SMC Networks | USER GUIDE

Manual abstract:

@@@@SMC reserves the right to change specifications at any time without notice. Copyright © 2009 by SMC Networks, Inc. 20 Mason Irvine, CA 92618 All rights reserved Trademarks: SMC is a registered trademark; and EZ Switch, TigerStack, TigerSwitch, and TigerAccess are trademarks of SMC Networks, Inc. Other product and company names are trademarks or registered trademarks of their respective holders. WARRANTY AND PRODUCT REGISTRATION To register SMC products and to review the detailed warranty statement, please refer to the Support Section of the SMC Website at http:// www.smc.com. 4 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 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. 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. For product available in the USA/Canada market, only channel 1~11 can be operated.

Selection of other channels is not possible. This device and its antenna(s) must not be co-located or operation in conjunction with any other antenna or transmitter. This device is going to be operated in 5.15~5.25GHz frequency range, it is restricted in indoor environment only.

5 COMPLIANCES 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 minimum distance 20 cm between the radiator & your body. IC STATEMENT : This Class B digital apparatus complies with Canadian ICES-003. Operation is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device. Cet appareil numérique de la classe B conforme á la norme NMB-003 du Canada. To reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the equivalent isotropically radiated power (e.i.r.p) is not more than that permitted for successful communication. This device has been designed to operate with the antennas listed below, and having a maximum gain of 5 dB.

Antennas not included in this list or having a gain greater than 5 dB are strictly prohibited for use with this device. The required antenna impedance is 50 ohms. The device could automatically discontinue transmission in case of absence of information to transmit, or operational failure. Note that this is not intended to prohibit transmission of control or signaling information or the use of repetitive codes where required by the technology. The device for the band 5150-5250 MHz is only for indoor usage to reduce potential for harmful interference to co-channel mobile satellite systems. The maximum antenna gain permitted (for devices in the band 5725-5825 MHz) to comply with the e.i.r.p. limits specified for point-to-point and non point-to-point operation as appropriate, as stated in section A9.

2(3). The maximum antenna gain permitted (for devices in the bands 5250-5350 MHz and 5470-5725 MHz) to comply with the e.i.r.p. limit. High-power radars are allocated as primary users (meaning they have priority) of the bands 5250-5350 MHz and 5650-5850 MHz and these radars could cause interference and/or damage to LE-LAN devices. IMPORTANT NOTE: IC RADIATION EXPOSURE STATEMENT: This equipment complies with IC RSS-102 radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20 cm between the radiator & your body. 6 COMPLIANCES AUSTRALIA/NEW ZEALAND AS/NZS 4771 ACN 066 352010 TAIWAN NCC 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 301 893 - Technical requirements for 5 GHz radio equipment EN 300 328 - Technical requirements for 2.4 GHz radio equipment EN 301 489-1 / EN 301 489-17 - EMC requirements for radio equipment This device is intended for use in the following European Community and EFTA countries: Austria Estonia Hungary Liechtenstein Norway Spain Belgium Finland Iceland Lithuania Poland Sweden Cyprus France Ireland Luxembourg Portugal Switzerland Czech Republic Germany Italy Malta Slovakia United Kingdom Denmark Greece Latvia Netherlands Slovenia Requirements for indoor vs. outdoor operation, license requirements and allowed channels of operation apply in some countries as described 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. 7 COMPLIANCES 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 employs a radar detection feature required for European Community operation in the 5 GHz band. This feature is automatically enabled when the country of operation is correctly configured for any European Community country. The presence of nearby radar operation may result in temporary interruption of operation of this device. The radar detection feature will automatically restart operation on a channel free of radar. The 5 GHz Turbo Mode feature is not allowed for operation in any European Community country. The current setting for this feature is found in the 5 GHz 802.

11a Radio Settings Window as described in the user guide. The 5 GHz radio's Auto Channel Select setting described in the user guide must always remain enabled to ensure that automatic 5 GHz channel selection complies with European requirements. The current setting for this feature is found in the 5 GHz 802.11a Radio Settings Window as described in the user guide. This device is restricted to indoor use when operated in the European Community using the 5. 15 - 5.35 GHz band: Channels 36, 40, 44, 48, 52, 56, 60, 64. See table below for allowed 5 GHz channels by country. 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. 8 COMPLIANCES OPERATION USING 5 GHZ CHANNELS IN THE EUROPEAN COMMUNITY The user/installer must use the provided configuration utility to check the current channel of operation and make necessary configuration changes to ensure operation occurs in conformance with European National spectrum usage laws as described below and elsewhere in this document. Allowed Frequency Bands 5.15 - 5.

25 GHz 5.15 - 5.35 GHz* 5.15 - 5.35* & 5.470 - 5.725 GHz Allowed Channel Numbers 36, 40, 44, 48 36, 40, 44, 48, 52, 56, 60, 64 36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140 Countries Austria, Belgium France, Switzerland, Liechtenstein Denmark, Finland, Germany, Iceland, Ireland, Italy, Luxembourg, Netherlands, Norway, Portugal, Spain, Sweden, U.K. Greece 5 GHz Operation Not Allowed None * Outdoor operation is not allowed using 5.15-5.*

