1900 Alameda de las Pulgas, #110
San Mateo, CA. 94403-1222 U.S.A.
Tel: 650-574-1257
Fax: 650-574-1286

*e*XS 5001 Wireless NODE
Version A

Technician Manual

Revision A.2.1
November, 2005

Contents

Introduction

The *e*XS® 5001 Wireless NODE is a dual-radio device that enable the network operator to deploy a wireless network, *e*XS ZONE™, without laying any data cables. The *e*XS NODE™ is designed to:

1. Mesh with other NODEs using the IEEE 802.11a radio
2. Service clients over the Ethernet port and the wireless access port (IEEE 802.11g radio)
3. The traffic is routed to the *e*XS NODE™ that is connected to the backhaul, otherwise known as the gateway.

The NODE is a layer-3 router that can be configured as a Repeater or as a Gateway. In the Repeater configuration the DHCP server internal to the NODE will service BOTH the LAN port and the wireless 802.11g access.

The NODE supports the installation of client devices like a SIP phones over the LAN interface.

The Gateway mode will configure the LAN interface to act as a WAN port to enable the unit to interface to the existing campus/corporate LAN or to the available backhaul. The port in this configuration can be configured to act as a DHCP CLIENT or with STATIC IP information.

The setup of the 802.11b/g access is performed through the "setup" tab while the mesh network configuration is done through the "Advanced" tab. It is important to remember to configure the mesh network after configuring the access.

Notation: Prompts and dialog scripts are shown in normal type. Technician typed inputs and names of tabs are shown in *italics*.

This manual follows industry practice of referring to this professional person as the "User". In this manual "User" does not mean the consumer, network subscriber or end user.

Professional installation: This system must be professionally configured, installed and maintained. The person configuring the NODEs must be knowledgeable in the radio and safety regulations for the country and location where this system will be installed, and is responsible for making the installation comply with those safety and radio regulations.

The NODE can be used with ANY brand and type of power over Ethernet (PoE) that is an approved power source for the installation location.

The professional planning the installation shall be responsible for ensuring that the proper antenna is employed so that the radio and safety requirements for that location are met.

In the USA, the PoE and antenna have to be the units tested for Certification, which are on the *e*XS Price List.

Web Configuration Manager Application

The *e*XS 5001 Wireless NODE is configured using a web browser such as Microsoft Internet Explorer or Netscape, from any wired or wireless station on the local area network.

Using the **https** protocol, enter https://<single_board_computer_IP_address> as the location.

The default address is: https://192.168.100.1

At which point you will be see the security alert below

Figure 1

Click the *Yes* button to access the NODE. You will be prompted then to type your username and password.

Figure 2

The defaults are:

Username: *admin*

Password: *admin*

When you enter the password, asterisks are displayed

When you have been authenticated to access the web configuration manager application, the Top page is displayed as shown in Figure 3.

Warning: there are web sites on the Internet that contain factory passwords for thousands of products. Be sure to set a unique Username and Password for each major network. It is good practice to change these whenever there is a change in personnel.

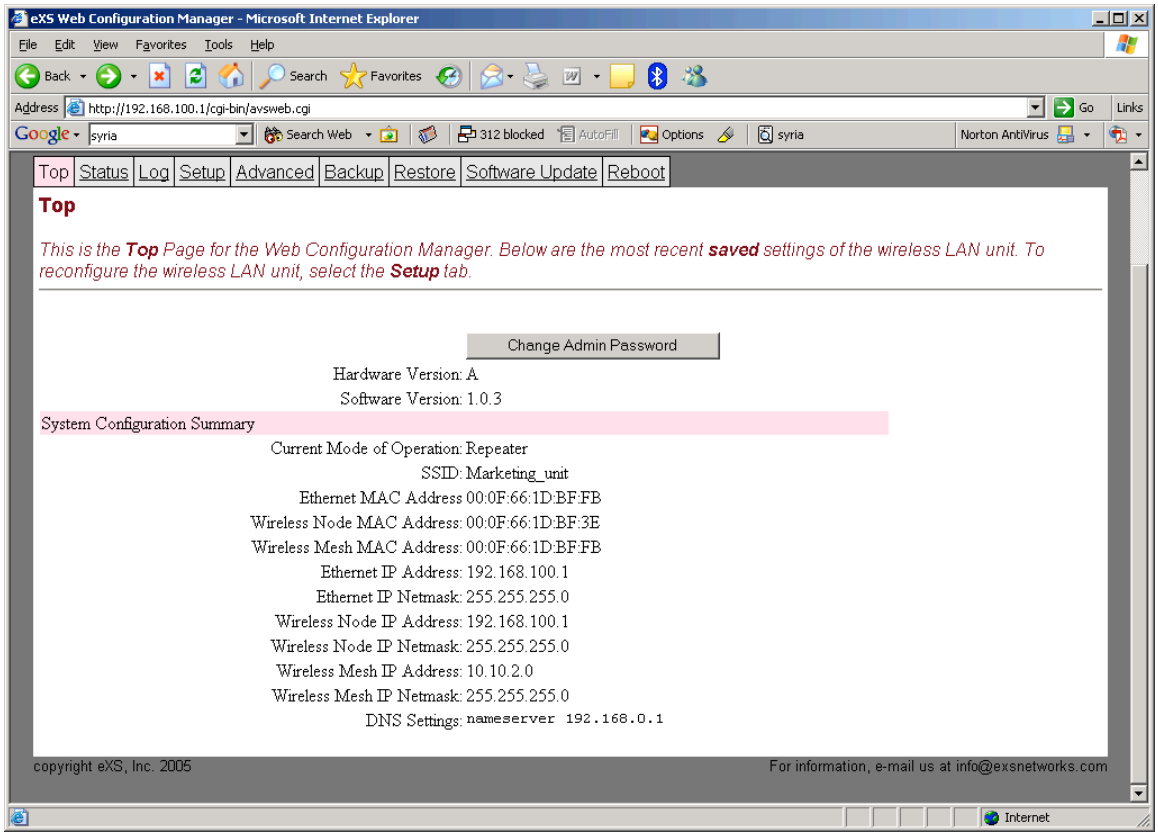

Figure 3

Top

The Top page is the first page displayed by the web configuration manager application as shown in above.

The web configuration application's main menu is a collection of tabs in the upper left side of the page. The Top page displays the values of various pieces of information in the center of the page, such as the host name and the current mode of operation. Additionally, the Top page provides a way to change the admin user password.

The values displayed on the Top page are from the NODE configuration data stored the last time the configuration was saved. When the NODE is first booted, the data on the Top page reflects the values of the configuration data under which the unit is currently operating. For example, in the previous figure showing a sample Top page, the current mode of operation is a Gateway.

Status

The Status main menu item displays a brief overview of the overall system as shown in the Figure 4. The values displayed on the Status page are from the saved configuration data. When the single board computer is first booted, the data on the Status page reflects the values of the configuration data under

which the NODE is currently operating.

