MANAGEMENT GUIDE

Manual abstract:

O.C. TEL: +886 3 5638888 Fax: +886 3 6686111 February 2012 Pub. @@(SMC) is believed to be accurate and reliable. @@@@SMC reserves the right to change specifications at any time without notice. Copyright © 2012 by SMC Networks, Inc. No. 1 Creation Road III, Hsinchu Science Park, 30077, Taiwan, R.O.C.

All rights reserved Trademarks: SMC is a registered trademark; and Barricade, EZ Switch, TigerStack, TigerSwitch, and TigerAccess are trademarks of SMC Networks, Inc. Other product and company names are trademarks or registered trademarks of their respective holders. WARRANTY AND PRODUCT REGISTRATION To register SMC products and to review the detailed warranty statement, please refer to the Support Section of the SMC Website at http:// www.smc.com.

4 ABOUT THIS GUIDE PURPOSE This guide gives specific information on how to operate and use the management functions of the switch. AUDIENCE The guide is intended for use by network administrators who are responsible for operating and maintaining network equipment; consequently, it assumes a basic working knowledge of general switch functions, the Internet Protocol (IP), and Simple Network Management Protocol (SNMP). CONVENTIONS The following conventions are used throughout this guide to show information: NOTE: Emphasizes important information or calls your attention to related features or instructions. CAUTION: Alerts you to a potential hazard that could cause loss of data, or damage the system or equipment. WARNING: Alerts you to a potential hazard that could cause personal injury.

RELATED PUBLICATIONS The following publication details the hardware features of the switch, including the physical and performance-related characteristics, and how to install the switch: The Installation Guide Also, as part of the switch's software, there is an online web-based help that describes all management related features. 5 ABOUT THIS GUIDE REVISION HISTORY This section summarizes the changes in each revision of this guide. FEBRUARY 2012 REVISION This is the second version of this guide. This guide is valid for software release v1.0.0.3. It includes the following changes: Updated phone and fax numbers for SMC headquarters Corrrected PVLAN ID range to 1-10 OCTOBER 2011 REVISION This is the first version of this guide. This guide is valid for software release v1.0.

0.3. 6 CONTENTS WARRANTY AND PRODUCT REGISTRATION ABOUT THIS GUIDE CONTENTS FIGURES TABLES 4 5 7 13 17 SECTION I GETTING STARTED 1 INTRODUCTION Key Features Description of Software Features System Defaults 19 20 20 21 25 2 INITIAL SWITCH CONFIGURATION 28 SECTION II WEB CONFIGURATION 3 USING THE WEB INTERFACE Navigating the Web Browser Interface Home Page Configuration Options Panel Display Main Menu 30 31 31 31 32 32 33 4 CONFIGURING THE SWITCH Configuring System Information Setting an IP Address Setting an IPv4 Address Setting an IPv6 Address Configuring NTP Service Configuring Remote Log Messages Configuring Power Reduction 41 41 42 42 44 46 47 48 7 CONTENTS Controlling LED Intensity Reducing Power to Idle Queue Circuits Configuring Thermal Protection Configuring Port Connections Configuring Security Configuring User Accounts Configuring User Privilege Levels Configuring The Authentication Method For Management Access Configuring SSH Configuring HTTPS Filtering IP Addresses for Management Access Using Simple Network Management Protocol Configuring Port Limit Controls Configuring Authentication Through Network Access Servers Filtering Traffic with Access Control Lists Configuring DHCP Snooping Configuring DHCP Relay and Option 82 Information Configuring IP Source Guard Configuring ARP Inspection Specifying Authentication Servers Creating Trunk Groups Configuring Static Trunks Configuring LACP Configuring the Spanning Tree Algorithm Configuring Global Settings for STA Configuring Multiple Spanning Trees Configuring Spanning Tree Bridge Priorities Configuring STP/RSTP/CIST Interfaces Configuring MIST Interfaces Multicast VLAN Registration IGMP Snooping Configuring Global and Port-Related Settings for IGMP Snooping Configuring VLAN Settings for IGMP Snooping and Query Configuring IGMP Filtering MLD Snooping Configuring Global and Port-Related Settings for MLD Snooping 48 50 51 52 55 55 57 59 61 62 63 65 75 77 88 99 101 102 106 109 111 112 114 116 118 122 124 125 129 130 133 134 137 139 140 140 8 CONTENTS Configuring VLAN Settings for MLD Snooping and Query Configuring MLD Filtering Link Layer Discovery Protocol Configuring LLDP Timing and TLVs Configuring LLDP-MED TLVs Power over Ethernet Configuring the MAC Address Table IEEE 802.1Q VLANs Assigning Ports to VLANs Configuring VLAN Attributes for Port Members Configuring Private VLANs Using Port Isolation Configuring MAC-based VLANs Protocol VLANs Configuring Protocol VLAN Groups Mapping Protocol Groups to Ports Managing VoIP Traffic Configuring VoIP Traffic Configuring Telephony OUI Quality of Service Configuring Port Classification Configuring Egress Port Scheduler Configuring Egress Port Shaper Configuring Port Remarking Mode Configuring Port DSCP Translation and Rewriting Configuring DSCP-based QoS Ingress Classification Configuring DSCP Translation Configuring DSCP Classification Configuring QoS Control Lists Configuring Storm Control Configuring Port Mirroring Configuring UPnP 143 145 146 146 149 155 158 160 161 162 165 166 167 168 169 170 171 172 174 175 176 178 181 181 184 186 187 188 189 193 194 196 5 MONITORING THE SWITCH Displaying Basic Information About the System Displaying System Information Displaying CPU Utilization 199 199 199 200 9 CONTENTS Displaying Log Messages Displaying Log Details Displaying Thermal Protection Displaying Information About Ports Displaying Port Status On the Front Panel Displaying an Overview of Port Statistics Displaying QoS Statistics Displaying QCL Status Displaying Detailed Port Statistics Displaying Information About Security Settings Displaying Access Management Statistics Displaying Information About Switch Settings for Port Security Displaying Information About Learned MAC Addresses Displaying Port Status for Authentication Services Displaying Port Statistics for 802.1X or Remote Authentication Service Displaying ACL Status Displaying Statistics for DHCP Snooping Displaying DHCP Relay Statistics Displaying MAC Address Bindings for ARP Packets Displaying Entries in the IP Source Guard Table Displaying Information on Authentication Servers Displaying a List of Authentication Servers Displaying Statistics for Configured Authentication Servers Displaying Information on LACP Displaying an Overview of LACP Groups Displaying LACP Port Status Displaying LACP Port Statistics Displaying Information on the Spanning Tree Displaying Bridge Status for STA Displaying Port Status for STA Displaying Port Statistics for STA Displaying MVR Information Displaying MVR Statistics Displaying MVR Group Information Showing IGMP Snooping Information Showing IGMP Snooping Status 10 201 203 203 204 204 205 205 206 207 210 210 211 213 214 215 219 221 222 223 224 225 225 226 229 229 230 231 232 232 234 235 236 236 237 238 238 CONTENTS Showing IGMP Snooping Group Information Showing IPv4 SSM Information Showing MLD Snooping Information Showing MLD Snooping Status Showing MLD Snooping Group Information Showing IPv6 SSM Information Displaying LLDP Information Displaying LLDP Neighbor Information Displaying LLDP-MED Neighbor Information Displaying LLDP Neighbor EEE Information Displaying LLDP Port Statistics Displaying LLDP Neighbor PoE Displaying PoE Status Displaying the MAC Address Table Displaying Information About VLANs VLAN Membership VLAN Port Status Displaying Information About MAC-based VLANs Information 239 240 241 241 242 243 244 244 245 247 249 250 251 252 253 253 254 256 6 PERFORMING BASIC DIAGNOSTICS Pinging an IPv4 or IPv6 Address Running Cable Diagnostics 257 257 258 7 PERFORMING SYSTEM MAINTENANCE Restarting the Switch Restoring Factory Defaults Upgrading Firmware Managing Configuration Files Saving Configuration Settings Restoring Configuration Settings 261 261 262 262 263 263 264 SECTION III APPENDICES A SOFTWARE SPECIFICATIONS Software Features Management Features Standards Management Information Bases 265 266 266 267 268 268 11 CONTENTS B TROUBLESHOOTING Problems Accessing the Management Interface Using System Logs 270 270 271 C LICENSE INFORMATION The GNU General Public License 272 272 GLOSSARY INDEX 276 284 12 FIGURES Figure 1: Home Page Figure 2: Front Panel Indicators Figure 3: System Information Configuration Figure 4: IP Configuration Figure 5: IPv6 Configuration Figure 6: NTP Configuration Figure 7: Configuring Settings for Remote

