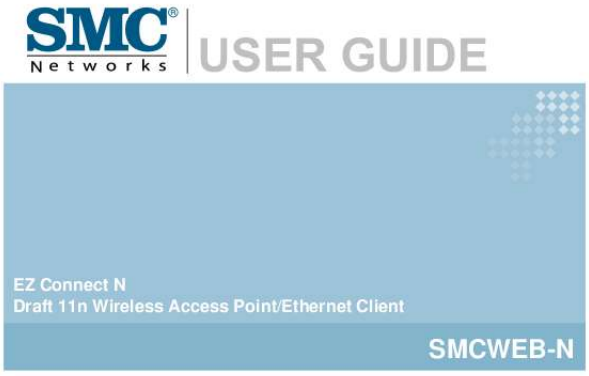
Your PDF Guides

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

User manual SMC WEB-N
User guide SMC WEB-N
Operating instructions SMC WEB-N
Instructions for use SMC WEB-N
Instruction manual SMC WEB-N



You're reading an excerpt. Click here to read official SMC WEB-N user guide
http://yourpdfguides.com/dref/3456912

Manual abstract:

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 website. 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 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 i 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 ii 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 minimum distance 20cm between the radiator & your body. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter. The availability of some specific channels and/or operational frequency bands are country dependent and are firmware programmed at the factory to match the intended destination. The firmware setting is not accessible by the end user. CE Mark Declaration of Conformance for EMI and Safety (EEC) This device complies with the essential requirements of the R&TTE Directive 1999/5/EC. The following references have been applied in order to prove presumption of compliance with the R&TTE Directive 1999/5/EC: · EN 300 328 · EN 301 489-1 · EN 301 489-17 · EN 60950-1 A copy of the CE Declaration of Conformity is available for download at: http://www.


You're reading an excerpt. Click here to read official SMC WEB-N user guide
http://yourpdfguides.com/dref/3456912

smc.com Intended for indoor use in the following countries: AT, BE, CZ, CY, DK, EE, FI, FR, DE, GR, HU, IS, IE, IT, LV, LT, LU, MT, NL, NO, PL, PT, SI, SK, ES, SE, CH, UK. iii Table of Contents Getting Started with the SMCWEB-N Package Contents Minimum System Requirements 2 2 2 Wireless LAN Networking Introduction Features 3 4 4 Hardware Overview Back/Side Panel Front Panel LED's Installation Considerations Getting Started 5 5 6 7 7 Using the Configuration Menu in AP Mode Basic Advanced Tools Status 8 9 17 25 30 Using the Configuration Menu in Client Mode Basic Advanced Tools Status 37 38 43 49 53 Glossary 59 1 Getting Started with the SMCWEB-N Congratulations on purchasing the SMCWEB-N! This manual provides information for setting up and configuring the SMCWEB-N. This manual is intended for both home users and professionals. Package Contents · · · · · · EZ ConnectTM N Wireless Access Point/Ethernet Client (SMCWEB-N) Yellow RJ-45 Ethernet Cable Power Adapter (12V, 1A) Documentation CD Quick Installation Guide Warranty Information Card Using a power supply with a different voltage than the one included with your product will cause damage and void the warranty for this product. Minimum System Requirements · 2.4GHz 802.11n draft wireless adapter or 2.

4GHz 802.11b/g wireless adapter or Ethernet Adapter installed on each PC. Internet Explorer 5.5 or above, Netscape 4.7 or above, Mozilla Firefox 1.0 or above · 2 Wireless LAN Networking The following figure provides an example of a wireless network with an AP. The wireless network is the part in the blue circle. In this wireless network, devices A and B are called wireless client. The wireless clients use the access point (AP) to interact with other devices (such as the printer) or with Internet. Every wireless network must follow those basic guidelines.

1. Every device in the same wireless network must use the same SSID. The SSID is the name of the wireless network. It stands for Service Set Identity. 2. If two wireless network overlap, they should use a different channel. Like radio stations or television channels, each wireless network uses a specific channel, or frequency, to send and receive information. 3. Every device in the same wireless network must use security compatible with the AP or peer computer. 3 Introduction The SMCWEB-N is a multi-function Wireless-N (802.

11n draft) networking device: Access Point and Ethernet Client modes. Designed for multimedia applications SMCWEB-N can be used in Access Point mode to add high-speed wireless connectivity to your network, or Client mode to simultaneously connect multiple Ethernet enabled devices such as a game console, digital media player or Network Attached Storage. The SMCWEB-N is 802.11n draft v2.0 compliant while maintaining full backwards compatibility with the Wireless-G (802.11g) and Wireless-B (802.11b) standards. This next generation wireless networking standard utilizes advanced MIMO (Multiple-In, Multiple-Out) technology to deliver incredible speed and range. With wireless speeds up to 300Mbps and extended coverage, there is enough bandwidth to simultaneously stream video and audio, play online games, transfer large files, make VoIP calls and surf the Internet. With security being a key consideration, SMCWEB-N supports the latest WPA and WPA2 wireless encryption standards, which prevent unauthorized access to wireless networks and ensure data is secure.

Wireless security can also be set up easily using Wi-Fi Protected SetupTM (WPS) that enables push button or PIN configuration. For an enhanced multimedia experience Wireless Intelligent Stream Handling technology automatically manages and prioritizes the flow of time-sensitive data in your wireless network, without the need for end user configuration. As a result time-sensitive applications like online gaming, voice and video, run smoothly without lag and breakup problems. Finally, configuration is made simple and straightforward with the Installation Wizard, intuitive web-based management interface and slide switch for easily selecting operating mode. Features Wi-Fi Compliant with IEEE 802.11n (draft) and IEEEE 802.11b/g Standards 2.412 to 2.462GHz frequency band operation Compliant with IEEE 802.3 & 3u standards Support OFDM and CCK modulation High-Speed up to 300Mbps Data Rate using IEEE 802.

