APPENDIX A

TROUBLESHOOTING

In This Appendix...

Troubleshooting Fiber Connections: A–2

Troubleshooting Real-Time Ring A–4

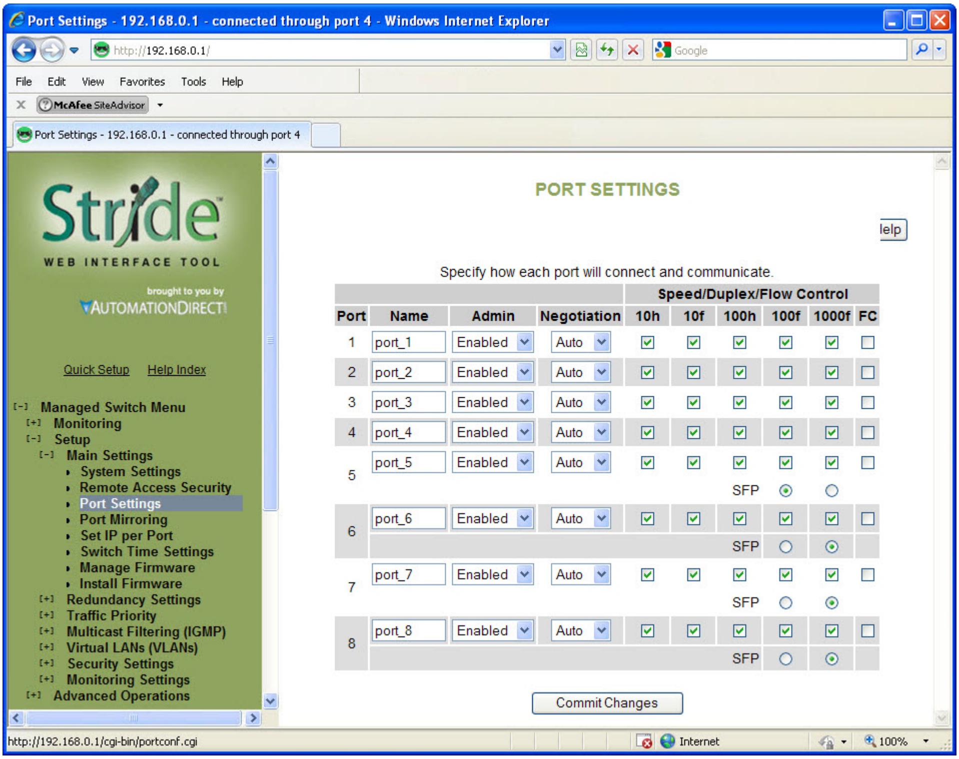
Troubleshooting VLANs A–6

Installing Switch Firmware A–8

Troubleshooting Fiber Connections:

1. If you are using a 100Mbps SFP in a Stride switch, you must manually change the port speed on the Port Settings page of the Switch Setup interface. Note that if matching 100Mbps SFPs are installed and connected by a proper mode-type patch cable but the Port Setting has not been changed from the default 1000Mbps (Gigabit speed), the Port Status and RSTP Port Status pages will not indicate the port speed mismatch. That is, the browser interface will not alert the user to this speed mismatch.

- Verify the type of SFP.
- Verify the port number.
- Verify the Port Speed Setting on the Main Settings – Port Settings page:



Specify how each port will connect and communicate.

				Speed/Duplex/Flow Control					
Port	Name	Admin	Negotiation	10h	10f	100h	100f	1000f	FC
1	port_1	Enabled	Auto	☑	☑	☑	☑	☑	□
2	port_2	Enabled	Auto	☑	☑	☑	☑	☑	□
3	port_3	Enabled	Auto	☑	☑	☑	☑	☑	□
4	port_4	Enabled	Auto	☑	☑	☑	☑	☑	□
5	port_5	Enabled	Auto	☑	☑	☑	☑	☑	□
						SFP	●	○	
6	port_6	Enabled	Auto	☑	☑	☑	☑	☑	□
						SFP	○	●	
7	port_7	Enabled	Auto	☑	☑	☑	☑	☑	□
						SFP	○	●	
8	port_8	Enabled	Auto	☑	☑	☑	☑	☑	□
						SFP	○	●	

2. Make sure that the speeds of both ends of a link match: a 100Mbps SFP on one switch must connect to a 100Mbps connection on the other switch or end device. Fiber ports do not negotiate speed.

