SMC Networks | USER GUIDE

Manual abstract:

@@@@@@Copyright © 2008 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. 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. SMC may, at its own discretion, repair or replace any product not operating as warranted with a similar or functionally equivalent product, during the applicable warranty term. SMC will endeavor to repair or replace any product returned under warranty within 30 days of receipt of the product. The standard limited warranty can be upgraded to a Limited Lifetime warranty by registering new products within 30 days of purchase from SMC or its Authorized Reseller.*

Registration can be accomplished via the enclosed product registration card or online via the SMC Web site. 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.

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 IT ANY OTHER LIABILITY IN CONNECTION WITH THE SALE, INSTALLATION, MAINTENANCE OR USE OF ITS PRODUCTS. SMC SHALL iv 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, NEGLECT, 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. 20 Mason Irvine, CA 92618 v vi COMPLIANCES Federal Communication Commission Interference Statement This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation.*

This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures: · Reorient or relocate the receiving antenna · Increase the separation between the equipment and receiver · Connect the equipment into an outlet on a circuit different from that to which the receiver is connected · Consult the dealer or an experienced radio/TV technician for help FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment. This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

IMPORTANT NOTE: FCC Radiation Exposure Statement This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20 centimeters (8 inches) between the radiator and your body. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter. i COMPLIANCES Industry Canada - Class B This digital apparatus does not exceed the Class B limits for radio noise emissions from digital apparatus as set out in the interference-causing equipment standard entitled "Digital Apparatus," ICES-003 of Industry Canada. Cet appareil numérique respecte les limites de bruits radioélectriques applicables aux appareils numériques de Classe B prescrites dans la norme sur le matérial brouilleur: "Appareils Numériques," NMB-003 édictée par l'Industrie. Taiwan DGT Japan VCCI Class B Australia/New Zealand AS/NZS 4771 N11846 ii COMPLIANCES EC Conformance Declaration Marking by the above symbol indicates compliance with the Essential Requirements of the R&TTE Directive of the European Union (1999/5/ EC). This equipment meets the following conformance standards: · EN 60950-1 (IEC 60950-1) - Product Safety · EN 300 328 - Technical requirements for 2.4 GHz radio equipment · EN 301 489-1 / EN 301 489-17 - EMC requirements for radio equipment Countries of Operation & Conditions of Use in the European Community This device is intended to be operated in all countries of the European Community. Requirements for indoor vs. outdoor operation, license requirements and allowed channels of operation apply in some countries as described below: Note: The user must use the configuration utility provided with this product to ensure the channels of operation are in conformance with the spectrum usage rules for European Community countries as described below.

· This device requires that the user or installer properly enter the current country of operation in the command line interface as described in the user guide, before operating this device. · This device will automatically limit the allowable channels determined by the current country of operation. Incorrectly entering the country of operation may result in illegal operation and may cause harmful interference to other systems. The user is obligated to ensure the device is operating according to the channel limitations, indoor/outdoor restrictions and license requirements for each European Community country as described in this document. · This device may be operated indoors or outdoors in all countries of the European Community using the 2.4 GHz band: Channels 1 - 13, except where noted below. - In Italy the end-user must apply for a license from the national spectrum authority to operate this device outdoors. - In Belgium outdoor operation is only permitted using the 2.46 2.4835 GHz band: Channel 13.
- In France outdoor operation is only permitted using the 2.4 - 2.454 GHz band: Channels 1 - 7. iii COMPLIANCES Declaration of Conformity in Languages of the European Community English Hereby, SMC, declares that this Radio LAN device is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC. Valmistaja SMC vakuuttaa täten että Radio LAN device tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.
Hierbij verklaart SMC dat het toestel Radio LAN device in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EG Bij deze SMC dat deze Radio LAN device voldoet aan de essentiële eisen en aan de overige relevante bepalingen van Richtlijn 1999/5/EC. French Par la présente SMC déclare que l'appareil Radio LAN device est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/CE Härmed intygar SMC att denna Radio LAN device står I överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EG. Undertegnede SMC erklærer herved, at følgende udstyr Radio LAN device overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF Hiermit erklärt SMC, dass sich dieser/diese/dieses Radio LAN device in Übereinstimmung mit den grundlegenden Anforderungen und den anderen relevanten Vorschriften der Richtlinie 1999/5/EG befindet". (BMWi) Hiermit erklärt SMC die Übereinstimmung des Gerätes Radio LAN device mit den grundlegenden Anforderungen und den anderen relevanten Festlegungen der Richtlinie 1999/5/EG. (Wien) Greek SMC radio LAN device 1999/5/ Con la presente SMC dichiara che questo Radio LAN device è conforme ai requisiti essenziali ed alle altre dispareil EN 60320/IEC 320.
· La prise secteur doit se trouver à proximité de l'appareil et son accès doit être facile. Vous ne pouvez mettre l'appareil hors circuit qu'en débranchant son cordon électrique au niveau de cette prise. · L'appareil fonctionne à une tension extrêmement basse de sécurité qui est conforme à la norme IEC 60950. Ces conditions ne sont maintenues que si l'équipement auquel il est raccordé fonctionne dans les mêmes conditions. France et Pérou uniquement: Ce groupe ne peut pas être alimenté par un dispositif à impédance à la terre. Si vos alimentations sont du type impédance à la terre, ce groupe doit être alimenté par une tension de 230 V (2 P+T) par le biais d'un transformateur d'isolement à rapport 1:1, avec un point secondaire de connexion portant l'appellation Neutre et avec raccordement direct à la terre (masse). Cordon électrique - Il doit être agréé dans le pays d'utilisation Etats-Unis et Canada: Le cordon doit avoir reçu l'homologation des UL et un certificat de la CSA. Les spécifications minimales pour un cable flexible sont AWG No. 18, ou AWG No. 16 pour un cable de longueur inférieure à 2 mètres.

- type SV ou SJ - 3 conducteurs Le cordon doit être en mesure d'acheminer un courant nominal d'au moins 10 A. La prise femelle de branchement doit être du type à mise à la terre (mise à la masse) et respecter la configuration NEMA 5-15P (15 A, 125 V) ou NEMA 6-15P (15 A, 250 V). Danemark: La prise mâle d'alimentation doit respecter la section 107-2 D1 de la norme DK2 1a ou DK2 5a. vii COMPLIANCES Cordon électrique - Il doit être agréé dans le pays d'utilisation Suisse: Europe La prise mâle d'alimentation doit respecter la norme SEV/ ASE 1011.

