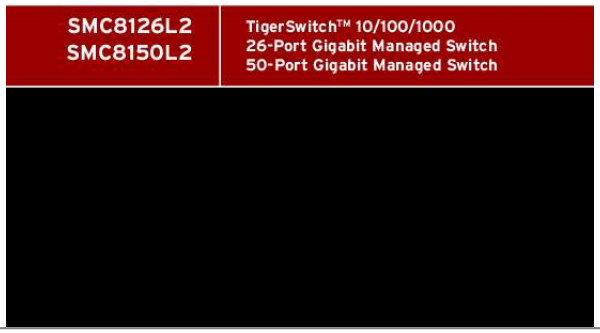
SMC Networks | MANAGEMENT GUIDE



Manual abstract:

@@@@SMC reserves the right to change specifications at any time without notice. Copyright © 2007 by SMC Networks, Inc. 20 Mason Irvine, CA 92618 All rights reserved. Printed in Taiwan Trademarks: SMC is a registered trademark; and EZ Switch, TigerStack and TigerSwitch are trademarks of SMC Networks, Inc. Other product and company names are trademarks or registered trademarks of their respective holders. Contents Chapter 1: Introduction Key Features Description of Software Features System Defaults Chapter 2: Initial Configuration Connecting to the Switch Configuration Options Required Connections Remote Connections Basic Configuration Console Connection Setting Passwords Setting an IP Address Manual Configuration Dynamic Configuration Enabling SNMP Management Access Community Strings (for SNMP version 1 and 2c clients) Trap Receivers Configuring Access for SNMP Version 3 Clients Saving Configuration Settings Managing System Files Chapter 3: Configuring the Switch Using the Web Interface Navigating the Web Browser Interface Home Page Configuration Options Panel Display Main Menu Basic Configuration Displaying System Information Displaying Switch Hardware/Software Versions Displaying Bridge Extension Capabilities Setting the Switch's IP Address Manual Configuration Using DHCP/BOOTP Enabling Jumbo Frames Managing Firmware Downloading System Software from a Server 1-1 1-1 1-2 1-6 2-1 2-1 2-1 2-2 2-3 2-3 2-3 2-4 2-4 2-4 2-5 2-6 2-6 2-7 2-8 2-8 2-9 3-1 3-1 3-2 3-2 3-3 3-3 3-4 3-10 3-10 3-11 3-13 3-14 3-15 3-16 3-17 3-17 3-18 i Contents Saving or Restoring Configuration Settings Downloading Configuration Settings from a Server Console Port Settings Telnet Settings Configuring Event Logging Displaying Log Messages System Log Configuration Remote Log Configuration Simple Mail Transfer Protocol Renumbering the System Resetting the System Setting the System Clock Configuring SNTP Setting the Time Zone Simple Network Management Protocol Setting Community Access Strings Specifying Trap Managers and Trap Types Enabling SNMP Agent Status Configuring SNMPv3 Management Access Setting the Local Engine ID Specifying a Remote Engine ID Configuring SNMPv3 Users Configuring Remote SNMPv3 Users Configuring SNMPv3 Groups Setting SNMPv3 Views User Authentication Configuring User Accounts Configuring Local/Remote Logon Authentication Configuring HTTPS Replacing the Default Secure-site Certificate Configuring the Secure Shell Configuring the SSH Server Generating the Host Key Pair Configuring Port Security Configuring 802.1X Port Authentication Displaying 802.1X Global Settings Configuring 802.1X Global Settings Configuring Port Settings for 802.1X Displaying 802.

1X Statistics Access Control Lists Configuring Access Control Lists Setting the ACL Name and Type Configuring a Standard IP ACL Configuring an Extended IP ACL Configuring a MAC ACL ii 3-19 3-20 3-21 3-23 3-25 3-25 3-26 3-27 3-28 3-30 3-30 3-31 3-31 3-32 3-33 3-33 3-34 3-35 3-36 3-36 3-37 3-37 3-40 3-41 3-45 3-46 3-46 3-48 3-52 3-53 3-54 3-56 3-57 3-59 3-60 3-61 3-62 3-63 3-66 3-67 3-67 3-68 3-69 3-69 3-72 Contents Binding a Port to an Access Control List Filtering IP Addresses for Management Access Port Configuration Displaying Connection Status Configuring Interface Connections Creating Trunk Groups Statically Configuring a Trunk Enabling LACP on Selected Ports Configuring LACP Parameters Displaying LACP Port Counters Displaying LACP Settings and Status for the Local Side Displaying LACP Settings and Status for the Remote Side Setting Broadcast Storm Thresholds Configuring Port Mirroring Configuring Rate Limits Rate Limit Configuration Showing Port Statistics Address Table Settings Setting Static Addresses Displaying the Address Table Changing the Aging Time Spanning Tree Algorithm Configuration Displaying Global Settings Configuring Global Settings Displaying Interface Settings Configuring Interface Settings Configuring Multiple Spanning Trees Displaying Interface Settings for MSTP Configuring Interface Settings for MSTP VLAN Configuration IEEE 802.1Q VLANs Enabling or Disabling GVRP (Global Setting) Displaying Basic VLAN Information Displaying Current VLANs Creating VLANs Adding Static Members to VLANs (VLAN Index) Adding Static Members to VLANs (Port Index) Configuring VLAN Behavior for Interfaces Configuring IEEE 802.1Q Tunneling Enabling QinQ Tunneling on the Switch Adding an Interface to a QinQ Tunnel Configuring Private VLANs Enabling Private VLANs Configuring Uplink and Downlink Ports Protocol VLANs 3-73 3-74 3-76 3-76 3-78 3-80 3-81 3-82 3-84 3-86 3-88 3-90 3-91 3-93 3-94 3-94 3-95 3-99 3-99 3-100 3-102 3-102 3-105 3-107 3-111 3-114 3-116 