3. Ensure that the cable type you are using matches the transceiver type. That is, Multimode cable requires Multimode transceivers, and Single-mode cable requires Single-mode transceivers.

4. Additionally, it is important that 62.5um is used with 62.5um and 50um used with 50um.

If the fiber cores are not aligned correctly significant attenuation will occur.

5. Make sure that all of your connectors are clean. Even a little bit of dust, dirt or grease on a connector face can significantly degrade a fiber signal. This includes the main fiber optic link as well as any patch cables that you may be using. When cleaning, it is important to use lint-free swabs or wipes, preferably of a clean room quality. These can be used dry or wet (with 99% isopropyl alcohol solutions).

- Make certain that you are not cleaning an active fiber, as the laser can cause permanent damage to your eyes should you look into the end face.
- Additionally, it is not necessary to scrub the end face, rather to just gently wipe it clean and then double-check the link. If additional cleaning is required simply repeat this process.

6. Make sure that all connectors are plugged completely into their proper ports. Again, if end faces are not lined up correctly with transceivers and/or mated fiber ends, the system may fail due to excess attenuation.

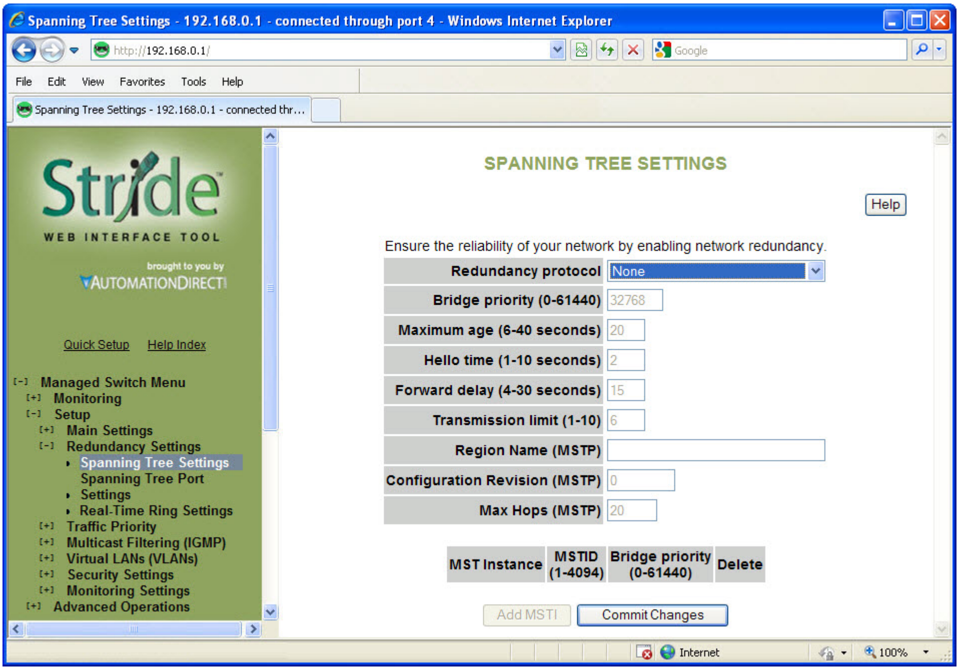
7. Make sure that the transmit cable at the near end is the receive cable at the far end. There needs to be a crossover for a fiber link to work correctly. Be sure to factor in all patch cords that may be used.

NOTE: *The physical connectors on the ends of a fiber cable do NOT need to match: a link may use an LC connector on one end and an SC connector on the other end.*

Troubleshooting Real-Time Ring

1. Typically a switch will be protected by either Real-Time Ring or RSTP. If Real-Time Ring is configured on a switch, disable RSTP.

