



# Your PDF Guides

You can read the recommendations in the user guide, the technical guide or the installation guide for SMC 6724AL2. You'll find the answers to all your questions on the SMC 6724AL2 in the user manual (information, specifications, safety advice, size, accessories, etc.). Detailed instructions for use are in the User's Guide.

**User manual SMC 6724AL2**  
**User guide SMC 6724AL2**  
**Operating instructions SMC 6724AL2**  
**Instructions for use SMC 6724AL2**  
**Instruction manual SMC 6724AL2**

## TigerSwitch 10/100

### 24-Port Fast Ethernet Switch

- ◆ 24 10BASE-T/100BASE-TX ports
- ◆ Optional 1000BASE-X or 100BASE-FX modules
- ◆ 8.8 Gbps of aggregate bandwidth
- ◆ Non-blocking switching architecture
- ◆ Spanning Tree Protocol
- ◆ Up to 4 port trunks
- ◆ RADIUS and TACACS+ authentication
- ◆ Rate limiting for bandwidth management
- ◆ CoS support for four-level priority
- ◆ Full support for VLANs with GVRP
- ◆ IP Multicasting with IGMP Snooping
- ◆ Manageable via console, Web, SNMP/RMON



**Management Guide**  
*SMC6724AL2*



[You're reading an excerpt. Click here to read official SMC 6724AL2 user guide](http://yourpdfguides.com/dref/3457299)  
<http://yourpdfguides.com/dref/3457299>

**Manual abstract:**

(SMC) is believed to be accurate and reliable. @@@@ Copyright © 2004 by SMC Networks, Inc. 38 Tesla Irvine, CA 92618 All rights reserved. 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. LIMITED WARRANTY Limited Warranty Statement: SMC Networks, Inc.

("SMC") warrants its products to be free from defects in workmanship and materials, under normal use and service, for the applicable warranty term. All SMC products carry a standard 90-day limited warranty from the date of purchase from SMC or its Authorized Reseller. @@@@ Failure to register will not affect the standard limited warranty. The Limited Lifetime warranty covers a product during the Life of that Product, which is defined as the period of time during which the product is an "Active" SMC product.

A product is considered to be "Active" while it is listed on the current SMC price list. As new technologies emerge, older technologies become obsolete and SMC will, at its discretion, replace an older product in its product line with one that incorporates these newer technologies. At that point, the obsolete product is discontinued and is no longer an "Active" SMC product. A list of discontinued products with their respective dates of discontinuance can be found at:

[http://www.smc.com/index.cfm?action=customer\\_service\\_warranty](http://www.smc.com/index.cfm?action=customer_service_warranty).

All products that are replaced become the property of SMC. Replacement products may be either new or reconditioned. Any replaced or repaired product carries either a 30-day limited warranty or the remainder of the initial warranty, whichever is longer.

SMC is not responsible for any custom software or firmware, configuration information, or memory data of Customer contained in, stored on, or integrated with any products returned to SMC pursuant to any warranty. Products returned to SMC should have any customer-installed accessory or add-on components, such as expansion modules, removed prior to returning the product for replacement. SMC is not responsible for these items if they are returned with the product. Customers must contact SMC for a Return Material Authorization number prior to returning any product to SMC. Proof of purchase may be required. Any product returned to SMC without a valid Return Material Authorization (RMA) number clearly marked on the outside of the package will be returned to customer at customer's expense. For warranty claims within North America, please call our toll-free customer support number at (800) 762-4968.

Customers are responsible for all shipping charges from their facility to SMC. SMC is responsible for return shipping charges from SMC to customer. **WARRANTIES EXCLUSIVE: IF AN SMC PRODUCT DOES NOT OPERATE AS WARRANTED ABOVE, CUSTOMER'S SOLE REMEDY SHALL BE REPAIR OR REPLACEMENT OF THE PRODUCT IN QUESTION, AT SMC'S OPTION.**

THE FOREGOING WARRANTIES AND REMEDIES ARE EXCLUSIVE AND ARE IN LIEU OF ALL OTHER WARRANTIES OR CONDITIONS, EXPRESS OR IMPLIED, EITHER IN FACT OR BY OPERATION OF LAW, STATUTORY OR OTHERWISE, INCLUDING WARRANTIES OR CONDITIONS OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. SMC NEITHER ASSUMES NOR AUTHORIZES ANY OTHER PERSON TO ASSUME FOR A LIMITED WARRANTY IT ANY OTHER LIABILITY IN CONNECTION WITH THE SALE, INSTALLATION, MAINTENANCE OR USE OF ITS PRODUCTS. SMC SHALL NOT BE LIABLE UNDER THIS WARRANTY IF ITS TESTING AND EXAMINATION DISCLOSE THE ALLEGED DEFECT IN THE PRODUCT DOES NOT EXIST OR WAS CAUSED BY CUSTOMER'S OR ANY THIRD PERSON'S MISUSE, NEGLIGENCE, IMPROPER INSTALLATION OR TESTING, UNAUTHORIZED ATTEMPTS TO REPAIR, OR ANY OTHER CAUSE BEYOND THE RANGE OF THE INTENDED USE, OR BY ACCIDENT, FIRE, LIGHTNING, OR OTHER HAZARD. LIMITATION OF LIABILITY: IN NO EVENT, WHETHER BASED IN CONTRACT OR TORT (INCLUDING NEGLIGENCE), SHALL SMC BE LIABLE FOR INCIDENTAL, CONSEQUENTIAL, INDIRECT, SPECIAL, OR PUNITIVE DAMAGES OF ANY KIND, OR FOR LOSS OF REVENUE, LOSS OF BUSINESS, OR OTHER FINANCIAL LOSS ARISING OUT OF OR IN CONNECTION WITH THE SALE, INSTALLATION, MAINTENANCE, USE, PERFORMANCE, FAILURE, OR INTERRUPTION OF ITS PRODUCTS, EVEN IF SMC OR ITS AUTHORIZED RESELLER HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SOME STATES DO NOT ALLOW THE EXCLUSION OF IMPLIED WARRANTIES OR THE LIMITATION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES FOR CONSUMER PRODUCTS, SO THE ABOVE LIMITATIONS AND EXCLUSIONS MAY NOT APPLY TO YOU. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS, WHICH MAY VARY FROM STATE TO STATE. NOTHING IN THIS WARRANTY SHALL BE TAKEN TO AFFECT YOUR STATUTORY RIGHTS. \* SMC will provide warranty service for one year following discontinuance from the active SMC price list. Under the limited lifetime warranty, internal and external power supplies, fans, and cables are covered by a standard one-year warranty from date of purchase. SMC Networks, Inc.