Logging of Error Messages Figure 8: Configuring LED Power Reduction Figure 9: Configuring EEE Power Reduction Figure 10: Configuring Thermal Protection Figure 11: Port Configuration Figure 12: Showing User Accounts Figure 13: Configuring User Accounts Figure 14: Configuring Privilege Levels Figure 15: Authentication Server Operation Figure 16: Authentication Method for Management Access Figure 17: SSH Configuration Figure 18: HTTPS Configuration Figure 19: Access Management Configuration Figure 20: SNMP System Configuration Figure 21: SNMPv3 Community Configuration Figure 22: SNMPv3 User Configuration Figure 23: SNMPv3 Group Configuration Figure 24: SNMPv3 View Configuration Figure 25: SNMPv3 Access Configuration Figure 26: Port Limit Control Configuration Figure 27: Using Port Security Figure 28: Network Access Server Configuration Figure 29: ACL Port Configuration Figure 30: ACL Rate Limiter Configuration Figure 31: Access Control List Configuration 13 31 32 42 44 46 47 48 49 51 52 54 56 57 58 59 61 62 63 64 69 70 72 73 74 75 77 78 88 90 91 98 FIGURES Figure 32: DHCP Snooping Configuration Figure 33: DHCP Relay Configuration Figure 34: Configuring Global and Port-based Settings for IP Source Guard Figure 35: Configuring Static Bindings for IP Source Guard Figure 36: Configuring Global and Port Settings for ARP Inspection Figure 37: Configuring Static Bindings for ARP Inspection Figure 38: Authentication Configuration Figure 39: Static Trunk Configuration Figure 40: LACP Port Configuration Figure 41: STP Root Ports and Designated Ports Figure 42: MSTP Region, Internal Spanning Tree, Multiple Spanning Tree Figure 43: Common Internal Spanning Tree, Common Spanning Tree, Internal Spanning Tree Figure 44: STA Bridge Configuration Figure 45: Adding a VLAN to an MST Instance Figure 46: Configuring STA Bridge Priorities Figure 47: STP/RSTP/CIST Port Configuration Figure 48: MSTI Port Configuration Figure 49: MVR Concept Figure 50: Configuring MVR Figure 51: Configuring Global and Port-related Settings for IGMP Snooping Figure 52: Configuring VLAN Settings for IGMP Snooping and Query Figure 53: IGMP Snooping Port Group Filtering Configuration Figure 54: Configuring Global and Port-related Settings for MLD Snooping Figure 55: Configuring VLAN Settings for MLD Snooping and Query Figure 56: MLD Snooping Port Group Filtering Configuration Figure 57: LLDP Configuration Figure 58: LLDP-MED Configuration Figure 59: Configuring PoE Settings Figure 60: MAC Address Table Configuration Figure 61: VLAN Membership Configuration Figure 62: VLAN Port Configuration Figure 63: Private VLAN Membership Configuration Figure 64: Port Isolation Configuration Figure 65: Configuring MAC-Based VLANs Figure 66: Configuring Protocol VLANs Figure 67: Assigning Ports to Protocol VLANs 14 101 102 104 106 108 109 110 114 116 117 117 118 122 124 125 128 130 131 133 136 138 139 143 145 146 149 155 158 160 162 164 166 166 168 170 171 FIGURES Figure 68: Configuring Global and Port Settings for a Voice VLAN Figure 69: Configuring an OUI Telephony List Figure 70: Configuring Ingress Port QoS Classification Figure 71: Configuring Ingress Port Tag Classification Figure 72: Displaying Egress Port Schedulers Figure 73: Configuring Egress Port Schedulers and Shapers Figure 74: Displaying Egress Port Shapers Figure 75: Displaying Port Tag Remarking Mode Figure 76: Configuring Port Tag Remarking Mode Figure 77: Configurand Restore Authentication Description Backup to management station using Web Telnet, Web user name/password, RADIUS, TACACS+ Web HTTPS Telnet SSH SNMP v1/2c - Community strings SNMP version 3 MD5 or SHA password Port IEEE 802.

1X, MAC address filtering Private VLANs Port Authentication Port Security DHCP Snooping (with Option 82 relay information) IP Source Guard Supports up to 256 rules Client Client and Proxy servicols. @@@@@@@@The switch supports flow control based on the IEEE 802.3x standard (now incorporated in IEEE 802.3-2002). RATE LIMITING This feature controls the maximum rate for traffic transmitted or received on an interface.

Rate limiting is configured on interfaces at the edge of a network to limit traffic into or out of the network. Traffic that falls within the rate limit is transmitted, while packets that exceed the acceptable amount of traffic are dropped. PORT MIRRORING The switch can unobtrusively mirror traffic from any port to a monitor port. You can then attach a protocol analyzer or RMON probe to this port to perform traffic analysis and verify connection integrity. PORT TRUNKING Ports can be combined into an aggregate connection.

Trunks can be manually set up or dynamically configured using Link Aggregation Control Protocol (LACP IEEE 802.3-2005). The additional ports dramatically increase the throughput across any connection, and provide redundancy by taking over the load if a port in the trunk should fail. The switch supports up to 5 trunks. STORM CONTROL Broadcast, multicast and unknown unicast storm suppression prevents traffic from overwhelming the network. When enabled on a port, the level of broadcast traffic passing through the port is restricted. If broadcast traffic rises above a pre-defined threshold, it will be throttled until the level falls back beneath the threshold. STATIC ADDRESSES A static address can be assigned to a specific interface on this switch. Static addresses are bound to the assigned interface and will not be moved. When a static address is seen on another interface, the address will 22 CHAPTER 1 | Introduction Description of Software Features be ignored and will not be written to the address table. Static addresses can be used to provide network security by restricting access for a known host to a specific port. IEEE 802.1D BRIDGE The switch supports IEEE 802.1D transparent bridging. The address table facilitates data switching by learning addresses, and then filtering or forwarding traffic based on this information.

The address table supports up to 16K addresses. STORE-AND-FORWARD The switch copies each frame into its memory before forwarding them to SWITCHING another port. This ensures that all frames are a standard Ethernet size and have been verified for accuracy with the cyclic redundancy check (CRC). This prevents bad frames from entering the network and wasting bandwidth. To avoid dropping frames on congested ports, the switch provides 8 MB for frame buffering. This buffer can queue packets awaiting transmission on congested networks. SPANNING TREE The switch supports these spanning tree protocols: ALGORITHM Spanning Tree Protocol (STP, IEEE 802.1D) Supported by using the STP backward compatible mode provided by RSTP. STP provides loop detection. When there are multiple physical paths between segments, this protocol will choose a single path and disable all others to ensure that only one route exists between any two stations on the network.

This prevents the creation of network loops. However, if the chosen path should fail for any reason, an alternate path will be activated to maintain the connection. Rapid Spanning Tree Protocol (RSTP, IEEE 802.1w) This protocol reduces the convergence time for network topology changes to about 3 to 5 seconds, compared to 30 seconds or more for the older IEEE 802.1D STP standard.