35 GHz bands (Channels 36 - 64). DECLARATION OF CONFORMITY IN LANGUAGES OF THE EUROPEAN COMMUNITY Czech Estonian Eesti English Finnish Suomi Dutch Nederlands Käesolevaga kinnitab SMC seadme Radio LAN device vastavust direktiivi 1999/5/EÜ põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele. 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 Français Swedish Svenska Danish Dansk German Deutsch 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/. 9 COMPLIANCES Hungarian Magyar Italian Italiano Latvian Latviski Lithuanian Alulírott, SMC nyilatkozom, hogy a Radio LAN device megfelel a vonatkozó alapvetõ követelményeknek és az 1999/5/EC irányelv egyéb elõírásainak. Con la presente SMC dichiara che questo Radio LAN device è conforme ai requisiti essenziali ed alle altre disposizioni pertinenticcess Points (VAPs) VAP Basic Settings WDS-STA Mode Wireless Security Settings Wired Equivalent Privacy (WEP) Quality of Service (QoS) 79 79 80 81 81 82 82 84 85 86 89 90 91 92 94 95 9 MAINTENANCE SETTINGS Upgrading Firmware Running Configuration Resetting the Access Point 100 100 103 104 10 STATUS INFORMATION AP Status 14 105 105 CONTENTS AP System Configuration AP Wireless Configuration Station Status Event Logs 105 107 107 108 SECTION III COMMAND LINE INTERFACE 11 USING THE COMMAND LINE INTERFACE Console Connection Telnet Connection Entering Commands Keywords and Arguments Minimum Abbreviation Command Completion Getting Help on Commands Showing Commands Negating the Effect of Commands Using Command History Understanding Command Modes Exec Commands Configuration Commands Command Line Processing 110 112 112 113 114 114 114 114 114 114 115 115 115 116 116 117 12 GENERAL COMMANDS 13 SYSTEM MANAGEMENT COMMANDS 14 SYSTEM LOGGING COMMANDS 15 SYSTEM CLOCK COMMANDS 16 DHCP RELAY COMMANDS 17 SNMP COMMANDS 18 FLASH/FILE COMMANDS 19 RADIUS CLIENT COMMANDS 20 802.1X AUTHENTICATION COMMANDS 21 MAC ADDRESS AUTHENTICATION COMMANDS 15 118 122 137 141 146 148 162 165 171 173 CONTENTS 22 FILTERING COMMANDS 23 SPANNING TREE COMMANDS 24 WDS BRIDGE COMMANDS 25 ETHERNET INTERFACE COMMANDS 26 WIRELESS INTERFACE COMMANDS 27 WIRELESS SECURITY COMMANDS 28 LINK LAYER DISCOVERY COMMANDS 29 VLAN COMMANDS 30 WMM COMMANDS 177 182 193 195 200 214 224 228 231 SECTION IV APPENDICES A TROUBLESHOOTING Diagnosing LED Indicators Before Contacting Technical Support 236 237 237 237 B WDS SETUP EXAMPLES Basic WDS Link Between Two APs WDS Links Between Three or More APs 240 241 246 C HARDWARE SPECIFICATIONS D CABLES AND PINOUTS Twisted-Pair Cable Assignments 10/100BASE-TX Pin Assignments Straight-Through Wiring Crossover Wiring 1000BASE-T Pin Assignments Console Port Pin Assignments 249 252 252 252 253 254 254 256 GLOSSARY INDEX 257 261 16 FIGURES Figure 1: Top Panel Figure 2: Rear Panel Figure 3: Ports Figure 4: External Antenna Connectors Figure 5: Screw-off External Antenna Connector - Close Up Figure 6: LEDs Figure 7: Infrastructure Wireless LAN Figure 8: Infrastructure Wireless LAN for Roaming Wireless PCs Figure 9: Bridging Mode Figure 10: Attach Feet Figure 11: Wall Mounting Figure 12: Login Page Figure 13: Home Page Figure 14: Set Configuration Changes Figure 15: Help Menu Figure 16: Quick Start - Step 1 Figure 17: Quick Start - Step 2 Figure 18: Quick Start - Step 3 Figure 19: Administration Figure 20: IP Configuration Figure 21: RADIUS Settings Figure 22: SNTP Settings Figure 23: SVP Settings Figure 24: Setting the VLAN Identity Figure 25: System Log Settings Figure 26: Remote Management Figure 27: Access Limitation Figure 28: SNMP Basic Settings Figure 29: SNMP Trap Settings Figure 30: SNMP VACM Figure 31: Configuring SNMPv3 Users 17 29 29 30 31 31 32 35 36 37 39 40 42 43 44 44 45 46 48 52 53 55 56 58 59 60 63 64 66 67 68 69 FIGURES Figure 32: SNMPv3 Targets Figure 33: SNMP Notification Filter Figure 34: Local Bridge Filter Figure 35: LLDP Settings Figure 36: Source ACLs Figure 37: Destination ACLs Figure 38: Ethernet Type Filter Figure 39: Spanning Tree Protocol Figure 40: Local Authentication Figure 41: RADIUS Authentication Figure 42: Interface Mode Figure 43: Radio Settings Figure 44: VAP Settings Figure 45: VAP Basic Settings Figure 46: WDS-STA Mode Figure 47: Configuring VAPs - Common Settings Figure 48: WEP Configuration Figure 49: WMM Backoff Wait Times Figure 50: QoS Figure 51: Firmware Figure 52: Running Configuration File Figure 53: Resetting the Access Point Figure 54: AP System Configuration Figure 55: AP Wireless Configuration Figure 56: Station Status Figure 57: Event Logs Figure 58: Basic WDS Link Between Two APs Figure 59: WDS Example -- Access Point A VAP Setting Figure 60: WDS Example -- Access Point A VAP Details Figure 61: WDS Example -- Access Point A WDS-AP VAP Setting Figure 62: WDS Example -- Access Point A VAP SSID and MAC Figure 63: WDS Example -- Access Point B VAP Details Figure 64: WDS Example -- Access Point B WDS-STA VAP