38 Tesla Irvine, CA 92618 vi CONTENTS I Switch Management . . . . .

. . . . .  
. . . . .

. . 1-1 Connecting to the Switch . . . . .

. . . . .  
. . . . .  
. . . . .

. . . . . 1-1 Configuration Options .

. . . . .  
. . . . .  
. . . . .

. . 1-1 Required Connections . . .

. . . . .  
. . . . .  
. . . . .

1-3 Remote Connections . . . . .

. . . . .  
. . . . .





.....  
.....  
.....  
... 2-21 Managing Firmware .....

.....  
.....  
.....  
.....  
... 2-23 Downloading System Software from a Server .....

.....  
.. 2-23 Saving or Restoring Configuration Settings ...  
.....

... 2-25 Downloading Configuration Settings from a Server .



[You're reading an excerpt. Click here to read official SMC 6724AL2 user guide](http://yourpdfguides.com/dref/3457299)

<http://yourpdfguides.com/dref/3457299>

.....  
.. 2-26 *Setting the Startup Configuration File* ...

.....  
.....

.. 2-26 *Copying the Running Configuration to a File* .....

.....  
.. 2-27 *vii CONTENTS Reset* ....

.....

.....

.....

.....

.....

..... *Setting the System Clock* ..

.....

.....

.....

.....  
.... *Configuring SNTP* .

.....

.....

.....

.....

.... *Setting the Time Zone* .

.....

.....

.....

. *Configuring SNMP* .....

.....

.....

.....

.....

. *Setting Community Access Strings* .....

.....

.....

... *Specifying Trap Managers* .....

.....

.....

.....

.. *Security* .....

.....

.....

.....

.....

.. *Configuring the Logon Password* ...

.....

.....

..... *Configuring RADIUS/TACACS Logon Authentication* .....

*Configuring HTTPS* .....

.....

.....

.....

.....

	.....
<i>Replacing the Default Secure-site Certificate</i>	.....
	.....
<i>Configuring SSH</i>	.....
	.....
	.....
	.....
<i>Configuring Port Security</i>	.....
	.....
	.....
<i>Configuring 802.1x Port Authentication</i>	.....
	.....
	.....
<i>Displaying 802.1x Global Settings</i>	.....
	.....
	.....
<i>Configuring Global dot1x Parameters</i>	.....
	.....
	.....
<i>Displaying 802.1x Statistics</i>	.....
	.....
	.....
<i>Access Control Lists</i>	.....
	.....
	.....
	.....
<i>Configuring Access Control Lists</i>	.....
	.....
	.....
<i>Binding a Port to an Access Control List</i>	.....
	.....
	.....
<i>Port Configuration</i>	.....
	.....
	.....
	.....
<i>Displaying Connection Status</i>	.....
	.....
	.....
<i>Configuring Interface Connections</i>	.....
	.....
	.....
<i>Trunk Configuration</i>	.....
	.....
	.....
	.....
<i>Statically Configuring a Trunk</i>	.....

.....  
.....  
.....  
.. *Dynamically Configuring a Trunk* .....

.....  
.....  
*Setting Broadcast Storm Thresholds* .....

.....  
.....  
..... *Configuring Port Mirroring* .....

.....  
.....  
..... *Configuring Rate Limits* .....

.....  
.....  
.....  
.....  
..... *Rate Limit Granularity* .....

.....  
.....  
..... *Rate Limit Port Configuration* .....

.....  
.....  
.....  
.....  
..... *Showing Port Statistics* .....

.....  
.....  
.....  
.....  
..... *Address Table Settings* .....

.....  
.....  
.....  
.....  
..... *Setting Static Addresses* .....

.....  
.....  
.....  
.....  
..... *Displaying the Ad...* .....

.....  
.....  
.....  
.....  
..... *3-2 Entering Commands* .....

.....  
.....  
.....  
.....  
..... *3-3 Keywords and Arguments* .....

.....  
.....  
.....  
.....  
..... *3-3 Minimum Abbreviation* .....



. 3-4 Command Completion . . . .	.....
.....	.....
.....	.....
.... 3-4 Getting Help on Commands .	.....
.....	.....
.....	.....
.. 3-4 Partial Keyword Lookup . . .	.....
.....	.....
.....	.....
... 3-6 Negating the Effect of Commands ..	.....
.....	.....
.....	.....
..... 3-6 Using Command History . . . .	.....
.....	.....
.....	.....
..... 3-6 Understanding Command Modes . . .	.....
.....	.....
.....	.....
.....	.....
. 3-6 Exec Commands . . . . .	.....
.....	.....
.....	.....
..... 3-7 Configuration Commands .	.....
.....	.....
.....	.....
..... 3-48 ip ssh server .	.....
.....	.....
.....	.....
.....	.....
.....	.....
.....	.....
.....	.....
.....	.....
..... 3-49 ip ssh . . . . .	.....
.....	.....
.....	.....
.....	.....
.....	.....
..... 3-50 show ip ssh . . . .	.....
.....	.....
.....	.....
.....	.....
.....	.....
.....	.....
.. 3-51 disconnect ssh . . .	.....
.....	.....
.....	.....
.....	.....
.....	.....
.....	.....

..... 3-51 show ssh .....

.....  
.....  
.....  
.....

..... 3-52 Port Security .....

.....  
.....  
.....

..... 3-53 SNTP Commands .....

.....  
.....  
.....  
.....

3-54 sntp client .....

.....  
.....  
.....

.. 3-55 sntp server ...

.....  
.....

..... 3-56 sntp poll .....

.....  
.....  
.....  
.....

..... 3-57 sntp broadcast client ..

.....  
.....  
.....

.. 3-58 show sntp ...

.....  
.....

..... 3-58 clock timezone .....

.....  
.....  
.....  
.....

.. 3-59 calendar set .....

.....  
.....  
.....

.....  
... 3-60 *show calendar* ..  
.....  
.....  
.....  
.....  
.. 3-61 *SNMP Commands* .....

.....  
.....  
.....  
.....

... 3-61 *xi CONTENTS snmp-server community* .....

.....  
.....  
.....

.... *snmp-server contact* .....

.....  
.....  
.....

..... *snmp-server location* ..

.....  
.....  
.....

.....  
.. *snmp-server host* .....

.....  
.....  
.....

.. *snmp-server enable traps* ...

.....  
.....  
.....

.. *show snmp* ...