It is intended as a complete replacement for STP, but can still interoperate with switches running the older standard by automatically reconfiguring ports to STP-compliant mode if they detect STP protocol messages from attached devices. Multiple Spanning Tree Protocol (MSTP, IEEE 802.1s) This protocol is a direct extension of RSTP. It can provide an independent spanning tree for different VLANs. It simplifies network management, provides for even faster convergence than RSTP by limiting the size of each region, and prevents VLAN members from being segmented from the rest of the group (as sometimes occurs with IEEE 802.

1D STP). 23 CHAPTER 1 | Introduction Description of Software Features VIRTUAL LANS The switch supports up to 4096 VLANs. A Virtual LAN is a collection of network nodes that share the same collision domain regardless of their physical location or connection point in the network. The switch supports tagged VLANs based on the IEEE 802.1Q standard. Members of VLAN groups can be manually assigned to a specific set of VLANs. This allows the switch to restrict traffic to the VLAN groups to which a user has been assigned. By segmenting your network into VLANs, you can: Eliminate broadcast storms which severely degrade performance in a flat network. Simplify network management for node changes/moves by remotely configuring VLAN membership for any port, rather than having to manually change the network connection. Provide data security by restricting all traffic to the originating VLAN.

Use private VLANs to restrict traffic to pass only between data ports and the uplink ports, thereby isolating adjacent ports within the same VLAN, and allowing you to limit the total number of VLANs that need to be configured. Use protocol VLANs to restrict traffic to specified interfaces based on protocol type. IEEE 802.1Q This feature is designed for service providers carrying traffic for multiple TUNNELING (QINQ) customers across their networks. QinQ tunneling is used to maintain customer-specific VLAN and Layer 2 protocol configurations even when different customers use the same internal VLAN IDs. This is accomplished by inserting Service Provider VLAN (SPVLAN) tags into the customer's frames when they enter the service provider's network, and then stripping the tags when the frames leave the network. TRAFFIC This switch prioritizes each packet based on the required level of service, PRIORITIZATION using four priority queues with strict or Weighted Round Robin queuing. It uses IEEE 802.1p and 802.1Q tags to prioritize incoming traffic based on input from the end-station application.

These functions can be used to provide independent priorities for delay-sensitive data and best-effort data. This switch also supports several common methods of prioritizing layer 3/4 traffic to meet application requirements. Traffic can be prioritized based on the priority bits in the IP frame's Type of Service (ToS) octet or the number of the TCP/UDP port. When these services are enabled, the priorities are mapped to a Class of Service value by the switch, and the traffic then sent to the corresponding output queue. 24 CHAPTER 1 | Introduction System Defaults QUALITY OF SERVICE Differentiated Services (DiffServ) provides policy-based management mechanisms used for prioritizing network resources to meet the requirements of specific traffic types on a per-hop basis.

Each packet is classified upon entry into the network based on access lists, DSCP values, or VLAN lists. Using access lists allows you select traffic based on Layer 2, Layer 3, or Layer 4 information contained in each packet. Based on network policies, different kinds of traffic can be marked for different kinds of forwarding. MULTICAST FILTERING Specific multicast traffic can be assigned to its own VLAN to ensure that it does not interfere with normal network traffic and to guarantee real-time delivery by setting the required priority level for the designated VLAN. The switch uses IGMP Snooping and Query to manage multicast group registration for IPv4 traffic, and MLD Snooping for IPv6 traffic.

It also supports Multicast VLAN Registration (MVR) which allows common multicast traffic, such as television channels, to be transmitted across a single network-wide multicast VLAN shared by hosts residing in other standard or private VLAN groups, while preserving security and data isolation for normal traffic. SYSTEM DEFAULTS The switch's system defaults are provided in the configuration file "Factory_Default_Config.cfg." To reset the switch defaults, this file should be set as the startup configuration file. The following table lists some of the basic system defaults. Table 2: System Defaults Function Authentication Parameter User Name Password RADIUS Authentication TACACS+ Authentication 802.1X Port Authentication HTTPS SSH Port Security IP Filtering Web Management HTTP Server HTTP Port Number HTTP Secure Server HTTP Secure Server Redirect Default "admin" "admin" Disabled Disabled Disabled Enabled Enabled Disabled Disabled Enabled 80 Disabled Disabled 25 CHAPTER 1 | Introduction System Defaults Table 2: System Defaults (Continued) Function SNMP Parameter SNMP Agent Community Strings Traps Default Disabled "public" (read only) "private" (read/write) Global: disabled Authentication traps: enabled Link-up-down events: enabled View: default_view Group: default_rw_group Enabled Enabled Disabled Disabled None Disabled Broadcast: Enabled (1 kpps) Multicast: disabled Unknown unicast: disabled Enabled, RSTP (Defaults: RSTP standard) Enabled 300 seconds 1 1 All Disabled SNMP V3 Port Configuration Admin Status Auto-negotiation Flow Control Rate Limiting Port Trunking Input and output limits Static Trunks LACP (all ports) Storm Protection Status Spanning Tree Algorithm Status Edge Ports Address Table Virtual LANs Aging Time Default VLAN PVID Acceptable Frame Type Ingress Filtering Switchport Mode (Egress Mode) Access Traffic Prioritization Ingress Port Priority Queue Mode Weighted Round Robin Ethernet Type VLAN ID VLAN Priority Tag ToS Priority IP DSCP Priority TCP/UDP Port Priority LLDP Status 0 Strict Queue: 0 1 2 3 4 5 6 7 Weight: Disabled in strict mode Disabled Disabled Disabled Disabled Disabled Disabled Enabled 26 CHAPTER 1 | Introduction System Defaults Table 2: System Defaults (Continued) Function IP Settings Parameter Management. VLAN IP Address Subnet Mask Default Gateway DHCP DNS Multicast Filtering IGMP Snooping MLD Snooping Multicast VLAN Registration System Log (console only) NTP Status Messages Logged to Flash Clock Synchronization Default VLAN 1 192.168.1.

10 255.255.255.0 0.0.0.0 Client: Disabled Snooping: Disabled Proxy service: Disabled Snooping: Disabled Querier: Disabled Disabled Disabled Disabled All levels Disabled 27 2 INITIAL SWITCH CONFIGURATION This chapter includes information on connecting to the switch and basic configuration procedures. To make use of the management features of your switch, you must first configure it with an IP address that is compatible with the network in which it is being installed. This should be done before you permanently install the switch in the network. Follow this procedure: 1.

Place the switch close to the PC that you intend to use for configuration. It helps if you can see the front panel of the switch while working on your PC. 2. Connect the Ethernet port of your PC to any port on the front panel of the switch. Connect power to the switch and verify that you have a link by checking the front-panel LEDs.

3. Check that your PC has an IP address on the same subnet as the switch. The default IP address of the switch is 192.168.1.

10 and the subnet mask is 255.255.255.0, so the PC and switch are on the same subnet if they both have addresses that start 192.168.1.x. If the PC and switch are not on the same subnet, you must manually set the PC's IP address to 192.168.1.

x (where "x" is any number from 1 to 254, except 10). 4. Open your web browser and enter the address http://192.168.1.10. If your PC is properly configured, you will see the login page of the switch. If you do not see the login page, repeat step 3. 5. Enter "admin" for the user name and password, and then click on the Login button.

6. From the menu, click System, and then IP. To request an address from a local DHCP Server, mark the DHCP Client check box. To configure a static address, enter the new IP Address, IP Mask, and other optional parameters for the switch, and then click on the Save button. If you need to configure an IPv6 address, select IPv6 from the System menu, and either submit a request for an address from a local DHCPv6 server by marking the Auto Configuration check box, or configure a static address by filling in the parameters for an address, network prefix length, and gateway router.