3-118 3-120 3-122 3-122 3-125 3-126 3-126 3-128 3-129 3-131 3-132 3-133 3-137 3-138 3-141 3-141 3-142 3-142 iii Contents Protocol VLAN Group Configuration Configuring Protocol VLAN Interfaces Class of Service Configuration Layer 2 Queue Settings Setting the Default Priority for Interfaces Mapping CoS Values to Egress Queues Enabling CoS Selecting the Queue Mode Setting the Service Weight for Traffic Classes Layer 3/4 Priority Settings Mapping Layer 3/4 Priorities to CoS Values Selecting IP Precedence/DSCP Priority Mapping IP Precedence Mapping DSCP Priority Mapping IP Port Priority Quality of Service Configuring Quality of Service Parameters Configuring a Class Map Creating QoS Policies Attaching a Policy Map to Ingress Queues Multicast Filtering Layer 2 IGMP (Snooping and Query) Configuring IGMP Snooping and Query Parameters Enabling IGMP Immediate Leave Displaying Interfaces Attached to a Multicast Router Specifying Static Interfaces for a Multicast Router Displaying Port Members of Multicast Services Assigning Ports to Multicast Services IGMP Filtering and Throttling Enabling IGMP Filtering and Throttling Configuring IGMP Filtering and Throttling for Interfaces Configuring IGMP Filter Profiles Multicast VLAN Registration Configuring Global MVR Settings Displaying MVR Interface Status Displaying Port Members of Multicast Groups Configuring MVR Interface Status Assigning Static Multicast Groups to Interfaces Configuring Domain Name Service Configuring General DNS Service Parameters Configuring Static DNS Host to Address Entries Displaying the DNS Cache DHCP Snooping DHCP Snooping Configuration DHCP Snooping VLAN Configuration iv 3-142 3-143 3-144 3-144 3-144 3-145 3-147 3-147 3-148 3-149 3-149 3-149 3-150 3-152 3-153 3-154 3-155 3-155 3-158 3-161 3-162 3-162 3-163 3-164 3-165 3-166 3-167 3-168 3-169 3-170 3-171 3-172 3-174 3-175 3-176 3-178 3-179 3-180 3-181 3-181 3-183 3-185 3-186 3-187 3-188 Contents DHCP Snooping Information Option Configuration DHCP Snooping Port Configuration DHCP Snooping Binding Information IP Source Guard IP Source Guard Port Configuration Static IP Source Guard Binding Configuration Dynamic IP Source Guard Binding Information Switch Clustering Cluster Configuration Cluster Member Configuration Cluster Member Information Cluster Candidate Information Chapter 4: Command Line Interface Using the Command Line Interface Accessing the CLI Console Connection Telnet Connection Entering Commands Keywords and Arguments Minimum Abbreviation Command Completion Getting Help on Commands Showing Commands Partial Keyword Lookup Negating the Effect of Commands Using Command History Understanding Command Modes Exec Commands Configuration Commands Command Line Processing Command Groups Line Commands line login password timeout login response exec-timeout password-thresh silent-time databits parity speed stopbits 3-188 3-189 3-190 3-191 3-191 3-192 3-193 3-194 3-195 3-196 3-197 3-198 4-1 4-1 4-1 4-1 4-2 4-3 4-3 4-3 4-3 4-3 4-4 4-5 4-5 4-5 4-5 4-6 4-7 4-8 4-9 4-10 4-11 4-11 4-12 4-13 4-13 4-14 4-15 4-15 4-16 4-17 4-17 v Contents disconnect show line General Commands enable disable configure show history reload end exit quit System Management Commands Device Designation Commands prompt hostname User Access Commands username enable password IP Filter Commands management show management Web Server Commands ip http port ip http server ip http secure-server ip http secure-port Telnet Server Commands ip telnet port ip telnet server Secure Shell Commands ip ssh server ip ssh timeout ip ssh authentication-retries ip ssh server-key size delete public-key ip ssh crypto host-key generate ip ssh crypto zeroize ip ssh save host-key show ip ssh show ssh show public-key Event Logging Commands logging on logging history logging host vi 4-18 4-18 4-19 4-19 4-20 4-21 4-21 4-22 4-22 4-23 4-23 4-24 4-24 4-24 4-25 4-25 4-25 4-26 4-27 4-27 4-28 4-29 4-29 4-30 4-30 4-31 4-32 4-32 4-33 4-33 4-35 4-36 4-37 4-37 4-38 4-38 4-39 4-39 4-40 4-40 4-41 4-43 4-43 4-44 4-45 Contents logging facility logging trap clear logging show logging show log SMTP Alert Commands logging sendmail host logging sendmail level logging sendmail source-email logging sendmail destination-email logging sendmail show logging sendmail Time Commands sntp client sntp server sntp poll show sntp clock timezone calendar set show calendar System Status Commands show startup-config show running-config show system show users show version Frame Size Commands jumbo frame Flash/File Commands copy delete dir whichboot boot system Authentication Commands Authentication Sequence authentication login authentication enable RADIUS Client radius-server host radius-server port radius-server key radius-server retransmit radius-server timeout show