1x Authentication Table 18: MAC Address Authentication Table 19: Filtering Commands Table 20: Spanning Tree Commands Table 21: WDS Bridge Commands Table 22: Ethernet Interface Commands Table 23: Wireless Interface Commands Table 24: Wireless Security Commands Table 25: Link Layer Discovery Commands Table 26: VLAN Commands Table 27: WMM Commands Table 28: AP Parameters Table 29: BSS Parameters Table 30: LED Indicators Table 31: 10/100BASE-TX MDI and MDI-X Port Pinouts 20 27 32 61 96 116 117 118 122 123 137 139 141 146 148 162 165 171 173 177 182 193 195 200 214 224 228 231 233 233 237 253 TABLES Table 32: 1000BASE-T MDI and MDI-X Port Pinouts Table 33: Console Port Pinouts 255 256 21 TABLES 22 INDEX OF CLI COMMANDS NUMERICS 802.1x enable 171 802.1x session-timeout 172 D dhcp-relay server dns 196 dtim-period 207 dual-image 162 146 A address filter default 173 address filter delete 174 address filter entry 174 a-mpdu 201 a-msdu 202 apmgmtui ssh enable 125 apmgmtip 130 apmgmtui http port 127 apmgmtui http server 127 apmgmtui http session-timeout 128 apmgmtui https port 128 apmgmtui https server 129 apmgmtui snmp 130 apmgmtui ssh port 126 apmgmtui telnet-server enable 126 assoc-timeout-interval 210 auth 214 auth-timeout-interval 210 E encryption end 119 exit 119 216 F filter filter filter filter filter filter acl-destination-address 179 acl-source-address 178 ap-manage 178 ethernet-type enabled 179 ethernet-type protocol 180 local-bridge 177 I interface ethernet 195 interface wireless 201 interface-radio-mode 204 ip address 196 ip dhcp 197 B beacon-interval 207 bridge stp br-conf forwarding-delay 183 bridge stp br-conf hello-time 184 bridge stp br-conf max-age 184 bridge stp br-conf priority 185 bridge stp port-conf interface 185 bridge stp service 183 bridge-link path-cost 186 bridge-link port-priority 186 K key 217 L lldp service 224 lldp transmit delay-to-local-change 226 lldp transmit interval 225 lldp transmit re-init-delay 226 lldp-transmit hold-muliplier 225 logging clear 139 logging console 138 logging host 138 logging level 139 logging on 137 C channel 202 cipher-suite 219 cli-session-timeout 119 closed-system 209 configure 118 copy 163 country 123 23 INDEX OF CLI COMMANDS M mac-authentication server 175 mac-authentication session-timeout 175 make-radius-effective 169 make-rf-setting-effective 205 make-security-effective 221 management-vlanid 229 P password 125 path-cost (STP Interface) 187 ping 120 pmksa-lifetime 221 port-priority (STP Interface) 188 preamble 205 prompt 124 R radius-server accounting address 167 radius-server accounting key 168 radius-server accounting port 168 radius-server accounting timeout-interim 169 radius-server address 166 radius-server enable 165 radius-server key 167 radius-server port 166 reset 121 rts-threshold 208 show sntp 144 show station 213 show system 131 show version 132 show wds wireless 194 shutdown 198 shutdown 211 snmp-server community 149 snmp-server contact 149 snmp-server enable server 150 snmp-server filter 157 snmp-server host 151 snmp-server location 150 snmp-server target 156 snmp-server trap 152 snmp-server user 155 snmp-server vacm group 154 snmp-server vacm view 153 sntp-server date-time 142 sntp-server daylight-saving 143 sntp-server enabled 142 sntp-server ip 141 sntp-server timezone 144 ssid 209 system name 124 T transmit-key 218 transmit-power 204 V vap 201 vap (STP Interface) vlan 228 vlan-id 230 187 S short-guard-interval 206 show apmanagement 131 show authentication 176 show bridge br-conf 189 show bridge forward address 191 show bridge port-conf interface 189 show bridge status 190 show bridge stp 188 show config 132 show dual-image 164 show event-log 140 show filters 181 show interface ethernet 198 show interface wireless 211 show line 121 show lldp 227 show logging 140 show radius 170 show snmp 159 show snmp filter 159 show snmp target 158 show snmp users 158 show snmp vacm group 160 show snmp vacm view 160 24 W wds ap 193 wds sta 193 wmm 231 wmm-acknowledge-policy 232 wmmparam 232 wpa-pre-shared-key 220 INDEX OF CLI COMMANDS 25 SECTION I GETTING STARTED This section provides an overview of the access point, and introduces some basic concepts about wireless networking. It also describes the basic settings required to access the management interface. This section includes these chapters: "Introduction" on page 27 "Network Topologies" on page 34 "Installing the Access Point" on page 38 "Initial Configuration" on page 42 26 1 INTRODUCTION The EliteConnectTM SMCE21011 is an IEEE 802.11n access point (AP) that meets draft 2.0 standards. It is fully interoperable with older 802.

11a/b/g standards, providing a transparent, wireless high speed data communication between the wired LAN and fixed or mobile devices. The unit includes three detachable dual-band 2.4/5 GHz antennas with the option to attach alternative antennas that can extend or shape the network coverage area. KEY HARDWARE FEATURES The following table describes the main hardware features of the AP. Table 1: Key Hardware Features Feature Antennas LAN Port Console Port Reset Button LEDs Power Mounting Options Description Three detachable dual-band 2.4/5 GHz MIMO antennas. One 1000BASE-T RJ-45 port that supports a Power over Ethernet (PoE) connection to power the device. Console connection through an RJ-45 port with included RS-232 serial cable. For resetting the unit and restoring factory defaults. Provides LED indicators for system status, wireless radio status, and LAN port status.
Power over Ethernet (PoE) support through the RJ-45 Ethernet port, or from an external AC power adapter. Can be mounted on a wall, or on any horizontal surface such as a desktop or shelf. DESCRIPTION OF CAPABILITIES The SMCE21011 supports up to eight Virtual Access Point (VAP) interfaces, which allow traffic to be separated for different user groups within the same AP service area. The VAPs can support up to a total of 64 wireless clients, whereby the clients associate with each VAP in the same way as they would with physically separate access points. This means that each VAP can be configured with its own Service Set Identification (SSID), security settings, VLAN assignments, and other parameters, allowing the AP to serve a diverse range of client needs in an area from a single unit.
27 CHAPTER 1 | Introduction Package Contents 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 tools. The SMCE21011 utilises MIMO technology and Spatial Multiplexing to achieve the highest possible data rate and throughput on the 802.11n frequency. The unit's PoE RJ-45 port provides a 1 Gbps full-duplex link to a wired LAN.