No other configuration changes are required at this stage, but it is recommended that you change the administrator's password before 28 CHAPTER 2 | Initial Switch Configuration logging out. To change the password, click Security and then Users. Select "admin" from the User Configuration list, fill in the Password fields, and then click Save. 29 SECTION II WEB CONFIGURATION This section describes the basic switch features, along with a detailed description of how to configure each feature via a web browser. This section includes these chapters: "Using the Web Interface" on page 31 "Configuring the Switch" on page 41 "Monitoring the Switch" on page 199 "Performing Basic Diagnostics" on page 257 "Performing System Maintenance" on page 261 30 3 USING THE WEB INTERFACE This switch provides an embedded HTTP web agent.

Using a web browser you can configure the switch and view statistics to monitor network activity. The web agent can be accessed by any computer on the network using a standard web browser (Internet Explorer 5.0, Netscape 6.2, Mozilla Firefox 2.0.0.0, or more recent versions). NAVIGATING THE WEB BROWSER INTERFACE To access the web-browser interface you must first enter a user name and password. The administrator has Read/Write access to all configuration parameters and statistics. The default user name and password for the administrator is "admin.

" HOME PAGE When your web browser connects with the switch's web agent, the home page is displayed as shown below. The home page displays the Main Menu on the left side of the screen and an image of the front panel on the right side. The Main Menu links are used to navigate to other menus, and display configuration parameters and statistics. Figure 1: Home Page 31 CHAPTER 3 | Using the Web Interface Navigating the Web Browser Interface CONFIGURATION Configurable parameters have a dialog box or a drop-down list. Once a OPTIONS configuration change has been made on a page, be sure to click on the Save button to confirm the new setting. The following table summarizes the web page configuration buttons. Table 3: Web Page Configuration Buttons Button Save Reset Action Sets specified values to the system. Cancels specified values and restores current values prior to pressing "Save." Logs out of the management interface. Displays help for the selected page.

NOTE: To ensure proper screen refresh, be sure that Internet Explorer is configured so that the setting "Check for newer versions of stored pages" reads "Every visit to the page." Internet Explorer 6.x and earlier: This option is available under the menu "Tools / Internet Options / General / Temporary Internet Files / Settings." Internet Explorer 7.x: This option is available under "Tools / Internet Options / General / Browsing History / Settings / Temporary Internet Files.

" PANEL DISPLAY The web agent displays an image of the switch's ports. The refresh mode is disabled by default. Click Auto-refresh to refresh the data displayed on the screen approximately once every 5 seconds, or click Refresh to refresh the screen right now. Clicking on the image of a port opens the Detailed Statistics page as described on page 207. Figure 2: Front Panel Indicators 32 CHAPTER 3 | Using the Web Interface Navigating the Web Browser Interface MAIN MENU Using the onboard web agent, you can define system parameters, manage and control the switch, and all its ports, or monitor network conditions.

The following table briefly describes the selections available from this program. Table 4: Main Menu Menu Configuration System Information IP IPv6 NTP Log Configures system contact, name and location Configures IPv4 and SNTP settings Configures IPv6 and SNTP settings Enables NTP, and configures a list of NTP servers Configures the logging of messages to a remote logging process, specifies the remote log server, and limits the type of system log messages sent 41 42 44 46 47 Description Page 41 Power Reduction LED EEE Reduces LED intensity during specified hours Configures Energy Efficient Ethernet for specified queues, and specifies urgent queues which are to transmit data after maximum latency expires regardless queue length Configures temperature priority levels, and assigns those priorities for port shut-down if exceeded Configures port connection settings 48 48 50 Thermal Protection Ports Security Switch Users Privilege Levels Auth Method SSH HTTPS Access Management SNMP System Communities Users Groups Views Access Network 51 52 55 55 Configures user names, passwords, and access levels Configures privilege level for specific functions Configures authentication method for management access via local database, RADIUS or TACACS+ Configures the Secure Shell server Configures secure HTTP settings Sets IP addresses of clients allowed management access via HTTP/HTTPS, and SNMP, and Telnet/SSH Simple Network Management Protocol Configures read-only and read/write community strings for SNMP v1/v2c, engine ID for SNMP v3, and trap parameters Configures community strings Configures SNMP v3 users on this switch Configures SNMP v3 groups Configures SNMP v3 views Assigns security model, security level, and read/write views to SNMP groups 55 57 59 61 62 63 65 66 69 70 72 73 74 33 CHAPTER 3 | Using the Web Interface Navigating the Web Browser Interface Table 4: Main Menu (Continued) Menu Limit Control Description Configures port security limit controls, including secure address aging; and per port security, including maximum allowed MAC addresses, and response for security breach Configures global and port settings for IEEE 802.1X Access Control Lists Assigns ACL, rate limiter, and other parameters to ports Configures rate limit policies Configures ACLs based on frame type, destination MAC type, VLAN ID, VLAN priority tag; and the action to take for matching packets Dynamic Host Configuration Protocol Enables DHCP snooping globally; and sets the trust mode for each port Configures DHCP relay information status and policy 99 101 Page 75 NAS ACL Ports Rate Limiters Access Control List DHCP Snooping Relay IP Source Guard Configuration Static Table ARP Inspection Configuration Static Table AAA 77 88 88 90 91 Filters IP traffic based on static entries in the IP Source 102 Guard table, or dynamic entries in the DHCP Snooping table Enables IP source guard and sets the maximum number of clients that can learned dynamically Adds a static addresses to the source-guard binding table Address Resolution Protocol Inspection Enables inspection globally, and per port Adds static entries based on port, VLAN ID, and source MAC address and IP address in ARP request packets Configures RADIUS authentication server, RADIUS accounting server, and TACACS+ authentication server settings 103 105 106 107 108 109 Aggregation Static LACP Spanning Tree Bridge Settings Configures global bridge settings for STP, RSTP and MSTP; also configures edge port settings for BPDU filtering, BPDU guard, and port error recovery Maps VLANs to a specific MSTP instance Configures the priority for the CIST and each MISTI Configures interface settings for STA Configures interface settings for an MST instance Configures Multicast VLAN Registration, including global status, MVR VLAN, port mode, and immediate leave IP Multicast Internet Group Management Protocol Snooping Configures global and port settings for multicast filtering Specifies ports to group into static trunks Allows ports to dynamically join trunks 111 112 114 116 118 MSTI Mapping MSTI Priorities CIST Ports MSTI Ports MVR IPMC IGMP Snooping Basic Configuration 122 124 125 129 130 133 134 34 CHAPTER 3 | Using the Web Interface Navigating the Web Browser Interface Table 4: Main Menu (Continued) Menu VLAN Configuration Port Group Filtering MLD Snooping Basic Configuration VLAN Configuration Port Group Filtering LLDP LLDP LLDP-MED PoE MAC Table VLANs VLAN Membership Ports Private VLANs PVLAN Membership Port Isolation VCL MAC-based VLAN Protocol-based VLAN Protocol to Group Group to VLAN Voice VLAN Configuration Configures global settings, including status, voice VLAN ID, VLAN aging time, and traffic priority; also configures port settings, including the way in which a port is added to the Voice VLAN, and blocking non-VoIP addresses Maps the OUI in the source MAC address of ingress packets to the VoIP device manufacturer Creates a protocol group, specifying supported protocols Maps a protocol group to a VLAN for specified ports Configures PVLAN groups Prevents communications between designated ports within the same private VLAN VLAN Control List Maps traffic with specified source MAC address to a VLAN 167 168 169 170 171 172 165 166 Description Configures IGMP snooping per VLAN interface Configures multicast groups to be filtered on specified port Multicast Listener Discovery Snooping Configures global and port settings for multicast filtering Configures MLD snooping per VLAN interface Configures multicast groups to be filtered on specified port Link Layer Discovery Protocol Configures global LLDP timing parameters, and port-specific TLV attributes Configures LLDP-MED attributes, including device location, emergency call server, and network policy discovery Configures Power-over-Ethernet settings for each port Configures address aging, dynamic learning, and static addresses Virtual LANs Configures VLAN groups Specifies default PVID and VLAN attributes Page 137 139 140 140 143 145 146 146 149 155 158 160 161 162 OUI QoS Port Classification 174 175 Configures default traffic class, drop priority, user priority, 176 drop eligible indicator, classification mode for tagged frames, and DSCP-based QoS classification 35 CHAPTER 3 | Using the Web Interface Navigating the Web Browser Interface Table 4: Main Menu (Continued) Menu Port Scheduler Description Provides overview of QoS Egress Port Schedulers, including the queue mode and weight; also configures egress queue mode, queue shaper (rate and access to excess bandwidth), and port shaper Provides overview of QoS Egress Port Shapers, including the rate for each queue and port; also configures egress queue mode, queue shaper (rate and access to excess bandwidth), and port shaper Provides overview of QoS Egress Port Tag Remarking; also sets the remarking mode (classified PCP/DEI values, default PCP/DEI values, or mapped versions of QoS class and drop priority) Configures ingress translation and classification settings and egress re-writing of DSCP values Configures DSCP-based QoS ingress classification settings Configures DSCP translation for ingress traffic or DSCP remapping for egress traffic Page 178 Port Shaping 181 Port Tag Remarking 181 Port DSCP DSCP-Based QoS DSCP Translation DSCP Classification QoS Control List 184 186 187 Maps DSCP values to a QoS class and drop precedence level 188 Configures QoS policies for handling ingress packets based on Ethernet type, VLAN ID, TCP/UDP port, DSCP, ToS, or VLAN priority tag Sets limits for broadcast, multicast, and unknown unicast traffic Sets source and target ports for