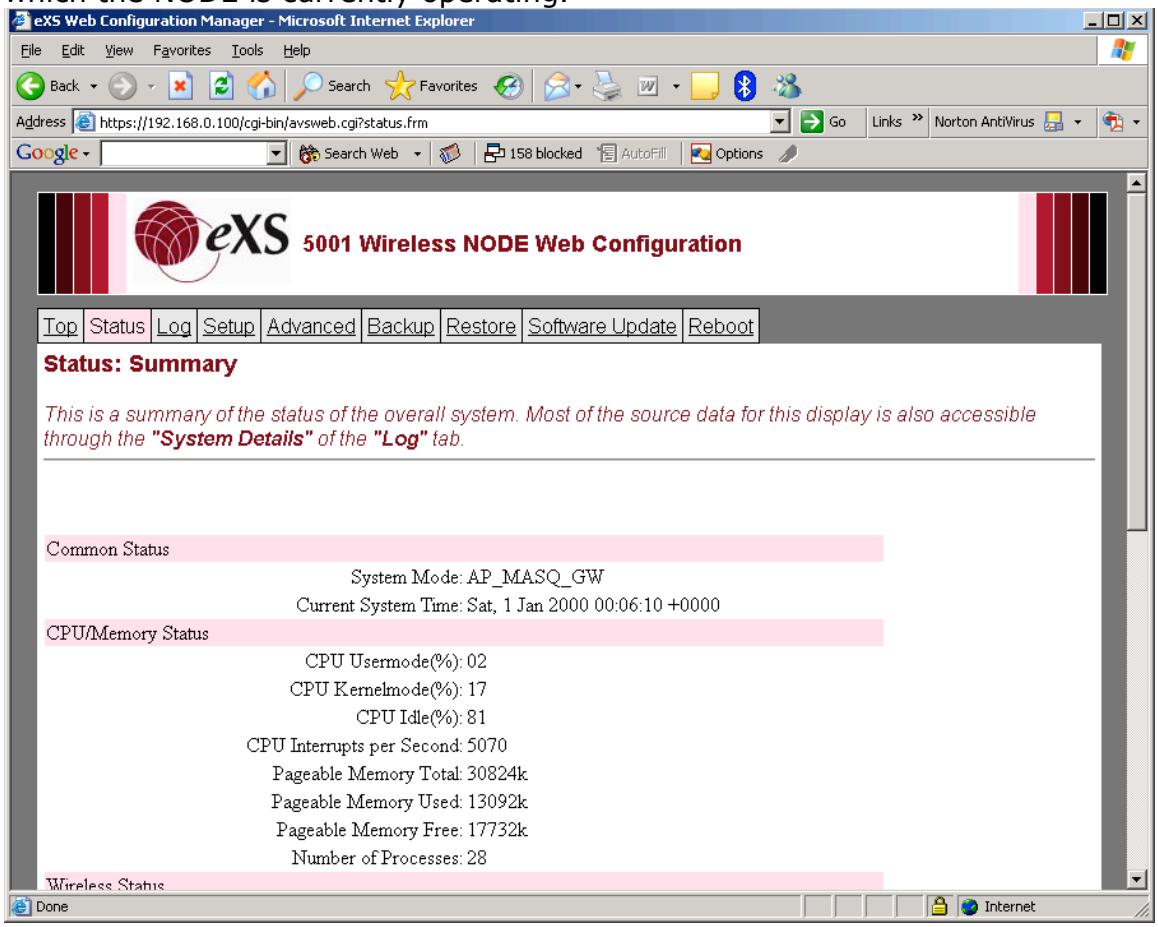

Figure 4

Log

The Log main menu item displays the System Log file. You can click on the System Details button which results in displaying the output of various system commands to provide a more detailed summary of the overall system.

The Current System Time in the NODE will reset itself at every power up cycle to 1 January 2000 at 00:00:00 hours.

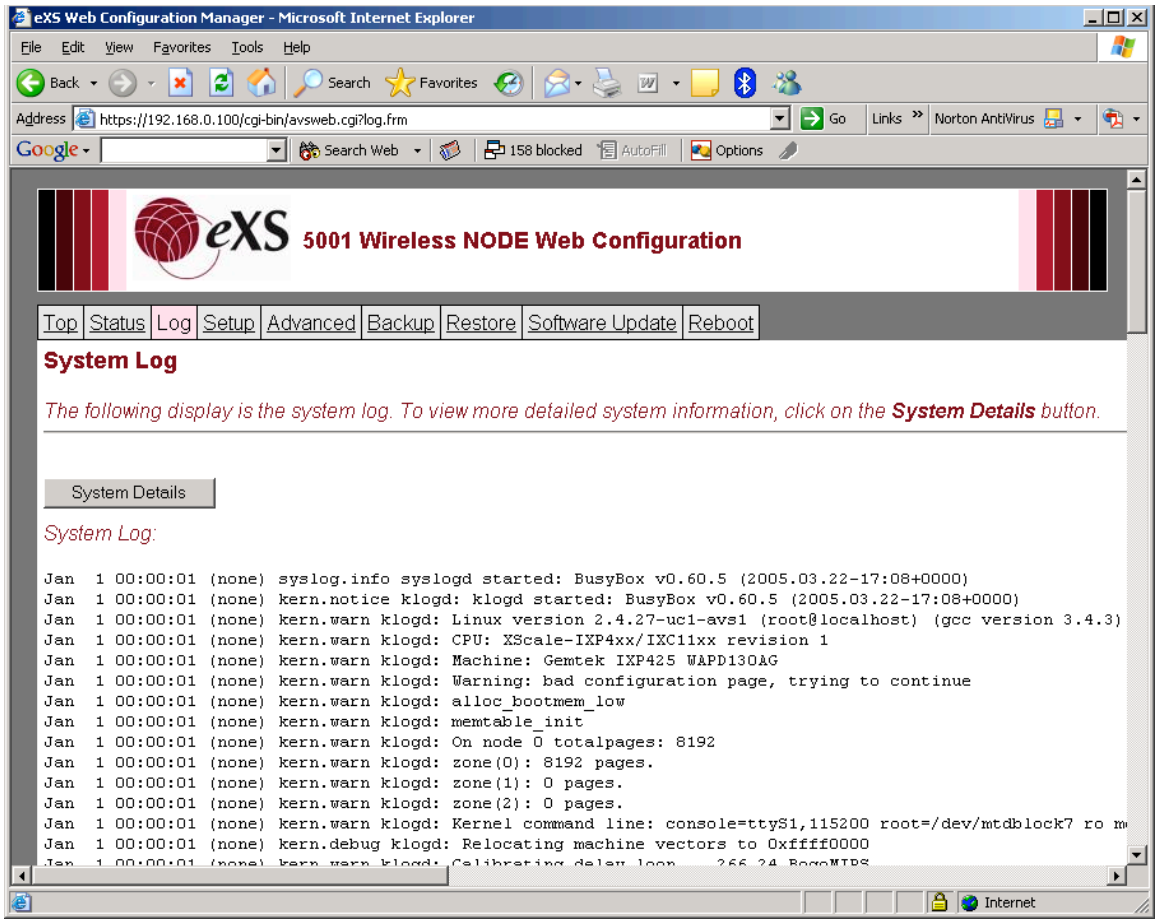

Figure 5

Setup

The Setup main menu item is for setting the mode of operation for the NODE. Two operating modes are available through the pull down menu gateway and Repeater as shown in the following figure.

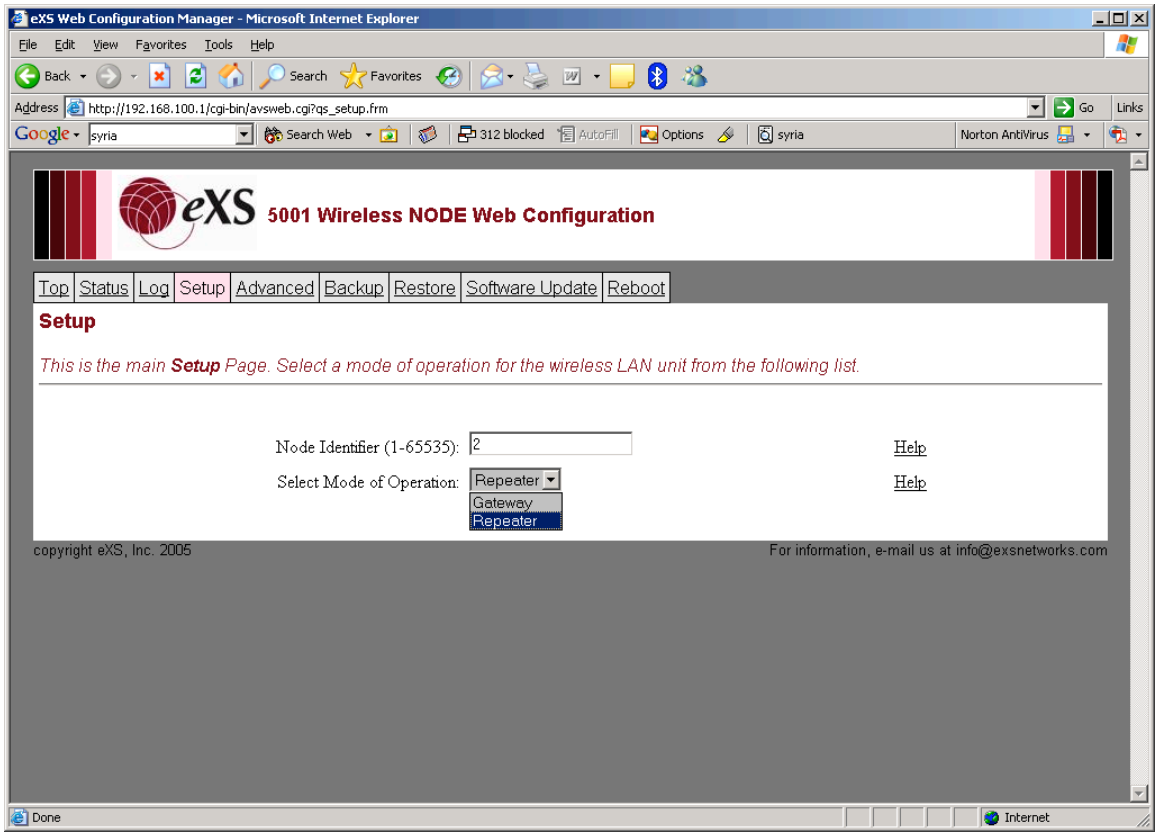

Figure 6

As mentioned before, the majority of NODEs are configured as Repeaters.

Web Configuration Manager Setup Feature

To select a mode of operation, open the pull-down menu and choose a mode by highlighting the mode and clicking on it. The mode you selected will be displayed in the field.

The NODE Identifier should be a unique number on the mesh network to help identify the unit.

The NODE is shipped configured as a Repeater. This configuration is the most common for a mesh NODE. The following subsections will show what web pages are displayed to configure the NODE for a repeater mode of operation.

IP Addresses and General Network Setup

In the repeater mode the wireless Access and the LAN port are serviced by a DHCP server. The next few screens cover the configuration of the network parameters for these two interfaces.

As shown in the figure below, the first screen is to configure the IP address and netmask of the NODE, that is the address used to access the NODE when connect through the Wireless Access port or the wired LAN Access port.