PACKAGE CONTENTS The EliteConnectTM SMCE21011 package includes: 11n Access Point (SMCE21011) RJ-45 to RS-232 console cable AC power adapter 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. 28 CHAPTER 1 | Introduction Hardware Description HARDWARE DESCRIPTION Figure 1: Top Panel Antennas LED Indicators Figure 2: Rear Panel DC Power Socket RJ-45 PoE Port 29 Reset Button CHAPTER 1 | Introduction Hardware Description Figure 3: Ports DC Power Port RJ-45 PoE Port RJ-45 Console Port ANTENNAS The access point includes three integrated external MIMO (multiple-input and multiple-output) antennas. MIMO uses multiple antennas for transmitting and receiving radio signals to improve data throughput and link range. Each antenna transmits the outgoing signal as a toroidal sphere (doughnut shaped), with the coverage extending most in a direction perpendicular to the antenna. Therefore, the antennas should be adjusted to an angle that provides the appropriate coverage for the service area. EXTERNAL ANTENNA The antennas supplied with the AP screw off in a clockwise manner and can CONNECTORS be replaced with alternative antennas that can extend or shape the coverage area. 30 CHAPTER 1 | Introduction Hardware Description Figure 4: External Antenna Connectors Figure 5: Screw-off External Antenna Connector - Close Up 31 CHAPTER 1 | Introduction Hardware Description LED INDICATORS The access point includes four status LED indicators, as described in the following figure and table. Figure 6: LEDs Ethernet Link/Activity 802.11 a/b/g/n Link/Activity System Error or Failure Power Table 2: LED Behavior LED LAN Status Off Blue Green Amber WLAN Off Green Yellow Diag/Fail Off Red Blinking Power Off Yellow Description Ethernet RJ-45 has no valid link.

network activity. network activity. Ethernet RJ-45 has a 1000 Mbps link. Blinking indicates Ethernet RJ-45 has a 100 Mbps link. Blinking indicates Ethernet RJ-45 has a 10 Mbps link. Blinking indicates network activity. The AP radio is disabled. The radio is operating at 5 GHz (802.11a/n). Blinking indicates network activity.

The radio is operating at 2.4 GHz (802.11b/g/n). Blinking indicates network activity. The AP is operating normally.

The AP has detected a fault. The system is initializing. The AP has no power. The AP is receiving power. 32 CHAPTER 1 | Introduction Hardware Description CONSOLE PORT This port is used to connect a console device to the access point through a serial cable.

The console device can be a PC or workstation running a VT100 terminal emulator, or a VT-100 terminal. A crossover RJ-45 to DB-9 cable is supplied with the unit for connecting to the console port. ETHERNET PORT The access point has one 1000BASE-T RJ-45 port that can be attached directly to 10BASE-T/100BASE-TX/1000BASE-TX LAN segments. 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 or power injector, that provides Power over Ethernet (PoE). 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, and supplies 12 volts DC power to the unit. 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: The access point supports both endspan and midspan PoE. If the access point is connected to a PoE source device and also connected to a local power source through the AC power adapter, AC power will be disabled. RESET BUTTON This button can be used to restart the AP. 33 2 NETWORK TOPOLOGIES Wireless networks support a standalone configuration as well as an integrated configuration with 10/100/1000 Mbps Ethernet LANs. The SMCE21011 also provides bridging services that can be configured independently on on any of the virtual AP (VAP) interfaces. Access points can be deployed to support wireless clients and connect wired LANs in the following configurations: Infrastructure for wireless LANs Infrastructure wireless LAN for roaming wireless PCs Infrastructure wireless bridge to connect wired LANs INTERFERENCE ISSUES The 802.11b, 802.11g and 802.11n frequency band operating at 2.4 GHz can easily encounter interference from other 2.4 GHz devices, such as other 802.11b/g/n 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 3 channels of separation for 802.11b, or up to 4 channels for 802.11a, or up to 5 channels for 802.11g) 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. 34 CHAPTER 2 | Network Topologies Infrastructure Wireless LAN for Roaming Wireless PCs The infrastructure configuration extends the accessibility of wireless PCs to the wired LAN. A wireless infrastructure can be used for access to a central database, or for connection between mobile workers, as shown in the following figure. Figure 7: Infrastructure Wireless LAN Wired LAN Extension to Wireless Clients Server Desktop PC Switch Access Point Notebook PC Desktop PC 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 - 35 CHAPTER 2 | Network Topologies Infrastructure Wireless Bridge wireless network cards and adapters and wireless access points within a specific ESS must be configured with the same SSID. Figure 8: Infrastructure Wireless LAN for Roaming Wireless PCs 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> 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 that are independently configurable on each VAP. There are two WDS modes; WDS-AP and WDSSTA. Otherwise, VAPs operate in a normal AP mode. AP Mode: The VAP provides services to clients as a normal access point.
WDS-AP Mode: The VAP operates as an access point in WDS mode, which accepts connections from client stations in WDS-STA mode. WDS-STA Mode: The VAP operates as a client station in WDS mode, which connects to an access point VAP in WDS-AP mode. The user needs to specify the MAC address of the VAP in WDS-AP mode to which it intends to connect. 36 CHAPTER 2 | Network Topologies Infrastructure Wireless Bridge Figure 9: Bridging Mode Network Core WDS Links Between Access Points VAP 2 AP Mode VAP 0 WDS-AP Mode VAP 0 WDS-STA Mode VAP 1 WDS-AP Mode VAP 2 AP Mode VAP 1 WDS-AP Mode VAP 0 WDS-STA Mode VAP 1 AP Mode VAP 0 WDS-STA Mode VAP 1 AP Mode 37 3 INSTALLING THE ACCESS POINT This chapter describes how to install the access point. LOCATION SELECTION 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 service area. For optimum performance, consider these guidelines: 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). The access point can be mounted on any horizontal surface, or a wall. 38 CHAPTER 3 | Installing the Access Point Mounting on a 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. Figure 10: Attach Feet 39 CHAPTER 3 | Installing the Access Point Mounting on a Wall MOUNTING ON A WALL To mount on a wall follow the instructions below. Figure 11: Wall Mounting Mounting Slots The access point should be mounted only to a wall or wood surface that is at least 1/2-inch plywood or its equivalent. To mount the access point on a wall, always use its wall-mounting bracket.