mirroring Enables UPNP and defines timeout values 189 Storm Control Mirroring UPnP Monitor System Information CPU Load Log Detailed Log Thermal Protection Ports State Traffic Overview QoS Statistics QCL Status Detailed Statistics Security Access Management Statistics Network 193 194 196 199 199 Displays basic system description, switch's MAC address, system time, and software version Displays graphic scale of CPU utilization Displays logged messages based on severity Displays detailed information on each logged message Shows the current chip temperature 199 200 201 203 203 204 Displays a graphic image of the front panel indicating active port connections Shows basic Ethernet port statistics Shows the number of packets entering and leaving the egress queues Shows the status of QoS Control List entries Shows detailed Ethernet port statistics 204 205 205 206 207 210 Displays the number of packets used to manage the switch via HTTP, HTTPS, and SNMP, Telnet, and SSH 210 36 CHAPTER 3 | Using the Web Interface Navigating the Web Browser Interface Table 4: Main Menu (Continued) Menu Port Security Switch Shows information about MAC address learning for each port, including the software module requesting port security services, the service state, the current number of learned addresses, and the maximum number of secure addresses allowed Shows the entries authorized by port security services, including MAC address, VLAN ID, the service state, time added to table, age, and hold state Shows global and port settings for IEEE 802.

1X Shows port status for authentication services, including 802.1X security state, last source address used for authentication, and last ID Displays authentication statistics for the selected port either for 802.1X protocol or for the remote authentication server depending on the authentication method Shows the status for different security modules which use ACL filtering, including ingress port, frame type, and forwarding action Dynamic Host Configuration Protocol Shows statistics for various types of DHCP protocol packets 221 Displays server and client statistics for packets affected by the relay information policy Displays entries in the ARP inspection table, sorted first by port, then VLAN ID, MAC address, and finally IP address Displays entries in the IP Source Guard table, sorted first by port, then VLAN ID, MAC address, and finally IP address Authentication, Authorization and Accounting Displays status of configured RADIUS authentication and accounting servers Displays the traffic and status associated with each configured RADIUS server Link Aggregation Control Protocol Displays administration key and associated local ports for each partner Displays administration key, LAG ID, partner ID, and partner ports for each local port Displays statistics for LACP protocol messages 222 223 224 225 225 226 229 229 230 231 232 Displays global bridge and port settings for STA Displays STA role, state, and uptime for each port Displays statistics for RSTP, STP and TCN protocol packets Multicast VLAN Registration Shows statistics for IGMP protocol messages used by MVR 232 234 235 236 236 237 214 211 Description Page Port 213 NAS Switch Port 215 ACL Status 219 DHCP Snooping Statistics Relay Statistics ARP Inspection IP Source Guard AAA RADIUS Overview RADIUS Details LACP System Status Port Status Port Statistics Spanning Tree Bridge Status Port Status Port Statistics MVR Statistics Group Information Shows information about the interfaces associated with multicast groups assigned to the MVR VLAN 37 CHAPTER 3 | Using the Web Interface Navigating the Web Browser Interface Table 4: Main Menu (Continued) Menu IPMC IGMP Snooping Status Group Information IPv4 SSM Information MLD Snooping Status Group Information IPv6 SSM Information LLDP Neighbors LLDP-MED Neighbors Displays statistics related to IGMP packets passed upstream to the IGMP Querier or downstream to multicast clients Displays active IGMP groups Displays IGMP Source-Specific Information including group, filtering mode (include or exclude), source address, and type (allow or deny) Multicast Listener Discovery Snooping Displays MLD querier status and protocol statistics Displays active MLD groups Displays MLD Source-Specific Information including group, filtering mode (include or exclude), source address, and type (allow or deny) Link Layer Discovery Protocol Displays LLDP information about a remote device connected to a port on this switch Displays information about a remote device connected to a port on this switch which is advertising LLDP-MED TLVs, including network connectivity device, endpoint device, capabilities, application type, and policy Displays status of all LLDP PoE neighbors, including power device type (PSE or PD), source of power, power priority, and maximum required power Displays Energy Efficient Ethernet information advertised through LLDP messages Displays statistics for all connected remote devices, and statistics for LLDP protocol packets crossing each port Displays the status for all PoE ports, including the PD class, requested power, allocated power, power and current used, and PoE priority Displays dynamic and static address entries associated with the CPU and each port Virtual LANs Description IP Multicast 238 238 239 240 Page 241 241 242 243 244 244 245 PoE 250 EEE Port Statistics PoE 247 249 251 MAC Table VLANs 252 253 253 254 VLAN Membership Shows the current port members for all VLANs configured by a selected software module VLAN Port Shows the VLAN attributes of port members for all VLANs configured by a selected software module which uses VLAN management, including PVID, VLAN aware, ingress filtering, frame type, egress filtering, and PVID VLAN Control List Displays MAC address to VLAN map entries VCL MAC-based VLAN Diagnostics Ping Ping6 256 257 Tests specified path using IPv4 ping Tests specified path using IPv6 ping 257 257 38 CHAPTER 3 | Using the Web Interface Navigating the Web Browser Interface Table 4: Main Menu (Continued) Menu VeriPHY Description Performs cable diagnostics for all ports or selected port to diagnose any cable faults (short, open etc.) and report the cable length Page 258 Maintenance Restart Device Factory Defaults Software Upload Configuration Save Upload Saves configuration settings to a file on the management station Restores configuration settings from a file on the management station Restarts the switch Restores factory default settings Updates software on the switch with a file specified on the management station 261 261 262 262 263 263 263 39 CHAPTER 3 | Using the Web Interface Navigating the Web Browser Interface 40 4 CONFIGURING THE SWITCH This chapter describes all of the basic configuration tasks. CONFIGURING SYSTEM INFORMATION Use the System Information Configuration page to identify the system by configuring contact information, system name, location of the switch, and time zone offset. PATH Configuration, System, Information PARAMETERS These parameters are displayed: System Contact Administrator responsible for the system. (Maximum length: 255 characters) System Name Name assigned to the switch system.