La prise secteur doit être conforme aux normes CEE 7/7 ("SCHUKO") LE cordon secteur doit porter la mention <HAR> ou <BASEC> et doit être de type HO3VVF3GO.75 (minimum). Bitte unbedingt vor dem Einbauen des Access Point die folgenden Sicherheitsanweisungen durchlesen (Germany): WARNUNG: Die Installation und der Ausbau des Geräts darf nur durch Fachpersonal erfolgen. · Das Gerät sollte nicht an eine ungeerdete Wechselstromsteckdose angeschlossen werden. · Das Gerät muß an eine geerdete Steckdose angeschlossen werden, welche die internationalen Sicherheitsnormen erfüllt. · Der Gerätestecker (der Anschluß an das Gerät, nicht der Wandsteckdosenstecker) muß einen gemäß EN 60320/IEC 320 konfigurierten Geräteeingang haben. · Die Netzsteckdose muß in der Nähe des Geräts und leicht zugänglich sein. Die Stromversorgung des Geräts kann nur durch Herausziehen des Gerätenetzkabels aus der Netzsteckdose unterbrochen werden. · Der Betrieb dieses Geräts erfolgt unter den SELV-Bedingungen (Sicherheitskleinstspannung) gemäß IEC 60950. Diese Bedingungen sind nur gegeben, wenn auch die an das Gerät angeschlossenen Geräte unter SELV-Bedingungen betrieben werden. · viii COMPLIANCES Stromkabel.

Dies muss von dem Land, in dem es benutzt wird geprüft werden: U.S.A und Kanada Der Cord muß das UL geprufi und war das CSA beglaubigt. Das Minimum spezifikation fur der Cord sind: - Nu. 18 AWG - nicht mehr als 2 meter, oder 16 AWG.

- Der typ SV oder SJ - 3-Leiter Der Cord muß haben eine strombelastbarkeit aus wenigstens 10 A Dieser Stromstecker muß hat einer erdschluss mit der typ NEMA 5-15P (15A, 125V) oder NEMA 6-15P (15A, 250V) konfiguration. Danemark Schweiz Europe Dieser Stromstecker muß die ebene 107-2-D1, der standard DK2-1a oder DK2-5a Bestimmungen einhalten. Dieser Stromstecker muß die SEV/ASE 1011Bestimmungen einhalten. Das Netzkabel muß vom Typ HO3VVF3GO.75 (Mindestanforderung) sein und die Aufschrift <HAR> oder <BASEC> tragen. Der Netzstecker muß die Norm CEE 7/7 erfüllen ("SCHUKO"). ix COMPLIANCES x Table of Contents Chapter 1: Introduction Package Checklist Hardware Description Antennas LED Indicators Security Slot Console Port Ethernet Port Reset Button Power Connector Features and Benefits System Defaults Chapter 2: Hardware Installation Chapter 3: Network Configuration Network Topologies Ad Hoc Wireless LAN (no Access Point) Infrastructure Wireless LAN Infrastructure Wireless LAN for Roaming Wireless PCs Infrastructure Wireless Bridge Infrastructure Wireless Repeater Chapter 4: Initial Configuration Initial Setup through the CLI Required Connections Initial Configuration Steps Logging In Chapter 5: System Configuration Advanced Configuration System Identification TCP / IP Settings RADIUS SSH Settings 1-1 1-2 1-2 1-3 1-3 1-4 1-4 1-4 1-5 1-5 1-5 1-6 2-1 3-1 3-2 3-2 3-3 3-4 3-5 3-6 4-1 4-1 4-1 4-2 4-3 5-1 5-2 5-3 5-5 5-7 5-11 xi Contents Authentication Filter Control VLAN WDS Settings AP Management Administration System Log SNMP Configuring SNMP and Trap Message Parameters Configuring SNMPv3 Users Configuring SNMPv3 Trap Filters Configuring SNMPv3 Targets Radio Interface Security Status Information Access Point Status Station Status Event Logs Chapter 6: 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 Partial Keyword Lookup Negating the Effect of Commands Using Command History Understanding Command Modes Exec Commands Configuration Commands Command Line Processing Command Groups General Commands configure end exit ping reset show history xii 5-12 5-17 5-19 5-21 5-27 5-28 5-33 5-37 5-38 5-43 5-45 5-47 5-49 5-66 5-85 5-85 5-88 5-91 6-1 6-1 6-1 6-1 6-1 6-2 6-2 6-3 6-3 6-3 6-4 6-4 6-4 6-4 6-5 6-5 6-6 6-6 6-7 6-8 6-8 6-8 6-9 6-10 6-10 Contents show line System Management Commands country prompt system name username password ip ssh-server enable ip ssh-server port ip telnet-server enable ip http port ip http server ip https port ip https server APmgmtIP APmgmtUI show apmagement show system show version show config show hardware System Logging Commands logging on logging host logging console logging level logging facility-type logging clear show logging show event-log System Clock Commands sntp-server ip sntp-server enable sntp-server date-time sntp-server daylight-saving sntp-server timezone show sntp DHCP Relay Commands dhcp-relay enable dhcp-relay show dhcp-relay SNMP Commands snmp-server community snmp-server contact snmp-server location 6-11 6-11 6-12 6-14 6-14 6-15 6-15 6-16 6-16 6-17 6-17 6-18 6-18 6-19 6-20 6-21 6-21 6-22 6-23 6-23 6-27 6-27 6-28 6-28 6-29 6-29 6-30 6-31 6-31 6-32 6-32 6-33 6-33 6-34 6-35 6-35 6-36 6-37 6-37 6-38 6-38 6-39 6-40 6-40 6-41 xiii Contents snmp-server enable server snmp-server host snmp-server trap snmp-server engine-id snmp-server user snmp-server targets snmp-server filter snmp-server filter-assignments show snmp groups show snmp users show snmp group-assignments show snmp target show snmp filter show snmp filter-assignments show snmp Flash/File Commands bootfile copy delete dir show bootfile RADIUS Client radius-server address radius-server port radius-server key radius-server retransmit radius-server timeout radius-server port-accounting radius-server timeout-interim radius-server radius-mac-format radius-server vlan-format show radius 802.1X Authentication 802.1x 802.1x broadcast-key-refresh-rate 802.