The access point must be mounted with the RJ-45 cable connector oriented upwards to ensure proper operation. 1. Mark the position of the three screw holes on the wall. For concrete or brick walls, you will need to drill holes and insert wall plugs for the screws. 2. Insert the included 20-mm M4 tap screws into the holes, leaving about 2-3 mm clearance from the wall. 3. Line up the three mounting points on the AP with the screws in the wall, then slide the AP down onto the screws until it is in a secured position. 40 CHAPTER 3 | Installing the Access Point Connecting and Powering On CONNECTING AND POWERING ON 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). CAUTION: Use ONLY the power adapter supplied with this access point. Otherwise, the product may be damaged. NOTE: If the access point is connected to both a PoE source device and an AC power source, AC will be disabled. 1.
Observe the Self Test When you power on the access point, verify that the Power indicator turns on, and that the other indicators start functioning as described under "LED Indicators" on page 32. If the red DIAG/FAIL LED does not turn off, the self test has not completed correctly. Refer to "Troubleshooting" on page 237. 2. Connect the Ethernet Cable The access point can be connected to a 10/100/1000 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 5E or better UTP Ethernet cable. When the access point and the connected device are powered on, the Ethernet Link LED should turn on indicating a valid network connection. NOTE: The RJ-45 port on the access point supports automatic MDI/MDI-X operation, so you can use straight-through cables for all network connections to PCs, switches, or hubs. 3. 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 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, all antennas should be positioned pointing vertically up to provide optimum coverage. 4. (Optional) Connect the Console Port Connect the RJ-45 console cable (included with access point) to the RS-232 console port for accessing the command-line interface.

You can manage the access point using the console port, the web interface, or SNMP management software. 41 4 INITIAL CONFIGURATION The SMCE21011 offers a user-friendly web-based management interface for the configuration of all the unit's features. Any PC directly attached to the unit can access the management interface using a web browser, such as Internet Explorer (version 6.0 or above) or Firefox (version 2.0 or above). CONNECTING TO THE LOGIN PAGE It is recommended to make initial configuration changes by connecting a PC directly to the SMCE21011's LAN port. The SMCE21011 has a default IP address of 192.168.2.1 and a subnet mask of 255.

255.255.0. You must set your PC IP address to be on the same subnet as the SMCE21011 (that is, the PC and SMCE21011 addresses must both start 192.168. 2.x). To access the access point management interface, follow these steps: 1. Use your web browser to connect to the management interface using the default IP address of 192.168.

2.1. 2. Log into the interface by entering the default username "admin" and password also "smcadmin," then click Login. NOTE: It is strongly recommended to change the default user name and password the first time you access the web interface. For information on changing user names and passwords, See "Administration Settings" on page 52. Figure 12: Login Page 42 CHAPTER 4 | Initial Configuration Home Page and Main Menu HOME PAGE AND MAIN MENU After logging in to the web interface, the Home page displays. The Home page shows some basic settings for the AP, including Country Code and the management access password. Figure 13: Home Page The web interface Main Menu menu provides access to all the configuration settings available for the access point. The following items are displayed on this page: System Name An alias for the access point, enabling the device to be uniquely identified on the network.

(Default: 11n_AP; Range: 1-32 characters) Username The name of the user is fixed as "admin" and is not configurable. Old Password Type your old password. The default password is "smcdamin." New Password The password for management access. (Length: 532 characters, case sensitive) Confirm New Password Enter the password again for verification. Country Code This command configures the access point's country code, which identifies the country of operation and sets the authorized radio channels. 43 CHAPTER 4 | Initial Configuration Common Web Page Buttons CAUTION: You must set the country code to the country of operation. 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. COMMON WEB PAGE BUTTONS The list below describes the common buttons found on most web management pages: Set Applies the new parameters and saves them to temporary RAM memory. Also displays a screen to inform you when it has taken affect.

Clicking 'OK' returns to the home page. The running configuration will not be saved upon a reboot unless you use the "Save Config" button. Figure 14: Set Configuration Changes Cancel Cancels the newly entered settings and restores the originals. Help Displays the help window. Figure 15: Help Menu 44 CHAPTER 4 | Initial Configuration Quick Start Logout Ends the web management session.

Save Config Saves the current configuration so that it is retained after a restart. QUICK START The Quick Start menu is designed to help you configure the basic settings required to get the access point up and running. Click 'System', followed by 'Quick Start'. STEP 1 The first page of the Quick Start configures the system identification, access password, and the Country Code. Figure 16: Quick Start - Step 1 The following items are displayed on the first page of the Quick Start wizard: IDENTIFICATION System Name -- The name assigned to the access point.