(Maximum length: 255 characters) System Location Specifies the system location. (Maximum length: 255 characters) System Timezone Offset (minutes) Sets the time zone as an offset from Greenwich Mean Time (GMT). Negative values indicate a zone before (east of) GMT, and positive values indicate a zone after (west of) GMT. WEB INTERFACE To configure System Information: 1. Click Configuration, System, Information. 2. Specify the contact information for the system administrator, as well as the name and location of the switch. Also indicate the local time zone by configuring the appropriate offset. 3. Click Save. 41 CHAPTER 4 | Configuring the Switch Setting an IP Address Figure 3: System Information Configuration SETTING AN IP ADDRESS This section describes how to configure an IP interface for management access to the switch over the network. This switch supports both IP Version 4 and Version 6, and can be managed simultaneously through either of these address types. You can manually configure a specific IPv4 or IPv6 address or direct the switch to obtain an IPv4 address from a DHCP server when it is powered on. An IPv6 address can either be manually configured or dynamically generated.

SETTING AN IPV4 Use the IP Configuration page to configure an IPv4 address for the switch.
ADDRESS The IP address for the switch is obtained via DHCP by default for VLAN 1. To manually configure an address, you need to change the switch's default settings to values that are compatible with your network. You may also need to a establish a default gateway between the switch and management stations that exist on another network segment. NOTE: An IPv4 address for this switch is obtained via DHCP by default. If the switch does not receive a response from a DHCP server, it will default to the IP address 192.
168.2.10 and subnet mask 255.255.255.0. You can manually configure a specific IP address, or direct the device to obtain an address from a DHCP server. Valid IPv4 addresses consist of four decimal numbers, 0 to 255, separated by periods. Anything other than this format will not be accepted by the CLI program. PATH Configuration, System, IP PARAMETERS These parameters are displayed: IP Configuration DHCP Client Specifies whether IP functionality is enabled via Dynamic Host Configuration Protocol (DHCP).

If DHCP is enabled, IP 42 CHAPTER 4 | Configuring the Switch Setting an IP Address will not function until a reply has been received from the server. Requests will be broadcast periodically by the switch for an IP address. DHCP values can include the IP address, subnet mask, and default gateway. (Default: Enabled) IP Address Address of the VLAN specified in the VLAN ID field. This should be the VLAN to which the management station is attached. Valid IP addresses consist of four numbers, 0 to 255, separated by periods. (Default: 192.168.2.10) IP Mask This mask identifies the host address bits used for routing to specific subnets.
(Default: 255.255.255.0) IP Router IP address of the gateway router between the switch and management stations that exist on other network segments. VLAN ID ID of the configured VLAN.
By default, all ports on the switch are members of VLAN 1. However, the management station can be attached to a port belonging to any VLAN, as long as that VLAN has been assigned an IP address. (Range: 1-4095; Default: 1) DNS Server A Domain Name Server to which client requests for mapping host names to IP addresses are forwarded. IP DNS Proxy Configuration DNS Proxy If enabled, the switch maintains a local database based on previous responses to DNS queries forwarded on behalf of attached clients. If the required information is not in the local database, the switch forwards the DNS query to a DNS server, stores the response in its local cache for future reference, and passes the response back to the client.
WEB INTERFACE To configure an IP address: 1. Click Configuration, System, IP. 2. Specify the IPv4 settings, and enable DNS proxy service if required. 3. Click Save. 43 CHAPTER 4 | Configuring the Switch Setting an IP Address Figure 4: IP Configuration SETTING AN IPV6 Use the IPv6 Configuration page to configure an IPv6 address for ADDRESS management access to the switch. IPv6 includes two distinct address types - link-local unicast and global unicast. A link-local address makes the switch accessible over IPv6 for all devices attached to the same local subnet. Management traffic using this kind of address cannot be passed by any router outside of the subnet.

A link-local address is easy to set up, and may be useful for simple networks or basic troubleshooting tasks. However, to connect to a larger network with multiple segments, the switch must be configured with a global unicast address. A link-local address must be manually configured, but a global unicast address can either be manually configured or dynamically assigned. PATH Configuration, System, IPv6 USAGE GUIDELINES All IPv6 addresses must be formatted according to RFC 2373 "IPv6 Addressing Architecture," using 8 colon-separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields. When configuring a link-local address, note that the prefix length is fixed at 64 bits, and the host portion of the default address is based on the modified EUI-64 (Extended Universal Identifier) form of the interface identifier (i.e., the physical MAC address). You can manually configure a link-local address by entering the full address with the network prefix FE80. To connect to a larger network with multiple subnets, you must configure a global unicast address.
There are several alternatives to configuring this address type: 44 CHAPTER 4 | Configuring the Switch Setting an IP Address The global unicast address can be automatically configured by taking the network prefix from router advertisements observed on the local interface, and using the modified EUI-64 form of the interface identifier to automatically create the host portion of the address. This option can be selected by enabling the Auto Configuration option. You can also manually configure the global unicast address by entering the full address and prefix length. The management VLAN to which the IPv6 address is assigned must be specified on the IP Configuration page. See "Setting an IPv4 Address" on page 42.
PARAMETERS These parameters are displayed: Auto Configuration Enables stateless autoconfiguration of IPv6 addresses on an interface and enables IPv6 functionality on the interface. The network portion of the address is based on prefixes received in IPv6 router advertisement messages, and the host portion is automatically generated using the modified EUI-64 form of the interface identifier; i.e., the switch's MAC address. (Default: Disabled) Address Manually configures a global unicast address by specifying the full address and network prefix length (in the Prefix field).
(Default: ::192.168.2.10) Prefix Defines the prefix length as a decimal value indicating how many contiguous bits (starting at the left) of the address comprise the prefix; i.e., the network portion of the address. (Default: 96 bits) Note that the default prefix length of 96 bits specifies that the first six colon-separated values comprise the network portion of the address. Router Sets the IPv6 address of the default next hop router. An IPv6 default gateway must be defined if the management station is located in a different IPv6 segment. An IPv6 default gateway can only be successfully set when a network interface that directly connects to the gateway has been configured on the switch.

WEB INTERFACE To configure an IPv6 address: 1. Click Configuration, System, IPv6. 2. Specify the IPv6 settings. The information shown below provides a example of how to manually configure an IPv6 address. 3. Click Save. 45 CHAPTER 4 | Configuring the Switch Configuring NTP Service Figure 5: IPv6 Configuration CONFIGURING NTP SERVICE Use the NTP Configuration page to specify the Network Time Protocol (NTP) servers to query for the current time.

NTP allows the switch to set its internal clock based on periodic updates from an NTP time server. Maintaining an accurate time on the switch enables the system log to record meaningful dates and times for event entries.

If the clock is not set, the switch will only record the time from the factory default set at the last bootup. When the NTP client is enabled, the switch periodically sends a request for a time update to a configured time server. You can configure up to five time server IP addresses. The switch will attempt to poll each server in the configured sequence. PATH Configuration, System, NTP PARAMETERS These parameters are displayed: Mode Enables or disables NTP client requests.

Server Sets the IPv4 or IPv6 address for up to five time servers. The switch attempts to update the time from the first server, if this fails it attempts an update from the next server in the sequence. The polling interval is fixed at 15 minutes. WEB INTERFACE To configure the NTP servers: 1. Click Configuration, System, NTP.

2. Enter the IP address of up to five time servers. 3. Click Save. 46 CHAPTER 4 | Configuring the Switch Configuring Remote Log Messages Figure 6: NTP Configuration CONFIGURING REMOTE LOG MESSAGES Use the System Log Configuration page to send log messages to syslog servers or other management stations. You can also limit the event messages sent to specified types. PATH Configuration, System, Log COMMAND USAGE When remote logging is enabled, system log messages are sent to the designated server. The syslog protocol is based on UDP and received on UDP port 514. UDP is a connectionless protocol and does not provide acknowledgments. The syslog packet will always be sent out even if the syslog server does not exist.