1x session-key-refresh-rate 802.1x session-timeout 802.1x-supplicant enable 802.1x-supplicant user show authentication MAC Address Authentication address filter default address filter entry address filter delete mac-authentication server xiv 6-41 6-42 6-43 6-45 6-45 6-47 6-48 6-49 6-49 6-50 6-50 6-51 6-51 6-52 6-53 6-54 6-54 6-55 6-56 6-57 6-57 6-58 6-58 6-59 6-59 6-60 6-60 6-61 6-61 6-62 6-62 6-63 6-64 6-64 6-65 6-66 6-66 6-67 6-67 6-68 6-69 6-69 6-70 6-70 6-71 Contents mac-authentication session-timeout Filtering Commands filter local-bridge filter ap-manage filter uplink enable filter uplink filter ethernet-type enable filter ethernet-type protocol show filters WDS Bridge Commands bridge role (WDS) bridge-link parent bridge-link child bridge dynamic-entry age-time show bridge aging-time show bridge filter-entry show bridge link Spanning Tree Commands bridge stp enable bridge stp forwarding-delay bridge stp hello-time bridge stp max-age bridge stp priority bridge-link path-cost bridge-link port-priority show bridge stp Ethernet Interface Commands interface ethernet dns server ip address ip dhcp speed-duplex shutdown show interface ethernet Wireless Interface Commands interface wireless vap speed multicast-data-rate channel transmit-power radio-mode preamble antenna control antenna id 6-71 6-72 6-72 6-73 6-73 6-74 6-74 6-75 6-76 6-76 6-77 6-77 6-78 6-79 6-79 6-80 6-80 6-82 6-82 6-83 6-83 6-84 6-84 6-85 6-85 6-86 6-87 6-87 6-88 6-88 6-89 6-90 6-91 6-91 6-92 6-94 6-94 6-95 6-95 6-96 6-96 6-97 6-98 6-98 6-99 xv Contents antenna location beacon-interval dtim-period fragmentation-length rts-threshold super-g description ssid closed-system max-association assoc-timeout-interval auth-timeout-value shutdown show interface wireless show station Rogue AP Detection Commands rogue-ap enable rogue-ap authenticate rogue-ap duration rogue-ap interval rogue-ap scan show rogue-ap Wireless Security Commands auth encryption key transmit-key cipher-suite mic_mode wpa-pre-shared-key pmksa-lifetime pre-authentication Link Integrity Commands link-integrity ping-detect link-integrity ping-host link-integrity ping-interval link-integrity ping-fail-retry link-integrity ethernet-detect show link-integrity IAPP Commands iapp VLAN Commands vlan management-vlanid vlan-id xvi 6-100 6-100 6-101 6-101 6-102 6-103 6-103 6-104 6-104 6-105 6-105 6-105 6-106 6-107 6-108 6-108 6-109 6-110 6-110 6-111 6-112 6-112 6-113 6-113 6-115 6-116 6-117 6-118 6-119 6-120 6-120 6-121 6-122 6-123 6-123 6-124 6-124 6-124 6-125 6-126 6-126 6-127 6-127 6-128 6-128 Contents WMM Commands wmm wmm-acknowledge-policy wmmparam Appendix A: Troubleshooting Appendix B: Cables and Pinouts Twisted-Pair Cable Assignments 10/100BASE-TX Pin Assignments Straight-Through Wiring Crossover Wiring Console Port Pin Assignments Wiring Map for Serial Cable Appendix C: Specifications General Specifications Sensitivity Transmit Power Operating Range Glossary Index 6-129 6-130 6-130 6-131 A-1 B-1 B-1 B-1 B-2 B-3 B-3 B-4 C-1 C-1 C-3 C-3 C-5 xvii Contents xviii Chapter 1: Introduction The 2.

4 GHz Wireless Access Point is an IEEE 802.11b/g access point that provides transparent, wireless high-speed data communications between the wired LAN and fixed or mobile devices equipped with an 802.11b, or 802.11g wireless adapter. This solution offers fast, reliable wireless connectivity with considerable cost savings over wired LANs (which include long-term maintenance overhead for cabling). Using 802.

11b and 802.11g technology, this access point can easily replace a 10 Mbps Ethernet connection or seamlessly integrate into a 10/100 Mbps Ethernet LAN. The access point supports up to eight Virtual Access Points. This allows traffic to be separated for different user groups using an access point that services one area. For each VAP, different security settings, VLAN assignments, and other parameters can be applied.

Each radio interface on the access point can operate in one of four modes: · Access Point Providing conectivity to wireless clients in the service area. · Repeater Providing an extended link to a remote access point from the wired LAN. In this mode, the access point does not have a cable connection to the wired Ethernet LAN. · Bridge Providing links to access points operating in "Bridge" or "Root Bridge" mode and thereby connecting other wired LAN segments. · Root Bridge Providing links to other access points operating in "Bridge" mode and thereby connecting other wired LAN segments.

Only one unit in the wireless bridge network can be set to "Root Bridge" mode. In addition, the access point offers full network management capabilities through an easy to configure web interface, a command line interface for initial configuration and troubleshooting, and support for Simple Network Management Protocol tools. Radio Characteristics The IEEE 802.11b/g standard uses a radio modulation technique known as Orthogonal Frequency Division Multiplexing (OFDM), and a shared collision domain (CSMA/CA). It operates at the 2.4 GHz Unlicensed National Information Infrastructure (UNII) band for connections to 802.11g clients. IEEE 802.11g includes backward compatibility with the IEEE 802.11b standard.

IEEE 802.11b also operates at 2.4 GHz, but uses Direct Sequence Spread Spectrum (DSSS) and Complementary Code Keying (CCK) modulation technology to achieve a communication rate of up to 11 Mbps. The access point supports a 54 Mbps half-duplex connection to Ethernet networks for each active channel. 1-1 1 Introduction Package Checklist The 2.4 GHz Wireless Access Point package includes: · · · · · · One 2.4 GHz Wireless Access Point One Category 5 network cable One RS-232 console cable One AC power adapter and power cord Four rubber feet User Guide CD Inform your dealer if there are any incorrect, missing or damaged parts. If possible, retain the carton, including the original packing materials. Use them again to repack the product in case there is a need to return it. Hardware Description Top Panel Antennas LED Indicators 1-2 Hardware Description Rear Panel 1 RJ-45 Port Security Slot 5 VDC Power Socket Reset Button Console Port Antennas The access point includes integrated diversity antennas for wireless communications.