(Default: 11n_AP) CHANGE PASSWORD Username -- The name of the user is fixed as "admin" and is not configurable. 45 Quick Start CHAPTER 4 | Initial Configuration Old Password -- If the unit has been configured with a password already, enter that password, otherwise enter the default password "smcdamin." New Password -- The password for management access. (Length: 5-32 characters, case sensitive) Confirm New Password -- Enter the password again for verification. COUNTRY CODE Country Code -- Configures the access point's country code from a drop down menu, which identifies the country of operation and sets the authorized radio channels. CAUTION: You must set the country code to the country of operation. 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. Cancel -- Cancels the newly entered settings and restores the orignals. Next -- Proceeds to the next page. STEP 2 The Step 2 page of the Quick Start configures IP settings and DHCP client status.

Figure 17: Quick Start - Step 2 46 CHAPTER 4 | Initial Configuration Quick Start The following items are displayed on this page: DHCP DHCP Status -- Enables/disables DHCP on the access point. (Default: disabled) IP Address -- Specifies an IP address for management of the access point. Valid IP addresses consist of four decimal numbers, 0 to 255, separated by periods. (Default: 192.168.2.1.) Subnet Mask -- Indicates the local subnet mask. Select the desired mask from the drop down menu. (Default: 255.

255.255.0) 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. (Default: 192.168.

2.254) 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. 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. (The default Primary and Secondary DNS addresses are null values.

) Prev -- Returns to the previous screen. Cancel -- Cancels the newly entered settings and restores the orignals. Next -- Proceeds to the final step in the Quick Start wizard. 47 Quick Start CHAPTER 4 | Initial Configuration STEP 3 The Step 3 page of the Quick Start configures radio interface settings. Figure 18: Quick Start - Step 3 The following items are displayed on this page: INTERFACE SETTING WiFi Mode -- Sets the mode of operation of the radio chip to 802.11n/g (2.4 GHz) or 802.11n/a (5 GHz).

(Default: 11n/g) BASIC SETTING SSID -- Sets the service set identifier for the primary VAP. (Default: vap_a0) SECURITY Association Mode -- Selects the security mode for association of other access points and wireless devices to the access point.

For more information, see "Wireless Security Settings" on page 92. (Default: Open System; Range: Open System, WPA, WPA-PSK, WPA2, WPA2-PSK, WPA-WPA2-mixed, or WPA-WPA2-PSK-mixed) Encryption Mode -- The available data encryption methods depend on the selected Association Mode. (Default: None) None: Implements no encryption for Open System association. WEP: WEP is used as the multicast encryption cipher. You should select WEP only when both WPA and WEP clients are supported. 48 CHAPTER 4 | Initial Configuration Main Menu Items TKIP: TKIP is used as the multicast encryption cipher. AES-CCMP: AES-CCMP is used as the multicast encryption cipher. AES-CCMP is the standard encryption cipher required for WPA2. AUTHENTICATION 802.1x -- Enables 802.

1X authentication. (Default: Disabled) 802.1x Reauthentication Refresh Rate -- The time period after which a connected client must be re-authenticated. During the reauthentication process of verifying the client's credentials on the RADIUS server, the client remains connected the network. Only if reauthentication fails is network access blocked.

(Default: 3600 seconds; Range: 0-65535 seconds; 0=disabled) NOTE: When 802.1X is enabled, be sure to configure RADIUS server details. For more information, see "RADIUS Settings" on page 54. MAIN MENU ITEMS To configure settings, click the relevant Main Menu item. Each Main Menu item is sumarized below with links to the relevant section in this guide where configuration parameters are described in detail: System -- Configures Management IP, WAN, LAN and QoS settings.

See "System Settings" on page 51. Management -- Configures SNMP, HTTP and Telnet settings. See "Management Settings" on page 62. Advanced -- Confiures LLDP and Access Control Lists. See "Advanced Settings" on page 73. Wireless -- Configures Wi-Fi access point settings. See "Wireless Settings" on page 79. Mantentance -- Congifures firmware upgrades remote and locally. See "Maintenance Settings" on page 100. Information -- Displays current system settings.

See "Status Information" on page 105. 49 SECTION II WEB CONFIGURATION This section provides details on configuring the access point using the web browser interface. This section includes these chapters: "System Settings" on page 51 "Management Settings" on page 62 "Advanced Settings" on page 73 "Wireless Settings" on page 79 "Maintenance Settings" on page 100 "Status Information" on page 105 50 5 SYSTEM SETTINGS This chapter describes basic system settings on the access point. It includes the following sections: "Administration Settings" on page 52 "IP Address" on page 53 "RADIUS Settings" on page 54 "System Time" on page 56 "SpectraLink Voice Priority" on page 58 "VLAN Configuration" on page 58 "System Logs" on page 60 "Quick Start Wizard" on page 61 51 CHAPTER 5 | System Settings Administration Settings ADMINISTRATION SETTINGS The Administration Settings page configures some basic settings for the AP, such as the system identification name, the management access password, and the wireless operation Country Code. Figure 19: Administration The following items are displayed on this page: System Name -- An alias for the access point, enabling the device to be uniquely identified on the network. (Default: 11n_AP; Range: 1-32 characters) Username -- The user name is fixed as "admin" and cannot be configured. Old Password -- Type your current password. New Password -- The password for management access. (Length: 5-32 characters, case sensitive) Confirm New Password -- Enter the password again for verification. Country Code -- This command configures the access point's country code, which identifies the country of operation and sets the authorized radio channels.

52 CHAPTER 5 | System Settings IP Address CAUTION: You must set the country code to the country of operation. 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. IP ADDRESS 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. 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 not be automatically configured with IP settings from a Dynamic Host Configuration Protocol (DHCP) server. The default IP address is 192.168.2.1, subnet mask 255.