- On the Redundancy Settings – Spanning Tree Settings page, set Redundancy protocol to "None"



SPANNING TREE SETTINGS

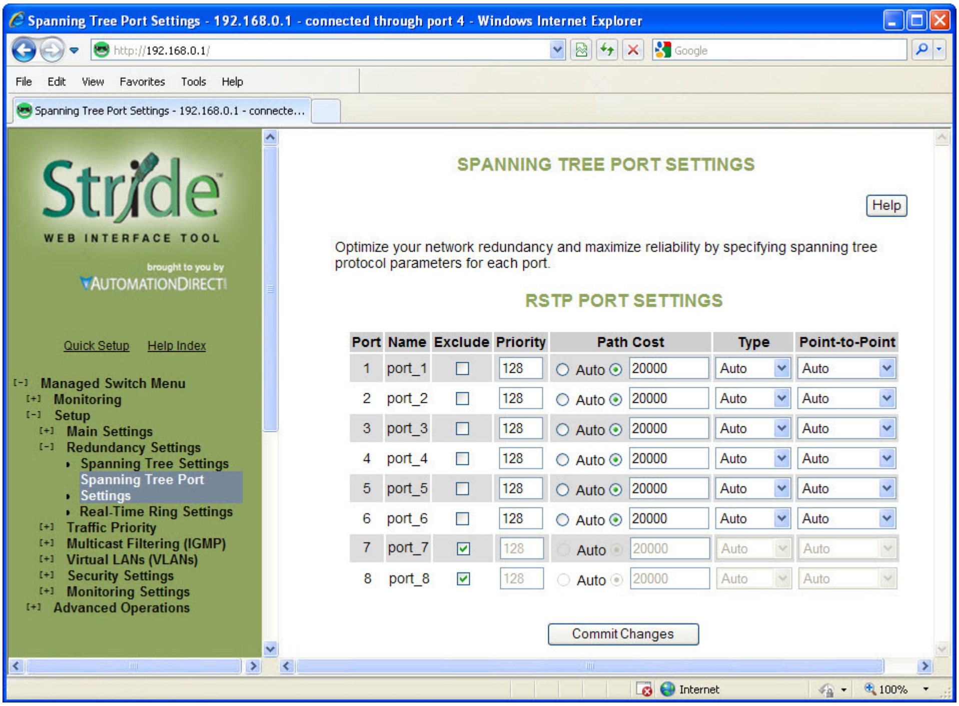
Ensure the reliability of your network by enabling network redundancy.

Redundancy protocol	None
Bridge priority (0-61440)	32768
Maximum age (6-40 seconds)	20
Hello time (1-10 seconds)	2
Forward delay (4-30 seconds)	15
Transmission limit (1-10)	6
Region Name (MSTP)	
Configuration Revision (MSTP)	0
Max Hops (MSTP)	20

MST Instance	MSTID (1-4094)	Bridge priority (0-61440)	Delete

2. It is possible for Real-Time Ring and RSTP to coexist on a switch. If a switch participates in both a Real-Time Ring and a spanning tree, exclude the Real-Time Ring ports from spanning tree:

- On the Redundancy Settings – Spanning Tree Port Settings page, check the boxes to exclude the Real-Time Ring ports from Spanning Tree



SPANNING TREE PORT SETTINGS

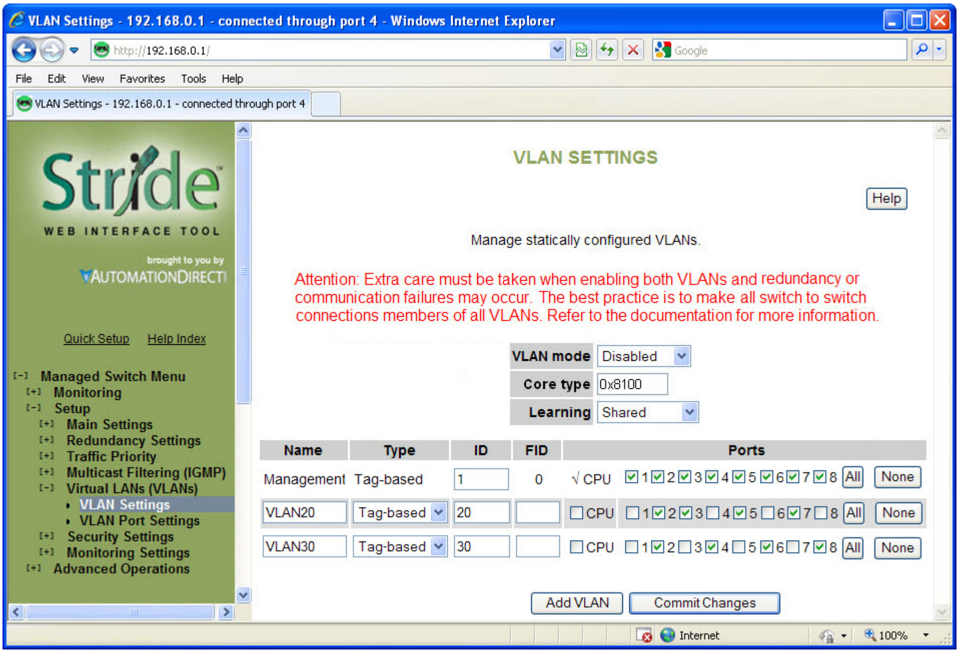
Optimize your network redundancy and maximize reliability by specifying spanning tree protocol parameters for each port.