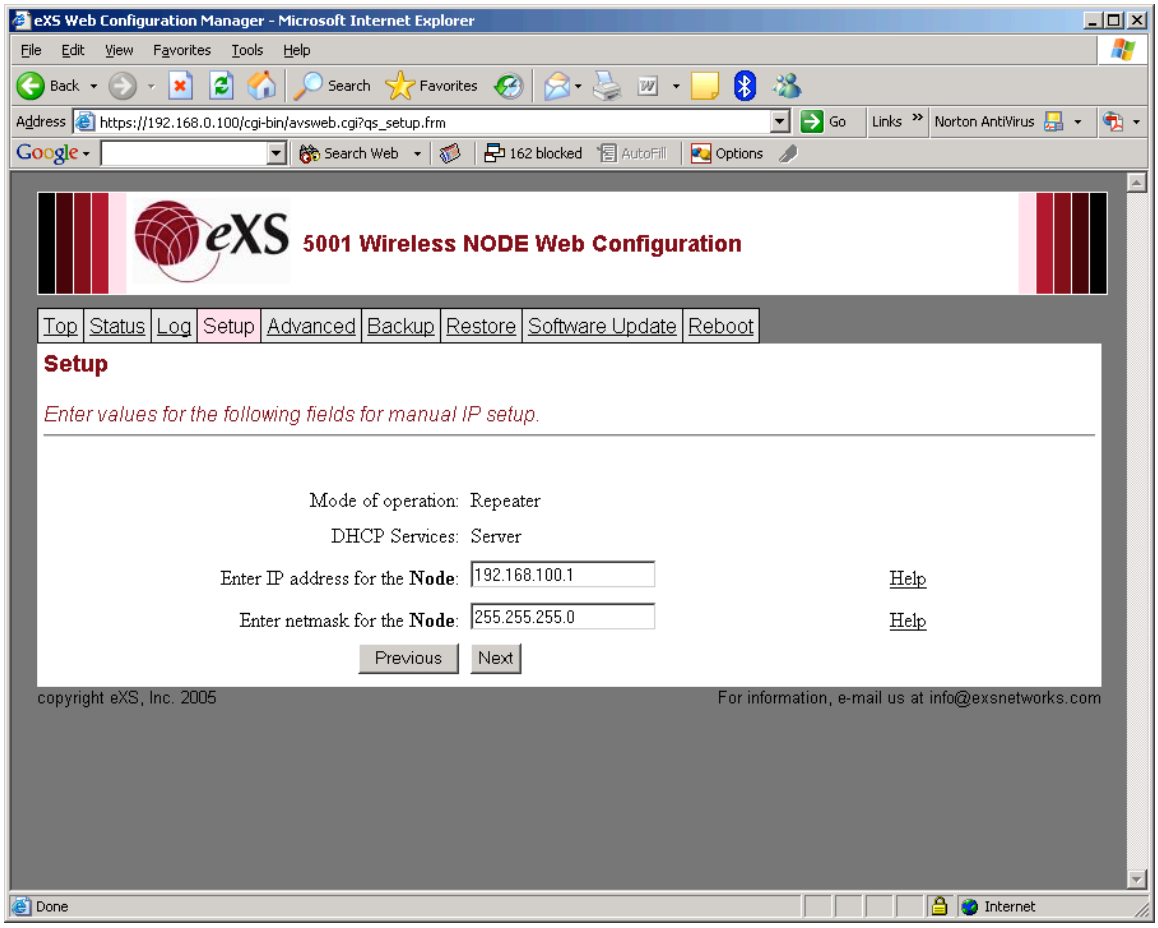

Figure 7

The following screen, will ask you to enter the DNS server IP addresses.

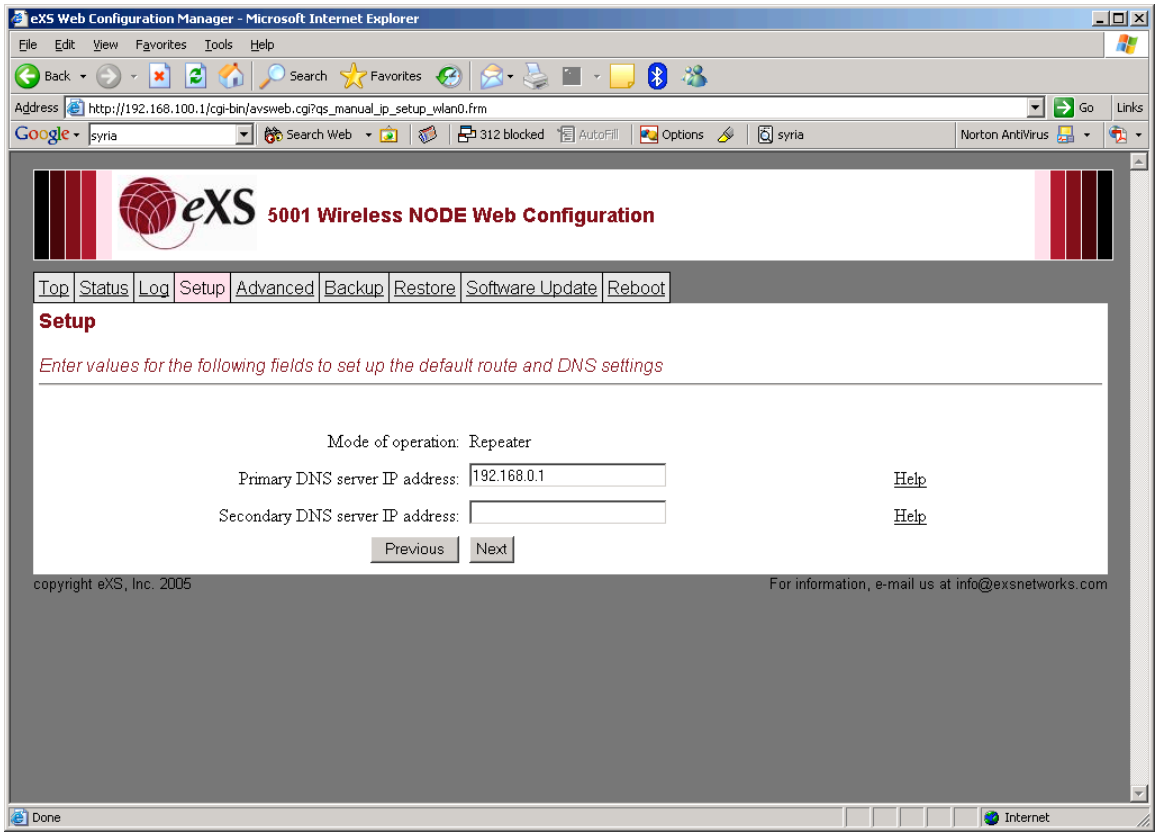

Figure 8

Once those parameters are configured the next screen allows the user to configure the DHCP server details such as the IP range and lease time duration.

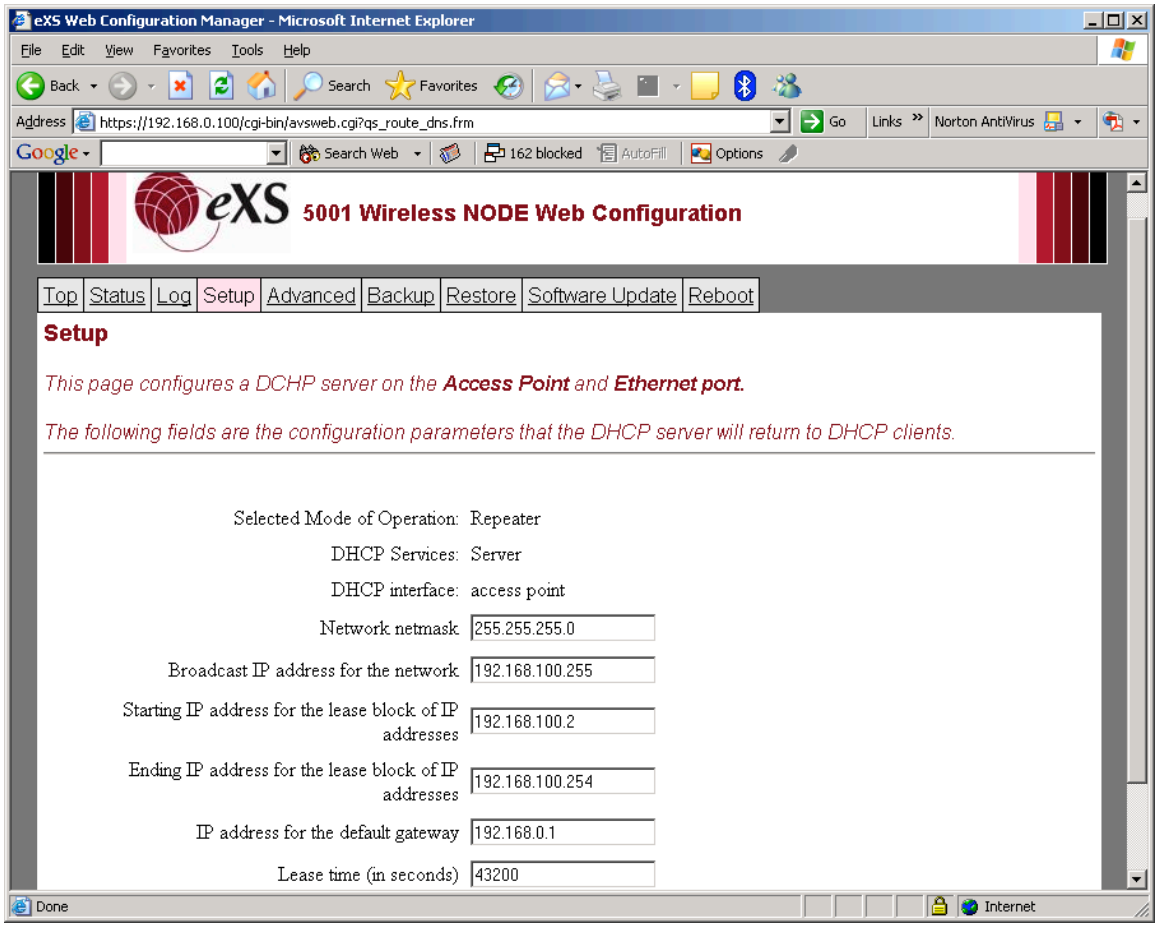

Figure 9

Wireless Access

The following steps would be to configure the wireless access features on the NODE the available options would be to configure the ESSID and the wireless security.