255.255.0 and a default gateway of 192.168.2.254. Figure 20: IP Configuration The following items are displayed on this page: DHCP Status -- Enables/disables DHCP on the access point. IP Address -- Specifies an IP address for management of the access point. Valid IP addresses consist of four decimal numbers, 0 to 255, separated by periods. (Default: 192.

168.2.1.) Subnet Mask -- Indicates the local subnet mask. Select the desired mask from the drop down menu. (Default: 255.255.255.0) 53 CHAPTER 5 | System Settings RADIUS Settings 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.

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. After you have network access to the access point, you can use the web browser interface to modify the initial IP configuration, if needed. 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.

168.2.1 RADIUS SETTINGS 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.

PRIMARY AND A primary RADIUS server must be specified for the access point to SECONDARY RADIUS implement IEEE 802. 1X network access control and Wi-Fi Protected Access SERVER SETUP (WPA) wireless security. A secondary RADIUS server may also be specified as a backup should the primary server fail or become inaccessible. In addition, you can configure a RADIUS Accounting server to receive usersession accounting information from the access point. RADIUS Accounting can be used to provide valuable information on user activity in the network. 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. 54 CHAPTER 5 | System Settings RADIUS Settings Figure 21: RADIUS Settings The following items are displayed on the RADIUS Settings page: RADIUS Status -- Enables/disables the primary RADIUS server. IP Address -- Specifies the IP address or host name of the RADIUS server. Port (1024-65535) -- 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) RADIUS ACCOUNTING The following items are displayed on the RADIUS Settings page: Account Status -- Enables/disables RADIUS accounting. IP Address -- Specifies the IP address or host name of the RADIUS accounting server. 55 System Time CHAPTER 5 | System Settings Port (1024-65535) -- The UDP port number used by the RADIUS accounting server for authentication messages. (Range: 1024-65535; Default: 1813) Key -- A shared text string used to encrypt messages between the access point and the RADIUS accounting 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) Interim Update Timeout (60-86400) -- The interval between transmitting accounting updates to the RADIUS server. (Range: 6086400; Default: 300 seconds) SYSTEM TIME Simple Network Time Protocol (SNTP) allows the access point to set its internal clock based on periodic updates from a time server (SNTP or NTP).

Maintaining an accurate time on the access point enables the system log to record meaningful dates and times for event entries. If the clock is not set, the access point will only record the time from the factory default set at the last bootup. The access point acts as an SNTP client, periodically sending time synchronization requests to specific time servers. You can configure up to two time server IP addresses. The access point will attempt to poll each server in the configured sequence.

Figure 22: SNTP Settings 56 CHAPTER 5 | System Settings System Time SNTP SERVER Configures the access point to operate as an SNTP client. When enabled, at SETTINGS least one time server IP address must be specified. SNTP Status -- Enables/disables SNTP. (Default: enabled) Primary Server -- The IP address of an SNTP or NTP time server that the access point attempts to poll for a time update. Secondary Server -- The IP address of a secondary SNTP or NTP time server.

The access point first attempts to update the time from the primary server; if this fails it attempts an update from the secondary server. TIME ZONE SETTING SNTP uses Greenwich Mean Time, or GMT (sometimes referred to as Coordinated Universal Time, or UTC) based on the time at the Earth's prime meridian, zero degrees longitude. To display a time corresponding to your local time, you must indicate the number of hours your time zone is located before (east) or after (west) GMT. Time Zone -- Select from the scroll down list the locale you are situated most close to, for example for New York, select '(GMT-05) Eastern Time (US & Canada)'. DAYLIGHT SAVING The access point provides a way to automatically adjust the system clock SETTINGS for Daylight Savings Time changes. To use this feature you must define the month and date to begin and to end the change from standard time. During this period the system clock is set back by one hour. Daylight Saving Status -- Enalbes/disables daylight savings time. (Default: disabled) When enabled, set the month, day, and week to start and stop the daylight savings time. 57 CHAPTER 5 | System Settings SpectraLink Voice Priority SPECTRALINK VOICE PRIORITY SpectraLink Voice Priority (SVP) is a voice priority mechanism for WLANs.

SVP is an open, straightforward QoS approach that has been adopted by most leading vendors of WLAN APs. SVP favors isochronous voice packets over asynchronous data packets when contending for the wireless medium and when transmitting packets onto the wired LAN. Figure 23: SVP Settings The following items are displayed on this page: SVP Status -- Enables/disables SVP on the access point. VLAN CONFIGURATION VLANs (virtual local area networks) are turned off by default when first installing the access point. If turned on they will automatically tag any packets received by the LAN port before sending them on to the relevant VAP (virtual access point). The access point can employ VLAN tagging support to control access to network resources and increase security. VLANs separate traffic passing between the access point, associated clients, and the wired network. There can be a default VLAN for each VAP (Virtual Access Point) interface, and a management VLAN for the access point. Note the following points about the access point's VLAN support: The management VLAN is for managing the access point through remote management tools, such as the web interface, SSH, SNMP, or Telnet. The access point only accepts management traffic that is tagged with the specified management VLAN ID.

All wireless clients associated to the access point are assigned to a VLAN. Wireless clients are assigned to the default VLAN for the VAP interface with which they are associated. The access point only allows traffic tagged with default VLAN IDs to access clients associated on each VAP interface. 58 CHAPTER 5 | System Settings VLAN Configuration When VLAN support is enabled on the access point, traffic passed to the wired network is tagged with the appropriate VLAN ID, either a VAP default VLAN ID, or the management VLAN ID. Traffic received from the wired network must also be tagged with one of these known VLAN IDs.