.....  
.....  
.....

..... *IP Interface Commands* ..

.....  
.....  
.....  
.....

..... *ip address* .....

.....  
.....  
.....

.....  
.....  
.....

... *ip dhcp restart* ..

.....  
.....  
.....

.....  
..... *ip default-gateway* .....

.....  
.....  
.....  
.....

... *show ip interface* .....

.....  
.....  
.....

.....  
*show ip redirects* .....

.....  
.....  
.....

.....  
.....  
.. *ping* .....

.....  
.....  
.....

..... *Line Commands* .....

.....  
.....  
.....

.....  
.....  
.. *line* .....

.....  
.....  
.....

..... *login* .....

.....  
.....  
.....

.....  
.....  
.. *password* .....

.....  
.....  
.....

..... *exec-timeout* .....

.....  
.....  
.....

.....  
.....  
*password-thresh* .....

.....



.....  
.....  
.. *speed-duplex* .....

.....  
.....  
.....

.. *negotiation* .....

.....  
.....  
.....

.....  
... *capabilities* ..

.....  
.....

.....  
.....  
.....  
..... *flowcontrol* .....

.....  
.....  
.....  
.....

..... *clear counters* .....

.....  
.....  
.....

.....  
.....  
.....  
..... *shutdown* .....

.....  
.....  
.....

..... *switchport broadcast octet-rate* ..

.....  
.....  
.....

... *show interfaces status* .....

.....  
.....  
.....

..... *show interfaces counters* .....

.....  
.....  
.....

..... 3-62 3-63 3-63 3-64 3-66 3-67 3-68 3-69 3-70 3-71 3-72 3-72 3-73 3-74 3-75 3-76 3-77 3-78 3-79 3-80 3-81 3-82 3-83 3-84 3-84 3-85 3-86 3-87 3-87  
3-89 3-90 3-91 3-93 3-94 3-94 3-95 3-97 xii CONTENTS *show interfaces switchport* .....

.....  
.....  
.....

..... 3-98 *Address Table Commands* .....

.....  
.....

.....  
..... 3-101 mac-address-table static .  
.....  
.....  
.....  
..... 3-102 show mac-address-table .  
.....  
.....  
.....  
..... 3-103 clear mac-address-table dynamic .  
.....  
.....  
.....  
.. 3-104 mac-address-table aging-time .....  
.....  
.....  
... 3-105 Spanning Tree Commands . .  
.....  
.....  
.....  
.. 3-106 spanning-tree .....  
.....  
.....  
.....  
.....  
. 3-107 spanning-tree mode .....  
.....  
.....  
.....  
.... 3-108 spanning-tree forward-time .....  
.....  
.....  
.....  
. 3-109 spanning-tree hello-time .....  
.....  
.....  
.....  
. 3-110 spanning-tree max-age .....  
.....  
.....  
.....  
.. 3-110 spanning-tree priority .....  
.....  
.....  
.....  
.... 3-111 spanning-tree pathcost method .....  
.....  
.....  
..... 3-112 spanning-tree transmission-limit . .  
.....  
.....  
.....  
.....  
. 3-113 spanning-tree cost .....  
.....

.....  
.....  
.....  
..... 3-114 spanning-tree port-priority .....  
.....  
.....  
.....



[You're reading an excerpt. Click here to read official SMC 6724AL2 user guide](http://yourpdfguides.com/dref/3457299)  
<http://yourpdfguides.com/dref/3457299>



..... 3-115 spanning-tree portfast .....
.....
.....
..... 3-116 spanning-tree edge-port ....
.....
.....
..... 3-117 spanning-tree protocol-migration ....
.....
.....
... 3-118 spanning-tree link-type ..
.....
.....
..... 3-119 show spanning-tree .
.....
.....
.....
... 3-120 VLAN Commands .....
.....
.....
.....
.....
... 3-122 vlan database .....
.....
.....
.....
... 3-123 vlan ...
.....
.....
.....
..... 3-124 interface vlan ..
.....
.....
.....
..... 3-125 switchport mode ...
.....
.....
.....
... 3-126 switchport acceptable-frame-types ..
.....
.....
..... 3-127 switchport ingress-filtering .....
.....
.....
.....

... 3-128 switchport native vlan .....  
.....  
.....

..... 3-129 switchport allowed vlan .....  
.....  
.....

..... 3-130 switchport forbidden vlan .....  
.....  
.....

... 3-131 show vlan .....  
.....  
.....

..... 3-132 Private VLAN Commands .  
.....  
.....

.. 3-133 private-vlan ...  
.....  
.....

..... 3-134 private-vlan association ...  
.....  
.....

..... 3-135 switchport mode private-vlan ..  
.....  
.....

... 3-136 xiii CONTENTS switchport private-vlan host-association .....  
.....  
.....

. switchport private-vlan mapping .....  
.....  
.....

.... show vlan private-vlan .....  
.....  
.....

..... GVRP and Bridge Extension Commands .....  
.....  
.....

..... switchport gvrp .....  
.....  
.....

... show gvrp configuration .....  
.....

.....  
.....  
.....

.. *garp timer* .....

.....  
.....  
.....

... *show garp timer* ..

.....  
.....

.... *bridge-ext gvrp* .

.....  
.....

..... *show bridge-ext* .....

.....  
.....  
.....  
.....

... *Mirror Port Commands* .....

.....  
.....  
.....

..... *port monitor* .

.....  
.....  
.....

... *show port monitor* ..

.....  
.....

.. *Link Aggregation Commands* .....

.....  
.....  
.....

... *channel-group* .....

.....  
.....  
.....  
.....

. *lacp* .....

.....  
.....  
.....

.. *Rate Limit Commands* ...

.....  
.....  
.....  
.....  
..... *rate-limit* .....

.....  
.....  
.....  
.....  
..... *show rate-limit* .....

.....  
... *Authentication Commands* ..

.....  
.....  
.....  
.....  
..... *authentication login* .....

.....  
.....  
.....  
..... *radius-server host* ..

.....  
.....  
.....  
..... *radius-server port* .....

.....  
.....  
.....  
..... *radius-server key* ..

.....  
.....  
.....  
.....  
..... *radius-server retransmit* .....

.....  
.....  
.....  
.....  
..... *radius-server timeout* .....

..... *show radius-server* ..

.....  
.....  
.....  
..... *tacacs-server host* .....

.....  
.....  
. tacacs-server port . . . . .  
.....

.....  
.....  
. tacacs-server key . . . . .