radius-server 4-45 4-46 4-46 4-47 4-48 4-49 4-49 4-50 4-51 4-51 4-52 4-52 4-53 4-53 4-54 4-55 4-55 4-56 4-56 4-57 4-57 4-57 4-59 4-61 4-61 4-62 4-63 4-63 4-64 4-64 4-67 4-68 4-69 4-69 4-70 4-70 4-71 4-72 4-73 4-74 4-74 4-75 4-75 4-76 4-76 vii Contents TACACS+ Client tacacs-server host tacacs-server port tacacs-server key show tacacs-server Port Security Commands port security 802.

1X Port Authentication dot1x system-auth-control dot1x default dot1x max-req dot1x port-control dot1x operation-mode dot1x re-authenticate dot1x re-authentication dot1x timeout quiet-period dot1x timeout re-authperiod dot1x timeout tx-period show dot1x Access Control List Commands IP ACLs access-list ip permit, deny (Standard ACL) permit, deny (Extended ACL) show ip access-list ip access-group show ip access-group MAC ACLs access-list mac permit, deny (MAC ACL) show mac access-list mac access-group show mac access-group ACL Information show access-list show access-group SNMP Commands snmp-server show snmp snmp-server community snmp-server contact snmp-server location snmp-server host snmp-server enable traps snmp-server engine-id viii 4-77 4-77 4-77 4-78 4-78 4-79 4-79 4-81 4-81 4-82 4-82 4-82 4-83 4-84 4-84 4-84 4-85 4-85 4-86 4-89 4-90 4-90 4-91 4-91 4-93 4-93 4-94 4-95 4-95 4-96 4-97 4-98 4-98 4-99 4-99 4-99 4-100 4-101 4-101 4-102 4-103 4-103 4-104 4-106 4-107 Contents show snmp engine-id snmp-server view show snmp view snmp-server group show snmp group snmp-server user show snmp user Interface Commands interface description speed-duplex negotiation capabilities flowcontrol shutdown switchport broadcast packet-rate clear counters show interfaces status show interfaces counters show interfaces switchport Mirror Port Commands port monitor show port monitor Rate Limit Commands rate-limit Link Aggregation Commands channel-group lacp lacp system-priority lacp admin-key (Ethernet Interface) lacp admin-key (Port Channel) lacp port-priority show lacp Address Table Commands mac-address-table static clear mac-address-table dynamic show mac-address-table mac-address-table aging-time show mac-address-table aging-time Spanning Tree Commands spanning-tree spanning-tree mode spanning-tree forward-time spanning-tree hello-time spanning-tree max-age 4-108 4-109 4-110 4-110 4-112 4-113 4-115 4-116 4-116 4-117 4-117 4-118 4-119 4-120 4-121 4-122 4-122 4-123 4-124 4-125 4-127 4-127 4-128 4-129 4-129 4-130 4-131 4-132 4-133 4-134 4-135 4-136 4-136 4-140 4-140 4-141 4-141 4-142 4-143 4-144 4-145 4-145 4-146 4-147 4-148 ix Contents spanning-tree priority spanning-tree pathcost method spanning-tree transmission-limit spanning-tree mst-configuration mst vlan mst priority name revision max-hops spanning-tree spanning-disabled spanning-tree cost spanning-tree port-priority spanning-tree edge-port spanni Problems Accessing the Management Interface Using System Logs Glossary Index 4-238 4-239 4-239 4-240 4-240 4-241 4-241 4-242 A-1 A-1 A-2 A-2 A-3 B-1 B-1 B-2 xiii Contents xiv Tables Table 1-1 Table 1-2 Table 3-1 Table 3-2 Table 3-3 Table 3-4 Table 3-5 Table 3-6 Table 3-7 Table 3-8 Table 3-9 Table 3-10 Table 3-11 Table 3-12 Table 3-13 Table 3-14 Table 4-1 Table 4-2 Table 4-3 Table 4-4 Table 4-5 Table 4-6 Table 4-7 Table 4-8 Table 4-9 Table 4-10 Table 4-11 Table 4-12 Table 4-13 Table 4-14 Table 4-15 Table 4-16 Table 4-17 Table 4-18 Table 4-19 Table 4-20 Table 4-21 Table 4-22 Table 4-23 Table 4-24 Table 4-25 Table 4-26 Key Features System Defaults Configuration Options Main Menu Logging Levels Supported Notification Messages HTTPS System Support 802.1X Statistics LACP Port Counters LACP Internal Configuration Information LACP Neighbor Configuration Information Port Statistics Mapping CoS Values to Egress Queues CoS Priority Levels Mapping IP Precedence Mapping DSCP Priority Values Command Modes Configuration Modes Command Line Processing Command Groups Line Commands General Commands System Management Commands Device Designation Commands User Access Commands Default Login Settings IP Filter Commands Web Server Commands HTTPS System Support Telnet Server Commands SSH Commands show ssh - display description Event Logging Commands Logging Levels show logging flash/ram - display description show logging trap - display description SMTP Alert Commands Time Commands System Status Commands Frame Size Commands Flash/File Commands File Directory Information 1-1 1-6 3-3 3-4 3-26 3-41 3-52 3-66 3-86 3-88 3-90 3-95 3-145 3-146 3-150 3-152 4-6 4-7 4-8 4-9 4-10 4-19 4-24 4-24 4-25 4-26 4-27 4-29 4-31 4-32 4-33 4-40 4-43 4-44 4-47 4-48 4-49 4-53 4-57 4-63 4-64 4-68 xv Tables Table 4-27 Table 4-28 Table 4-29 Table 4-30 Table 4-31 Table 4-32 Table 4-33 Table 4-34 Table 4-35 Table 4-36 Table 4-37 Table 4-38 Table 4-39 Table 4-40 Table 4-41 Table 4-42 Table 4-43 Table 4-44 Table 4-45 Table 4-46 Table 4-47 Table 4-48 Table 4-49 Table 4-50 Table 4-51 Table 4-52 Table 4-53 Table 4-54 Table 4-55 Table 4-56 Table 4-57 Table 4-58 Table 4-58 Table 4-58 Table 4-58 Table 4-59 Table 4-60 Table 4-61 Table 4-62 Table 4-63 Table 4-64 Table 4-65 Table 4-66 Table 4-67 Table 4-68 xvi Authentication Commands Authentication Sequence RADIUS Client Commands TACACS Commands Port Security Commands 802.1X Port Authentication Access Control Lists IP ACLs MAC ACL Commands ACL Information SNMP Commands show snmp engine-id - display description show snmp view - display description show snmp group - display description show snmp user - display description Interface Commands Interfaces Switchport Statistics Mirror Port Commands Rate Limit Commands Link Aggregation Commands show lacp counters - display description show lacp internal - display description show lacp neighbors - display description show lacp sysid - display description Address Table Commands Spanning Tree Commands VLANs GVRP and Bridge Extension Commands Editing VLAN Groups Configuring VLAN Interfaces Show VLAN Commands Command Function Mode Page Private VLAN Commands Protocol-based VLAN Commands Priority Commands Priority Commands (Layer 2) Default CoS Values to Egress Queues Priority Commands (Layer 3 and 4) IP DSCP to CoS Vales Quality of Service Commands Multicast Filtering Commands IGMP Snooping Commands 4-70 4-70 4-73 4-77 4-79 4-81 4-89 4-90 4-95 4-99 4-100 4-108 4-110 4-113 4-115 4-116 4-126 4-127 4-129 4-130 4-137 4-138 4-139 4-139 4-140 4-144 4-163 4-163 4-167 4-169 4-175 4-176 4-176 4-176 4-176 4-179 4-181 4-184 4-184 4-187 4-189 4-190 4-193 4-201 4-201 Tables Table 4-69 Table 4-70 Table 4-71 Table 4-72 Table 4-73 Table 4-74 Table 4-75 Table 4-76 Table 4-77 Table 4-78 Table 4-79 Table B-1 IGMP Query Commands (Layer 2) Static Multicast Routing Commands IGMP Filtering and Throttling Commands Multicast VLAN Registration Commands show mvr - display description show mvr interface - display description show mvr members - display description IP Interface Commands IP Source Guard Commands DHCP Snooping Commands Switch Cluster Commands Troubleshooting Chart 4-206 4-209 4-211 4-217 4-221 4-222 4-222 4-223 4-227 4-231 4-237 B-1 xvii Tables xviii Figures Figure 3-1 Figure 3-2 Figure 3-3 Figure 3-4 Figure 3-5 Figure 3-6 Figure 3-7 Figure 3-8 Figure 3-9 Figure 3-10 Figure 3-11 Figure 3-12 Figure 3-13 Figure 3-14 Figure 3-15 Figure 3-16 Figure 3-17 Figure 3-18 Figure 3-19 Figure 3-20 Figure 3-21 Figure 3-22 Figure 3-23 Figure 3-24 Figure 3-25 Figure 3-26 Figure 3-27 Figure 3-28 Figure 3-29 Figure 3-30 Figure 3-31 Figure 3-32 Figure 3-33 Figure 3-34 Figure 3-35 Figure 3-36 Figure 3-37 Figure 3-38 Figure 3-39 Figure 3-40 Figure 3-41 Figure 3-42 Home Page Panel Display System Information Switch Information Bridge Extension Configuration Manual IP Configuration DHCP IP Configuration Bridge Extension Configuration Copy Firmware Setting the Startup Code Deleting Files Downloading Configuration Settings for Startup Setting the Startup Configuration Settings Console Port Settings Enabling Telnet Displaying Logs System Logs Remote Logs Enabling and Configuring SMTP Renumbering the System Resetting the System SNTP Configuration Setting the System Clock Configuring SNMP Community Strings Configuring IP Trap Managers Enabling SNMP Agent Status Setting an Engine ID Setting a Remote Engine ID Configuring SNMPv3 Users Configuring Remote SNMPv3 Users Configuring SNMPv3 Groups Configuring SNMPv3 Views Access Levels Authentication Settings HTTPS Settings SSH Server Settings SSH Host-Key Settings Configuring Port Security 802.