11n (draft) connection 64/128-bits WEP and WPA/WPA2 Personal/Enterprise security support Wi-Fi Protected SetupTM (WPS) DHCP Server Support up to 252 leases, and up to 24 reservations (AP mode only) MAC address filtering support up to 24 filtering entries Support WEB UI management, firmware upgrade and configuration backup and restore Support 4 x 10/100Mbps Auto-MDIX LAN ports 4 Built-in 3 External Antennas to support high speed performance and great coverage AP and Client modes selectable with slide switch Wireless Intelligent Stream Handling Technology Hardware OveP. 2. Using the yellow RJ-45 cable connect port LAN1 on the SMCWEB-N to your network or Ethernet client device(s). Now connect the power supply. Ethernet LAN ports of the SMCWEB-N are Auto MDI/MDIX and will work with both Straight-through and Cross-Over cable.

3. To access the default management IP address your PC must have an IP address in the range 192.168.2.3~254, with subnet mask 255.

255.255.0. 4. Start web browser and enter address http://192.168.2.2 (default). When prompted enter password smcadmin then click [Log In]. Note: The User Name must be set to Admin.

5. Click [Wireless Network Setup Wizard] and follow the on screen instructions to complete the set-up and reboot. 7 Using the Configuration Menu in AP Mode Whenever you want to configure your SMCWEB-N, you can access the Configuration Menu through your PC by opening the Web-browser and typing in the IP Address of the SMCWEB-N. The SMCWEB-N's default IP Address is http://192.168.2.2. Open the Web browser. Type in the IP Address of the SMCWEB-N (http://192.168.

2. 2). Select Admin in the User Name field. Enter Password: smcadmin (default). Click Login In.

8 Basic The Basic tab provides the following configuration options: Wireless Settings and Network Settings. Basic_ Wireless Settings The wireless section is used to configure the wireless settings for your access point. Note that changes made in this section may also need to be duplicated on wireless clients that you want to connect to your wireless network. To protect your privacy, use the wireless security mode to configure the wireless security features. This device supports three wireless security modes including: WEP, WPA-Personal, and WPA-Enterprise.

WEP is the original wireless encryption standard. WPA provides a higher level of security. WPA-Personal does not require an authentication server. The WPA-Enterprise option does require a RADIUS authentication server. 9 Enable Wireless This option turns off and on the wireless connection feature of the access point.


You're reading an excerpt. Click here to read official SMC WEB-N user guide
http://yourpdfguides.com/dref/3456912

When you set this option, the following parameters are in effect. Wireless Network Name When you are browsing for available wireless networks, this is the name that will appear in the list (unless Visibility Status is set to invisible, see below). This name is also referred to as the SSID. For security purposes, it is highly recommended to change from the pre-configured network name. Enable Auto Channel Scan If you select this option, the access point automatically finds the channel with least interference and uses that channel for wireless networking.

If you disable this option, the access point uses the channel that you specify with the following Wireless Channel option. Wireless Channel A wireless network uses specific channels in the wireless spectrum to handle communication between clients. Some channels in your area may have interference from other electronic devices. Choose the clearest channel to help optimize the performance and coverage of your wireless network. 802.11 Mode If all of the wireless devices you want to connect with this access point can connect in the same transmission mode, you can improve performance slightly by choosing the appropriate "Only" mode. If you have some devices that use a different transmission mode, choose the appropriate "Mixed" mode. Channel Width The "Auto 20/40 MHz" option is usually best. The other options are available for special circumstances. Transmission Rate By default the fastest possible transmission rate will be selected.

You have the option of selecting the speed if necessary. Number of Spatial Streams Selecting more than one spatial stream can increase throughput, but can in some cases decrease signal quality. Select the option that works best for your installation. Visibility Status The Invisible option allows you to hide your wireless network. When this option is set to Visible, your wireless network name is broadcast to anyone within the range of your signal.

If you're not using encryption then they could connect to your network. When Invisible mode is enabled, you must enter the Wireless Network Name (SSID) on the client manually to connect to the network. Security Mode Unless one of these encryption modes is selected, wireless transmissions to and from your wireless network can be easily intercepted and interpreted by unauthorized users. WEP A method of encrypting data for wireless communication intended to provide the same level of privacy as a wired network. WEP is not as secure as WPA encryption.

To gain access to a WEP network, you must know the key. The key is a string of characters that you create. When using WEP, you must determine the level of encryption. The type of encryption determines the key length. 128-bit encryption requires a longer key than 64-bit encryption. Keys are defined by entering in a string in HEX (hexadecimal - using characters 0-9, A-F) or ASCII (American Standard Code for Information Interchange - alphanumeric characters) format. ASCII format is provided so you can enter a string that is easier to remember. The ASCII string is converted to HEX for use over the network. Four keys can be defined so that you can change keys easily. A default key is selected for use on the network.

10 Example: 64-bit hexadecimal keys are exactly 10 characters in length. (12345678FA is a valid string of 10 characters for 64-bit encryption.) 128-bit hexadecimal keys are exactly 26 characters in length. (456FBCDF123400122225271730 is a valid string of 26 characters for 128-bit encryption.) 64-bit ASCII keys are up to 5 characters in length (DMODE is a valid string of 5 characters for 64-bit encryption.) 128-bit ASCII keys are up to 13 characters in length (2002HALOSWIN1 is a valid string of 13 characters for 128-bit encryption.) Note that, if you enter fewer characters in the WEP key than required, the remainder of the key is automatically padded with zeros. WPA-Personal and WPA-Enterprise Both of these options select some variant of Wi-Fi Protected Access (WPA) -- security standards published by the Wi-Fi Alliance. The WPA Mode further refines the variant that the access point should employ. WPA Mode: WPA is the older standard; select this option if the clients that will be used with the access point only support the older standard.

WPA2 is the newer implementation of the stronger IEEE 802.11i security standard. With the "WPA2" option, the access point tries WPA2 first, but falls back to WPA if the client only supports WPA. With the "WPA2 Only" option, the access point associates only with clients that also support WPA2 security. Cipher Type: The encryption algorithm used to secure the data communication.

