Filtering (IGMP)" configuration section.

- **IGMP version:** Displays the configured version of IGMP for this switch. The choices are Version 1 or Version 2. The specific details of these versions are discussed in more detail in the "Multicast Filtering (IGMP)" configuration section.

- **Querier**: Indicates what device is sending out IGMP query messages. When the switch is set to "Active IGMP handling", the Querier will most often be this same switch.
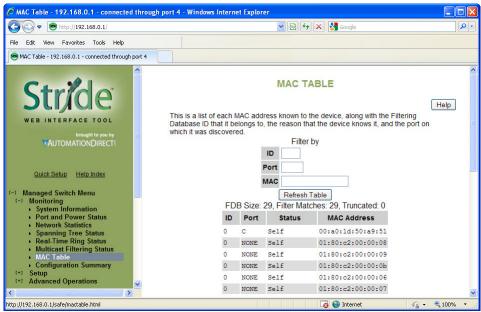
IGMP Group Status:

- **Group:** Displays the Multicast IP address of a particular multicast group.

- **Port:** Displays the port that the particular multicast group is active on.

- **Reporter:** Displays the IP address of the last host to report membership in this group on this port. Hosts send IGMP reports to a switch or router for the purpose of having the switch or router include them into a particular multicast group.

- **Age:** The number of seconds since this group was last reported on this port.

- **Expiration:** The number of seconds until this group will be dropped unless a new report is received.
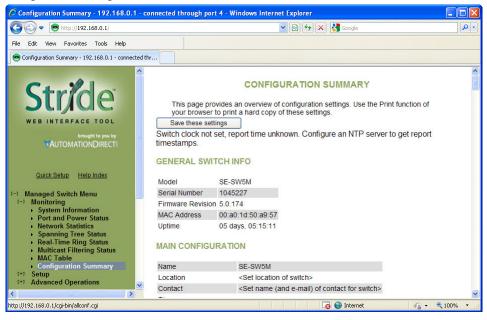
MAC Table

The MAC address table page displays the current MAC address table of the switch. This data can be filtered by the Filter Database ID (FID: Values that are applied as the devices are encountered, no other significance to the value), the port(s) of discovery or by all or part of the MAC address. Please note that Port 33 or 65 is the internal CPU port, depending upon the model.

Entries in the MAC table will time out after 300 seconds of inactivity. Alternatively, the MAC table can be flushed by power cycling the switch.

Configuration Summary

The Configuration Summary Page provides a complete overview of the configuration settings of the switch. The summary is generated in a print-friendly format. If an NTP (Network Time Protocol) server is configured, the report will also report a timestamp. To save these settings to a configuration file, click the "Save these settings" button to be redirected to the Configuration Management screen.

NOTE: *This page is for viewing settings only. To change settings, please go to the individual configuration screens.*