1X Global Information 802.1X Global Configuration 802.1X Port Configuration Displaying 802.1X Port Statistics 3-2 3-3 3-10 3-12 3-13 3-15 3-16 3-17 3-18 3-18 3-19 3-20 3-21 3-22 3-24 3-25 3-27 3-28 3-29 3-30 3-30 3-31 3-32 3-34 3-35 3-35 3-36 3-37 3-39 3-40 3-44 3-45 3-47 3-50 3-52 3-56 3-58 3-60 3-62 3-62 3-64 3-66 xix Figures Figure 3-43 Figure 3-44 Figure 3-45 Figure 3-46 Figure 3-47 Figure 3-48 Figure 3-49 Figure 3-50 Figure 3-51 Figure 3-52 Figure 3-53 Figure 3-54 Figure 3-55 Figure 3-56 Figure 3-57 Figure 3-58 Figure 3-59 Figure 3-60 Figure 3-61 Figure 3-62 Figure 3-63 Figure 3-64 Figure 3-65 Figure 3-66 Figure 3-67 Figure 3-68 Figure 3-69 Figure 3-70 Figure 3-71 Figure 3-72 Figure 3-73 Figure 3-74 Figure 3-75 Figure 3-76 Figure 3-77 Figure 3-78 Figure 3-79 Figure 3-80 Figure 3-81 Figure 3-82 Figure 3-83 Figure 3-84 Figure 3-85 Figure 3-86 Figure 3-87 xx Selecting ACL Type Configuring Standard IP ACLs Configuring Extended IP ACLs Configuring MAC ACLs Configuring ACL Port Binding Creating an IP Filter List Displaying Port/Trunk Information Port/Trunk Configuration Configuring Static Trunks LACP Trunk Configuration LACP Port Configuration LACP - Port Counters Information LACP - Port Internal Information LACP - Port Neighbors Information Port Broadcast Control Mirror Port Configuration Input Rate Limit Port Configuration Port Statistics Configuring a Static Address Table Configuring a Dynamic Address Table Setting the Address Aging Time Displaying Spanning Tree Information Configuring Spanning Tree Displaying Spanning Tree Port Information Configuring Spanning Tree per Port Configuring Multiple Spanning Trees Displaying MSTP Interface Settings Displaying MSTP Interface Settings Globally Enabling GVRP Displaying Basic VLAN Information Displaying Current VLANs Configuring a VLAN Static List Configuring a VLAN Static Table VLAN Static Membership by Port Configuring VLANs per Port 802. 1Q Tunnel Status Tunnel Port Configuration Private VLAN Status Private VLAN Link Status Protocol VLAN Configuration Protocol VLAN Port Configuration Port Priority Configuration Traffic Classes Enable Traffic Classes Queue Mode 3-68 3-69 3-71 3-73 3-74 3-75 3-77 3-79 3-81 3-83 3-85 3-87 3-89 3-90 3-92 3-93 3-94 3-98 3-100 3-101 3-102 3-106 3-110 3-113 3-115 3-117 3-119 3-122 3-125 3-126 3-127 3-129 3-131 3-131 3-133 3-137 3-139 3-141 3-142 3-143 3-143 3-145 3-146 3-147 3-148 Figures Figure 3-88 Figure 3-89 Figure 3-90 Figure 3-91 Figure 3-92 Figure 3-93 Figure 3-94 Figure 3-95 Figure 3-96 Figure 3-97 Figure 3-98 Figure 3-99 Figure 3-100 Figure 3-101 Figure 3-102 Figure 3-103 Figure 3-104 Figure 3-105 Figure 3-106 Figure 3-107 Figure 3-108 Figure 3-109 Figure 3-110 Figure 3-111 Figure 3-112 Figure 3-113 Figure 3-114 Figure 3-115 Figure 3-116 Figure 3-117 Figure 3-118 Figure 3-119 Figure 3-120 Figure 3-121 Figure 3-122 Figure 3-123 Figure 3-124 Figure 3-125 Figure 3-126 Configuring Queue Scheduling IP Precedence/DSCP Priority Status Mapping IP Precedence Priority Values Mapping IP DSCP Priority Values IP Port Priority Status IP Port Priority Configuring Class Maps Configuring Policy Maps Service Policy Settings IGMP Configuration IGMP Immediate Leave Displaying Multicast Router Port Information Static Multicast Router Port Configuration IP Multicast Registration Table IGMP Member Port Table Enabling IGMP Filtering and Throttling IGMP Filter and Throttling Port Configuration IGMP Profile Configuration MVR Global Configuration MVR Port Information MVR Group IP Information MVR Port Configuration MVR Group Member Configuration DNS General Configuration DNS Static Host Table DNS Cache DHCP Snooping Configuration DHCP Snooping VLAN Configuration DHCP Snooping Information Option Configuration DHCP Snooping Port Configuration DHCP Snooping Binding Information IP Source Guard Port Configuration Static IP Source Guard Binding Configuration Dynamic IP Source Guard Binding Information Cluster Member Choice Cluster Configuration Cluster Member Configuration Cluster Member Information Cluster Candidate Information 3-148 3-150 3-151 3-152 3-153 3-154 3-157 3-160 3-161 3-164 3-165 3-166 3-167 3-168 3-169 3-170 3-172 3-173 3-176 3-177 3-178 3-180 3-181 3-182 3-184 3-185 3-187 3-188 3-189 3-190 3-191 3-192 3-193 3-194 3-195 3-196 3-197 3-197 3-198 xxi Figures xxii Chapter 1: Introduction This switch provides a broad range of features for Layer 2 switching. It includes a management agent that allows you to configure the features listed in this manual. The default configuration can be used for most of the features provided by this switch. However, there are many options that you should configure to maximize the switch's performance for your particular network environment. Key Features Table 1-1 Key Features Feature Configuration Backup and Restore Authentication Description Backup to TFTP server Console, 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 Supports up to 128 ACLs, 96 MAC rules and 96 rules per system Supported Supported with Option 82 relay information Speed, duplex mode and flow control Input rate and output limiting per port One or more port mirrored to a single analysis port Supports up to 32 trunks using either static or dynamic trunking (LACP) Supported Up to 8K MAC addresses in the forwarding table Supports dynamic data switching and addresses learning Access Control Lists DHCP Client DHCP Snooping Port Configuration Rate Limiting Port Mirroring Port Trunking Broadcast Storm Control Static Address IEEE 802.1D Bridge Store-and-Forward Switching Supported to ensure wire-speed switching while eliminating bad frames Spanning Tree Algorithm Virtual LANs Traffic Prioritization Qualify of Service Multicast Filtering Supports standard STP, and Rapid Spanning Tree Protocol (RSTP) and Multiple Spanning Trees(MSTP) Up to 256 using IEEE 802.1Q, port-based, protocol-based or private VLANs Default port priority, traffic class map, queue scheduling, or Differentiated Services Code Point (DSCP), and TCP/UDP Port Supports Differentiated Services (DiffServ) Supports IGMP snooping and query, as well as Multicast VLAN Registration 1-1 1 Introduction Table 1-1 Key Features Feature Switch Clustering Description Supports up to 16 Member switches in a cluster Description of Software Features The switch provides a wide range of advanced performance enhancing features. Flow control eliminates the loss of packets due to bottlenecks caused by port saturation. Broadcast storm suppression prevents broadcast traffic storms from engulfing the network.

Port-based, private VLANs and protocol-based VLANs, plus support for automatic GVRP VLAN registration provide traffic security and efficient use of network bandwidth. CoS priority queueing ensures the minimum delay for moving real-time multimedia data across the network. While multicast filtering provides support for real-time network applications.