Received traffic that has an unknown VLAN ID or no VLAN tag is dropped. When VLAN support is disabled, the access point does not tag traffic passed to the wired network and ignores the VLAN tags on any received frames. NOTE: Before enabling VLAN tagging on the access point, be sure to configure the attached network switch port to support tagged VLAN frames from the access point's management VLAN ID and default VLAN IDs.

Otherwise, connectivity to the access point will be lost when you enable the VLAN feature. Figure 24: Setting the VLAN Identity The following items are displayed on this page: VLAN Classification -- Enables/disables VLAN packet tagging.

(Default: disabled) Native VLAN ID(1-4094) -- If enabled the packets received by the LAN port must be tagged within the Management VLAN ID (native VLAN ID). (Range: 1-4094) 59 System Logs CHAPTER 5 | System Settings SYSTEM LOGS The access point can be configured to send event and error messages to a System Log Server. The system clock can also be synchronized with a time server, so that all the messages sent to the Syslog server are stamped with the correct time and date. Figure 25: System Log Settings The following items are displayed on this page: Syslog Status -- Enables/disables the logging of error messages. (Default: enabled) Server 1~4 -- Enables the sending of log messages to a Syslog server host. Up to four Syslog servers are supported on the access point. (Default: disabled) IP -- The IP address or name of a Syslog server. (Server 1 Default: 10.7.16.

98; Server 2 Default: 10.7.13.48; Server 3 Default: 10.7.123.123; Server 4 Default: 10.7.13.77) UDP Port -- The UDP port used by a Syslog server. (Range: 514 or 11024-65535; Server 1~2 Default: 514; Server 3 Default: 6553; Server 4 Default: 5432) Logging Console -- Enables the logging of error messages to the console. (Default: disabled) 60 CHAPTER 5 | System Settings Quick Start Wizard Logging Level -- Sets the minimum severity level for event logging. (Default: Debug) The system allows you to limit the messages that are logged by specifying a minimum severity level. The following table lists the error message levels from the most severe (Emergency) to least severe (Debug). The message levels that are logged include the specified minimum level up to the Emergency level.

Table 3: Logging Levels Error Level Emergency Alerts Critical Error Warning Notice Informational Debug Description System unusable Immediate action needed Critical conditions (e.g., memory allocation, or free memory error - resource exhausted) Error conditions (e.g., invalid input, default used) Warning conditions (e.

g., return false, unexpected return) Normal but significant condition, such as cold start Informational messages only Debugging messages QUICK START WIZARD The Quick Start menu item is described in the preceding chapter, see "Quick Start" on page 45. 61 6 MANAGEMENT SETTINGS This chapter describes management access settings on the access point. It includes the following sections: "Remote Management Settings" on page 62 "Access Limitation" on page 64 "Simple Network Management Protocol" on page 65 REMOTE MANAGEMENT SETTINGS The Web, Telnet, and SNMP management interfaces are enabled and open to all IP addresses by default. To provide more security for management access to the access point, specific interfaces can be disabled and management restricted to a single IP address or a limited range of IP addresses. Once you specify an IP address or range of addresses, access to management interfaces is restricted to the specified addresses. If anyone tries to access a management interface from an unauthorized address, the access point will reject the connection. 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 SSHenabled 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 SSH protocol. Both HTTP and HTTPS service can be enabled independently. If you enable HTTPS, you must indicate this in the URL: https://device:port_number] When you start HTTPS, the connection is established in this way: The client authenticates the server using the server's digital certificate. The client and server negotiate a set of security protocols to use for the connection. 62 CHAPTER 6 | Management Settings Remote Management Settings The client and server generate session keys for encrypting and decrypting data. The client and server establish a secure encrypted connection. A padlock icon should appear in the status bar for Internet Explorer. Figure 26: Remote Management The following items are displayed on Admin Interface page: Telnet Access -- Enables/disables management access from Telnet interfaces.

(Default: enabled) Telnet Access Port -- Sets the specified Telnet port for communication. (Default: 23) SSH Server -- Enables/disables management access from SSH Servers. (Default: enabled) SSH Server Port -- Sets the specified SSH Server port for communication. (Default: 22) HTTP Access -- Enables/disables management access from any IP address. (Default: enabled) HTTP Timeout -- Specifies the time after which the HTTP connection will be lost with a period of inactivity.

(Default: 1800 seconds; Range: 1-1800 seconds; 0=disabled) HTTP Port -- Specifies the HTTP port for IP connectivity. (Default: 80; Range 1024-65535) 63 CHAPTER 6 | Management Settings Access Limitation HTTPS Server -- Enables/disables management access from a HTTPS server. (Default: enabled) HTTPS Port -- Specifies the HTTPS port for secure IP connectivity. (Default: 443; Range 1024-65535) SNMP Access -- Enables/disables management access from SNMP interfaces. (Default: enabled) ACCESS LIMITATION The Access Limitation page limits management access to the access point from specified IP addresses or wireless clients.

Figure 27: Access Limitation The following items are displayed on the Access Limitation page: IP MANAGEMENT CONTROL Any IP -- Indicates that any IP address is allowed management access. Single IP -- Specifies a single IP address that is allowed management access. Multiple IP -- Specifies an address range as defined by the entered IP address and subnet mask. For example, IP address 192.168.1.6 and subnet mask 255.255.255.0, defines all IP addresses from 192.

168.1.1 to 192.168.1.254. IP Address -- Specifies the IP address. 64 CHAPTER 6 | Management Settings Simple Network Management Protocol Subnet Mask -- Specifies the subnet mask in the form 255.255.255.

x RESTRICT MANAGEMENT Enable/Disable -- Enables/disables management of the device by a wireless client. (Default: disabled) SIMPLE NETWORK MANAGEMENT PROTOCOL Simple Network Management Protocol (SNMP) is a communication protocol designed specifically for managing devices on a network.