A diversity antenna system uses two identical antennas to receive and transmit signals, helping to avoid multipath fading effects. When receiving, the access point checks both antennas and selects the one with the strongest signal. When transmitting, it will continue to use the antenna previously selected for receiving. The access point never transmits from both antennas at the same time. The antennas transmit the outgoing signal as a toroidal sphere (doughnut shaped), with the coverage extending most in a direction perpendicular to the antenna.

The antenna should be adjusted to an angle that provides the appropriate coverage for the service area. For further information, see "Positioning the Antennas" on 2-2. LED Indicators The access point includes three status LED indicators, as described in the following figure and table. 802.11b/g Wireless Link/Activity Power Ethernet Link/Activity 1-3 1 Introduction LED PWR Status On Flashing Link On Flashing 11g On Flashing Off Description Indicates that the system is working normally.

Indicates running a self-test or loading the software program. Indicates a valid 10/100 Mbps Ethernet cable link. Indicates that the access point is transmitting or receiving data on a 10/100 Mbps Ethernet LAN. Flashing rate is proportional to network activity. Indicates that the 802.11b/g radio is enabled. Indicates that the access point is transmitting or receiving data through wireless links. Flashing rate is proportional to network activity. Indicates that the 802.11b/g radio is disabled.

Flashing (Prolonged) Indicates system errors. Security Slot The access point includes a Kensington security slot on the rear panel. You can prevent unauthorized removal of the access point by wrapping the Kensington security cable (not provided) around an unmovable object, inserting the lock into the slot, and turning the key. Console Port This port is used to connect a console device to the access point through a serial cable. This connection is described under "Console Port Pin Assignments" on page B-3. The console device can be a PC or workstation running a VT-100 terminal emulator, or a VT-100 terminal. Ethernet Port The access point has one 10BASE-T/100BASE-TX RJ-45 port that can be attached directly to 10BASE-T/100BASE-TX LAN segments. These segments must conform to the IEEE 802.3 or 802.3u specifications.

This port supports automatic MDI/MDI-X operation, so you can use straight-through cables for all network connections to PCs, switches, or hubs. The access point appears as an Ethernet node and performs a bridging function by moving packets from the wired LAN to remote workstations on the wireless infrastructure. Note: The RJ-45 port also supports Power over Ethernet (PoE) based on the IEEE 802.3af standard. Refer to the description for the "Power Connector" for information on supplying power to the access point's network port from a network device, such as a switch, that provides Power over Ethernet (PoE).

1-4 Features and Benefits 1 Reset Button This button is used to reset the access point or restore the factory default configuration. If you hold down the button for less than 5 seconds, the access point will perform a hardware reset. If you hold down the button for 5 seconds or more, any configuration changes you may have made are removed, and the factory default configuration is restored to the access point. Power Connector The access point does not have a power switch. It is powered on when connected to the AC power adapter, and the power adapter is connected to a power source.

The power adapter automatically adjusts to any voltage between 100-240 volts at 50 or 60 Hz.

No voltage range settings are required. The access point may also receive Power over Ethernet (PoE) from a switch or other network device that supplies power over the network cable based on the IEEE 802.3af standard. Note that if the access point is connected to a PoE source device and also connected to a local power source through the AC power adapter, PoE will be disabled. Features and Benefits · Local network connection via 10/100 Mbps Ethernet ports or 54 Mbps wireless interface (supporting up to 128 mobile users) · IEEE 802.11b and 802.11g compliant · Interoperable with multiple vendors based on the IEEE 802.11f protocol · Advanced security through 64/128/152-bit Wired Equivalent Protection (WEP) encryption, IEEE 802.1X authentication via a RADIUS server, Wi-Fi Protected Access (WPA), and MAC address filtering features to protect your sensitive data and authenticate only authorized users to your network · Provides seamless roaming within the IEEE 802.

11b and 802.11g WLAN environment · Scans all available channels and selects the best channel for each client based on the signal-to-noise ratio · Allows the country of operation to be set to match regulatory requirements (for countries outside of the United States) 1-5 1 Introduction System Defaults The following table lists some of the access point's basic system defaults. To reset the access point defaults, use the CLI command "reset configuration" from the Exec level prompt. Table 1-1. System Defaults Feature Identification Administration Parameter System Name User Name Password General HTTP Server HTTP Server Port HTTP Server HTTP Server Port TCP/IP DHCP IP Address Subnet Mask Default Gateway Primary DNS IP Secondary DNS IP RADIUS (Primary and Secondary) IP Address Port Key Timeout Retransmit attempts Accounting Port Interim Update Timeout SSH Server Status Server Port PPPoE PPPoE Status Default SMC admin smcadmin Enabled 80 Enabled 443 Enabled 192.168.2.2 255.255.255.
0 0.0.0.0 0.0.
0.0 0.0.0.0 0.
0.0.0 1812 DEFAULT 5 seconds 3 0 (Disabled) 3600 seconds Enabled 22 Disabled 1-6 System Defaults Table 1-1. System Defaults Feature MAC Authentication Parameter MAC Authentication Session Timeout Local MAC System Default Local MAC Permission 802.1X Authentication Status Broadcast Key Refresh Session Key Refresh Reauthentication Refresh Rate Supplicant VLAN Management VLAN ID VLAN ID (VAP Interface) VLAN Tag Support QoS QoS Mode SVP (SpectraLink Voice Priority) Filter Control Local Bridge AP Management Ethernet Type SNMP Status Location Contact Community (Read Only) Community (Read/Write) Traps Trap Destination (1-4) Trap Destination IP Address Trap Destination Community Name SNMP v3 Groups Default Disabled 0 minutes (disabled) Allowed Allowed Disabled 0 minutes (disabled) 0 minutes (disabled) 0 seconds (disabled) Disabled 1 1 Disabled Off Disabled Disabled Enabled Disabled Enabled null null Public Private Enabled Disabled null Public RO RWAuth RWPriv none 1 SNMP v3 Users 1-7 1 Introduction Table 1-1. System Defaults Feature System Logging Parameter Syslog Logging Host Logging Console IP Address / Host Name Logging Level Logging Facility Type System Clock SNTP Server Status SNTP Server 1 IP SNTP Server 2 IP Date and Time Daylight Saving Time Time Zone Ethernet Interface Wireless Interface 802.11b/g Speed and Duplex IAPP SSID Radio Mode Status Auto Channel Select Closed System Transmit Power Max Station Data Rate Multicast Data Rate Preamble Length Beacon Interval Default Disabled Disabled Disabled 0.0.0.0 Informational 16 Enabled 137.