Some of the management features are briefly described below. Configuration Backup and Restore You can save the current configuration settings to a file on a TFTP server, and later download this file to restore the switch configuration settings. Authentication This switch authenticates management access via the console port, Telnet or web browser. User names and passwords can be configured locally or can be verified via a remote authentication server (i.e., RADIUS or TACACS+). Port-based authentication is also supported via the IEEE 802.

1X protocol. This protocol uses the Extensible Authentication Protocol over LANs (EAPOL) to request user credentials from the 802.1X client, and then verifies the client's right to access the network via an authentication server. Other authentication options include HTTPS for secure management access via the web, SSH for secure management access over a Telnet-equivalent connection, IP address filtering for SNMP/web/Telnet management access, and MAC address filtering for port access. Access Control Lists ACLs provide packet filtering for IP frames (based on address, protocol, or TCP/UDP port number) or any frames (based on MAC address or Ethernet type).

ACLs can be used to improve performance by blocking unnecessary network traffic or to implement security controls by restricting access to specific network resources or protocols. Port Configuration You can manually configure the speed, duplex mode, and flow control used on specific ports, or use auto-negotiation to detect the connection settings used by the attached device. Use the full-duplex mode on ports whenever possible to double the throughput of switch connections. Flow control should also be enabled to control network traffic during periods of congestion and prevent the loss of packets when port buffer thresholds are exceeded. The switch supports flow control based on the IEEE 802.

3x standard. 1-2 Description of Software Features 1 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 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 IEEE 802.3ad Link Aggregation Control Protocol (LACP). 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 32 trunks. Broadcast Storm Control Broadcast suppression prevents broadcast 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 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 8K addresses. Store-and-Forward Switching The switch copies each frame into its memory before forwarding them to 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 SMC8126L2 and SMC8150L2 provide 4 Mbits respectively for frame buffering. This buffer can queue packets awaiting transmission on congested networks. Spanning Tree Algorithm The switch supports these spanning tree protocols: Spanning Tree Protocol (STP, IEEE 802.1D) This protocol provides loop detection and recovery by allowing two or more redundant connections to be created between a pair of LAN segments.

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 3 to 5 seconds, compared to 30 1-3 1 Introduction 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). Virtual LANs The switch supports up to 256 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 dynamically learned via GVRP, or ports 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. Traffic Prioritization This switch prioritizes each packet based on the required level of service, 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 DSCP field in the IP frame.

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. 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, IP Precedence or 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. 1-4 Description of Software Features 1 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. 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. 1-5 1 Introduction 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 (page 3-19). The following table lists some of the basic system defaults. Table 1-2 System Defaults Function Console Port Connection Parameter Baud Rate Data bits Stop bits Parity Local Console Timeout Authentication Privileged Exec Level Normal Exec Level Default 9600 8 1 none 0 (disabled) Username "admin", Password "admin" Username "guest", Password "guest" Enable Privileged Exec from Normal Password "super" Exec Level 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 Port Number SNMP SNMP Agent Community Strings Traps SNMP V3 Disabled Disabled Disabled Enabled Disabled Disabled Disabled Enabled 80 Enabled 443 Enabled "public" (read only), "private" (read/write) Authentication traps: enabled Link-up-down events: enabled View: default view Group: public (read only) private (read/write) 1-6 System Defaults Table 1-2 System Defaults (Continued) Function Port Configuration Parameter Admin Status Auto-negotiation Flow Control Rate Limiting Port Trunking Input and output limits Static Trunks LACP (all ports) Broadcast Storm Protection Spanning Tree Algorithm Status Broadcast Limit Rate Status Fast Forwarding (Edge Port) Address Table Virtual LANs Aging Time Default VLAN PVID Acceptable Frame Type Ingress Filtering Switchport Mode (Egress Mode) GVRP (global) GVRP (port interface) Traffic Prioritization Ingress Port Priority Weighted Round Robin IP DSCP Priority IP Settings IP Address Subnet Mask Default Gateway DHCP BOOTP Multicast Filtering IGMP Snooping Multicast VLAN Registration Default Enabled Enabled Disabled Disabled None Disabled Enabled (all ports) 500 packets per second 1 Enabled, RSTP (Defaults: All values based on IEEE 802.1w) Disabled 300 seconds 1 1 All Enabled Hybrid: tagged/untagged frames Disabled Disabled 0 Queue: 0 1 2 3 Weight: 1 2 4 8 Disabled DHCP assigned, otherwise 192.168.1.1 255.255.255.

0 0.0.0.0 Client: Enabled Disabled Snooping: Enabled Querier: Enabled Disabled 1-7 1 Introduction Table 1-2 System Defaults (Continued) Function System Log Parameter Status Messages Logged Messages Logged to Flash Default Enabled Levels 0-7 (all) Levels 0-3 Enabled (but no server defined) Disabled Disabled Disabled (all ports) Enabled Disabled SMTP Email Alerts SNTP DHCP Snooping IP Source Guard Switch Clustering Event Handler Clock Synchronization Status Status Status Commander 1-8 Chapter 2: Initial Configuration Connecting to the Switch Configuration Options The switch includes a built-in network management agent. The agent offers a variety of management options, including SNMP, RMON (Groups 1, 2, 3, 9) and a web-based interface.

A PC may also be connected directly to the switch for configuration and monitoring via a command line interface (CLI). Note: The IP address for this switch is obtained via DHCP by default. To change this address, see "Setting an IP Address" on page 2-4. The switch's HTTP web agent allows you to configure switch parameters, monitor port connections, and display statistics using a standard web browser such as Netscape version 6.2 and higher or Microsoft IE version 5.

0 and higher. The switch's web management interface can be accessed from any computer attached to the network. The CLI program can be accessed by a direct connection to the RS-232 serial console port on the switch, or remotely by a Telnet connection over the network. The switch's management agent also supports SNMP (Simple Network Management Protocol). This SNMP agent permits the switch to be managed from any system in the network using network management software such as HP OpenView. The switch's web interface, CLI configuration program, and SNMP agent allow you to perform the following management functions: · · · · · · · · · · · · · · · Set user names and passwords Set an IP interface for a management VLAN Configure SNMP parameters Enable/disable any port Set the speed/duplex mode for any port Configure the bandwidth of any port by limiting input rates Control port access through IEEE 802.1X security or static address filtering Filter packets using Access Control Lists (ACLs) Configure up to 256 IEEE 802.1Q VLANs Enable GVRP automatic VLAN registration Configure IGMP multicast filtering Upload and download system firmware via TFTP Upload and download switch configuration files via TFTP Configure Spanning Tree parameters Configure Class of Service (CoS) priority queuing 2-1 2 · · · · Initial Configuration Configure up to 32 static or LACP trunks Enable port mirroring Set broadcast storm control on any port Display system information and statistics Required Connections The switch provides an RS-232 serial port that enables a connection to a PC or terminal for monitoring and configuring the switch.

A null-modem console cable is provided with the switch. Attach a VT100-compatible terminal, or a PC running a terminal emulation program to the switch.

You can use the console cable provided with this package, or use a null-modem cable that complies with the wiring assignments shown in the Installation Guide. To connect a terminal to the console port, complete the following steps: 1. Connect the console cable to the serial port on a terminal, or a PC running terminal emulation software, and tighten the captive retaining screws on the RS-232 connector. Connect the other end of the cable to the RS-232 serial port on the switch. Make sure the terminal emulation software is set as follows: · · · · · · Select the appropriate serial port (COM port 1 or COM port 2). Set the baud rate to 9600 bps. Set the data format to 8 data bits, 1 stop bit, and no parity. Set flow control to none. Set the emulation mode to VT100. When using HyperTerminal, select Terminal keys, not Windows keys.