RSTP PORT SETTINGS

Port	Name	Exclude	Priority	Path Cost	Type	Point-to-Point
1	port_1	□	128	○ Auto ● 20000	Auto	Auto
2	port_2	□	128	○ Auto ● 20000	Auto	Auto
3	port_3	□	128	○ Auto ● 20000	Auto	Auto
4	port_4	□	128	○ Auto ● 20000	Auto	Auto
5	port_5	□	128	○ Auto ● 20000	Auto	Auto
6	port_6	□	128	○ Auto ● 20000	Auto	Auto
7	port_7	☑	128	○ Auto ● 20000	Auto	Auto
8	port_8	☑	128	○ Auto ● 20000	Auto	Auto

Troubleshooting VLANs

The most common VLAN is the Tag-based VLAN. A typical tag-based VLAN implementation requires configuring the VLANs on the VLAN Settings page AND configuring the ports for each VLAN on the VLAN Port Settings page:



VLAN SETTINGS

Manage statically configured VLANs.

Attention: Extra care must be taken when enabling both VLANs and redundancy or communication failures may occur. The best practice is to make all switch to switch connections members of all VLANs. Refer to the documentation for more information.

VLAN mode	Disabled
Core type	0x8100
Learning	Shared

Name	Type	ID	FID	Ports
Management	Tag-based	1	0	√ CPU ☑1 ☑2 ☑3 ☑4 ☑5 ☑6 ☑7 ☑8 All None
VLAN20	Tag-based	20		□CPU □1 ☑2 ☑3 □4 ☑5 □6 ☑7 □8 All None
VLAN30	Tag-based	30		□CPU □1 ☑2 □3 ☑4 □5 ☑6 □7 ☑8 All None

For a Tag-based VLAN (commonly referred to as an 802.1q or a Dot 1q VLAN)

On the VLAN Settings page:

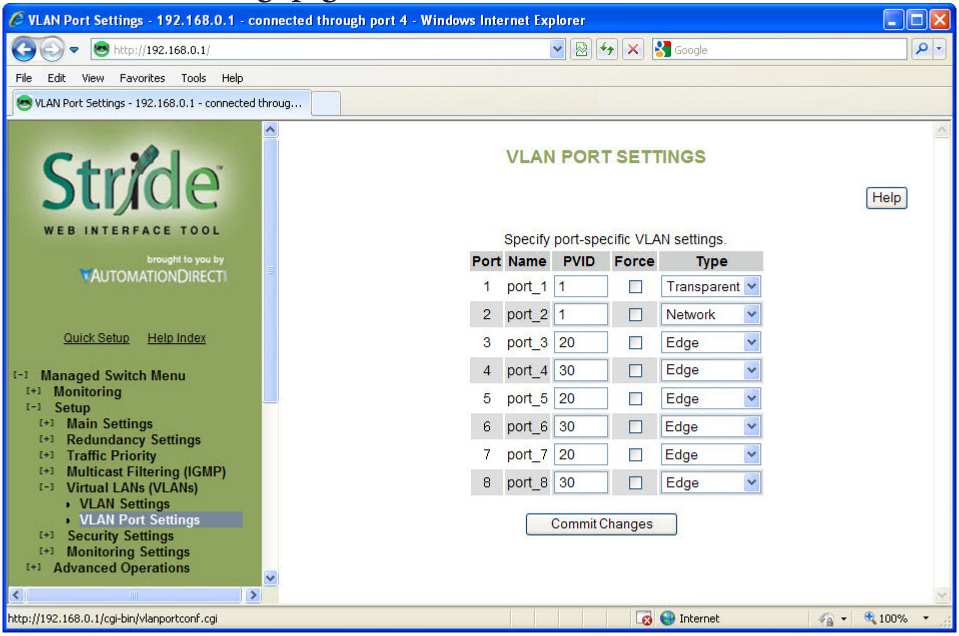
Set VLAN mode to Standard

Add the VLANs you wish to have configured, leaving the Type selection "Tag-based." In our example, we are creating two VLANs called VLAN 20 and VLAN 30. The names are for your convenience. The IDs on this page will match the PVIDs we configure on the VLAN Port Settings page and will determine VLAN participation.