92.140.80 192.43.244.18 00:00, Jan 1, 1970 (when there is no time server) Disabled GMT-5 (Eastern Time, US and Canada) Auto Enabled SMC b+g Disabled Enabled Disabled Full 54 Mbps 5.5 Mbps Long 100 TUs Data Beacon Rate (DTIM Interval) 1 beacon RTS Threshold Association Timeout Interval Authentication Timeout Interval Rogue AP Detection Antenna Control Method 2347 bytes 30 minutes 60 minutes Disabled Diversity 1-8 System Defaults Table 1-1. System Defaults Feature Wireless Interface 802.11b/g (contd.) Wireless Security 802.
11b/g Parameter Antenna ID Antenna Location Authentication Type Data Encryption WEP Key Length WEP Key Type WEP Transmit Key Number WEP Keys WPA Configuration Mode WPA Key Management WPA PSK Type Multicast Cipher Link Integrity Status Ping Interval Fail Retry Count Default 0x0000 Indoor Open System Disabled 128 bits Hexadecimal 1 null WEP Only (Disabled) WPA Pre-shared Key Alphanumeric WEP Disabled 30 seconds 6 1 1-9 1 Introduction 1-10 Chapter 2: Hardware Installation 1. Select a Site Choose a proper place for the access point. In general, the best location is at the center of your wireless coverage area, within line of sight of all wireless devices. Try to place the access point in a position that can best cover its Basic Service Set (refer to "Infrastructure Wireless LAN" on page 3-3). For optimum performance, consider these points: · Mount the access point as high as possible above any obstructions in the coverage area.
· Avoid mounting next to or near building support columns or other obstructions that may cause reduced signal or null zones in parts of the coverage area. · Mount away from any signal absorbing or reflecting structures (such as those containing metal). 2. Mount the Access Point The access point can be mounted on any horizontal surface. Mounting on a horizontal surface To keep the access point from sliding on the surface, attach the four rubber feet provided in the accessory kit to the marked circles on the bottom of the access point.
3. Lock the Access Point in Place To prevent unauthorized removal of the access point, you can use a Kensington Slim MicroSaver security cable (not included) to attach the access point to a fixed object. 2-1 2 4. Hardware Installation Connect the Power Cord Connect the power adapter to the access point, and the power cord to an AC power outlet. Otherwise, the access point can derive its operating power directly from the RJ-45 port when connected to a device that provides IEEE 802.3af compliant Power over Ethernet (PoE). Note: If the access point is connected to both a PoE source device and an AC power source, AC power will be disabled. Caution: Use ONLY the power adapter supplied with this access point. Otherwise, the product may be damaged. 5.

Observe the Self Test When you power on the access point, verify that the PWR indicator stops flashing and remains on, and that the other indicators start functioning as described under "LED Indicators" on page 1-3. If the PWR LED does not stop flashing, the self test has not completed correctly. Refer to "Troubleshooting" on page A-1. Connect the Ethernet Cable The access point can be wired to a 10/100 Mbps Ethernet through a network device such as a hub or a switch. Connect your network to the RJ-45 port on the back panel with category 3, 4, or 5 UTP Ethernet cable.

When the access point and the connected device are powered on, the Ethernet Link LED should light indicating a valid network connection. If this LED fails to turn on refer to "Troubleshooting" on page A-1. 6. Note: The RJ-45 port on the access point supports auto=MDI/MDI-X operation, so you can use either straight-through or crossover cable to connect to switches or PCs. 7.

Position the Antennas Each antenna emits a radiation pattern that is toroidal (doughnut shaped), with the coverage extending most in the direction perpendicular to the antenna. Therefore, the antennas should be oriented so that the radio coverage pattern fills the intended horizontal space. Also, the diversity antennas should both be positioned along the same axes, providing the same coverage area. For example, if the access point is mounted on a horizontal surface, both antennas should be positioned pointing vertically up to provide optimum coverage. Connect the Console Port Connect the console cable (included) to the RS-232 console port for accessing the command-line interface.

You can manage the access point using the console port (Chapter 6), the web interface (Chapter 5), or SNMP management software such as SMC's EliteView. 8. 2-2 Chapter 3: Network Configuration Wireless networks support a stand-alone configuration as well as an integrated configuration with 10/100 Mbps Ethernet LANs. The 2.4 GHz Wireless Access Point also provides repeater and bridging services.

Access points can be deployed to support wireless clients and connect wired LANs in the following configurations: · · · · · Ad hoc for departmental, SOHO or enterprise LANs Infrastructure for wireless LANs Infrastructure wireless LAN for roaming wireless PCs Infrastructure wireless bridge to connect wired LANs Infrastructure wireless repeater for extended range The 802.11b and 802.11g frequency band which operates at 2.4 GHz can easily encounter interference from other 2.4 GHz devices, such as other 802.11b or g wireless devices, cordless phones and microwave ovens. If you experience poor wireless LAN performance, try the following measures: · · · · Limit any possible sources of radio interference within the service area Increase the distance between neighboring access points Decrease the signal strength of neighboring access points Increase the channel separation of neighboring access points (e.g. up to 5 channels of separation for 802.11b and 802.

11g) 3-1 3 Network Configuration Network Topologies Ad Hoc Wireless LAN (no Access Point) An ad hoc wireless LAN consists of a group of computers, each equipped with a wireless adapter, connected via radio signals as an independent wireless LAN. Computers in a specific ad hoc wireless LAN must therefore be configured to the same radio channel. An ad hoc wireless LAN can be used for a branch office or SOHO operation. Ad Hoc Wireless LAN Notebook with Wireless USB Adapter Notebook with Wireless PC Card PC with Wireless PCI Adapter 3-2 Network Topologies 3 Infrastructure Wireless LAN The access point also provides access to a wired LAN for wireless workstations. An integrated wired/wireless LAN is called an Infrastructure configuration. A Basic Service Set (BSS) consists of a group of wireless PC users, and an access point that is directly connected to the wired LAN. Each wireless PC in this BSS can talk to any computer in its wireless group via a radio link, or access other computers or network resources in the wired LAN infrastructure via the access point. The infrastructure configuration not only extends the accessibility of wireless PCs to the wired LAN, but also increases the effective wireless transmission range for wireless PCs by passing their signal through one or more access points. A wireless infrastructure can be used for access to a central database, or for connection between mobile workers, as shown in the following figure. Wired LAN Extension to Wireless Clients Server Desktop PC Switch Access Point Notebook PC Desktop PC 3-3 3 Network Configuration Infrastructure Wireless LAN for Roaming Wireless PCs The Basic Service Set (BSS) defines the communications domain for each access point and its associated wireless clients.