.....  
.....  
..... show tacacs-server . . . . .

.....  
.....  
.....

. authentication dot1x default . . . . .  
.....  
..... dot1x default . . . . .

.....  
.....  
.....

..... dot1x max-req . . . . .  
.....  
.....

.....  
.....  
dot1x port-control . . . . .  
.....

.....  
.....  
..... dot1x re-authenticate . . . . .  
.....

.....  
.....  
.....  
. dot1x re-authentication . . . . .

.....  
.....  
.....

. 3-137 3-138 3-139 3-140 3-141 3-141 3-142 3-143 3-144 3-145 3-146 3-146 3-147 3-149 3-150 3-151 3-153 3-153 3-154 3-155 3-157 3-158 3-159 3-159  
3-160 3-161 3-161 3-162 3-162 3-163 3-163 3-164 3-164 3-165 3-165 3-166 3-166 xiv CONTENTS dot1x timeout quiet-period . . . . .

.....  
.....  
..... 3-167 dot1x timeout re-authperiod . . . . .  
.....

.....  
.....  
3-167 dot1x timeout tx-period . . . . .  
.....

.....

.....  
3-168 show dot1x .....  
.....  
.....  
.....  
..... 3-169 Access Control List Commands .....  
.....  
.....  
.....  
..... 3-172 IP ACLs .....  
.....  
.....  
.....  
..... 3-173 access-list ip ....  
.....  
.....  
.....  
.....  
3-174 permit, deny (Standard ACL) ....  
.....  
.....  
3-175 permit, deny (Extended ACL) ....  
.....  
.....  
..... 3-176 ip access-group ....  
.....  
.....  
.....  
..... 3-179 show ip access-group ..  
.....  
.....  
.....  
3-180 show ip access-list .....  
.....  
.....  
.....  
3-180 map access-list ip .....  
.....  
.....  
.....  
..... 3-181 show map access-list ip .....  
.....  
.....  
.....  
..... 3-182 MAC ACLs .....  
.....  
.....  
.....



.....	
.....	
.....	
.....	3-192 queue cos-map . . .
.....	
.....	
.....	
.....	3-193 show queue mode . . . . .
.....	
.....	
.....	
.....	3-195 show queue bandwidth .
.....	
.....	
.....	
.....	3-195 show queue cos-map . . . . .
.....	
.....	
.....	
.....	3-196 map ip port (Global Configuration) . . .
.....	
.....	
.....	
.....	3-196 map ip port (Interface Configuration) . . . . .
.....	
.....	
.....	3-197 map ip precedence (Global Configuration) . . . . .
.....	
.....	
.....	3-198 map ip precedence (Interface Configuration) . . .
.....	
.....	
.....	3-199 map ip dscp (Global Configuration) . . . . .
.....	
.....	
.....	3-200 map ip dscp (Interface Configuration) . . . . .
.....	
.....	
.....	3-201 xv CONTENTS show map ip port .
.....	
.....	
.....	
.....	show map ip precedence . . . . .
.....	
.....	
.....	
.....	show map ip dscp . . . . .
.....	
.....	
.....	
.....	Multicast Filtering Commands . .
.....	
.....	
.....	
.....	ip igmp snooping . .
.....	



.....	
.....	
.....	
... ip igmp snooping vlan static ...	
.....	
.....	
ip igmp snooping version .....	
.....	
.....	
..... show ip igmp snooping .	
.....	
.....	
..... show mac-address-table multicast .	
.....	
.....	
.....	
. ip igmp snooping querier .....	
.....	
.....	
.....	
ip igmp snooping query-count .....	
.....	
..... ip igmp snooping query-interval .....	
.....	
.....	
... ip igmp snooping query-max-response-time ..	
.....	
.....	
.. ip igmp snooping router-port-expire-time .....	
.....	
... ip igmp snooping vlan mrouter ..	
.....	
.....	
.. show ip igmp snooping mrouter ...	
.....	
.....	
.....	
..... 3-202 3-203 3-204 3-205 3-206 3-207 3-208 3-208 3-209 3-210 3-211 3-212 3-212 3-213 3-214 3-215 A B Troubleshooting .....	
.....	
.....	
.....	
.....	
.A-1 Troubleshooting Chart .....	
.....	
.....	
.....	
.....	
A-1 Upgrading Firmware via the Serial Port .....	
..B-1 Glossary Index xvi CHAPTER 1 SWITCH MANAGEMENT Connecting to the Switch Configuration Options The SMC6724AL2 24-port, Layer 2 switch includes a built-in network management agent.	



**[You're reading an excerpt. Click here to read official SMC 6724AL2 user guide](http://yourpdfguides.com/dref/3457299)**  
<http://yourpdfguides.com/dref/3457299>

The agent offers a variety of management options, including SNMP, RMON 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 assigned via DHCP by default. To change this address, see "Setting an IP Address" on page 1-6. The switch's HTTP Web agent allows you to configure switch parameters, monitor port connections, and display statistics graphically using a standard Web browser such as Netscape Navigator 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 switch's management agent is based on SNMP (Simple Network Management Protocol). This SNMP agent permits the switch to be managed from any system in the network using management software. 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. 1-1 SWITCH MANAGEMENT The switch's CLI configuration program, Web interface, 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 rate limiting Configure up to 255 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 Configure up to four static or LACP trunks Enable port mirroring Enable broadcast storm control Display system information and statistics 1-2 CONNECTING TO THE SWITCH 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 "Console Port Pin Assignments" on page B-7 of 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 DB-9 connector. 2. Connect the other end of the cable's to the RS-232 serial port on the switch. 3. Make sure the terminal emulation software is set as follows: . . . . . Select the appropriate serial port (COM port 1 or COM port 2).

Set the data rate to 9600 baud. 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.

Notes: 1. When using HyperTerminal with Microsoft® Windows® 2000, make sure that you have Windows 2000 Service Pack 2 or later installed. Windows 2000 Service Pack 2 fixes the problem of arrow keys not functioning in HyperTerminal's VT100 emulation. See [www.microsoft.com](http://www.microsoft.com) for information on Windows 2000 service packs. 1-3 SWITCH MANAGEMENT 2. Refer to "Line Commands" on page 3-74 for a complete description of console configuration options. 3. 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 3-1. For a list of all the CLI commands and detailed information on using the CLI, refer to "Command Groups" on page 3-10. 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 assigned 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 1-6.