2. 3. Notes: 1. Refer to "Line Commands" on page 4-10 for a complete description of console configuration options. 2.

Once you have set up the terminal correctly, the console login screen will be displayed. For a description of how to use the CLI, see "Using the Command Line Interface" on page 4-1. For a list of all the CLI commands and detailed information on using the CLI, refer to "Command Groups" on page 4-9. 2-2 Basic Configuration 2 Remote Connections Prior to accessing the switch's onboard agent via a network connection, you must first configure it with a valid IP address, subnet mask, and default gateway using a console connection, DHCP or BOOTP protocol. The IP address for this switch is obtained via DHCP by default.

To manually configure this address or enable dynamic address assignment via DHCP or BOOTP, see "Setting an IP Address" on page 2-4. Note: This switch supports four concurrent Telnet/SSH sessions. After configuring the switch's IP parameters, you can access the onboard configuration program from anywhere within the attached network. The onboard configuration program can be accessed using Telnet from any computer attached to the network. The switch can also be managed by any computer using a web browser (Internet Explorer 5.0 or above, or Netscape 6.2 or above), or from a network computer using SNMP network management software. Note: The onboard program only provides access to basic configuration functions. To access the full range of SNMP management functions, you must use SNMP-based network management software. Basic Configuration Console Connection The CLI program provides two different command levels -- normal access level (Normal Exec) and privileged access level (Privileged Exec).

The commands available at the Normal Exec level are a limited subset of those available at the Privileged Exec level and allow you to only display information and use basic utilities. To fully configure the switch parameters, you must access the CLI at the Privileged Exec level. Access to both CLI levels are controlled by user names and passwords. The switch has a default user name and password for each level. To log into the CLI at]the Privileged Exec level using the default user name and password, perform these steps: 1. 2. 3. 4. To initiate your console connection, press <Enter>. The "User Access Verification" procedure starts.

At the Username prompt, enter "admin." At the Password prompt, also enter "admin." (The password characters are not displayed on the console screen.) The session is opened and the CLI displays the "Console#" prompt indicating you have access at the Privileged Exec level. 2-3 2 Initial Configuration Setting Passwords Note: If this is your first time to log into the CLI program, you should define new passwords for both default user names using the "username" command, record them and put them in a safe place.

Passwords can consist of up to 8 alphanumeric characters and are case sensitive. To prevent unauthorized access to the switch, set the passwords as follows: 1. 2. 3. 4.

Open the console interface with the default user name and password "admin" to access the Privileged Exec level. Type "configure" and press <Enter>. Type "username guest password 0 password," for the Normal Exec level, where password is your new password. Press <Enter>. Type "username admin password 0 password," for the Privileged Exec level, where password is your new password. Press <Enter>. Note: '0' specifies the password in plain text, '7' specifies the password in encrypted form. Username: admin Password: CLI session with the TigerSwitch 10/100/1000 is opened. To end the CLI session, enter [Exit]. Console#configure Console(config)#username guest password 0 [password] Console(config)#username admin password 0 [password] Console(config)# Setting an IP Address You must establish IP address information for the stack to obtain management access through the network.

This can be done in either of the following ways: Manual -- You have to input the information, including IP address and subnet mask. If your management station is not in the same IP subnet as the stack's master unit, you will also need to specify the default gateway router. Dynamic -- The switch sends IP configuration requests to BOOTP or DHCP address allocation servers on the network. Manual Configuration You can manually assign an IP address to the switch. You may also need to specify a default gateway that resides between this device and management stations that exist on another network segment. Valid IP addresses consist of four decimal numbers, 0 to 255, separated by periods. Anything outside this format will not be accepted by the CLI program. Note: The IP address for this switch is obtained via DHCP by default. 2-4 Basic Configuration Before you can assign an IP address to the switch, you must obtain the following information from your network administrator: · IP address for the switch · Default gateway for the network · Network mask for this network To assign an IP address to the switch, complete the following steps: 1. 2.

3. 4. 2 From the Privileged Exec level global configuration mode prompt, type "interface vlan 1" to access the interface-configuration mode. Press <Enter>. Type "ip address ip-address netmask," where "ip-address" is the switch IP address and "netmask" is the network mask for the network.

Press <Enter>. Type "exit" to return to the global configuration mode prompt. Press <Enter>. To set the IP address of the default gateway for the network to which the switch belongs, type "ip default-gateway gateway," where "gateway" is the IP address of the default gateway. Press <Enter>. Console(config)#interface vlan 1 Console(config-if)#ip address 192.

168.1.5 255.255.255.0 Console(config-if)#exit Console(config)#ip default-gateway 192.168.1.254 Console(config)# Dynamic Configuration If you select the "bootp" or "dhcp" option, IP will be enabled but will not function until a BOOTP or DHCP reply has been received.

You therefore need to use the "ip dhcp restart" command to start broadcasting service requests. Requests will be sent periodically in an effort to obtain IP configuration information. (BOOTP and DHCP values can include the IP address, subnet mask, and default gateway.) If the "bootp" or "dhcp" option is saved to the startup-config file (step 6), then the switch will start broadcasting service requests as soon as it is powered on. To automatically configure the switch by communicating with BOOTP or DHCP address allocation servers on the network, complete the following steps: 1. 2. From the Global Configuration mode prompt, type "interface vlan 1" to access the interface-configuration mode. Press <Enter>. At the interface-configuration mode prompt, use one of the following commands: · To obtain IP settings via DHCP, type "ip address dhcp" and press <Enter>. · To obtain IP settings via BOOTP, type "ip address bootp" and press <Enter>.

3. 4. Type "end" to return to the Privileged Exec mode. Press <Enter>. Type "ip dhcp restart" to begin broadcasting service requests. Press <Enter>. 2-5 2 5. 6. Initial Configuration Wait a few minutes, and then check the IP configuration settings by typing the "show ip interface" command. Press <Enter>.

Then save your configuration changes by typing "copy running-config startup-config." Enter the startup file name and press <Enter>. Console(config)#interface vlan 1 Console(config-if)#ip address dhcp Console(config-if)#end Console#ip dhcp restart Console#show ip interface IP address and netmask: 192.168.1.54 255.255.255.0 on VLAN 1, and address mode: User specified. Console#copy running-config startup-config Startup configuration file name []: startup \Write to FLASH Programming.