We will configure port 2 as a Network (Trunking) port on the VLAN Port Settings page, so here on the VLAN Settings page we include Port 2 in both of our VLANs.

For security, we have chosen to reserve Port 1 as the only port through which the Switch Configuration utility can be accessed; we have eliminated all other ports from the Management VLAN and we have not included port 1 in the other VLANs.

On the VLAN Port Settings page:



VLAN PORT SETTINGS

Specify port-specific VLAN settings.

Port	Name	PVID	Force	Type
1	port_1	1	□	Transparent
2	port_2	1	□	Network
3	port_3	20	□	Edge
4	port_4	30	□	Edge
5	port_5	20	□	Edge
6	port_6	30	□	Edge
7	port_7	20	□	Edge
8	port_8	30	□	Edge

Set Port 2's type to Network. We will connect another managed switch configured with VLANs 20 and 30 to port 2.

For ports 3 through 8, enter the PVID (Port VLAN ID) to match the VLAN ID that each port was configured to participate in on the VLAN Settings page. In our example, a device such as a PLC, HMI, etc is assumed to be connected to ports 3-8; no managed switch is connected to these ports. So they are identified as Edge ports here.

With this configuration committed to the switch, a device on port 3 can communicate with devices on ports 5 and 7 as well as devices on the VLAN 20 ports from the switch connected to port 2. None of those devices (ports 3, 5 or 7 here or any device on a VLAN 20 port on the switch connected to port 2) can communicate with devices connected to ports 4,6 or 8, or VLAN 30 ports on the switch connected to port 2.

Devices on ports 4, 6 and 8 can communicate with each other and with devices connected to VLAN 30 ports on the switch connected to port2, but not to the VLAN 20 devices.

Port 1 is reserved for switch management and is assumed to have a laptop occasionally connected for that purpose

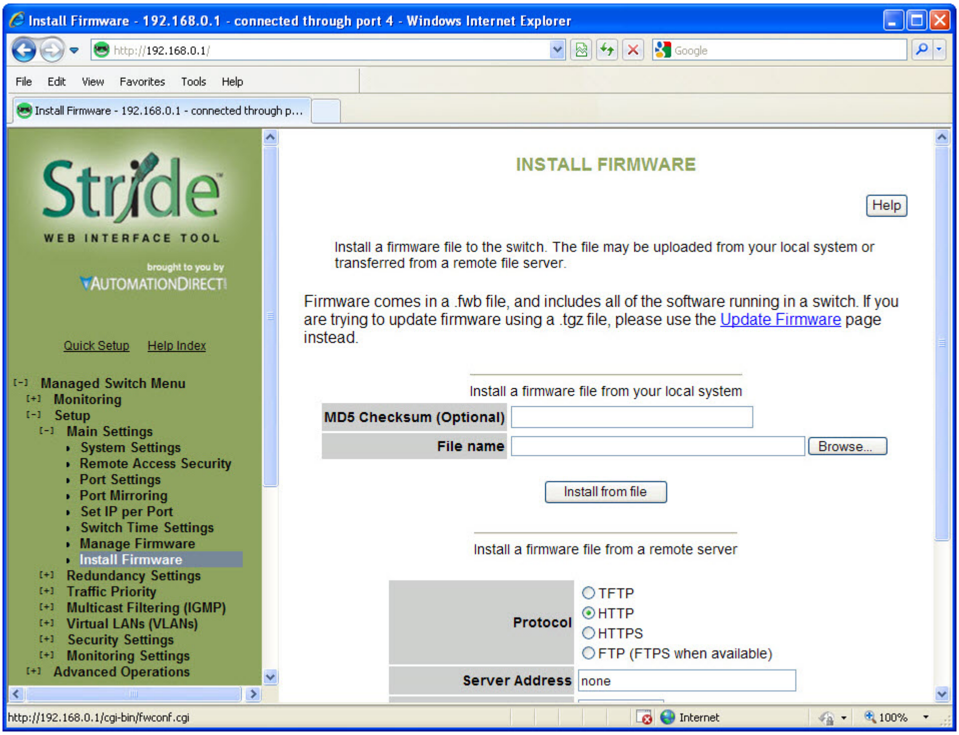
Although the tag-based VLANs are the most common and most versatile, the Port-based VLANs are the simplest. The Port-based VLANs are restricted to ports on this one switch. There is no Network (trunking) port to carry the VLANs across multiple switches.