PARAMETERS These parameters are displayed: Server Mode Enables/disables the logging of debug or error messages to the remote logging process. (Default: Disabled) Server Address Specifies the IPv4 address or alias of a remote server which will be sent syslog messages. Syslog Level Limits log messages that are sent to the remote syslog server for the specified types. Messages options include the following: Info Send informations, warnings and errors. (Default setting) Warning Send warnings and errors. Error Send errors. 47 CHAPTER 4 | Configuring the Switch Configuring Power Reduction WEB INTERFACE To configure the logging of error messages to remote servers: 1. Click Configuration, System, Log. 2. Enable remote logging, enter the IP address of the remote server, and specify the type of syslog messages to send.

3. Click Apply. Figure 7: Configuring Settings for Remote Logging of Error Messages CONFIGURING POWER REDUCTION The switch provides power saving methods including controlling the intensity of LEDs, and powering down the circuitry for port queues when not in use. CONTROLLING LED Use the LED Power Reduction Configuration page to reduces LED intensity INTENSITY during specified hours. PATH Configuration, Power Reduction, LED COMMAND USAGE The LEDs power consumption can be reduced by lowering the intensity.

LED intensity could for example be lowered during night time, or turned completely off. It is possible to set the LEDs intensity for each of the 24 hours of the day. When a network administrator performs maintenance of the switch (e.g., adding or moving users) he might want to have full LED intensity during the maintenance period.

Therefore it is possible to specify set the LEDs at full intensity for a specific period of time. Maintenance time is the number of seconds that the LEDs are set to full intensity after a port changes link state. 48 CHAPTER 4 | Configuring the Switch Configuring Power Reduction PARAMETERS These parameters are displayed: LED Intensity Timers Time Time at which LED intensity is set. Intensity LED intensity (Range: 0-100%, in increments of 10%, where 0% means off and 100% means full power) Maintenance On time at link change LEDs set at full intensity for a specified period when a link change occurs. (Default: 10 seconds) On at errors LEDs set at full intensity when a link error occurs. WEB INTERFACE To configure LED intensity: 1. Click Configuration, Power Reduction, LED. 2. Set LED intensity for any required hour of the day. Click Add Time to set additional entries.

3. Set the duration of full intensity when a link change occurs. 4. Specify whether or not to use full intensity when a link error occurs. 5. Click Apply. Figure 8: Configuring LED Power Reduction 49 CHAPTER 4 | Configuring the Switch Configuring Power Reduction REDUCING POWER TO Use the EEE Configuration page to configure Energy Efficient Ethernet IDLE QUEUE CIRCUITS (EEE) for specified queues, and to specify urgent queues which are to PATH Configuration, Power Reduction, EEE transmit data after maximum latency expires regardless of queue length. COMMAND USAGE EEE works by powering down circuits when there is no traffic. When a port gets data to be transmitted all relevant circuits are powered up. The time it takes to power up the circuits is call the wakeup time.

The default wakeup time is 17 µs for 1 Gbps links and 30 µs for other link speeds. EEE devices must agree upon the value of the wakeup time in order 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 the device wakeup time using LLDP protocol. To maximize power savings, the circuit is not started as soon as data is ready to be transmitted from a port, but instead waits until 3000 bytes of data is queued at the port. To avoid introducing a large delay when the queued data is less then 3000 bytes, data is always transmitted after 48 µs, giving a maximum latency of 48 µs plus the wakeup time.

If required, it is possible to minimize the latency for specific frames by mapping the frames to a specific queue (EEE Urgent Queues). When an urgent queue gets data to be transmitted, the circuits will be powered up at once and the latency will be reduced to the wakeup time. PARAMETERS These parameters are displayed: Port Port identifier. EEE Enabled Enables or disables EEE for the specified port. EEE Urgent Queues Specifies which are to transmit data after the maximum latency expires regardless queue length.

WEB INTERFACE To configure the power reduction for idle queue circuits: 1. Click Configuration, Power Reduction, EEE. 2. Select the circuits which will use EEE. 3. If required, also specify urgent queues which will be powered up once data is queued and the default wakeup time has passed. 4. Click Save. 50 CHAPTER 4 | Configuring the Switch Configuring Thermal Protection Figure 9: Configuring EEE Power Reduction CONFIGURING THERMAL PROTECTION Use the Thermal Protection Configuration page to set temperature priority levels, and assign those priorities for port shut-down if exceeded.

PATH Configuration, Thermal Protection COMMAND USAGE Thermal protection is used to protect the switch ASIC from overheating.

When the internal temperature of the switch exceeds a specified protection level, ports can be turned off to decrease power consumption. Port shut down can be prioritized based on assigned temperatures. PARAMETERS These parameters are displayed: Temperature settings for priority groups Priority A priority assigned to a specific temperature. (Range: 0-3) Temperature The temperature at which the ports with the corresponding priority will be turned off. (Range: 0-255° C) Port priorities Port Port identifier. Priority The priority level at which to shut down a port. (Range: 0-3) 51 CHAPTER 4 | Configuring the Switch Configuring Port Connections WEB INTERFACE To configure the thermal protection: 1. Click Configuration, Thermal Protection. 2. Select the circuits which will use EEE.

3. Se the temperature threshold for each priority, and then assign a priority level to each of the ports. 4. Click Save. Figure 10: Configuring Thermal Protection CONFIGURING PORT CONNECTIONS Use the Port Configuration page to configure the connection parameters for each port.

This page includes options for enabling auto-negotiation or manually setting the speed and duplex mode, enabling flow control, setting the maximum frame size, specifying the response to excessive collisions, or enabling power saving mode. PATH Configuration, Ports PARAMETERS These parameters are displayed: Link Indicates if the link is up or down. 52 CHAPTER 4 | Configuring the Switch Configuring Port Connections Speed Sets the port speed and duplex mode using auto-negotiation or manual selection. The following options are supported: Disabled - Disables the interface. You can disable an interface due to abnormal behavior (e.

g., excessive collisions), and then reenable it after the problem has been resolved. You may also disable an interface for security reasons. Auto - Enables auto-negotiation. When using auto-negotiation, the optimal settings will be negotiated between the link partners based on their advertised capabilities. 1Gbps FDX - Supports 1 Gbps full-duplex operation 100Mbps FDX - Supports 100 Mbps full-duplex operation 100Mbps HDX - Supports 100 Mbps half-duplex operation 10Mbps FDX - Supports 10 Mbps full-duplex operation 10Mbps HDX - Supports 10 Mbps half-duplex operation (Default: Autonegotiation enabled; Advertised capabilities for RJ-45: 1000BASE-T - 10half, 10full, 100half, 100full, 1000full; SFP: 1000BASE-SX/LX/LH - 1000full) NOTE: The 1000BASE-T standard does not support forced mode. Autonegotiation should always be used to establish a connection over any 1000BASE-T port or trunk. If not used, the success of the link process cannot be guaranteed when connecting to other types of switches. Flow Control Flow control can eliminate frame loss by "blocking" traffic from end stations or segments connected directly to the switch when its buffers fill. When enabled, back pressure is used for halfduplex operation and IEEE 802.

3-2005 (formally IEEE 802.3x) for fullduplex operation. (Default: Disabled) When auto-negotiation is used, this parameter indicates the flow control capability advertised to the link partner. When the speed and duplex mode are manually set, the Current Rx field indicates whether pause frames are obeyed by this port, and the Current Tx field indicates if pause frames are transmitted from this port. Avoid using flow control on a port connected to a hub unless it is actually required to solve a problem. Otherwise back pressure jamming signals may degrade overall performance for the segment attached to the hub. Maximum Frame Size Sets the maximum transfer unit for traffic crossing the switch. Packets exceeding the maximum frame size are dropped. (Range: 9600-1518 bytes; Default: 9600 bytes) Excessive Collision Mode Sets the response to take when excessive transmit collisions are detected on a port. Discard - Discards a frame after 16 collisions (default).