TKIP (Temporal Key Integrity Protocol) provides per-packet key generation and is based on WEP. AES (Advanced Encryption Standard) is a very secure block based encryption. With the "TKIP and AES" option, the access point negotiates the cipher type with the client, and uses AES when available. Group Key Update Interval: The amount of time before the group key used for broadcast and multicast data is changed. WPA-Personal This option uses Wi-Fi Protected Access with a Pre-Shared Key (PSK).

Pre-Shared Key: The key is entered as a pass-phrase of up to 63 alphanumeric characters in ASCII (American Standard Code for Information Interchange) format at both ends of the wireless connection. It cannot be shorter than eight characters, although for proper security it needs to be of ample length and should not be a commonly known phrase. This phrase is used to generate session keys that are unique for each wireless client. Example: Wireless Networking technology enables ubiquitous communication WPA-Enterprise This option works with a RADIUS Server to authenticate wireless clients. Wireless clients should have established the necessary credentials before attempting to authenticate to the Server through this Gateway. Furthermore, it may be necessary to configure the RADIUS Server to allow this Gateway to authenticate users. Authentication Timeout: Amount of time before a client will be required to re-authenticate. RADIUS Server IP Address: The IP address of the authentication server. RADIUS Server Port: The port number used to connect to the authentication server. RADIUS Server Shared Secret: A pass-phrase that must match with the authentication server.

MAC Address Authentication: If this is selected, the user must connect from the same computer whenever logging into the wireless network. Advanced: 11 Optional Backup RADIUS Server This option enables configuration of an optional second RADIUS server. A second RADIUS server can be used as backup for the primary RADIUS server. The second RADIUS server is consulted only when the primary server is not available or not responding. The fields Second RADIUS Server IP Address, RADIUS Server Port, Second RADIUS server Shared Secret, Second MAC Address Authentication provide the corresponding parameters for the second RADIUS Server 12 Basic_Network Settings Access Point Settings These are the settings of the LAN (Local Area Network) interface for the access point.


You're reading an excerpt. Click here to read official SMC WEB-N user guide
http://yourpdfguides.com/dref/3456912

The access point's local network (LAN) settings are configured based on the IP Address and Subnet Mask assigned in this section. The IP address is also used to access this Web-based management interface. It is recommended that you use the default settings if you do not have an existing network. 13 DHCP Server Settings DHCP stands for Dynamic Host Configuration Protocol. The DHCP section is where you configure the built-in DHCP Server to assign IP addresses to the computers and other devices on your local area network (LAN).

Enable DHCP Server Once your access point is properly configured and this option is enabled, the DHCP Server will manage the IP addresses and other network configuration information for computers and other devices connected to your Local Area Network. There is no need for you to do this yourself. The computers (and other devices) connected to your LAN also need to have their TCP/IP configuration set to "DHCP" or "Obtain an IP address automatically". When you set Enable DHCP Server, the following options are displayed. DHCP IP Address Range These two IP values (from and to) define a range of IP addresses that the DHCP Server uses when assigning addresses to computers and devices on your Local Area Network.

Any addresses that are outside of this range are not managed by the DHCP Server; these could, therefore, be used for manually configured devices or devices that cannot use DHCP to obtain network address details automatically. It is possible for a computer or device that is manually configured to have an address that does reside within this range. In this case the address should be reserved (see DHCP Reservation below), so that the DHCP Server knows that this specific address can only be used by a specific computer or device. Your access point, by default, has a static IP address of 192.168.

2.2. This means that addresses 192.168.2.3 to 192.168.2.254 can be made available for allocation by the DHCP Server. Example: Your access point uses 192.

168.2.2 for the IP address. You've assigned a computer that you want to designate as a Web server with a static IP address of 192.168.2.3. You've assigned another computer that you want to designate as an FTP server with a static IP address of 192.168.2.

4. Therefore the starting IP address for your DHCP IP address range needs to be 192.168.2.5 or greater.

Example: Suppose you configure the DHCP Server to manage addresses From 192.168.2.100 To 192.168.

2.199. This means that 192.168.2.3 to 192.168.2.99 and 192.168.

2.200 to 192.168.2.254 are NOT managed by the DHCP Server. Computers or devices that use addresses from these ranges are to be manually configured. Suppose you have a web server computer that has a manually configured address of 192.168.2.100.

Because this falls within the "managed range" be sure to create a reservation for this address and match it to the relevant computer (see Static DHCP Client below). DHCP Lease Time The amount of time that a computer may have an IP address before it is required to renew the lease. The lease functions just as a lease on an apartment would. The initial lease designates the amount of time before the lease expires. If the tenant wishes to retain the address when the lease is expired then a new lease is established.

If the lease expires and the address is no longer needed than another tenant may use the address. Always Broadcast If all the computers on the LAN successfully obtain their IP addresses from the access point's DHCP server as expected, this option can remain disabled. However, if one of the computers on the LAN fails to obtain an IP address from the access point's DHCP server, it may have an old DHCP client that incorrectly turns off the broadcast flag of DHCP packets. Enabling this option will cause the access point to always broadcast its responses to all clients, thereby working around the problem, at the cost of increased broadcast traffic on the LAN. NetBIOS Advertisement Check this box to allow the DHCP Server to offer NetBIOS configuration settings to the LAN hosts.

NetBIOS allow LAN hosts to discover all other computers within the network, e.g. within Network Neighbourhood. 14 Primary WINS Server IP address Configure the IP address of the preferred WINS server. WINS Servers store information regarding network hosts, allowing hosts to 'register' themselves as well as discover other available hosts, e.g. for use in Network Neighbourhood. Secondary WINS Server IP address Configure the IP address of the backup WINS server, if any. NetBIOS Scope This is an advanced setting and is normally left blank. This allows the configuration of a NetBIOS 'domain' name under which network hosts operate.