Enter the desired SSID. The SSID is case sensitive.

The SSID on the Access side is visible to client software that scans for available wireless networks, unless that broadcast ID feature is disabled (see below).

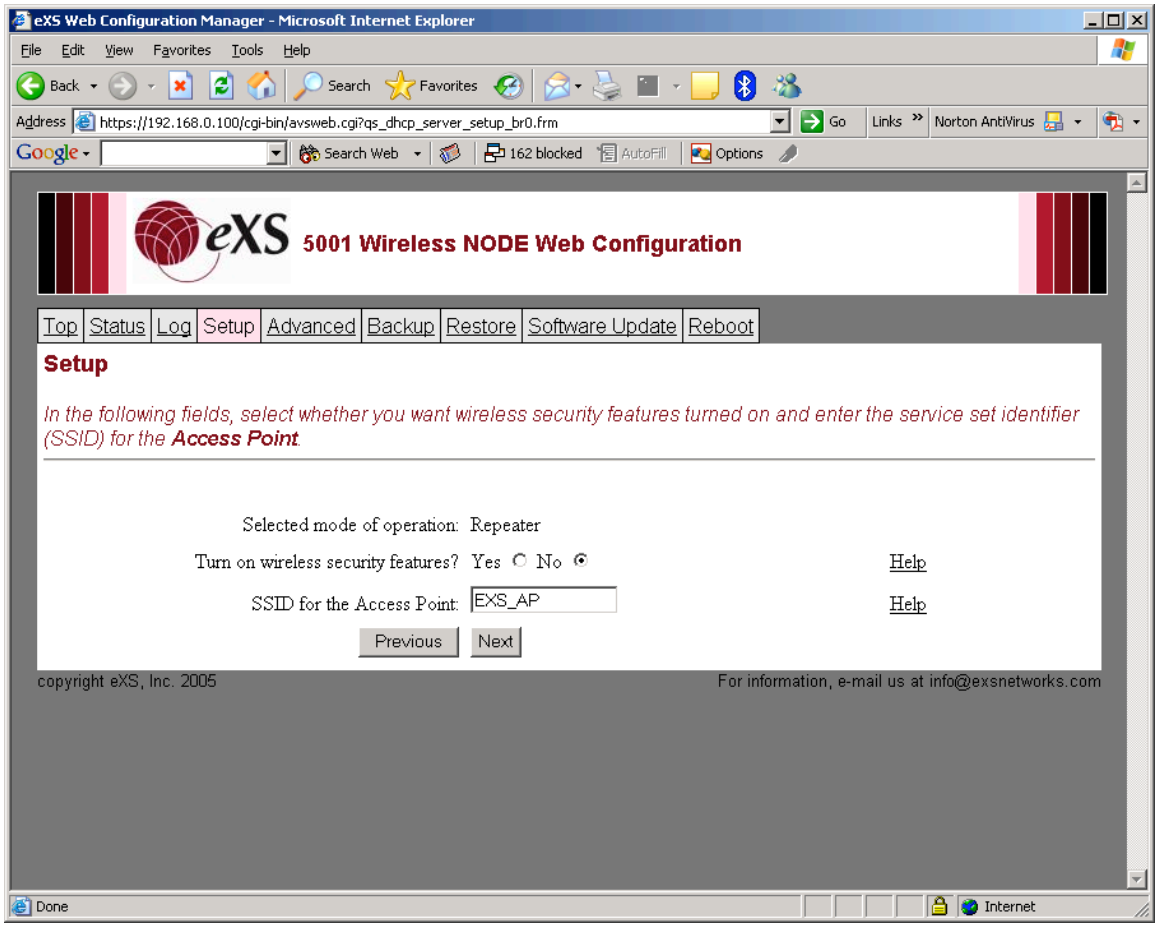

Figure 10

The first security feature is choosing an encryption type. The NODE supports the security defined by the IEEE 802.11 standards for use between clients and an Access Point.

If you want to enable WEP, select one of the WEP buttons which indicate the size of the WEP key, such as WEP128 for 128_bit WEP keys. If you do not want to enable WEP, select the *None* button.

The next security feature is whether you want to hide the SSID in beacon frames. If this feature is enabled, the SSID field of beacon frames will be empty. This feature helps to prevent associations from stations that do not know the NODE's Access SSID, default (EXS_AP_DEFAULT). We recommend hiding the SSID beacon.

The last security feature is whether you want to discard broadcast SSID probe requests. If this feature is enabled, the NODE will not send responses to "broadcast SSID" probe request frames. This feature also helps to prevent associations from stations that do not know the AP's SSID. We recommend discarding probe requests.

When you have selected which wireless security features you want to enable/disable, click the Next button to proceed to the next setup page.

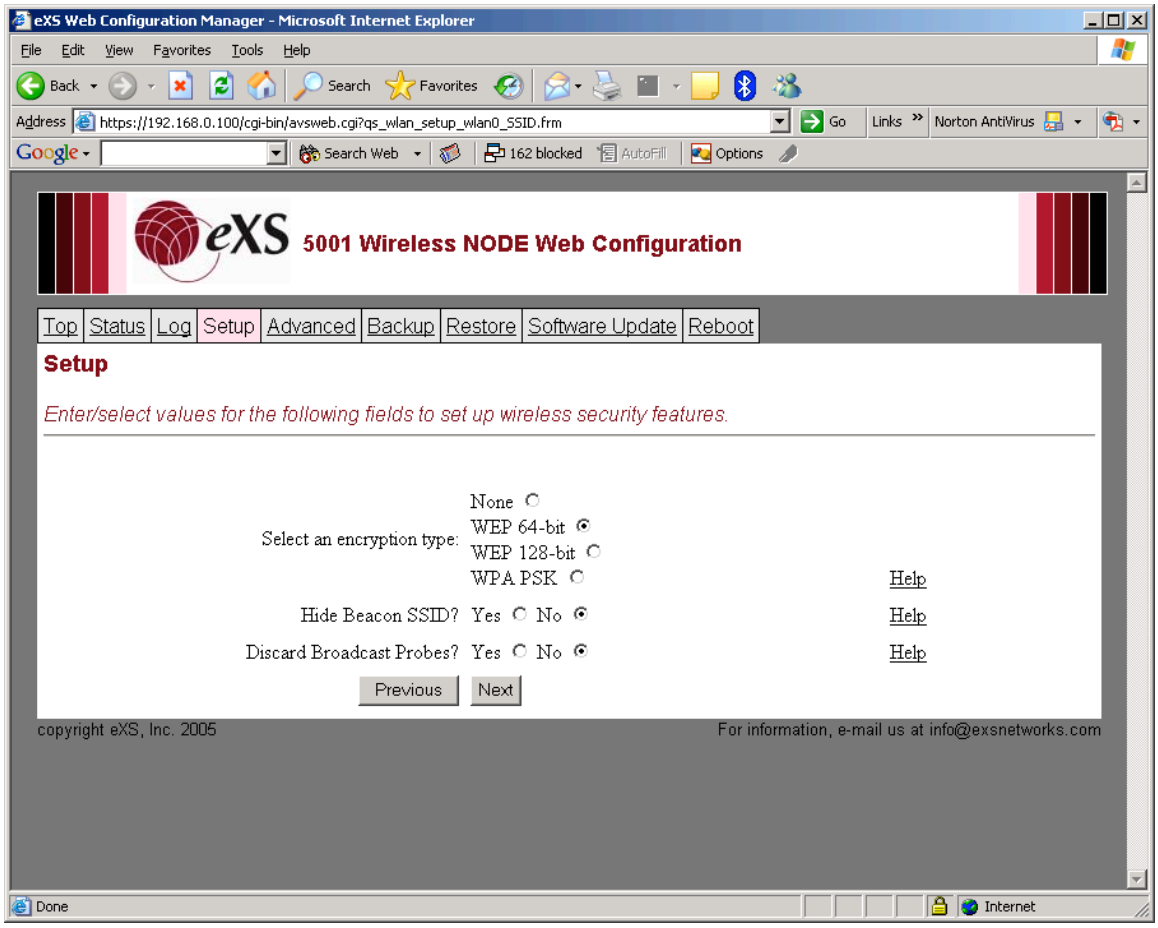

Figure 11

Wi_Fi Protected Access (WPA-PSK)

If you chose to enable Wi-Fi Protected Access (WPA) instead of WEP, a setup page for entering the WPA Pre-Shared Key (PSK) is displayed as shown in the following example. Enter the WPA Pre-Shared Key. It should be at least 20 characters long. When you have entered the key, click the *Next* button to continue.