Restart - Restarts the backoff algorithm after 16 collisions. 53 CHAPTER 4 | Configuring the Switch Configuring Port Connections Power Control Adjusts the power provided to ports based on the length of the cable used to connect to other devices. Only sufficient power is used to maintain connection requirements. IEEE 802.3 defines the Ethernet standard and subsequent power requirements based on cable connections operating at 100 meters. Enabling power saving mode can significantly reduce power used for cable lengths of 20 meters or less, and continue to ensure signal integrity. The following options are supported: Disabled All power savings mechanisms disabled (default). Enabled Both link up and link down power savings enabled. ActiPHY Link down power savings enabled. PerfectReach Link up power savings enabled.

WEB INTERFACE To configure port connection settings: 1. Click Configuration, Ports. 2. Make any required changes to the connection settings. 3. Click Save. Figure 11: Port Configuration 54 CHAPTER 4 | Configuring the Switch Configuring Security CONFIGURING SECURITY You can configure this switch to authenticate users logging into the system for management access or to control client access to the data ports. Management Access Security (Switch menu) Management access to the switch can be controlled through local authentication of user names and passwords stored on the switch, or remote authentication of users via a RADIUS or TACACS+ server. Additional authentication methods includes Secure Shell (SSH), Secure Hypertext Transfer Protocol (HTTPS) over the Secure Socket Layer (SSL), static configuration of client addresses, and SNMP. General Security Measures (Network menu) This switch supports many methods of segregating traffic for clients attached to each of the data ports, and for ensuring that only authorized clients gain access to the network.

Private VLANs and port-based authentication using IEEE 802.1X are commonly used for these purposes. In addition to these methods, several other options of providing client security are supported by this switch. These include limiting the number of users accessing a port. The addresses assigned to DHCP clients can also be carefully controlled using static or dynamic bindings with DHCP Snooping and IP Source Guard commands. ARP Inspection can also be used to validate the MAC address bindings for ARP packets, providing protection against ARP traffic with invalid MAC to IP address bindings, which forms the basis for "man-in-themiddle" attacks. CONFIGURING USER Use the User Configuration page to control management access to the ACCOUNTS switch based on manually configured user names and passwords. PATH Configuration, Security, Switch, Users COMMAND USAGE The default guest name is "guest" with the password "guest.

" The default administrator name is "admin" with the password "admin." The guest only has read access for most configuration parameters. However, the administrator has write access for all parameters governing the onboard agent. You should therefore assign a new administrator password as soon as possible, and store it in a safe place. The administrator has a privilege level of 15, with access to all process groups and full control over the device. If the privilege level is set to any other value, the system will refer to each group privilege level. The user's privilege should be same or greater than the group privilege level to have the access of a group.

By default, most of the group privilege levels are set to 5 which provides read-only access and privilege level 10 which also provides read/write access. To perform system maintenance (software upload, factory defaults, etc.) the user's privilege level should be set to 15. Generally, the privilege level 15 can 55 CHAPTER 4 | Configuring the Switch Configuring Security be used for an administrator account, privilege level 10 for a standard user account, and privilege level 5 for a guest account. PARAMETERS These parameters are displayed: User Name The name of the user.

(Maximum length: 8 characters; maximum number of users: 16) Password Specifies the user password. (Range: 0-8 characters plain text, case sensitive) Password (again) Re-type the string entered in the previous field to ensure no errors were made. The switch will not change the password if these two fields do not match. Privilege Level Specifies the user level. (Options: 1 - 15) Access to specific functions are controlled through the Privilege Levels configuration page (see page 57). The default settings provide four access levels: 1 Read access of port status and statistics. 5 Read access of all system functions except for maintenance and debugging 10 read and write access of all system functions except for maintenance and debugging 15 read and write access of all system functions including maintenance and debugging. WEB INTERFACE To show user accounts: 1. Click Configuration, System, Switch, Users. Figure 12: Showing User Accounts To configure a user account: 1.

Click Configuration, System, Switch, Users. 2. Click "Add new user." 3. Enter the user name, password, and privilege level. 4. Click Save. 56 CHAPTER 4 | Configuring the Switch Configuring Security Figure 13: Configuring User Accounts CONFIGURING USER Use the Privilege Levels page to set the privilege level required to read or PRIVILEGE LEVELS configure specific software modules or system settings. PATH Configuration, Security, Switch, Privilege Levels PARAMETERS These parameters are displayed: Group Name The name identifying a privilege group. In most cases, a privilege group consists of a single module (e.

g., LACP, RSTP or QoS), but a few groups contains more than one module. The following describes the groups which contain multiple modules or access to various system settings: System: Contact, Name, Location, Timezone, Log. Security: Authentication, System Access Management, Port (contains Dot1x port, MAC based and the MAC Address Limit), ACL, HTTPS, SSH, ARP Inspection, and IP source guard. IP: Everything except for ping.

Port: Everything except for VeriPHY. Diagnostics: ping and VeriPHY. Maintenance: CLI - System Reboot, System Restore Default, System Password, Configuration Save, Configuration Load and Firmware Load. Web - Users, Privilege Levels and everything in Maintenance. Debug: Only present in CLI. Privilege levels Every privilege level group can be configured to access the following modules or system settings: Configuration Readonly, Configuration/Execute Read-write, Status/Statistics Read-only, and Status/Statistics Read-write (e.g., clearing statistics). The default settings provide four access levels: 1 Read access of port status and statistics. 57 CHAPTER 4 | Configuring the Switch Configuring Security 5 Read access of all system functions except for maintenance and debugging 10 read and write access of all system functions except for maintenance and debugging 15 read and write access of all system functions including maintenance and debugging. WEB INTERFACE To configure privilege levels: 1. Click Configuration, Security, Switch, Privilege Levels. 2. Set the required privilege level for any software module or functional group. 3.

Click Save. Figure 14: Configuring Privilege Levels 58 CHAPTER 4 | Configuring the Switch Configuring Security CONFIGURING THE AUTHENTICATION METHOD FOR MANAGEMENT ACCESS Use the Authentication Method Configuration page to specify the authentication method for controlling management access through the console, Telnet, SSH or HTTP/HTTPS. Access can be based on the (local) user name and password configured on the switch, or can be controlled with a RADIUS or TACACS+ remote access authentication server. Note that the RADIUS servers used to authenticate client access for IEEE 802.1X port authentication are also configured on this page (see page 77). Remote Authentication Dial-in User Service (RADIUS) and Terminal Access Controller Access Control System Plus (TACACS+) are logon authentication protocols that use software running on a central server to control access to RADIUS-aware or TACACS-aware devices on the network. An authentication server contains a database of multiple user name/password pairs with associated privilege levels for each user that requires management access to the switch. Figure 15: Authentication Server Operation Web RADIUS/ TACACS+ server 1. Client attempts management access. 2.

Switch contacts authentication server . 3. Authentication server challenges client. 4. Client responds with proper password or .

key 5. Authentication server approves access. 6. Switch grants management access. PATH Configuration, Security, Switch, Auth Method USAGE GUIDELINES The switch supports the following authentication services: Authorization of users that access the Telnet, SSH, the web, or console management interfaces on the switch.

Accounting for users that access the Telnet, SSH, the web, or console management interfaces on the switch. Accounting for IEEE 802.1X authenticated users that access the network through the switch. This accounting can be used to provide reports, auditing, and billing for services that users have accessed. By default, management access is always checked against the authentication database stored on the local switch. If a remote authentication server is used, you must specify the authentication method and the corresponding parameters for the remote authentication protocol on the Network Access Server Configuration page. Local and remote logon authentication can be used to control 59 CHAPTER 4 | Configuring the Switch Configuring Security management access via Telnet, SSH, a web browser, or the console interface.