NetBIOS Registration mode Indicates how network hosts are to perform NetBIOS name registration and discovery. H-Node, this indicates a Hybrid-State of operation. First WINS servers are tried, if any, followed by local network broadcast. This is generally the preferred mode if you have configured WINS servers. M-Node (default), this indicates a Mixed-Mode of operation. First Broadcast operation is performed to register hosts and discover other hosts, if broadcast operation fails, WINS servers are tried, if any. This mode favours broadcast operation which may be preferred if WINS servers are reachable by a slow network link and the majority of network services such as servers and printers are local to the LAN. P-Node, this indicates to use WINS servers ONLY. This setting is useful to force all NetBIOS operation to the configured WINS servers. You must have configured at least the primary WINS server IP to point to a working WINS server.

B-Node, this indicates to use local network broadcast ONLY. This setting is useful where there are no WINS servers available, however, it is preferred you try M-Node operation first. Add/Edit DHCP Reservation This option lets you reserve IP addresses, and assign the same IP address to the network device with the specified MAC address any time it requests an IP address. This is almost the same as when a device has a static IP address except that the device must still request an IP address from the access point. The access point will provide the device the same IP address every time.

DHCP Reservations are helpful for server computers on the local network that are hosting applications such as Web and FTP. Servers on your network should either use a static IP address or use this option. Enable Specifies whether the entry will be active or inactive. Computer Name You can assign a name for each computer that is given a reserved IP address. This may help you keep track of which computers are assigned this way.

Example: Game Server. IP Address: The LAN address that you want to reserve. MAC Address To input the MAC address of your system, enter it in manually or connect to the access point's Web-Management interface from the system and click the Copy Your PC's MAC Address button. A MAC address is usually located on a sticker on the bottom of a network device. The MAC address is comprised of twelve digits.


You're reading an excerpt. Click here to read official SMC WEB-N user guide
http://yourpdfguides.com/dref/3456912

Each pair of hexadecimal digits are usually separated by dashes or colons such as 00-0D-88-11-22-33 or 00:0D:88:11:22:33. If your network device is a computer and the network card is already located inside the computer, you can connect to the access point from the computer and click the Copy Your PC's MAC Address button to enter the MAC address. As an alternative, you can locate a MAC address in a specific operating system by following the steps below: Windows 98 Windows Me Go to the Start menu, select Run, type in winipcfg, and hit Enter. A popup window will be displayed. Select the appropriate adapter from the pull-down menu and you will see the Adapter Address.

This is the MAC address of the device. 15 Windows 2000 Windows XP Mac OS X Save/Update Go to your Start menu, select Programs, select Accessories, and select Command Prompt. At the command prompt type ipconfig /all and hit Enter. The physical address displayed for the adapter connecting to the access point is the MAC address. Go to the Apple Menu, select System Preferences, select Network, and select the Ethernet Adapter connecting to the access point. Select the Ethernet button and the Ethernet ID will be listed. This is the same as the MAC address. Record the changes you have made into the following list. Clear Re-initialize this area of the screen, discarding any changes you have made. DHCP Reservations List This shows clients that you have specified to have reserved DHCP addresses.

Click the Enable checkbox at the left to directly activate or de-activate the entry. An entry can be changed by clicking the Edit icon or can be deleted by clicking the Delete icon. When you click the Edit icon, the item is highlighted, and the "Edit DHCP Reservation" section is activated for editing. Number of Dynamic DHCP Clients In this section you can see what LAN devices are currently leasing IP addresses. Revoke The Revoke option is available for the situation in which the lease table becomes full or nearly full, you need to recover space in the table for new entries, and you know that some of the currently allocated leases are no longer needed.

Clicking Revoke cancels the lease for a specific LAN device and frees an entry in the lease table. Do this only if the device no longer needs the leased IP address, because, for example, it has been removed from the network. Reserve The Reserve option converts this dynamic IP allocation into a DHCP Reservation and adds the corresponding entry to the DHCP Reservations List. 16 Advanced The Advanced tab provides the following configuration options: MAC Address Filter, Advanced Wireless, WISH, Wi-Fi Protected Setup Advanced_ MAC Address Filter The MAC address filter section can be used to filter network access by machines based on the unique MAC addresses of their network adapter(s). It is most useful to prevent unauthorized wireless devices from connecting to your network.

A MAC address is a unique ID assigned by the manufacturer of the network adapter. 16 -- MAC Filtering Rules Configure MAC Filtering When "OFF" is selected, MAC addresses are not used to control network access. When "ALLOW" is selected, only computers with MAC addresses listed in the MAC Address List are granted network access. When "DENY" is selected, any computer with a MAC address listed in the MAC Address List is refused access to the network. MAC Address Enter the MAC address of the desired. Computers that have obtained an IP address from the access point's DHCP server will be in the DHCP Client List. Select a device from the drop down menu, then click the arrow to add that device's MAC address to the list. Clear Click the Clear button to remove the MAC address from the MAC Filtering list. 17 Advanced_Advanced Wireless Transmit Power Normally the wireless transmitter operates at 100% power. In some circumstances, however, there might be a need to isolate specific frequencies to a smaller area.

By reducing the power of the radio, you can prevent transmissions from reaching beyond your corporate/home office or designated wireless area. Beacon Period Beacons are packets sent by a wireless access point to synchronize wireless devices. Specify a Beacon Period value between 20 and 1000. The default value is set to 100 milliseconds. RTS Threshold When an excessive number of wireless packet collisions are occurring, wireless performance can be improved by using the RTS/CTS (Request to Send/Clear to Send) handshake protocol. The wireless transmitter will begin to send RTS frames (and wait for CTS) when data frame size in bytes is greater than the RTS Threshold. This setting should remain at its default value of 2346 bytes. Fragmentation Threshold Wireless frames can be divided into smaller units (fragments) to improve performance in the presence of RF interference and at the limits of RF coverage. Fragmentation will occur when frame size in bytes is greater than the Fragmentation Threshold. This setting should remain at its default value of 2346 bytes. Setting the Fragmentation value too low may result in poor performance. 18 DTIM Interval A DTIM is a countdown informing clients of the next window for listening to broadcast and multicast messages. When the wireless access point has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM Interval value. Wireless clients detect the beacons and awaken to receive the broadcast and multicast messages. The default value is 1.