The BSS ID is a 48-bit binary number based on the access point's wireless MAC address, and is set automatically and transparently as clients associate with the access point. The BSS ID is used in frames sent between the access point and its clients to identify traffic in the service area. The BSS ID is only set by the access point, never by its clients. The clients only need to set the Service Set Identifier (SSID) that identifies the service set provided by one or more access points. The SSID can be manually configured by the clients, can be detected in an access point's beacon, or can be obtained by querying for the identity of the nearest access point.

For clients that do not need to roam, set the SSID for the wireless card to that used by the access point to which you want to connect. A wireless infrastructure can also support roaming for mobile workers. More than one access point can be configured to create an Extended Service Set (ESS). By placing the access points so that a continuous coverage area is created, wireless users within this ESS can roam freely. All wireless network cards and adapters and wireless access points within a specific ESS must be configured with the same SSID.

Seamless Roaming Between Access Points Server Desktop PC Switch Switch Access Point Notebook PC Notebook PC Access Point <BSS 2> <BSS 1> Desktop PC <ESS> 3-4 Network Topologies 3 Infrastructure Wireless Bridge The IEEE 802.11 standard defines a WIreless Distribution System (WDS) for bridge connections between BSS areas (access points). The access point uses WDS to forward traffic on links between units. The access point supports WDS bridge links on the 2.4 GHz (802.11b/g) band and can be used with various external antennas to offer flexible deployment options. Up to six WDS bridge links can be specified for each unit in the wireless bridge network. One unit only must be configured as the "root bridge" in the wireless network. The root bridge should be the unit connected to the main core of the wired LAN. Other bridges must configure one "parent" link to the root bridge or to a bridge connected to the root bridge.

The other five available WDS links can be specified as "child" links to other bridges. This forms a tiered-star topology for the wireless bridge network. When set to WDS bridging mode, only other units set to bridge mode can associate to the access point. The access point cannot support wireless clients and bridging at the same time. Network Core Wireless Bridge Links Between Access Points Root Bridge Radio Bridge Link Bridge Radio Bridge Link Radio Bridge Link Bridge Bridge 3-5 3 Network Configuration Infrastructure Wireless Repeater The access point can also operate in a bridge "repeater" mode to extend the range of links to wireless clients.

The access point uses WDS to forward traffic between the repeater bridge and the root bridge. The access point supports up to six WDS repeater links. In repeater mode, the access point does not support an Ethernet link to a wired LAN. Note that when the access point operates in this mode only half the normal throughput is possible. This is because the access point has to receive and then re-transmit all data on the same channel.

Network Core Wireless Repeater Links Between Access Points Root Bridge 802.11g Radio Repeater Link 802.11g Radio Repeater Link Repeater 802.11g Radio AP Link 802.11g Radio AP Link Repeater 3-6 Chapter 4: Initial Configuration The 2.

4 GHz Wireless Access Point offers a variety of management options, including a web-based interface, a direct connection to the console port, Telnet, Secure Shell (SSH), or using SNMP software. The initial configuration steps can be made through the web browser interface or CLI. The access point requests an IP address via DHCP by default. If no response is received from the DHCP server, then the access point uses the default address 192.168.

2.2. If this address is not compatible with your network, you can first use the command line interface (CLI) as described below to configure a valid address. Note: Units sold in countries outside the United States are not configured with a specific country code. You must use the CLI to set the country code and enable wireless operation (page 4-3). Initial Setup through the CLI Required Connections The access point provides an RS-232 serial port that enables a connection to a PC or terminal for monitoring and configuration. Attach a VT100-compatible terminal, or a PC running a terminal emulation program to the access point. You can use the console cable provided with this package, or use a cable that complies with the wiring assignments shown on page B-3. To connect 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.

Connect the other end of the cable to the RS-232 serial port on the access point. Make sure the terminal emulation software is set as follows: · · · · · · 4. Select the appropriate serial port (COM port 1 or 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. 2. 3.

Once you have set up the terminal correctly, press the [Enter] key to initiate the console connection. The console login screen will be displayed. 4-1 4 Initial Configuration For a description of how to use the CLI, see "Using the Command Line Interface" on page 6-1. For a list of all the CLI commands and detailed information on using the CLI, refer to "Command Groups" on page 6-6. Initial Configuration Steps Logging In Enter "admin" for the user name, and "smcadmin" for the password.

The CLI prompt appears displaying the access point's name. Username: admin Password: smcadmin Enterprise AP# Setting the IP Address By default, the access point is configured to obtain IP address settings from a DHCP server. If a DHCP server is not available, the IP address defaults to 192.168.2.

2, which may not be compatible with your network. You will therefore have to use the command line interface (CLI) to assign an IP address that is compatible with your network. Type "configure" to enter configuration mode, then type "interface ethernet" to access the Ethernet interface-configuration mode. Enterprise AP#configure Enterprise AP(config)#interface ethernet Enterprise AP(config-if)# Type "no ip dhcp" to disable DHCP client mode. Then type "ip address ip-address netmask gateway," where "ip-address" is the access point's IP address, "netmask" is the network mask for the network, and "gateway" is the default gateway router. Check with your system administrator to obtain an IP address that is compatible with your network. Enterprise AP(if-ethernet)#no ip dhcp Enterprise AP(if-ethernet)#ip address 192.168.2.2 255.

255.255.0 192.168.2.254 Enterprise AP(if-ethernet)# After configuring the access point's IP parameters, you can access the management interface from anywhere within the attached network. The command line interface can also be accessed using Telnet from any computer attached to the network. 4-2 Logging In Setting the Country Code Units sold in the United States are configured by default to use only radio channels 1-11 in 802.11b or 802.11g mode as defined by FCC regulations.

Units sold in other countries are configured by default without a country code (i.e., 99). You must use the CLI to set the country code. Setting the country code restricts operation of the access point to the radio channels and transmit power levels permitted for wireless networks in the specified country.

Type "exit" to leave configuration mode. Then type "country ?" to display the list of countries. Select the code for your country, and enter the country command again, following by your country code (e.g., tw for Taiwan).

Enterprise AP#country tw Enterprise AP# 4 Note: The CLI examples shown later in this manual abbreviate the console prompt to just "AP." The console prompt can be configured using the "prompt" command (page 6-14). Logging In There are only a few basic steps you need to complete to connect the access point to your corporate network, and provide network access to wireless clients. The access point can be managed by any computer using a web browser (Internet Explorer 5.0 or above, or Netscape 6.2 or above). Enter the default IP address: http://192.168.2.2 Logging In Enter the username "admin," and password "smcadmin" then click LOGIN.