MAC Address Authentication

This part of the setup is for MAC address authentication. You can further restrict which stations are allowed to join the wireless LAN via MAC address authentication.

When an access point receives an authentication request, it will check its Access Control List (ACL) for the client MAC address. Depending on the authentication mode, the client request will be accepted or denied.

The following figure is the page for configuring the MAC address authentication.

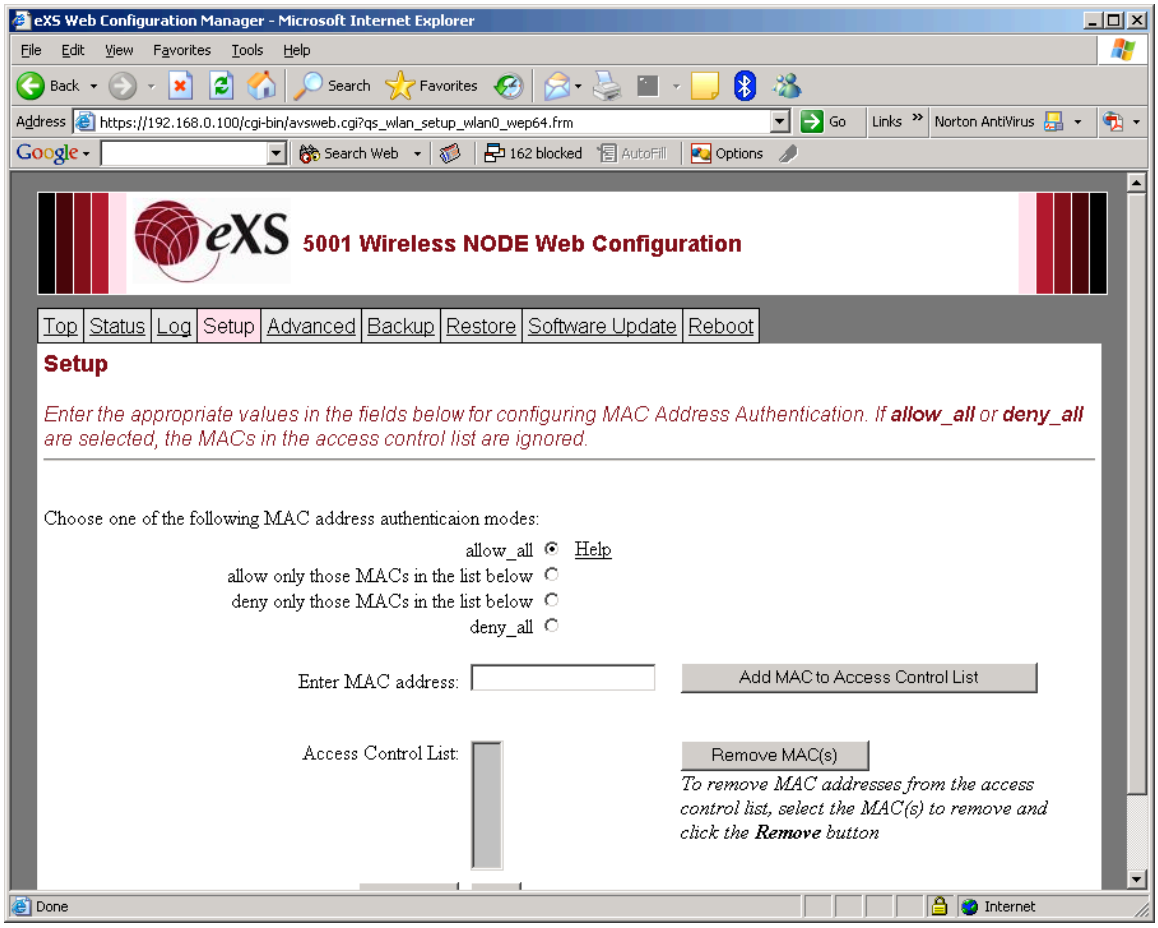

Figure 12

To configure MAC address authentication, select from one of the following MAC address authentication modes:

• *allow all* _ authentication requests are accepted by any MAC address. The access control list is ignored.

• *allow only those MACs in the access list* _ by choosing this mode, the access point will process authentication requests from only those MAC addresses in the access control list. Authentication requests from any MAC address not in the access control list are ignored.

• *deny only those MACs in the access list* _ by choosing this mode, the access point will deny authentication requests from MAC addresses in the access control list. Authentication requests from any MAC address NOT in the access control list are processed.

• *deny all* _ all authentication requests are denied. The access control list is ignored.

Next, build an access control if you selected a mode other than *allow all* or *deny all*. To build the access control list, enter a MAC address in the MAC address field and click on the *Add MAC to Access Control List* button (refer to the previous figure).

The format of the MAC address is a six hexadecimal byte address separated by colons (e.g. 01:02:03:04:05:06). Continue doing this for each MAC address you wish to add to the access control list. When you have finished with MAC address authentication, click the Next button to continue with the setup

Channel Setup

Following the setup for Repeater capability is the channel setup. The following figure shows the setup page for selecting the channel in which the wireless LAN device should operate. The channel selection is a drop down menu, and only one channel may be selected as shown in the next figure. Click the Next button to proceed to the next setup page.

In many countries the preferred channels are 1, 6 & 11.

So many consumer devices come from the factory with channel 6 as the default that it is better to use channels 1 and 11 where possible.

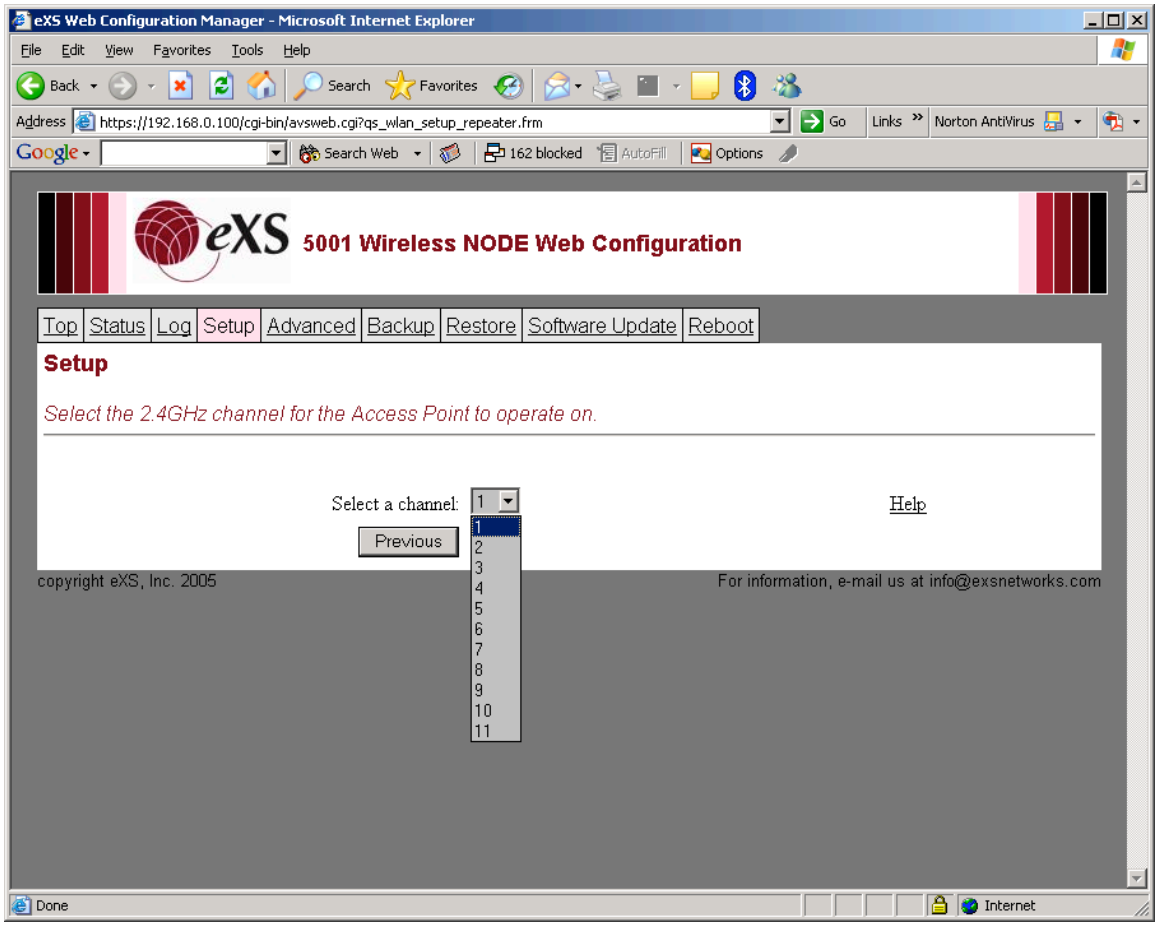

Figure 13

Committing Your Changes

After the setup is completed, the page to permanently commit your changes is displayed as shown below. To permanently commit your changes, click the *Commit Changes* button.