\Write to FLASH finish. Success. Enabling SNMP Management Access The switch can be configured to accept management commands from Simple Network Management Protocol (SNMP) applications such as HP OpenView. You can configure the switch to (1) respond to SNMP requests or (2) generate SNMP traps. When SNMP management stations send requests to the switch (either to return information or to set a parameter), the switch provides the requested data or sets the specified parameter. The switch can also be configured to send information to SNMP managers (without being requested by the managers) through trap messages, which inform the manager that certain events have occurred. The switch includes an SNMP agent that supports SNMP version 1, 2c, and 3 clients. To provide management access for version 1 or 2c clients, you must specify a community string. The switch provides a default MIB View (i.e. , an SNMPv3 construct) for the default "public" community string that provides read access to the entire MIB tree, and a default view for the "private" community string that provides read/write access to the entire MIB tree. However, you may assign new views to version 1 or 2c community strings that suit your specific security requirements (see page 3-45). Community Strings (for SNMP version 1 and 2c clients) Community strings are used to control management access to SNMP version 1 and 2c stations, as well as to authorize SNMP stations to receive trap messages from the switch. You therefore need to assign community strings to specified users, and set the access level. 2-6 Basic Configuration The default strings are: 2 · public - with read-only access. Authorized management stations are only able to retrieve MIB objects. · private - with read-write access. Authorized management stations are able to both retrieve and modify MIB objects. To prevent unauthorized access to the switch from SNMP version 1 or 2c clients, it is recommended that you change the default community strings. To configure a community string, complete the following steps: 1.

From the Privileged Exec level global configuration mode prompt, type "snmp-server community string mode," where "string" is the community access string and "mode" is rw (read/write) or ro (read only). Press <Enter>. (Note that the default mode is read only.) To remove an existing string, simply type "no snmp-server community string," where "string" is the community access string to remove. Press <Enter>. Console(config)#snmp-server community admin rw Console(config)#snmp-server community private Console(config)# 4-102 2. Note: If you do not intend to support access to SNMP version 1 and 2c clients, we recommend that you delete both of the default community strings. If there are no community strings, then SNMP management access from SNMP v1 and v2c clients is disabled. Trap Receivers You can also specify SNMP stations that are to receive traps from the switch. To configure a trap receiver, use the "snmp-server host" command.

From the Privileged Exec level global configuration mode prompt, type: "snmp-server host host-address community-string [version {1 | 2c | 3 {auth | noauth | priv}}]" where "host-address" is the IP address for the trap receiver, "community-string" specifies access rights for a version 1/2c host, or is the user name of a version 3 host, "version" indicates the SNMP client version, and "auth | noauth | priv" means that authentication, no authentication, or authentication and privacy is used for v3 clients. Then press <Enter>. For a more detailed description of these parameters, see "snmp-server host" on page 4-104. The following example creates a trap host for each type of SNMP client. Console(config)#snmp-server host 10.1.19.23 batman4-104 Console(config)#snmp-server host 10.1.19.

98 robin version 2c Console(config)#snmp-server host 10.1.19.34 barbie version 3 auth Console(config)# 2-7 2 Initial Configuration Configuring Access for SNMP Version 3 Clients To configure management access for SNMPv3 clients, you need to first create a view that defines the portions of MIB that the client can read or write, assign the view to a group, and then assign the user to a group. The following example creates one view called "mib-2" that includes the entire MIB-2 tree branch, and then another view that includes the IEEE 802.

1d bridge MIB. It assigns these respective read and read/ write views to a group call "r&d" and specifies group authentication via MD5 or SHA. In the last step, it assigns a v3 user to this group, indicating that MD5 will be used for authentication, provides the password "greenpeace" for authentication, and the password "einstien" for encryption.

Console(config)#snmp-server view mib-2 1.3.
6.1.2.1 included4-109 Console(config)#snmp-server view 802.1d 1.3.6.1.2.1.

17 included Console(config)#snmp-server group r&d v3 auth mib-2 802.1d4-110 Console(config)#snmp-server user steve group r&d v3 auth md5 greenpeace priv des56 einstien4-113 Console(config)# For a more detailed explanation on how to configure the switch for access from SNMP v3 clients, refer to "Simple Network Management Protocol" on page 3-33, or refer to the specific CLI commands for SNMP starting on page 4-100. Saving Configuration Settings Configuration commands only modify the running configuration file and are not saved when the switch is rebooted. To save all your configuration changes in nonvolatile storage, you must copy the running configuration file to the start-up configuration file using the "copy" command. To save the current configuration settings, enter the following command: 1. 2. From the Privileged Exec mode prompt, type "copy running-config startup-config" and press <Enter>. Enter the name of the start-up file. Press <Enter>. Console#copy running-config startup-config Startup configuration file name [ ]: startup \Write to FLASH Programming.
\Write to FLASH finish. Success. Console# 2-8 Managing System Files 2 Managing System Files The switch's flash memory supports three types of system files that can be managed by the CLI program, web interface, or SNMP. The switch's file system allows files to be uploaded and downloaded, copied, deleted, and set as a start-up file. The three types of files are: · Configuration -- This file stores system configuration information and is created when configuration settings are saved.
Saved configuration files can be selected as a system start-up file or can be uploaded via TFTP to a server for backup. A file named "Factory_Default_Config.cfg" contains all the system default settings and cannot be deleted from the system. See "Saving or Restoring Configuration Settings" on page 3-19 for more information. · Operation Code -- System software that is executed after boot-up, also known as run-time code.
This code runs the switch operations and provides the CLI and web management interfaces. See "Managing Firmware" on page 3-17 for more information. · Diagnostic Code -- Software that is run during system boot-up, also known as POST (Power On Self-Test). Due to the size limit of the flash memory, the switch supports only two operation code files. However, you can have as many diagnostic code files and configuration files as available flash memory space allows. In the system flash memory, one file of each type must be set as the start-up file. During a system boot, the diagnostic and operation code files set as the start-up file are run, and then the start-up configuration file is loaded. Note that configuration files should be downloaded using a file name that reflects the contents or usage of the file settings. If you download directly to the running-config, the system will reboot, and the settings will have to be copied from the running-config to a permanent file. 2-9 2 Initial Configuration 2-10 Chapter 3: Configuring the Switch 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 or above, or Netscape 6.2 or above). Note: You can also use the Command Line Interface (CLI) to manage the switch over a serial connection to the console port or via Telnet. For more information on using the CLI, refer to Chapter 4: "Command Line Interface." Prior to accessing the switch from a web browser, be sure you have first performed the following tasks: 1. Configure the switch with a valid IP address, subnet mask, and default gateway using an out-of-band serial connection, BOOTP or DHCP protocol. (See "Setting an IP Address" on page 2-4.) 2. Set user names and passwords using an out-of-band serial connection. Access to the web agent is controlled by the same user names and passwords as the onboard configuration program. (See "Setting Passwords" on page 2-4.) After you enter a user name and password, you will have access to the system configuration program. failed attempt the current connection is terminated.
3. Notes: 1. You are allowed three attempts to enter the correct password; on the third 2. If you log into the web interface as guest (Normal Exec level), you can view the configuration settings or change the guest password. If you log in as "admin" (Privileged Exec level), you can change the settings on any page. 3. If the path between your management station and this switch does not pass through any device that uses the Spanning Tree Algorithm, then you can set the switch port attached to your management station to fast forwarding (i.e., enable Admin Edge Port) to improve the switch's response time to management commands issued through the web interface. See "Configuring Interface Settings" on page 3-114. 3-1 3 Configuring the Switch 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 System Information on the right side.