Note: This switch supports four concurrent Telnet 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 Navigator 6.2 or above), or from a network computer using network management software. Note: The onboard program only provides access to basic configuration functions. To access the full of SNMP management functions, you must use SNMP-based network management software. 1-4 BASIC CONFIGURATION 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 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. To initiate your console connection, press <Enter>.

The "User Access Verification" procedure starts. 2. At the Username prompt, enter "admin." 3. At the Password prompt, also enter "admin." (The password characters are not displayed on the console screen.) 4. The session is opened and the CLI displays the "Console#" prompt indicating you have access at the Privileged Exec level. 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: 1-5 SWITCH MANAGEMENT 1. Open the console interface with the default user name and password "admin" to access the Privileged Exec level. 2. Type "configure" and press <Enter>. 3.

Type "username guest password 0 password," for the Normal Exec level, where password is your new password.



[You're reading an excerpt. Click here to read official SMC 6724AL2 user guide](http://yourpdfguides.com/dref/3457299)  
<http://yourpdfguides.com/dref/3457299>

Press <Enter>. 4. Type "username admin password 0 password," for the Privileged Exec level, where password is your new password. Press <Enter>. User Access Verification Username: admin Password: CLI session with the SMC6724AL2 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 switch 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 switch, 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. Note: Only one VLAN interface can be assigned an IP address (the default is VLAN 1). This defines the management VLAN, the only VLAN through which you can gain management access to the switch. If you assign an IP address to any other VLAN, the new IP address overrides the original IP address and this becomes the new management VLAN.

1-6 BASIC CONFIGURATION 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 assigned via DHCP by default. 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.

From the Privileged Exec level global configuration mode prompt, type "interface vlan 1" to access the interface-configuration mode. Press <Enter>. 2. 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>. 3. Type "exit" to return to the global configuration mode prompt. Press <Enter>. 4. 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>. 1-7 SWITCH MANAGEMENT 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, 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. From the Privileged Exec level global configuration mode prompt, type "interface vlan 1" to access the interface-configuration mode. Press <Enter>. 2. At the interface-configuration mode prompt, use one of the following commands: · · To obtain IP settings through DHCP, type "ip address dhcp" and press <Enter>.

To obtain IP settings through BOOTP, type "ip address bootp" and press <Enter>. 3. Type "exit" to return to the global configuration mode. Press <Enter>. 1-8 BASIC CONFIGURATION 4. Type "ip dhcp restart" to begin broadcasting service requests. Press <Enter>. 5. Wait a few minutes, and then check the IP configuration settings by typing the "show ip interface" command. Press <Enter>.

6. 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)#exit Console#ip dhcp restart Console#show ip interface IP interface vlan IP address and netmask: 10.1.0.54 255.255.255.0 on VLAN 1, and address mode: User specified.

Console#copy running-config startup-config Startup configuration file name []: startup Console# Enabling SNMP Management Access The switch can be configured to accept management commands from Simple Network Management Protocol (SNMP) applications. 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. Community Strings Community strings are used to control management access to SNMP stations, as well as to authorize SNMP stations to receive trap messages 1-9 SWITCH MANAGEMENT from the switch.

You therefore need to assign community strings to specified users or user groups, and set the access level. The default strings are: · · public - Specifies read-only access. Authorized management stations are only able to retrieve MIB objects. private - Specifies read-write access. Authorized management stations are able to both retrieve and modify MIB objects.

Note: If you do not intend to utilize SNMP, it is recommended that you delete both of the default community strings. If there are no community strings, then SNMP management access to the switch is disabled. To prevent unauthorized access to the switch via SNMP, 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>. 2. 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 abc rw Console(config)#snmp-server community private Console(config)# Trap Receivers You can also specify SNMP stations that are to receive traps from the switch.



[You're reading an excerpt. Click here to read official SMC 6724AL2 user guide](http://yourpdfguides.com/dref/3457299)  
<http://yourpdfguides.com/dref/3457299>

**1-10 BASIC CONFIGURATION** To configure a trap receiver, complete the following steps: 1. From the Privileged Exec level global configuration mode prompt, type "snmp-server host host-address community-string," where "host-address" is the IP address for the trap receiver and "community-string" is the string associated with that host. Press <Enter>. 2. In order to configure the switch to send SNMP notifications, you must enter at least one snmp-server enable traps command. Type "snmp-server enable traps type," where "type" is either authentication or link-up-down. Press <Enter>. Console(config)#snmp-server enable traps link-up-down Console(config)# 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.

From the Privileged Exec mode prompt, type "copy running-config startup-config" and press <Enter>. 2. Enter the name of the start-up file. Press <Enter>. Console#copy running-config startup-config Startup configuration file name [: startup Console# 1-11 SWITCH MANAGEMENT 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 -- These files store system configuration information and are 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 2-25 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, Web and SNMP management interfaces. See "Managing Firmware" on page 2-23 for more information. Diagnostic Code -- Software that is run during system boot-up, also known as POST (Power On Self-Test). This code also provides a facility to upload firmware files to the system directly through the console port. See "Upgrading Firmware via the Serial Port" on page B-1. · Due to the size limit of the flash memory, the switch supports only two operation code files, and two diagnostic code files. However, you can have as many 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. 1-12 MANAGING SYSTEM FILES 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. 1-13 SWITCH MANAGEMENT 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. (See "Setting the Startup Configuration File" on page 2-26.) The following table lists some of the basic system defaults. Function IP Settings Parameter Management VLAN DHCP BOOTP User Specified IP Address Subnet Mask Default Gateway Web Management HTTP Server HTTP Port Number SNMP Community Strings Authentication Failure Traps Link-up-Down Traps Security Privileged Exec Level Normal Exec Level Enable Privileged Exec from Normal Exec Level Authentication Default 1 Enabled Disabled Disabled 0.0.0.0 0.0.255.0.0.0.0.