A reboot will occur so the NODE will boot and initialize using your new values. You will need to wait a minute or so until after the NODE has completely rebooted. Once the reboot sequence has completed, you may access the web configuration again by clicking the *Go to Top* button as shown in the next figure.

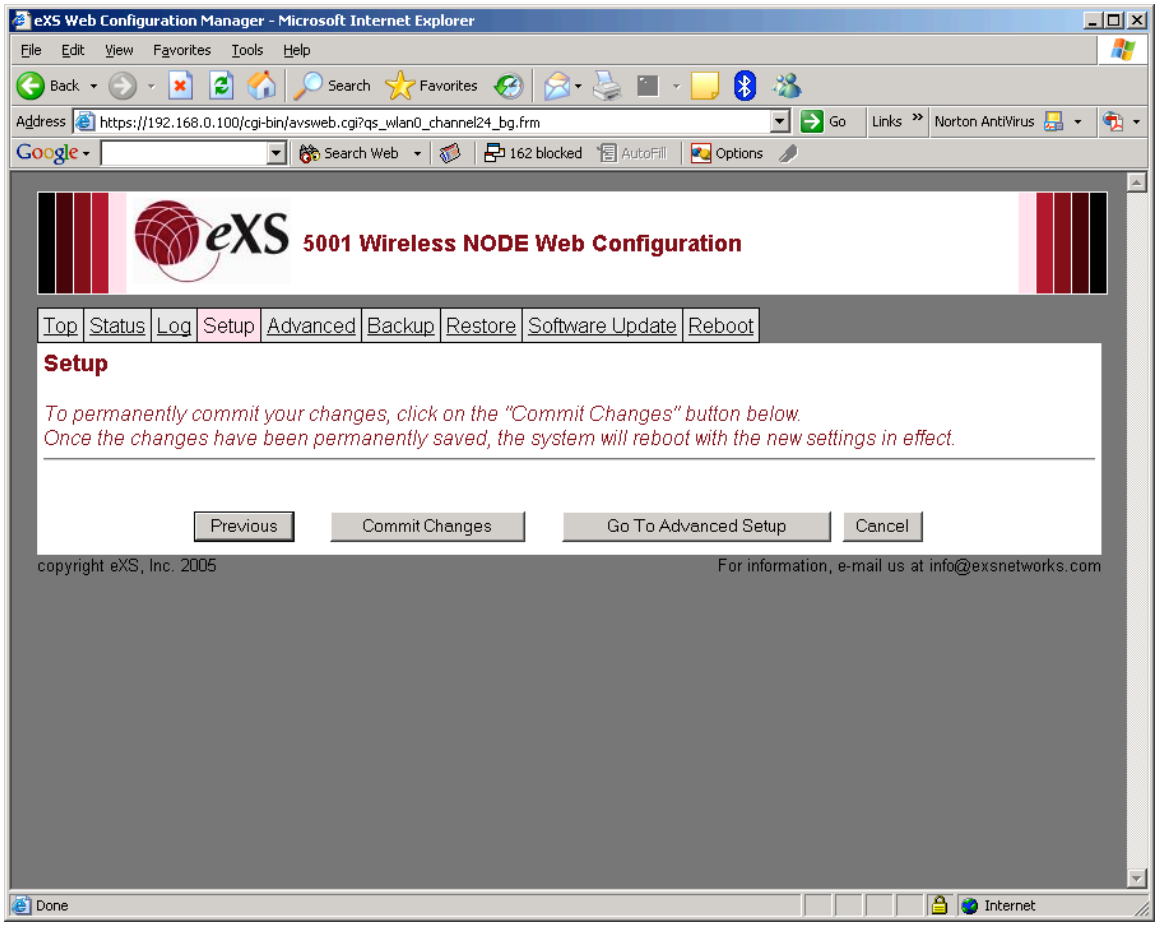

Figure 14

Advanced

The Advanced main menu item provides access to all of the NODE configuration variables. This tab does not contain the configuration wizard of the setup tab, so changes to one field will not result in auto-configuration of the others, i.e. when changing the mode of operation from Repeater to

Gateway, the LAN port will not be configured automatically for you. Understanding such relationships is necessary when using the *Advanced* features in order for the NODE to function properly the next time it's rebooted.

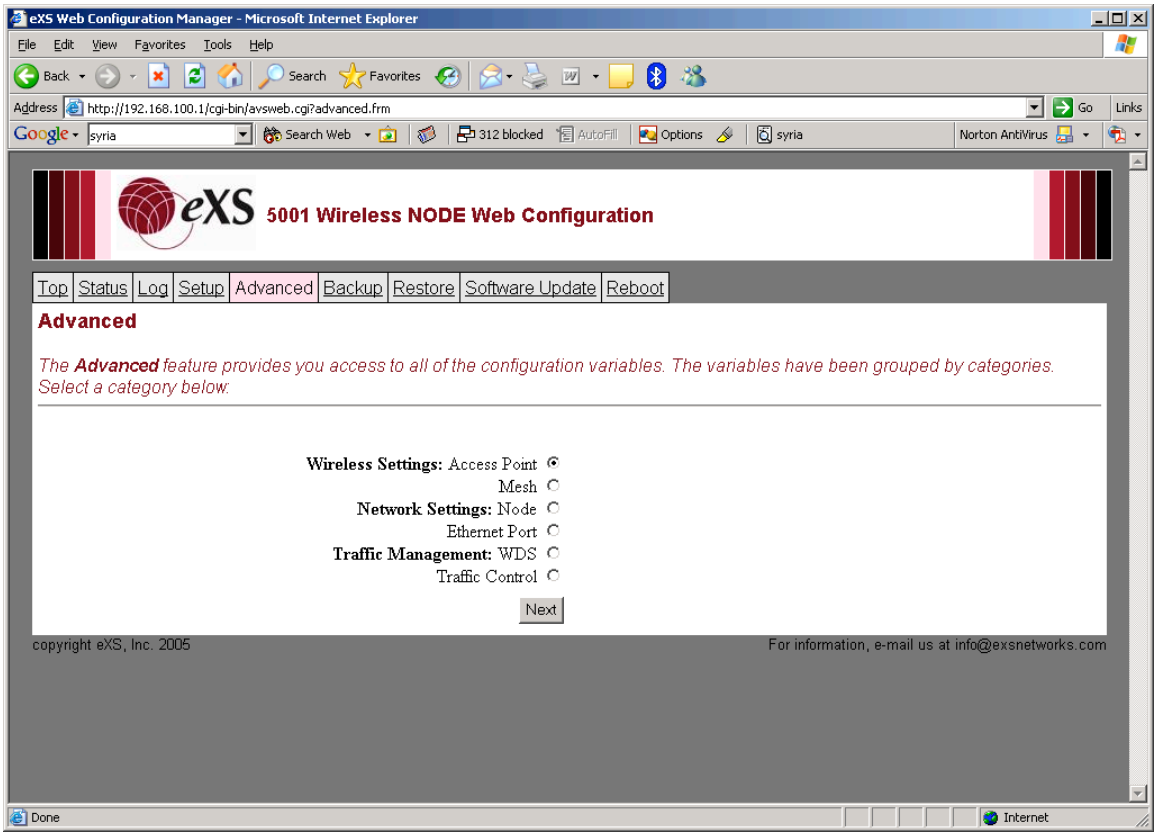

Figure 15

Wireless Setting for the Access Point

In this tab the user can configure the Access Point features in the NODE. The Wireless Access (SSID, rates); Radio specifications (channel assignment, power levels) and wireless security (WEP 64&128 & WPA-PSK, Broadcast ESSID and MAC address authentication) are set.

Wireless Setting for the Mesh Network

In this tab the user can configure the Mesh Network features in the NODE. The Mesh (SSID, rates); Radio specifications (channel assignment, power levels) and wireless security (WEP 64&128 & WPA-PSK, Broadcast ESSID and MAC address authentication) are set.