The Main Menu links are used to navigate to other menus, and display configuration parameters and statistics. Figure 3-1 Home Page Note: The examples in this chapter are based on the SMC8126L2. Other than the number of fixed ports, there are no other differences between the SMC8126L2 and SMC8150L2. The panel graphics for both switch types are shown on the following page. 3-2 Navigating the Web Browser Interface 3 Configuration Options Configurable parameters have a dialog box or a drop-down list. Once a configuration change has been made on a page, be sure to click on the Apply button to confirm the new setting. The following table summarizes the web page configuration buttons. Table 3-1 Configuration Options Button Revert Apply Help Action Cancels specified values and restores current values prior to pressing Apply. Sets specified values to the system. Links directly to webhelp.
Notes: 1. To ensure proper screen refresh, be sure that Internet Explorer 5.x is configured as follows: Under the menu "Tools / Internet Options / General / Temporary Internet Files / Settings," the setting for item "Check for newer versions of stored pages" should be "Every visit to the page.

" 2. When using Internet Explorer 5.

0, you may have to manually refresh the screen after making configuration changes by pressing the browser's refresh button. Panel Display The web agent displays an image of the switch's ports. The Mode can be set to display different information for the ports, including Active (i.e., up or down), Duplex (i. e., half or full duplex, or Flow Control (i.e., with or without flow control). Clicking on the image of a port opens the Port Configuration page as described on page 3-78. SMC8126L2 SMC8150L2 Figure 3-2 Panel Display 3-3 3 Configuring the Switch 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 3-2 Main Menu Menu System System Information Switch Information Bridge Extension Configuration IP Configuration Jumbo Frames File Management Copy Operation Delete Set Start-Up Line Console Telnet Log Logs System Logs Remote Logs SMTP Renumbering Reset SNTP Configuration Clock Time Zone SNMP Configuration Agent Status SNMPv3 Configures community strings and related trap functions Enables or disables SNMP Agent Status Configures SNTP client settings, including broadcast mode or a specified list of servers Sets the local time zone for the system clock Stores and displays error messages Sends error messages to a logging process Configures the logging of messages to a remote logging process Sends an SMTP client message to a participating server. Renumbers the units in the stack Restarts the switch Sets console port connection parameters Sets Telnet connection parameters Allows the transfer and copying files Allows deletion of files from the flash memory Sets the startup file Provides basic system description, including contact information Shows the number of ports, hardware/firmware version numbers, and power status Shows the bridge extension parameters Sets the IP address for management access Enables jumbo frame packets. Description Page 3-10 3-10 3-11 3-13 3-14 3-17 3-17 3-17 3-18 3-18 3-21 3-21 3-23 3-25 3-25 3-26 3-27 3-28 3-30 3-30 3-31 3-31 3-32 3-33 3-33 3-35 3-36 3-4 Navigating the Web Browser Interface Table 3-2 Main Menu (Continued) Menu Engine ID Remote Engine ID Users Remote Users Groups Views Security User Accounts Authentication Settings HTTPS Settings SSH Settings Host-Key Settings Port Security 802.

1X Information Configuration Port Configuration Statistics ACL Configuration Port Binding IP Filter Port Port Information Trunk Information Port Configuration Trunk Configuration Trunk Membership LACP Configuration Allows ports to dynamically join trunks Displays port connection status Displays trunk connection status Configures port connection settings Configures trunk connection settings Specifies ports to group into static trunks Configures packet filtering based on IP or MAC addresses Binds a port to the specified ACL Sets IP addresses of clients allowed management access via the web, SNMP, and Telnet Configures Secure Shell server settings Generates the host key pair (public and private) Configures per port security, including status, response for security breach, and maximum allowed MAC addresses Port authentication Displays global configuration settings Configures the global configuration setting Sets parameters for individual ports Displays protocol statistics for the selected port Assigns a new password for the current user Configures authentication sequence, RADIUS and TACACS Configures secure HTTP settings Description Sets the SNMP v3 engine ID on this switch Sets the SNMP v3 engine ID for a remote device Configures SNMP v3 users on this switch Configures SNMP v3 users from a remote device Configures SNMP v3 groups Configures SNMP v3 views 3 3-36 3-37 3-37 3-40 3-41 3-45 3-46 3-46 3-48 3-52 3-54 3-59 3-57 3-59 3-60 3-62 3-62 3-63 3-66 3-67 3-67 3-73 3-74 3-76 3-76 3-76 3-78 3-78 3-81 3-82 3-82 Page 3-5 3 Configuring the Switch Table 3-2 Main Menu (Continued) Menu Aggregation Port Port Counters Information Port Internal Information Port Broadcast Control Trunk Broadcast Control Mirror Port Configuration Rate Limit Input Port Configuration Input Trunk Configuration Output Port Configuration Port Statistics Address Table Static Addresses Dynamic Addresses Address Aging Spanning Tree STA Information Configuration Port Information Trunk Information Port Configuration Trunk Configuration MSTP VLAN Configuration Port Information Trunk Information Port Configuration Trunk Configuration Description Configures parameters for link aggregation group members Displays statistics for LACP protocol messages Displays settings and operational state for the local side Sets the broadcast storm threshold for each port Sets the broadcast storm threshold for each trunk Sets the source and target ports for mirroring Sets the input rate limit for each port Sets the input rate limit for each trunk Sets the output rate limit for ports Lists Ethernet and RMON port statistics Displays entries for interface, address or VLAN Displays or edits static entries in the Address Table Sets timeout for dynamically learned entries Page 3-84 3-86 3-88 3-90 3-91 3-91 3-93 3-94 3-94 3-94 3-94 3-94 3-95 3-99 3-99 3-100 3-102 3-102 3-102 Port Neighbors Information Displays settings and operational state for the remote side Output Trunk Configuration Sets the output rate limit for trunks Displays STA values used for the bridge Configures global bridge settings for STA and RSTP Displays individual port settings for STA Displays individual trunk settings for STA Configures individual port settings for STA Configures individual trunk settings for STA Configures priority and VLANs for a spanning tree instance Displays port settings for a specified MST instance Displays trunk settings for a specified MST instance Configures port settings for a specified MST instance Configures trunk settings for a specified MST instance 3-105 3-107 3-111 3-111 3-114 3-114 3-116 3-116 3-118 3-118 3-120 3-120 3-6 Navigating the Web Browser Interface Table 3-2 Main Menu (Continued) Menu VLAN 802.1Q VLAN GVRP Status 802.1Q Tunnel Configuration Basic Information Current Table Static List Static Table Enables GVRP VLAN registration protocol Enables QinQ Tunneling on the switch Displays information on the VLAN type supported by this switch Shows the current port members of each VLAN and whether or not the port is tagged or untagged Used to create or remove VLAN groups Modifies the settings for an existing VLAN Description 3 3-122 3-122 3-125 3-126 3-126 3-126 3-128 3-129 3-131 3-132 3-132 3-138 3-138 3-141 3-141 3-141 3-142 3-142 3-143 3-144 Page Static Membership by Port Configures membership type for interfaces, including tagged, untagged or forbidden Port Configuration Trunk Configuration Tunnel Port Configuration Private VLAN Status Link Status Protocol VLAN Configuration Port Configuration Priority Default Port Priority Default Trunk Priority Traffic Classes Traffic Classes Status Queue Mode Queue Scheduling Sets the default priority for each port Sets the default priority for each trunk Maps IEEE 802.