Valid settings are between 1 and 255. Wireless Isolation Enabling Wireless Isolation prevents associated wireless clients from communicating with each other. WMM Enable Enabling WMM can help control latency and jitter when transmitting multimedia content over a wireless connection. Short GI Using a short (400ns) guard interval can increase throughput. However, it can also increase error rate in some installations, due to increased sensitivity to radio-frequency reflections.

Select the option that works best for your installation. Extra Wireless Protection Extra protection for neighboring 11b wireless networks. Turn this option off to reduce the adverse effect of legacy wireless networks on 802.11ng performance. This option is available only when 802.11 Mode is set to an 11n Only option. (Refer to the Basic Wireless page.) WDS Enable When WDS is enabled, this access point functions as a wireless repeater and is able to wirelessly communicate with other APs via WDS links. Note that WDS is incompatible with WPA -- both features cannot be used at the same time. A WDS link is bidirectional; so this AP must know the MAC Address (creates the WDS link) of the other AP, and the other AP must have a WDS link back to this AP.

Make sure the APs are configured with same channel number. WDS AP MAC Address Specifies one-half of the WDS link. The other AP must also have the MAC address of this AP to create the WDS link back to this AP. Enter a MAC address for each of the other APs that you want to connect with WDS.


You're reading an excerpt. Click here to read official SMC WEB-N user guide
http://yourpdfguides.com/dref/3456912

19 Advanced_ WISH WISH is short for Wireless Intelligent Stream Handling, a technology developed to enhance your experience of using a wireless network by prioritizing the traffic of different applications. WISH Enable WISH Enable this option if you want to allow WISH to prioritize your traffic. 20 Priority Classifiers HTTP Allows the access point to recognize HTTP transfers for many common audio and video streams and prioritize them above other traffic. Such streams are frequently used by digital media players. Windows Media Center Enables the access point to recognize certain audio and video streams generated by a Windows Media Center PC and to prioritize these above other traffic. Such streams are used by systems known as Windows Media Extenders, such as the Xbox 360.

Automatic When enabled, this option causes the access point to automatically attempt to prioritize traffic streams that it doesn't otherwise recognize, based on the behaviour that the streams exhibit. This acts to deprioritize streams that exhibit bulk transfer characteristics, such as file transfers, while leaving interactive traffic, such as gaming or VoIP, running at a normal priority. Add/Edit WISH Rule A WISH Rule identifies a specific message flow and assigns a priority to that flow. For most applications, the priority classifiers ensure the right priorities and specific WISH Rules are not required. WISH supports overlaps between rules.

If more than one rule matches for a specific message flow, the rule with the highest priority will be used. Enable Specifies whether the entry will be active or inactive. Name Create a name for the rule that is meaningful to you. Priority The priority of the message flow is entered here. Four priorities are defined: · · · · BK: Background (least urgent).

BE: Best Effort. VI: Video. VO: Voice (most urgent). Protocol The protocol used by the messages. Host 1 IP Range The rule applies to a flow of messages for which one computer's IP address falls within the range set here. Host 1 Port Range The rule applies to a flow of messages for which host 1's port number is within the range set here. Host 2 IP Range The rule applies to a flow of messages for which the other computer's IP address falls within the range set here. Host 2 Port Range The rule applies to a flow of messages for which host 2's port number is within the range set here. 21 Save/Update Record the changes you have made into the following list. Clear Re-initialize this area of the screen, discarding any changes you have made.

WISH Rules This section lists the defined WISH Rules. Click the Enable checkbox at the left to directly activate or de-activate the entry. An entry can be changed by clicking the Edit icon or can be deleted by clicking the Delete icon. When you click the Edit icon, the item is highlighted, and the "Edit WISH Rule" section is activated for editing. 22 Advanced_ Wi-Fi Protected Setup Wi-Fi Protected Setup Enable Enable the Wi-Fi Protected Setup feature. Lock Wireless Security Settings Locking the wireless security settings prevents the settings from being changed by any new external registrar using its PIN. @@@@The default PIN is printed on the bottom of the access point. For extra security, a new PIN can be generated. You can restore the default PIN at any time. @@Reset PIN to Default Restore the default PIN of the access point.

Generate New PIN Create a random number that is a valid PIN. This becomes the access point's PIN. You can then copy this PIN to the user interface of the registrar. @@@@@@@@There are several ways to add a wireless device to your network. @@@@@@By default there is no password configured. @@@@@@@@@@@@@@Time Zone Select your local time zone from pull down menu. @@@@@@@@@@(Make sure that computer's time is set correctly.) Note: If the access point loses power for any reason, it cannot keep its clock running, and will not have the correct time when it is started again. To maintain correct time for schedules and logs, either you must enter the correct time after you restart the access point, or you must enable the NTP Server option. 27 Tools_System This section allows you to manage the access point's configuration settings, reboot the access point, and restore the access point to the factory default settings.

Restoring the unit to the factory default settings will erase all settings, including any rules that you've created. Save To Local Hard Drive This option allows you to save the access point's configuration to a file on your computer. Be sure to save the configuration before performing a firmware upgrade. Load From Local Hard Drive Use this option to restore previously saved access point configuration settings. Restore To Factory Default This option restores all configuration settings back to the settings that were in effect at the time the access point was shipped from the factory. Any settings that have not been saved will be lost. If you want to save your access point configuration settings, use the Save Settings option above. Reboot The Device This restarts the access point. Useful for restarting when you are not near the device. 28 Tools_Firmware Use the Firmware section to install the latest firmware to improve functionality and performance.

To upgrade the firmware, follow these steps: 1. 2. 3. 4. Click the Browse button to locate the upgrade file on your computer. Once you have found the file to be used, click the Upload button below to start the firmware upgrade process. This can take a minute or more. Wait for the access point to reboot. This can take another minute or more. Confirm updated firmware revision on status page.