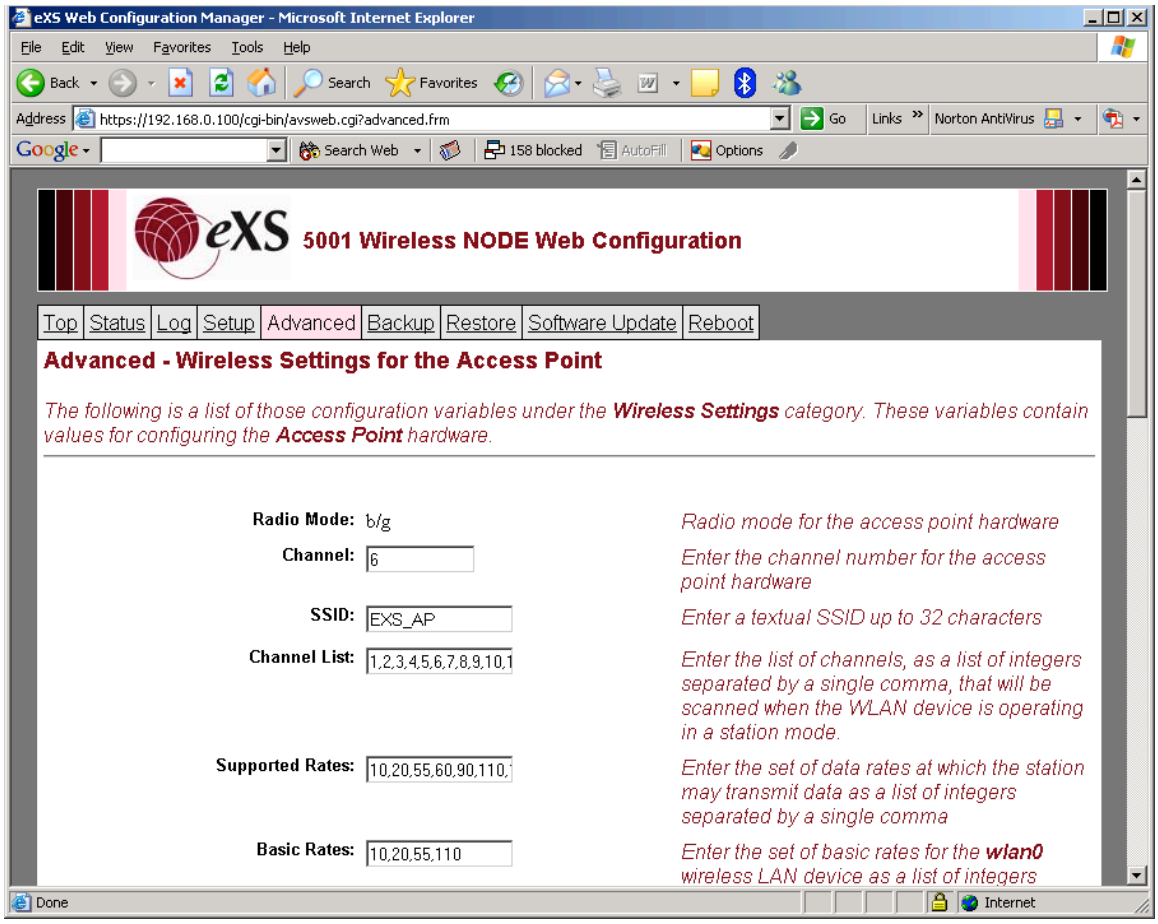

Figure 16

Network Settings for the NODE

In this tab the user can configure the DNS & DHCP parameters for the NODE.

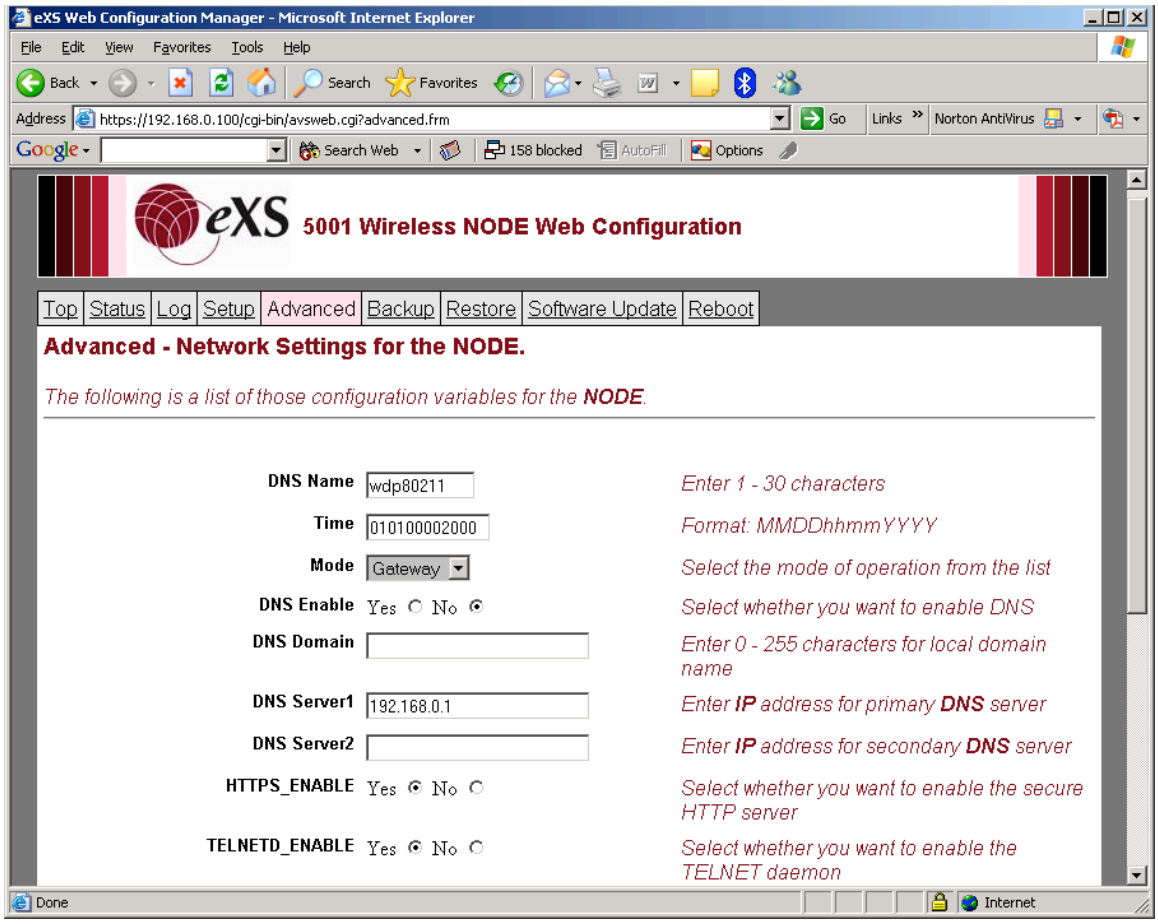

Figure 17

Network Settings for the Ethernet port

When the NODE is acting as a gateway, the user will need to configure the Ethernet/LAN port to act as a WAN interface and communicate correctly with the distribution system. This tab allows the user to configure the port to act as a DHCP in case there is a DHCP server on the LAN or to be configured with a Static IP address.

NOTE: in the repeater mode the Ethernet port will act as a DHCP server and assign IP addresses to clients.

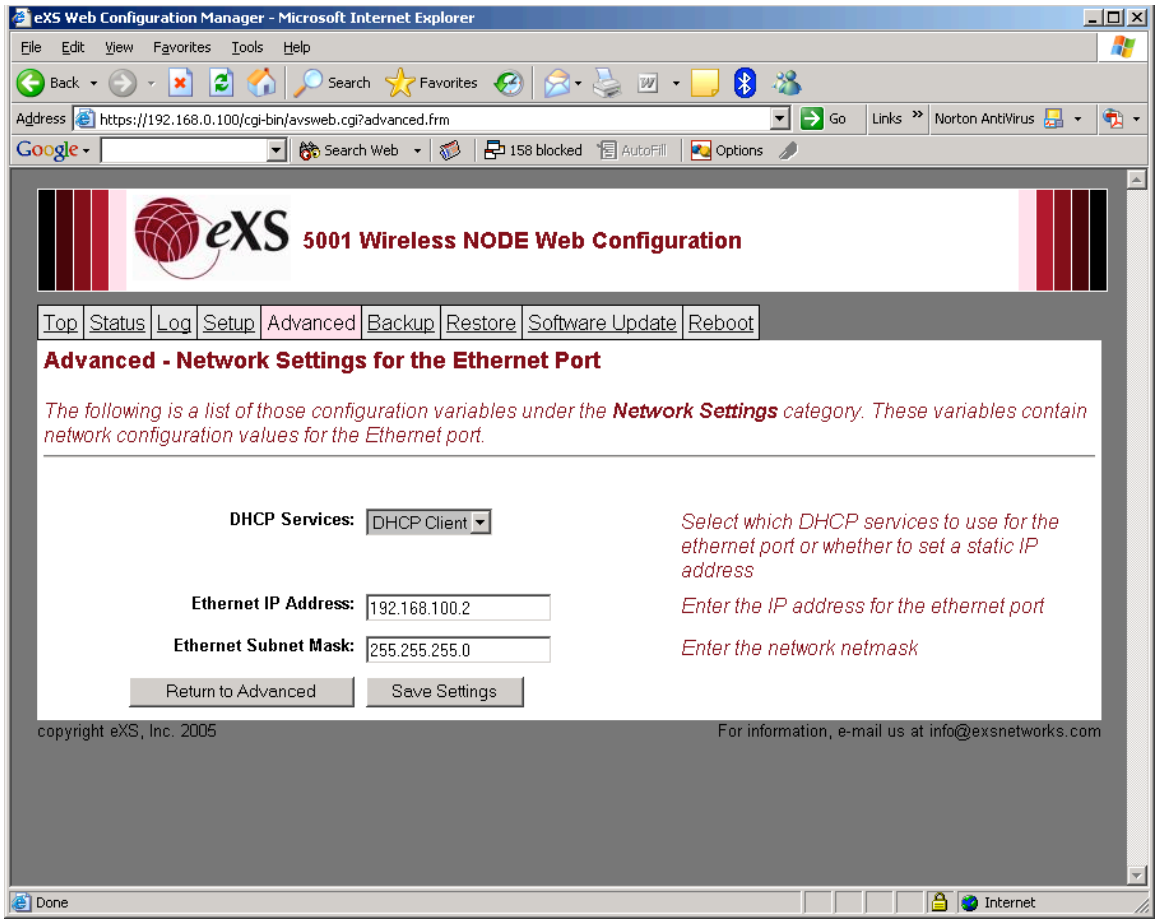
eXS Web Configuration Manager - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address https://192.168.0.100/cgi-bin/avsweb.cgi?advanced.frm
Go Links Norton AntiVirus
Google Search Web 158 blocked AutoFill Options
eXS 5001 Wireless NODE Web Configuration
Top Status Log Setup Advanced Backup Restore Software Update Reboot
Advanced - Network Settings for the Ethernet Port
The following is a list of those configuration variables under the Network Settings category. These variables contain network configuration values for the Ethernet port.
DHCP Services: DHCP Client
Select which DHCP services to use for the ethernet port or whether to set a static IP address
Ethernet IP Address: 192.168.100.2
Enter the IP address for the ethernet port
Ethernet Subnet Mask: 255.255.255.0
Enter the network netmask
Return to Advanced
Save Settings
copyright eXS, Inc. 2005
For information, e-mail us at info@exsnetworks.com
Done
Internet