Set VLAN mode to Port-based and Add VLANs with Type set to Port-based. Select which ports belong to each VLAN. A port should belong to only one Port-based VLAN. CPU should be checked for each Port-based VLAN.

Installing Switch Firmware

Installing switch firmware from the browser interface requires 3 steps:

1. Install the firmware .fwb file from the Main Settings – Install Firmware page



INSTALL FIRMWARE

Install a firmware file to the switch. The file may be uploaded from your local system or transferred from a remote file server.

Firmware comes in a .fwb file, and includes all of the software running in a switch. If you are trying to update firmware using a .tgz file, please use the Update Firmware page instead.

Install a firmware file from your local system

MD5 Checksum (Optional)	
File name	

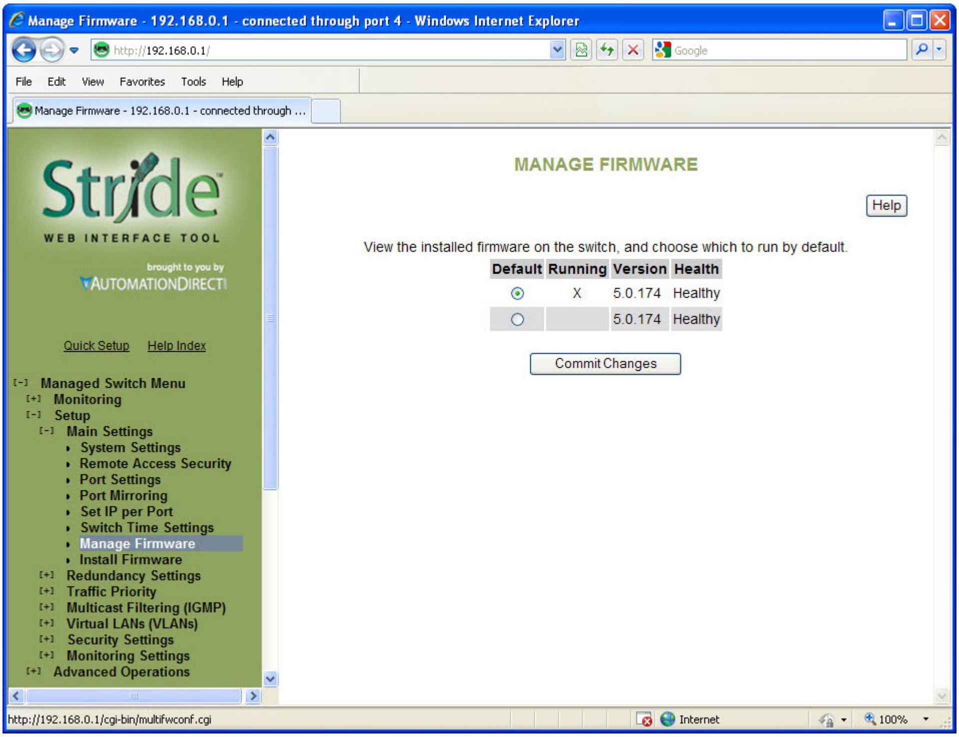
Install a firmware file from a remote server

Protocol	○ TFTP ● HTTP ○ HTTPS ○ FTP (FTPS when available)
Server Address	none

Browse to the file either on your local system or from a remote server. The MD5 Checksum is an error detection value that your IT department may calculate and give you, especially when they install firmware from a remote server. It is not required. The purpose of the Checksum is to verify the file you are using to upgrade exactly matches the version sent.

Click the Install from File or Install from Server button

2. After the firmware file has been installed, go to the Main Settings - Manage Firmware page:



MANAGE FIRMWARE

View the installed firmware on the switch, and choose which to run by default.

Default	Running	Version	Health
●	X	5.0.174	Healthy
○		5.0.174	Healthy

Set the Default radio button to the new version you installed

3. Either power cycle the switch or go to the Advanced Operations – Reset Switch page. There, click the Yes check box then click the Reset Switch button.

After the switch has been reset, the new firmware version will be identified on the Manage Firmware page as the Running version.