0.0.0.0 Enabled 80 "public" (read only) "private" (read/write) Enabled Enabled Username "admin" Password "admin" Username "guest" Password "guest" Password "super" Local 1-14 SYSTEM DEFAULTS Function Console Port Connection Parameter Baud Rate Data bits Stop bits Parity Local Console Timeout Port Status Default 9600 8 1 none 0 (disabled) Enabled Enabled Disabled 10BASE-T 10 Mbps half duplex 10 Mbps full duplex Full-duplex flow control disabled 100BASE-TX/FX 10 Mbps half duplex 10 Mbps full duplex 100 Mbps half duplex 100 Mbps full duplex Full-duplex flow control disabled 1000BASE-T 10 Mbps half duplex 10 Mbps full duplex 100 Mbps half duplex 100 Mbps full duplex 1000 Mbps full duplex Full-duplex flow control disabled Symmetric flow control disabled 1000BASE-X 1000 Mbps full duplex Full-duplex flow control disabled Symmetric flow control disabled Link Aggregation Static Trunks LACP (all ports) None Disabled Admin Status Auto-negotiation Flow Control Capabilities 1-15 SWITCH MANAGEMENT Function Spanning Tree Protocol Parameter Status Default Enabled (Defaults: All parameters based on IEEE 802.1w) Fast Forwarding Address Table Virtual LANs Aging Time Default VLAN PVID Acceptable Frame Type Ingress Filtering GVRP (global) GVRP (port interface) Private VLAN Class of Service Ingress Port Priority Weighted Round Robin IP Precedence Priority IP DSCP Priority IP Port Priority Multicast Filtering IGMP Snooping Act as Querier Broadcast Storm Protection System Log Status Broadcast Limit Rate Status Messages Logged Messages Logged to Flash Rate Limit 802.1x Status Re-authentication Status Mode Disabled 300 seconds 1 1 All Disabled Disabled Disabled No Private VLAN 0 1:2:4:6 Disabled Disabled Disabled Enabled Enabled Enabled (all ports) 32000 octets/second Enabled Levels 0-7 (all) Levels 0-3 Disabled Disabled Disabled Force-Authorized (all ports) 1-16 CHAPTER 2 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 Navigator 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 3 "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 the IP Address" on page 2-16).



[You're reading an excerpt. Click here to read official SMC 6724AL2 user guide](http://yourpdfguides.com/dref/3457299)  
<http://yourpdfguides.com/dref/3457299>



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 "Configuring the Logon Password" on page 2-35.) Note: If you log into the Web interface as guest (Normal Exec level), you can view page information but only change the guest password. If you

log in as admin (Privileged Exec level), you can apply changes on all pages. 2-1 CONFIGURING THE SWITCH 3. After you enter a user name and password, you will have access to the system configuration program. Note: 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 to improve the switch's response time to management commands issued through the Web interface. (See "Displaying Interface Settings" on page 2-98.) 2-2

NAVIGATING THE WEB BROWSER INTERFACE 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. If this is your first time to access the management agent, you should define a new Administrator user name and password, record them and put them in a safe place.

Select Security from the Main Menu, and then enter a new user name and password for the Administrator. Note that user names and passwords can consist of up to 8 alphanumeric characters and are case sensitive. 2-3 CONFIGURING THE SWITCH You are allowed three attempts to enter the correct password; on the third failed attempt the current connection is terminated. 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. Button Apply Revert Help Action Sets specified values to the system. Cancels specified values and restores current values prior to pressing Apply. Links directly to webhelp. Panel Display The Web agent displays an image of the switch's ports, indicating whether each link is up or down. Clicking on the image of a port opens the Port Configuration page as described on page 2-67. 2-4 MAIN MENU 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. Menu System System Information Provides basic system description, including contact information Switch Information Shows the number of ports, hardware/firmware version numbers, and power status Bridge Extension IP Configuration System Logs Logs Remote Logs Firmware Configuration Reset SNMP SNMP Configuration Configures SNMP client settings, including broadcast mode or a specified list of servers Clock Time Zone SNMP SNMP Security Passwords Authentication Settings Assigns a new password for the logon user name Configures RADIUS/TACACS+ authentication parameters Configures community strings and related trap functions Sets the local time zone for the clock Shows the configuration for bridge extension commands; enables GVRP multicast protocol Sets the IP address for management access Sends error messages to a logging process Stores and displays error messages Configures the logging of messages to a remote logging process Manages code image files Manages switch configuration files Restarts the switch Description Page 2-9 2-9 2-11 2-14 2-16 2-19 2-21 2-21 2-23 2-25 2-28 2-28 2-29 2-30 2-31 2-31 2-35

2-35 2-36 2-5 CONFIGURING THE SWITCH Menu HTTPS Settings SSH Settings Port Security Configuration dot1X (IEEE 802.1x) dot1X Information Displays general port authentication status information dot1X Configuration dot1X Port Configuration dot1X Statistics ACL ACL Configuration Configures packet filtering based on IP or MAC addresses ACL Port Binding Binds a port to the specified ACL Port Port Information Trunk Information Port Configuration Displays port connection status Displays trunk connection status Configures port connection settings Description Configures secure HTTP settings Configures Secure Shell settings Configures port security Page 2-40 2-43 2-45 2-48 2-49 Enables the changing of general port authentication 2-52 features Enables the changing of port authentication features Displays a per-port statistical readout 2-53 2-55 2-57 2-57 2-64 2-65 2-65 2-65 2-67 2-69 2-71 2-72 2-74 2-76 2-77 Enables or disables the rate limit feature Sets the rate limit for each port Lists Ethernet and RMON port statistics 2-78 2-79 2-80 Trunk

Configuration Configures trunk connection settings Trunk Membership Specifies ports to group into static trunks LACP Configuration Allows ports to dynamically join trunks Port Broadcast Control Mirror Rate Limit Rate Limit Granularity Rate Limit Port Configuration Port Statistics Sets the broadcast storm threshold Sets the source and target ports for mirroring 2-6 MAIN MENU Menu Address Table Static Addresses Address Aging Spanning Tree STA Information STA Configuration STA Port Information STA Trunk Information STA Port Configuration STA Trunk Configuration VLAN VLAN Basic Information VLAN Current Table VLAN Static List VLAN Static Membership VLAN Port Configuration VLAN Trunk Configuration Private VLAN Information Private VLAN Configuration Private VLAN Association Displays basic information on the VLAN type supported by this switch Displays STA values used for the bridge Configures global bridge settings for STA Displays individual port settings for STA Displays individual trunk settings for STA Configures individual port settings for STA Configures individual trunk settings for STA Displays entries for interface, address or VLAN Sets timeout for dynamically learned entries Description Page 2-86 2-86 2-89 2-90 2-91 2-91 2-98 2-98 2-102 2-102 2-106 2-110 Dynamic Addresses Displays or edits static entries in the

Address Table 2-87 Shows the current port members of each VLAN 2-111 and whether or not the port is tagged or untagged Used to create or remove VLAN groups Configures membership type for interfaces, including tagged, untagged or forbidden Specifies default PVID and VLAN attributes 2-113 2-115 2-117 2-118 VLAN Static Table Modifies the settings for an existing VLAN Specifies default trunk VID and VLAN attributes 2-118 Displays Private VLAN feature information This page is used to create/remove primary or community VLANs 2-123 2-124 Each community VLAN must be associated with a 2-126 primary VLAN 2-7 CONFIGURING THE SWITCH Menu Description Page 2-127 2-128 2-131 Sets the default priority for each port Sets the default priority for each trunk 2-131 2-131 Private VLAN Port/ Displays the interfaces associated with private Trunk Information VLANs Private VLAN Port/ Sets the private VLAN interface type, and Trunk Configuration associates the interfaces with a private VLAN Priority Port Priority Configuration Trunk Priority Configuration Traffic Classes Queue Mode Queue Scheduling Maps IEEE 802.