For information on configuring a user name and password, see page 5-28. 4-3 4 Initial Configuration The home page displays the Main Menu. 4-4 Chapter 5: System Configuration Before continuing with advanced configuration, first complete the initial configuration steps described in Chapter 4 to set up an IP address for the access point. The access point can be managed by any computer using a web browser (Internet Explorer 5.0 or above, or Netscape 6.2 or above). Enter the configured IP address of the access point, or use the default address: http://192.168.2.2 To log into the access point, enter the default user name "admin" and the password "smcadmin", then press "LOGIN".

When the home page displays, click on Advanced Setup. The following page will display. The information in this chapter is organized to reflect the structure of the web screens for easy reference. However, it is recommended that you configure a user name and password as the first step under "Administration" to control management access to this device (page 5-28).

5-1 5 System Configuration Advanced Configuration The Advanced Configuration pages include the following options.

Table 5-2. Menu Menu System Identification TCP / IP Settings RADIUS SSH Settings Authentication Filter Control Description Configures basic administrative and client access Specifies the host name Configures the IP address, subnet mask, gateway, and domain name servers Configures the RADIUS server for wireless client authentication and accounting Configures Secure Shell management access Configures 802.1X client authentication, with an option for MAC address authentication Filters communications between wireless clients, access to the management interface from wireless clients, and traffic matching specific Ethernet protocol types Enables VLAN support and sets the management VLAN ID Configures bridge or repeater modes for each radio interface and sets spanning tree parameters Configures access to management interfaces Configures user name and password for management access; upgrades software from local file, FTP or TFTP server; resets configuration settings to factory defaults; and resets the access point Controls logging of error messages; sets the system clock via SNTP server or manual configuration Configures SNMP settings Controls access to this access point from management stations using SNMP, as well as the hosts that will receive trap messages Defines trap filters for SNMPv3 users Specifies SNMPv3 users that will receive trap messages Configures the IEEE 802.11g interface Configures common radio signal parameters and other settings for each VAP interface Enables each VAP interface, sets the SSID, and configures wireless security Displays information about the access point and wireless clients Displays configuration settings for the basic system and the wireless interface Page 5-3 5-3 5-5 5-7 5-11 5-12 5-17 VLAN WDS Settings AP Management Administration 5-19 5-21 5-27 5-28 System Log SNMP SNMP SNMP Trap Filters SNMP Targets Radio Interface G Radio Settings Security Status AP Status 5-33 5-37 5-37 5-45 5-47 5-49 5-49 5-66 5-85 5-85 5-2 Advanced Configuration Table 5-2. Menu Menu Station Station Event Logs Description Shows the wireless clients currently associated with the access point Shows log messages stored in memory 5 Page 5-88 5-91 System Identification The system name for the access point can be left at its default setting.

However, modifying this parameter can help you to more easily distinguish different devices in your network. System Name An alias for the access point, enabling the device to be uniquely identified on the network. (Default: Enterprise Wireless AP; Range: 1-32 characters) 5-3 5 System Configuration CLI Commands for System Identification Enter the global configuration mode, and use the system name command to specify a new system name. Then return to the Exec mode, and use the show system command to display the changes to the system identification settings. Enterprise Enterprise Enterprise Enterprise AP#config AP(config)#system name R&D AP(config)#end AP#show system 6-14 6-87 6-22 6-8 6-14 6-87 6-22 Enterprise AP#config Enter configuration commands, one per line. Enterprise AP(config)#system name R&D Enterprise AP(config)#end Enterprise AP#show system System Information ========== Serial Number : System Up time : 0 days, 0 hours, 32 minutes, 22 seconds System Name : R&D System Location : System Contact : Contact System Country Code : US - UNITED STATES MAC Address : 00-12-CF-12-34-60 Radio A MAC Address : 00-12-CF-12-34-61 Radio G MAC Address : 00-12-CF-12-34-65 IP Address : 192.168.2.2 Subnet Mask : 255.255.

255.0 Default Gateway : 0.0.0.0 VLAN State : DISABLED Management VLAN ID(AP): 1 IAPP State : ENABLED DHCP Client : ENABLED HTTP Server : ENABLED HTTP Server Port : 80 HTTPS Server : ENABLED HTTPS Server Port : 443 Slot Status : Single band(b/g) Boot Rom Version : v1.1.5 Software Version : v5.0.0.0 SSH Server : ENABLED SSH Server Port : 22 Telnet Server : ENABLED DHCP Relay : DISABLED ========== Enterprise AP# 5-4 Advanced Configuration 5 TCP / IP Settings Configuring the access point with an IP address expands your ability to manage the access point.

A number of access point features depend on IP addressing to operate. Note: You can use the web browser interface to access IP addressing only if the access point already has an IP address that is reachable through your network. By default, the access point will be automatically configured with IP settings from a Dynamic Host Configuration Protocol (DHCP) server. However, if you are not using a DHCP server to configure IP addressing, use the CLI to manually configure the initial IP values (see page 4-2). After you have network access to the access point, you can use the web browser interface to modify the initial IP configuration, if needed.

Note: If there is no DHCP server on your network, or DHCP fails, the access point will automatically start up with a default IP address of 192.168.2.2. DHCP Client (Enable) Select this option to obtain the IP settings for the access point from a DHCP (Dynamic Host Configuration Protocol) server. The IP address, subnet mask, default gateway, and Domain Name Server (DNS) address are dynamically assigned to the access point by the network DHCP server. (Default: Enabled) DHCP Client (Disable) Select this option to manually configure a static address for the access point. · IP Address: The IP address of the access point. Valid IP addresses consist of four decimal numbers, 0 to 255, separated by periods. 5-5 5 System Configuration · Subnet Mask: The mask that identifies the host address bits used for routing to specific subnets. · Default Gateway: The default gateway is the IP address of the router for the access point, which is used if the requested destination address is not on the local subnet. If you have management stations, DNS, RADIUS, or other network servers located on another subnet, type the IP address of the default gateway router in the text field provided. Otherwise, leave the address as all zeros (0.0.0.