Firmware Information Here are displayed the version numbers of the firmware currently installed in your access point and the most recent upgrade that is available. Firmware Upgrade Note: Firmware upgrade cannot be performed from a wireless device. To perform an upgrade, ensure that you are using a PC that is connected to the access point by wire. Note: Some firmware upgrades reset the configuration options to the factory defaults. Before performing an upgrade, be sure to save the current configuration from the Tools System screen.

Upload Once you have a firmware update on your computer, use this option to browse for the file and then upload the information into the access point. 29 Status The Status tab provides the following configuration options: Device Info, Wireless, Logs, Statistics and WISH Sessions. Status_Device info All of your network connection details are displayed on the Device Info page. The firmware version is also displayed here. 30 Wireless LAN This area of the screen reflects configuration settings from the Setup Wireless Settings page and the Advanced WISH page.

The MAC Address is the factory-assigned identifier of the wireless card. LAN Computers This area of the screen continually updates to show all DHCP enabled computers and devices connected to the LAN side of your access point.

You're reading an excerpt. Click here to read official SMC WEB-N user guide

http://yourpdfguides.com/dref/3456912

The detection "range" is limited to the address range as configured in DHCP Server. Computers that have an address outside of this range will not show. If the DHCP Client (i.e. a computer configured to "Automatically obtain an address") supplies a Host Name then that will also be shown. Any computer or device that has a static IP address that lies within the detection "range" may show, however its host name will not. 31 Status_Wireless The wireless section allows you to view the wireless clients that are connected to your wireless access point. MAC Address The Ethernet ID (MAC address) of the wireless client.

IP Address The LAN-side IP address of the client. Mode The transmission standard being used by the client. Values are 11a, 11b, or 11g for 802.11a, 802.11b, or 802.11g respectively. Rate The actual transmission rate of the client in megabits per second. Signal This is a relative measure of signal quality. The value is expressed as a percentage of theoretical best quality. Signal quality can be reduced by distance, by interference from other radio-frequency sources (such as cordless telephones or neighboring wireless networks), and by obstacles between the access point and the wireless device.
32 Status_Logs The access point automatically logs (records) events of possible interest in its internal memory. If there is not enough internal memory for all events, logs of older events are deleted, but logs of the latest events are retained. The Logs option allows you to define the level of events to view. View Levels Select the level of events that you want to view. · · · Critical Warning Informational Apply Log Settings Now Click this button after changing Log Options to make them effective and permanent.
33 Refresh Clicking this button refreshes the display of log entries. There may be new events since the last time you accessed the log. Clear Clicking this button erases all log entries. Save Log Select this option to save the access point log to a file on your computer. Status_Statistics The Statistics page displays all of the LAN, WAN, and Wireless packet transmit and receive statistics.
Sent The number of packets sent from the access point. Received The number of packets received by the access point. 34 TX Packets Dropped The number of packets that were dropped while being sent, due to errors, collisions, or access point resource limitations. RX Packets Dropped The number of packets that were dropped while being received, due to errors, collisions, or access point resource limitations. Collisions The number of packets that were dropped due to Ethernet collisions (two or more devices attempting to use an Ethernet circuit at the same time). Errors The number of transmission failures that cause loss of a packet. A noisy radio-frequency environment can cause a high error rate on the wireless LAN. Status_WISH Sessions The WISH Sessions page displays full details of active local wireless sessions through your access point when WISH has been enabled. A WISH session is a conversation between a program or application on a wirelessly connected LAN-side computer and another computer, however connected. Originator The IP address and, where appropriate, port number of the computer that originated a network connection.

Target The IP address and, where appropriate, port number of the computer to which a network connection has been made. Protocol The communications protocol used for the conversation. 35 State State for sessions that use the TCP protocol. · · · · · · · Priority NO: None -- This entry is used as a placeholder for a future connection that may occur. SS: SYN Sent -- One of the systems is attempting to start a connection. EST: Established -- the connection is passing data. FW: FIN Wait -- The client system has requested that the connection be stopped. CW: Close Wait -- the server system has requested that the connection be stopped. TW: Time Wait -- Waiting for a short time while a connection that was in FIN Wait is fully closed. LA: Last ACK -- Waiting for a short time while a connection that was in Close Wait is fully closed.
CL: Closed -- The connection is no longer active but the session is being tracked in case there are any retransmitted packets still pending. The priority given to packets sent wirelessly over this conversation by the WISH logic. The priorities are: · · · · Time Out BK: Background (least urgent). BE: Best Effort. VI: Video.
VO: Voice (most urgent). The number of seconds of idle time until the access point considers the session terminated. The initial value of Time Out depends on the type and state of the connection. 300 seconds UDP connections. 240 seconds Reset or closed TCP connections.
The connection does not close instantly so that lingering packets can pass or the connection can be re-established. 7800 seconds Established or closing TCP connections. 36 Using the Configuration Menu in Client Mode Whenever you want to configure your SMCWEB-N, you can access the Configuration Menu through your PC by opening the Web-browser and typing in the IP Address of the SMCWEB-N. The SMCWEB-N's default IP Address is http://192.168.2.2. Open the Web browser. Type in the IP Address of the Client (http://192.168.

2. 2). Select admin in the User Name field. Enter Password: smcadmin (default). Click Login In. 37 Basic The Basic tab provides the following configuration options: Wizard, Wireless, Network Settings Basic_Wizard If you want to connect a new wireless network, click on Setup Wizard and the bridge will guide you through a few steps to get your network up and running. 38 Basic_ Wireless The wireless section is used to configure the wireless settings for your bridge. Note that some options in this section must agree with options selected for your wireless access point or wireless router. To protect your privacy, use the wireless security mode to configure the wireless security features. This device supports three wireless security modes including: WEP, WPA-Personal, and WPA-Enterprise.
WEP is the original wireless encryption standard. WPA provides a higher level of security. WPA-Personal does not require an authentication server. The WPA-Enterprise option does require a RADIUS authentication server. 39 Enable Wireless This option turns off and on the wireless connection feature of the bridge.
When you set this option, the following parameters are in effect. Wireless Network Name This is the name of the wireless access point that this station will associate to. Leave this field blank to associate to any access point. Enable Auto Channel Scan If you select this option, the bridge automatically finds the channel with least interference and uses that channel for wireless networking. If you disable this option, the bridge uses the channel that you specify with the following Wireless Channel option.