[You're reading an excerpt. Click here to read official SMC 6724AL2 user guide](http://yourpdfguides.com/dref/3457299)  
<http://yourpdfguides.com/dref/3457299>

*Ip priority tags to output queues 2-133 Sets queue mode to strict priority or Weighted Round-Robin Configures Weighted Round Robin queuing 2-136 2-137 IP Precedence/ Globally selects IP Precedence or DSCP Priority, or 2-138 DSCP Priority Status disables both IP Precedence Priority IP DSCP Priority IP Port Priority Status IP Port Priority Sets IP Type of Service priority, mapping the precedence tag to a class-of-service value 2-140 Sets IP Differentiated Services Code Point priority, 2-142 mapping a DSCP tag to a class-of-service value Globally enables or disables IP Port Priority Sets TCP/UDP port priority, defining the socket number and associated class-of-service value 2-144 2-144 ACL CoS Mapping Sets the CoS value and corresponding output queue 2-146 for packets matching an ACL rule IGMP Snooping IGMP Configuration Multicast Router Port Information Static Multicast Router Port Configuration Enables multicast filtering; configures parameters for multicast query Displays the ports that are attached to a neighboring multicast router/switch for each VLAN ID Assigns ports that are attached to a neighboring multicast router/switch 2-148 2-151 2-152 2-8 BASIC CONFIGURATION Menu IP Multicast Registration Table IGMP Member Port Table Description Page Displays all multicast groups active on this switch, 2-153 including multicast IP addresses and VLAN ID Indicates multicast addresses associated with the selected VLAN 2-154 Basic Configuration Displaying System Information You can easily identify the system by providing a descriptive name, location and contact information. Command Attributes . . . . System Name Name assigned to the switch system. Object ID MIB II object ID for switch's network management subsystem. Location Specifies the system location. Contact Administrator responsible for the system. System Up Time Length of time the management agent has been up. 2-9 CONFIGURING THE SWITCH Web Click System, System Information. Specify the system name, location, and contact information for the system administrator, then click Apply. (This page also includes a Telnet button that allows you to access the Command Line Interface via Telnet.) 2-10 DISPLAYING SWITCH HARDWARE/SOFTWARE VERSIONS CLI Specify the hostname, location and contact information.*

*Console(config)#hostname SMC6724AL2 3-28 Console(config)#snmp-server location TPS - 3rd Floor 3-62 Console(config)#snmp-server contact Chris 3-61 Console#show system 3-41 System description: TigerSwitch 10/100 6724AL2 System OID string: 1.3.6.1.4.1.202.20.31 System information System Up time: 0 days, 1 hours, 44 minutes, and 20.41 seconds System Name : SMC6724AL2 System Location : TPS - 3rd Floor System Contact : Chris MAC address : 00-30-F1-8A-22-E0 Web server : enable Web server port : 80 Web secure server : enable Web secure server port : 443 POST result DUMMY Test 1.*

*.....*

*.....PASS UART LOOP BACK Test....*

*.....*

*.....PASS DRAM Test....*

*.....*

*.....PASS Timer Test....*

*.....*

*.....*

*.....PASS RTC Initialization.....*

*.....PASS Switch Int Loopback test....*

*.PASS ----- DONE -----Console# Displaying Switch Hardware/Software Versions Use the Switch Information page to display hardware/firmware version numbers for the main board and management software, as well as the power status of the system. Command Attributes Main Board . . . Serial Number The serial number of the switch. Number of Ports Number of built-in RJ-45 ports and expansion ports. Hardware Version Hardware version of the main board.*

*2-11 CONFIGURING THE SWITCH . . Internal Power Status Displays the status of the internal power supply. Redundant Power Status\* Displays the status of the redundant power supply. \* CLI only. Management Software . . . Loader Version Version number of loader code. Boot-ROM Version Version number of Power-On Self-Test (POST) and boot code.*

*Operation Code Version Version number of runtime code. Role Shows if the switch is stacked or operating stand-alone. Expansion Slot . Expansion Slot 1/2 Slots for expansion modules. 2-12 DISPLAYING SWITCH HARDWARE/SOFTWARE VERSIONS Web Click System, Switch Information. CLI Use the following command to display version information. Console#show version Unit1 Serial number Service tag Hardware version Module A type Module B type Number of ports Main power status Redundant power status Agent(master) Unit id Loader version Boot rom version Operation code version Console# 3-43 :ag1005 : : :not present :not present :24 :up :not present :1 :2.1.0.3 :2.0.*

*1.0 :2.0.4.2 2-13 CONFIGURING THE SWITCH Displaying Bridge Extension Capabilities The Bridge MIB includes extensions for managed devices that support Multicast Filtering, Traffic Classes, and Virtual LANs. You can access these extensions to display default settings for the key variables, or to configure the global setting for GARP VLAN Registration Protocol (GVRP). Command Attributes . Extended Multicast Filtering Services This switch does not support the filtering of individual multicast addresses based on GMRP (GARP Multicast Registration Protocol). Traffic Classes This switch provides mapping of user priorities to multiple traffic classes. (Refer to "Class of Service Configuration" on page 2-131.) Static Entry Individual Port This switch allows static filtering for unicast and multicast addresses.*

*(Refer to "Setting Static Addresses" on page 2-86.) VLAN Learning This switch uses Independent VLAN Learning (IVL), where each port maintains its own filtering database. Configurable PVID Tagging This switch allows you to override the default Port VLAN ID (PVID used in frame tags) and egress status (VLAN-Tagged or Untagged) on each port. (Refer to "VLAN Configuration" on page 2-106.) Local VLAN Capable This switch does not support multiple local bridges (i. e., multiple Spanning Trees). GMRP GARP Multicast Registration Protocol (GMRP) allows network devices to register endstations with multicast groups. This switch does not support GMRP; it uses the Internet Group . . . . . 2-14 DISPLAYING BRIDGE EXTENSION CAPABILITIES Management Protocol (IGMP) to provide automatic multicast filtering. . GVRP GARP VLAN Registration Protocol (GVRP) defines a way for switches to exchange VLAN information in order to register necessary VLAN members on ports across the network.*