0). · Primary and Secondary DNS Address: The IP address of Domain Name Servers on the network. A DNS maps numerical IP addresses to domain names and can be used to identify network hosts by familiar names instead of the IP addresses. If you have one or more DNS servers located on the local network, type the IP addresses in the text fields provided. Otherwise, leave the addresses as all zeros (0.0.0.0). CLI Commands for TCP/IP Settings From the global configuration mode, enter the interface configuration mode with the interface ethernet command. Use the ip dhcp command to enable the DHCP client, or no ip dhcp to disable it.

To manually configure an address, specify the new IP address, subnet mask, and default gateway using the ip address command.

To specify DNS server addresses use the dns server command. Then use the show interface ethernet command from the Exec mode to display the current IP settings. Enterprise AP(config)#interface ethernet 6-87 Enter Ethernet configuration commands, one per line. Enterprise AP(if-ethernet)#no ip dhcp 6-89 Enterprise AP(if-ethernet)#ip address 192.
168.1.2 255.255.255.
0 192.168.1.253 6-88 Enterprise AP(if-ethernet)#dns primary-server 192.168.1.556-88 Enterprise AP(if-ethernet)#dns secondary-server 10.1.0.556-88 Enterprise AP(config)#end 6-8 Enterprise AP#show interface ethernet 6-91 Ethernet Interface Information
========== IP Address : 192.

168.1.2 Subnet Mask : 255.255.255.0 Default Gateway : 192.168.1.253 Primary DNS : 192.168.
1.55 Secondary DNS : 10.1.0.55 Speed-duplex : 100Base-TX Full Duplex Admin status : Up Operational status : Up
========== Enterprise AP# 5-6 Advanced Configuration 5 RADIUS Remote Authentication Dial-in User Service (RADIUS) is an authentication protocol that uses software running on a central server to control access to RADIUS-aware devices on the network.
An authentication server contains a database of user credentials for each user that requires access to the network. A primary RADIUS server must be specified for the access point to implement IEEE 802.1X network access control and Wi-Fi Protected Access (WPA) wireless security. A secondary RADIUS server may also be specified as a backup should the primary server fail or become inaccessible. In addition, the configured RADIUS server can also act as a RADIUS Accounting server and receive user-session accounting information from the access point.
RADIUS Accounting can be used to provide valuable information on user activity in the network. Note: This guide assumes that you have already configured RADIUS server(s) to support the access point. Configuration of RADIUS server software is beyond the scope of this guide, refer to the documentation provided with the RADIUS server software. 5-7 5 System Configuration 5-8 Advanced Configuration MAC Address Format MAC addresses can be specified in one of four formats, using no delimeter, with a single dash delimeter, with multiple dash delimeters, and with multiple colon delimeters. 5 VLAN ID Format A VLAN ID (a number between 1 and 4094) can be assigned to each client after successful authentication using IEEE 802.1X and a central RADIUS server. The user VLAN IDs must be configured on the RADIUS server for each user authorized to access the network. VLAN IDs can be entered as hexadecimal numbers or as ASCII strings. Primary Radius Server Setup Configure the following settings to use RADIUS authentication on the access point. · IP Address: Specifies the IP address or host name of the RADIUS server.

· Port: The UDP port number used by the RADIUS server for authentication messages. (Range: 1024-65535; Default: 1812) · Key: A shared text string used to encrypt messages between the access point and the RADIUS server. Be sure that the same text string is specified on the RADIUS server. Do not use blank spaces in the string. (Maximum length: 255 characters) · Timeout: Number of seconds the access point waits for a reply from the RADIUS server before resending a request. (Range: 1-60 seconds; Default: 5) · Retransmit attempts: The number of times the access point tries to resend a request to the RADIUS server before authentication fails. (Range: 1-30; Default: 3) · Accounting Port: The RADIUS Accounting server UDP port used for accounting messages. (Range: 0 or 1024-65535; Default: 0, disabled) · Interim Update Timeout: The interval between transmitting accounting updates to the RADIUS server. (Range: 60-86400; Default: 3600 seconds) Note: For the Timeout and Retransmit attempts fields, accept the default values unless you experience problems connecting to the RADIUS server over the network. Secondary Radius Server Setup Configure a secondary RADIUS server to provide a backup in case the primary server fails.
The access point uses the secondary server if the primary server fails or becomes inaccessible. Once the access point switches over to the secondary server, it periodically attempts to establish communication again with primary server. If communication with the primary server is re-established, the secondary server reverts to a backup role. 5-9 5 System Configuration CLI Commands for RADIUS From the global configuration mode, use the radius-server address command to specify the address of the primary or secondary RADIUS servers. (The following example configures the settings for the primary RADIUS server.) Configure the other parameters for the RADIUS server. Then use the show show radius command from the Exec mode to display the current settings for the primary and secondary RADIUS servers. Enterprise Enterprise Enterprise Enterprise Enterprise Enterprise Enterprise Enterprise Enterprise AP(config)#radius-server AP(config)#radius-server AP(config)#radius-server AP(config)#radius-server AP(config)#radius-server AP(config)#radius-server AP(config)#radius-server AP(config)#exit AP#show radius address 192.168.1.
*256-58 port 181 6-59 key green 6-59 timeout 10 6-60 retransmit 5 6-60 port-accounting 18136-61 timeout-interim 5006-61 6-63 Radius Server Information ========== IP : 192.168.1.25 Port : 181 Key : ***** Retransmit :5 Timeout : 10 Radius MAC format : no-delimiter Radius VLAN format : HEX ========== Radius Secondary Server Information ========== IP : 0.0.0.0 Port : 1812 Key : ***** Retransmit :3 Timeout :5 Radius MAC format : no-delimiter Radius VLAN format : HEX ========== Enterprise AP# 5-10 Advanced Configuration 5 SSH Settings Telnet is a remote management tool that can be used to configure the access point from anywhere in the network. However, Telnet is not secure from hostile attacks. The Secure Shell (SSH) can act as a secure replacement for Telnet. The SSH protocol uses generated public keys to encrypt all data transfers passing between the access point and SSH-enabled management station clients and ensures that data traveling over the network arrives unaltered.*

Clients can then securely use the local user name and password for access authentication. Note that SSH client software needs to be installed on the management station to access the access point for management via the SH protocol. Notes: 1. The access point supports only SSH version 2.0. 2. After boot up, the SSH server needs about two minutes to generate host encryption keys. The SSH server is disabled while the keys are being generated. SSH Settings · Telnet Server Status: Enables or disables the Telnet server. (Default: Enabled) · SSH Server Status: Enables or disables the SSH server. (Default: Enabled) · SSH Server Port: Sets the UDP port for the SSH server.