You're reading an excerpt. Click here to read official SMC WEB-N user guide
http://yourpdfguides.com/dref/3456912

Wireless Channel A wireless network uses specific channels in the wireless spectrum to handle communication between clients. Some channels in your area may have interference from other electronic devices.Your wireless bridge will use the channel that is used by the access point it associates with. But here you can select your channel preference to help optimize the performance and coverage of your wireless network. 802.11 Mode If all of the wireless devices in your wireless network can connect in the same transmission mode, you can improve performance slightly by choosing the appropriate "Only" mode. If you have some devices that use a different transmission mode, choose the appropriate "Mixed" mode. Channel Width The "Auto 20/40 MHz" option is usually best. The other options are available for special circumstances. Transmission Rate By default the fastest possible transmission rate will be selected.

You have the option of selecting the speed if necessary. Number of Spatial Streams Selecting more than one spatial stream can increase throughput, but can in some cases decrease signal quality. Select the option that works best for your installation. Security Mode Unless one of these encryption modes is selected, wireless transmissions to and from your wireless network can be easily intercepted and interpreted by unauthorized users. WEP A method of encrypting data for wireless communication intended to provide the same level of privacy as a wired network. WEP is not as secure as WPA encryption. To gain access to a WEP network, you must know the key. The key is a string of characters that you create. When using WEP, you must determine the level of encryption. The type of encryption determines the key length.
128-bit encryption requires a longer key than 64-bit encryption. Keys are defined by entering in a string in HEX (hexadecimal - using characters 0-9, A-F) or ASCII (American Standard Code for Information Interchange - alphanumeric characters) format. ASCII format is provided so you can enter a string that is easier to remember. The ASCII string is converted to HEX for use over the network. Four keys can be defined so that you can change keys easily.
A default key is selected for use on the network. Example: 64-bit hexadecimal keys are exactly 10 characters in length. (12345678FA is a valid string of 10 characters for 64-bit encryption.) 128-bit hexadecimal keys are exactly 26 characters in length. (456FBCDF123400122225271730 is a valid string of 26 characters for 128-bit encryption.
) 40 64-bit ASCII keys are up to 5 characters in length (DMODE is a valid string of 5 characters for 64-bit encryption.) 128-bit ASCII keys are up to 13 characters in length (2002HALOSWIN1 is a valid string of 13 characters for 128-bit encryption.) Note that, if you enter fewer characters in the WEP key than required, the remainder of the key is automatically padded with zeros. WPA-Personal and WPA-Enterprise Both of these options select some variant of Wi-Fi Protected Access (WPA) -- security standards published by the Wi-Fi Alliance. The WPA Mode further refines the variant that the bridge should employ. WPA Mode: WPA is the older standard; select this option if the Access Point that will be used with the bridge only support the older standard. WPA2 is the newer implementation of the stronger IEEE 802.11i security standard. With the WPA2 option, the bridge tries WPA2 first, but falls back to WPA if the client only supports WPA. With the WPA2 Only option, the bridge associates only with clients that also support WPA2 security.

Cipher Type: The encryption algorithm used to secure the data communication. TKIP (Temporal Key Integrity Protocol) provides per-packet key generation and is based on WEP. AES (Advanced Encryption Standard) is a very secure block based encryption. With the TKIP or AES option, the bridge negotiates the cipher type with the access point, and uses AES when available. Group Key Update Interval: The amount of time before the group key used for broadcast and multicast data is changed. WPA-Personal This option uses Wi-Fi Protected Access with a Pre-Shared Key (PSK). The WPA Mode further refines the variant that the bridge should employ.This option uses Wi-Fi Protected Access with a Pre-Shared Key (PSK). Pre-Shared Key: The key is entered as a pass-phrase of up to 63 alphanumeric characters in ASCII (American Standard Code for Information Interchange) format at both ends of the wireless connection. It cannot be shorter than eight characters, although for proper security it needs to be of ample length and should not be a commonly known phrase.
This phrase is used to generate session keys that are unique for each wireless client. Example: Wireless Networking technology enables ubiquitous communication WPA-Enterprise This option works with a RADIUS Server to authenticate wireless clients. Wireless clients should have established the necessary credentials before attempting to authenticate to the Server through this bridge. EAP Type: The EAP type which is used for the authentication. These types are EAP-TLS, EAP-TTLS and PEAP.
Inner Authentication Method for TTLS: If the authentication type is selected as EAP-TTLS, it uses an inner authentication method after the TLS-securedtunnel is established between the client and server. The supported inner authentication types for EAP-TTLS are PAP, CHAP and MS-CHAPv2. Inner Authentication Method for PEAP: If the authentication type is selected as PEAP, it uses an inner authentication method after the TLS-secured tunnel is established between the client and server. The supported inner authentication type for PEAP is MS-CHAPv2. EAP Username: The username of the wireless client for the tunnel establishment and the inner authentication method.
EAP Password: The password of the wireless client for EAP-MD5 or the inner authentication methods of PEAP and EAP-TTLS. EAP Certificate Password: The password of the user certificate file. 41 EAP User Certificate: The user certificate file. It is mandatory for EAP-TLS, but optional for PEAP and EAP-TTLS. If it is not uploaded for PEAP and EAP-TTLS, the bridge may establish a relatively unsecure system. We support .p12 and .pfx formats with a maximum size of 8192 bytes. EAP Root Certificate: The root certificate file. It is mandatory to upload a root certificate to be able to authenticate the server certificate.

We support .der and .cer formats with a maximum size of 8192 bytes. Basic_ Network Settings LAN Settings These are the settings of the LAN (Local Area Network) interface for the bridge. The IP address is also used to access this Web-based management interface. It is recommended that you use the default settings if you do not have an existing network. IP Address Mode Select DHCP to get the IP settings from a DHCP server on your network. Select Static to use the IP settings specified on this page. IP Address The IP address of your bridge on the local area network. For example, 192.
168.1.24 The address you choose must be consistent with the LAN settings of your router.