*This function should be enabled to permit VLAN groups which extend beyond the local switch. Web Click System, Bridge Extension Configuration. CLI Enter the following command. Console#show bridge-ext Max support vlan numbers: 255 Max support vlan ID: 4094 Extended multicast filtering services: No Static entry individual port: Yes VLAN learning: IVL Configurable PVID tagging: Yes Local VLAN capable: No Traffic classes: Enabled Global GVRP status: Enabled GMRP: Disabled Console# 3-143 2-15 CONFIGURING THE SWITCH Setting the IP Address An IP address may be used for management access to the switch over your network.*



[You're reading an excerpt. Click here to read official SMC 6724AL2 user guide](http://yourpdfguides.com/dref/3457299)  
<http://yourpdfguides.com/dref/3457299>

By default, the switch uses DHCP to assign IP settings to VLAN 1 on the switch. You can manually configure a specific IP address, or direct the device to obtain an address from a BOOTP or DHCP server when it is powered on. 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. Command Attributes · Management VLAN This is the only VLAN through which you can gain management access to the switch. By default, all ports on the switch are members of VLAN 1, so a management station can be connected to any port on the switch.

However, if other VLANs are configured and you change the Management VLAN, you may lose management access to the switch. In this case, you should reconnect the management station to a port that is a member of the Management VLAN. IP Address Mode Specifies whether IP functionality is enabled via manual configuration (Static), Dynamic Host Configuration Protocol (DHCP), or Boot Protocol (BOOTP). If DHCP/BOOTP is enabled, IP 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/BOOTP values can include the IP address, subnet mask, and default gateway.) IP Address Address of the VLAN interface that is allowed management access. @Subnet Mask This mask identifies the host address bits used for routing to specific subnets. · · · 2-16 DISPLAYING BRIDGE EXTENSION CAPABILITIES · Gateway IP Address IP address of the gateway router between this device and management stations that exist on other network segments. MAC Address The MAC address of this switch.

· Manual Configuration Web Click System, IP Configuration. Specify the management interface, IP address and default gateway, then click Apply. CLI Specify the management interface, IP address and default gateway. Console#config Console(config)#interface vlan 1 Console(config-if)#ip address 192.168.10.3 255.255.255.0 Console(config-if)#exit Console(config)#ip default-gateway 0.

0.0.0 Console(config)# 3-68 3-70 2-17 CONFIGURING THE SWITCH Using DHCP/BOOTP If your network provides DHCP/BOOTP services, you can configure the switch to be dynamically configured by these services. Web Click System, IP. Specify the Management VLAN, set the IP Address Mode to DHCP or BOOTP. Then click Apply to save your changes. The switch will broadcast a request for IP configuration settings on the next power reset. Otherwise, you can click Restart DHCP to immediately request a new address. If you lose your management connection, use a console connection and enter "show ip interface" to determine the new switch address. CLI Specify the management interface, and set the IP Address Mode to DHCP or BOOTP.

Console#config 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: 10.1.0.54 255.255.255.0 on VLAN 1, and address mode: User specified. Console# 3-85 3-68 3-69 3-71 Renewing DHCP DHCP may lease addresses to clients indefinitely or for a specific period of time. If the address expires or the switch is moved to another network segment, you will lose management access to the switch. In this case, you can reboot the switch or submit a client request to restart DHCP service.

Web If the address assigned by DHCP is no longer functioning, you will not be able to renew the IP settings via the Web interface. You can only restart DHCP service via the Web interface if the current address is still available. CLI Enter the following command to restart DHCP service. Console#ip dhcp restart 3-69 2-18 SYSTEM LOGS CONFIGURATION System Logs Configuration The system can be configured to send debug and error messages to a logging process. This logging process controls the type of error messages that are stored in switch memory or sent to a remote syslog server. The system allows you to specify which levels are logged to RAM or flash memory. Severe error messages that are logged to flash memory are permanently stored in the switch to assist in troubleshooting network problems. Up to 4096 log entries can be stored in the flash memory, with the oldest entries being overwritten first when the available log memory (256 kilobytes) has been exceeded. Logs The Logs page allows you to scroll through the logged system and event messages. The switch can store up to 2048 log entries in temporary random access memory (RAM; i.

e., memory flushed on power reset) and up to 4096 entries in permanent flash memory. Web Click System, Log, Logs. System Logs The System Logs page allows you to configure and limit system messages that are logged to flash or RAM memory. The default is for levels 0 to 3 to be logged to flash and levels 0 to 7 to be logged to RAM. 2-19 CONFIGURING THE SWITCH Command Attributes · · System Log Status Enables/disables the logging of debug or error messages to the logging process. Flash Level Limits log messages saved to the switch's permanent flash memory for all levels up to the specified level. For example, if level 3 is specified, all messages from level 0 to level 3 will be logged to flash. RAM Level Limits log messages saved to the switch's temporary RAM memory for all levels up to the specified level. For example, if level 7 is specified, all messages from level 0 to level 7 will be logged to RAM.

· Note: The Flash Level must be equal to or less than the Ram Level. Web Click System, Log, System Logs. Specify System Log Status, then change the level of messages, and click Apply. CLI Specify the hostname, location and contact information. Console(config)#logging on Console(config)#logging history ram 0 Console(config)# Console#show logging flash Syslog logging: Disable History logging in FLASH: level errors Console# 3-31 3-31 3-36 2-20 SYSTEM LOGS CONFIGURATION Remote Logs Configuration The Remote Logs page allows you to configure the logging of messages that are sent to syslog servers or other management stations. You can also limit the error messages sent to only those messages of a specified level. Command Attributes · · Remote Log Status Enables/disables the logging of debug or error messages to the remote logging process. (Default: enabled) Logging Facility Sets the facility type for remote logging of syslog messages. There are eight facility types specified by values of 16 to 23. The facility type is used by the syslog server to dispatch log messages to an appropriate service.

(Default: 23) Logging Trap Limits log messages that are sent to the remote syslog server for all levels up to the specified level. For example, if level 3 is specified, all messages from level 0 to level 3 will be sent to the remote server.



[You're reading an excerpt. Click here to read official SMC 6724AL2 user guide](http://yourpdfguides.com/dref/3457299)  
<http://yourpdfguides.com/dref/3457299>