You're reading an excerpt. Click here to read official SMC WEB-N user guide
http://yourpdfguides.com/dref/3456912

Subnet Mask The subnet mask of the local area network. 42 Default Gateway This is the IP address of the gateway or router that connects you to the internet. Advanced The Advanced tab provides the following configuration options: Advanced Wireless, WISH, Wi-Fi Protected Setup Advanced_Advanced Wireless MAC Cloning Mode This feature controls the MAC Address of the Bridge as seen by other devices (wired or wireless). If set to Ethernet Client, the MAC Address from the first Ethernet client that transmits data through the Bridge will be used. This setting is useful when connected to an Xbox or if there is only one Ethernet device connected to the Bridge. When multiple Ethernet devices are connected to the Bridge, it may not be obvious which MAC Address is being used. If set to WLAN Card, the MAC Address of the WLAN Card (typically written on the back of the card) will be used.

When multiple Ethernet devices are connected to the Bridge, the MAC Address of the Bridge will not change. 43 Transmit Power Normally the wireless transmitter operates at 100% power. In some circumstances, however, there might be a need to isolate specific frequencies to a smaller area. By reducing the power of the radio, you can prevent transmissions from reaching beyond your corporate/home office or designated wireless area. RTS Threshold When an excessive number of wireless packet collisions are occurring, wireless performance can be improved by using the RTS/CTS (Request to Send/Clear to Send) handshake protocol. The wireless transmitter will begin to send RTS frames (and wait for CTS) when data frame size in bytes is greater than the RTS Threshold. This setting should remain at its default value of 2346 bytes. Fragmentation Threshold Wireless frames can be divided into smaller units (fragments) to improve performance in the presence of RF interference and at the limits of RF coverage. Fragmentation will occur when frame size in bytes is greater than the Fragmentation Threshold. Setting the Fragmentation value too low may result in poor performance.

WMM Enable Enabling WMM can help control latency and jitter when transmitting multimedia content over a wireless connection. Short GI Using a short (400ns) guard interval can increase throughput. However, it can also increase error rate in some installations, due to increased sensitivity to radio-frequency reflections. Select the option that works best for your installation. 44 Advanced_Wish WISH is short for Wireless Intelligent Stream Handling, a technology developed to enhance your experience of using a wireless network by prioritizing the traffic of different applications. WISH Enable WISH Enable this option if you want to allow WISH to prioritize your traffic. 45 Priority Classifiers HTTP Allows the router to recognize HTTP transfers for many common audio and video streams and prioritize them above other traffic. Such streams are frequently used by digital media players. Windows Media Center Enables the router to recognize certain audio and video streams generated by a Windows Media Center PC and to prioritize these above other traffic. Such streams are used by systems known as Windows Media Extenders, such as the Xbox 360.

Automatic When enabled, this option causes the router to automatically attempt to prioritize traffic streams that it doesn't otherwise recognize, based on the behaviour that the streams exhibit. This acts to deprioritize streams that exhibit bulk transfer characteristics, such as file transfers, while leaving interactive traffic, such as gaming or VoIP, running at a normal priority. WISH Rules A WISH Rule identifies a specific message flow and assigns a priority to that flow. For most applications, the priority classifiers ensure the right priorities and specific WISH Rules are not required. WISH supports overlaps between rules. If more than one rule matches for a specific message flow, the rule with the highest priority will be used. Name Create a name for the rule that is meaningful to you. Priority The priority of the message flow is entered here. Four priorities are defined: · · · · BK: Background (least urgent). BE: Best Effort. VI: Video. VO: Voice (most urgent). Protocol The protocol used by the messages. Host 1 IP Range The rule applies to a flow of messages for which one computer's IP address falls within the range set here. Host 1 Port Range The rule applies to a flow of messages for which host 1's port number is within the range set here. Host 2 IP Range The rule applies to a flow of messages for which the other computer's IP address falls within the range set here. Host 2 Port Range The rule applies to a flow of messages for which host 2's port number is within the range set here. -- WISH Rules This section is where you define WISH Rules. Enable or disable defined rules with the checkboxes at the left. 46 Advanced_ Wi-Fi Protected Setup PIN Settings A PIN is a unique number that can be used to add the SMCWEB-N to an existing network or to create a new network.

The default PIN is printed on the bottom of the unit. For extra security, a new PIN can be generated. You can restore the default PIN at any time. Only the Administrator ("admin" account) can change or reset the PIN. Current PIN Shows the current value of the bridge's PIN. Reset PIN to Default Restore the default PIN of the bridge. Generate New PIN Create a random number that is a valid PIN. This becomes the bridge's PIN. You can then copy this PIN to the user interface of the registrar. Set Up Wireless This Wizard helps you add wireless devices to the wireless network.

@@If the device supports Wi-Fi Protected Setup and has a configuration button, you can add it to the network by pressing the configuration button on the device and then pressing the button on the router within 120 seconds. Each device 47 has an LED, and the LED will start flashing if the button is pressed. The LED on the router will turn solid ON if the device has been successfully added to the network. If something goes wrong during configuration, the flashing pattern of the LED changes. There are several ways to add a wireless device to your network.

@@@@The router acts as a registrar for the network, although other devices may act as a registrar as well. After the device is in WiFi Protected Setup configured state, holding the button for more than 5 seconds will reset the device to unconfigured state, and the device will discard the current wireless security settings and will start to run WiFi Protected Setup protocol to find the new security settings. Set UP Wireless Wizard Start the wizard. 48 Tools The Tools tab provides the following configuration options: Admin, System, Firmware Tools_Admin The Admin option is used to set a password for access to the Web-based management. By default there is no password configured.

It is highly recommended that you create a password to keep your new bridge secure. Admin Password Enter a password for the user admin, who will have full access to the Web-based management interface.

You're reading an excerpt. Click here to read official SMC WEB-N user guide

http://yourpdfguides.com/dref/3456912