Figure 18

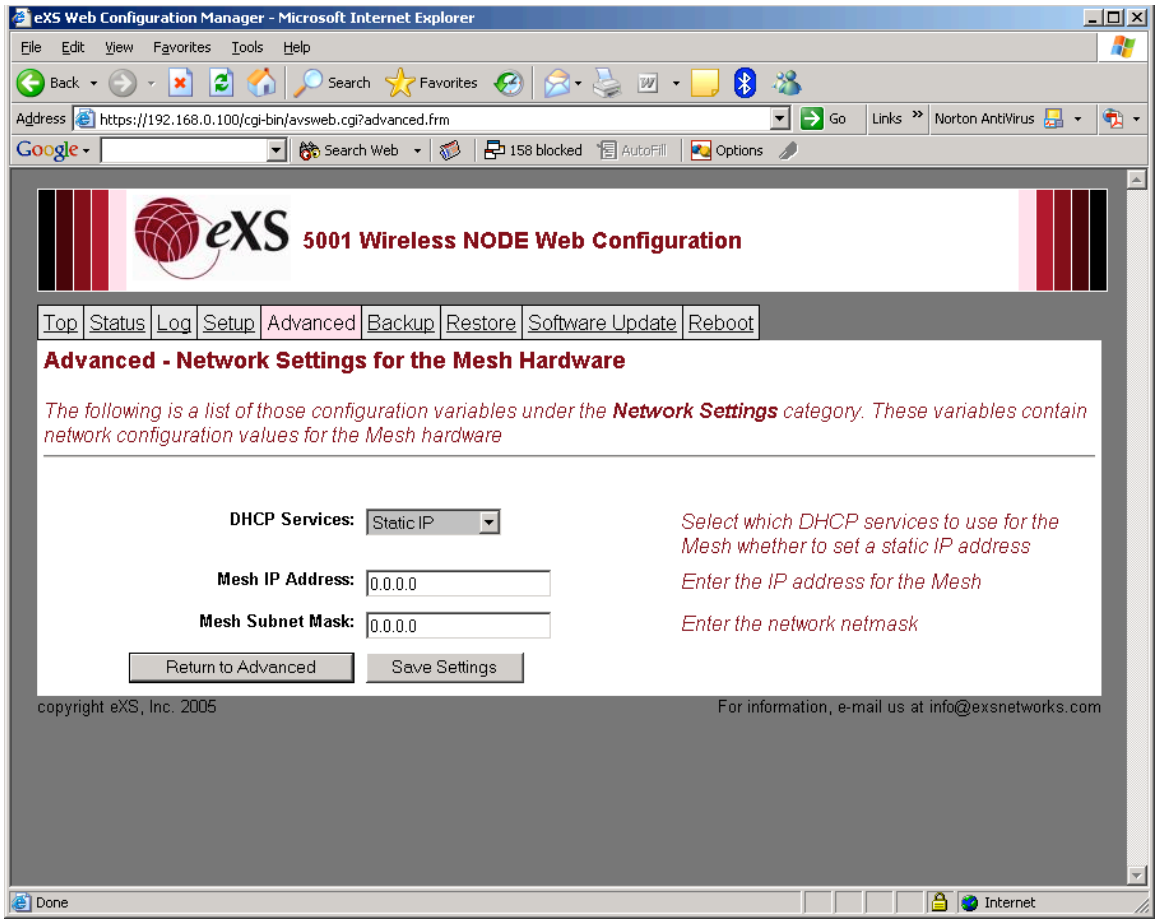

Figure 19

WDS

If the user would like to specify a link manually, you could go under WDS configuration and manually configure the link, that value will be retained in the configuration, while the automatically generated links will refreshed and updated according to the mesh status.

To configure a WDS (Wireless Distribution System) link enter the MAC address of the 802.11a radio on the remote NODE in the Link field

NOTE: for a WDS link to be active, the configuration must be done on the NODEs on each end of the link and the wireless mesh settings on each NODE must be configured with the same security configuration.

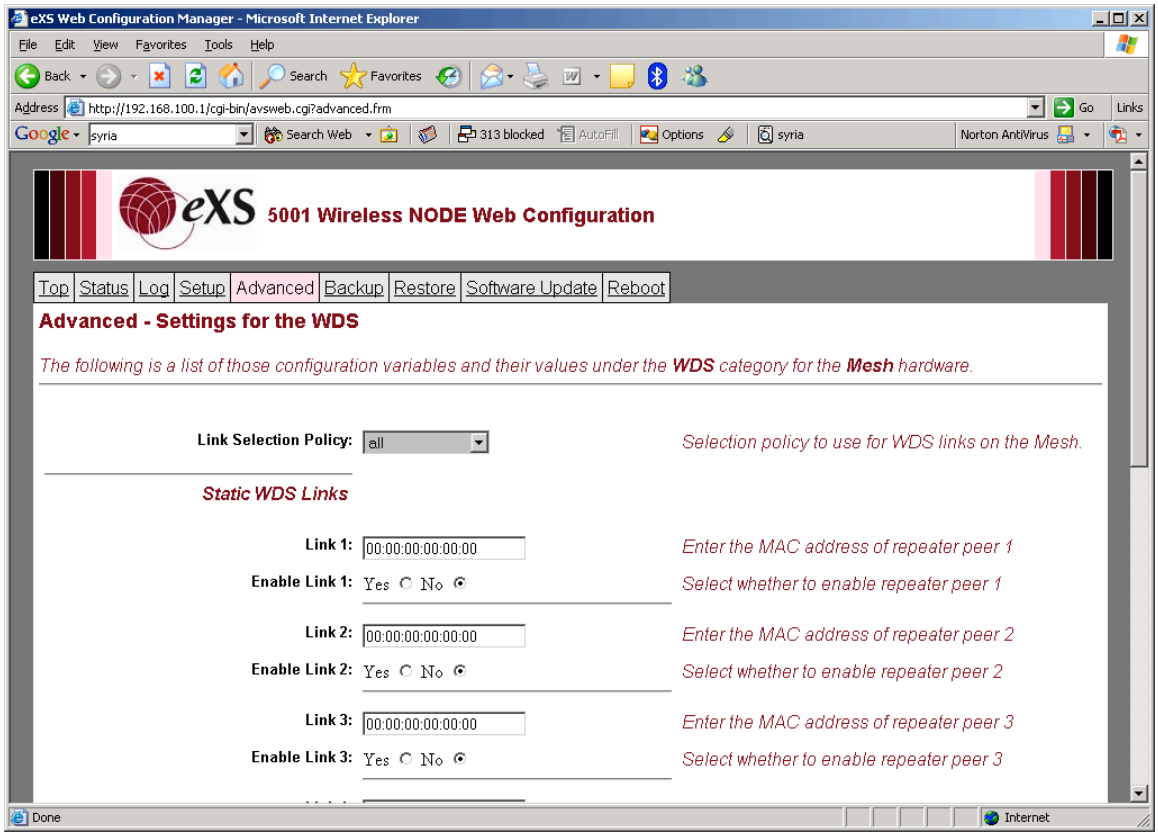

Figure 20

Traffic control:

The NODE support the ability to specify the average and maximum throughput a user can enjoy on the wired AND wireless access interfaces in the repeater mode and the settings will only affect the wireless interface in the Gateway mode.

The mesh will not be affected by the traffic control setting.

If VoIP is going to be implemented on the mesh it is not recommended to specify anything less than 90 kbps for the traffic control.

There are 3 levels of service possible: Gold, Silver and Bronze. Each level average rate and maximum burst rate are settable. It is not advisable to set the Average rate below 64 kbps.

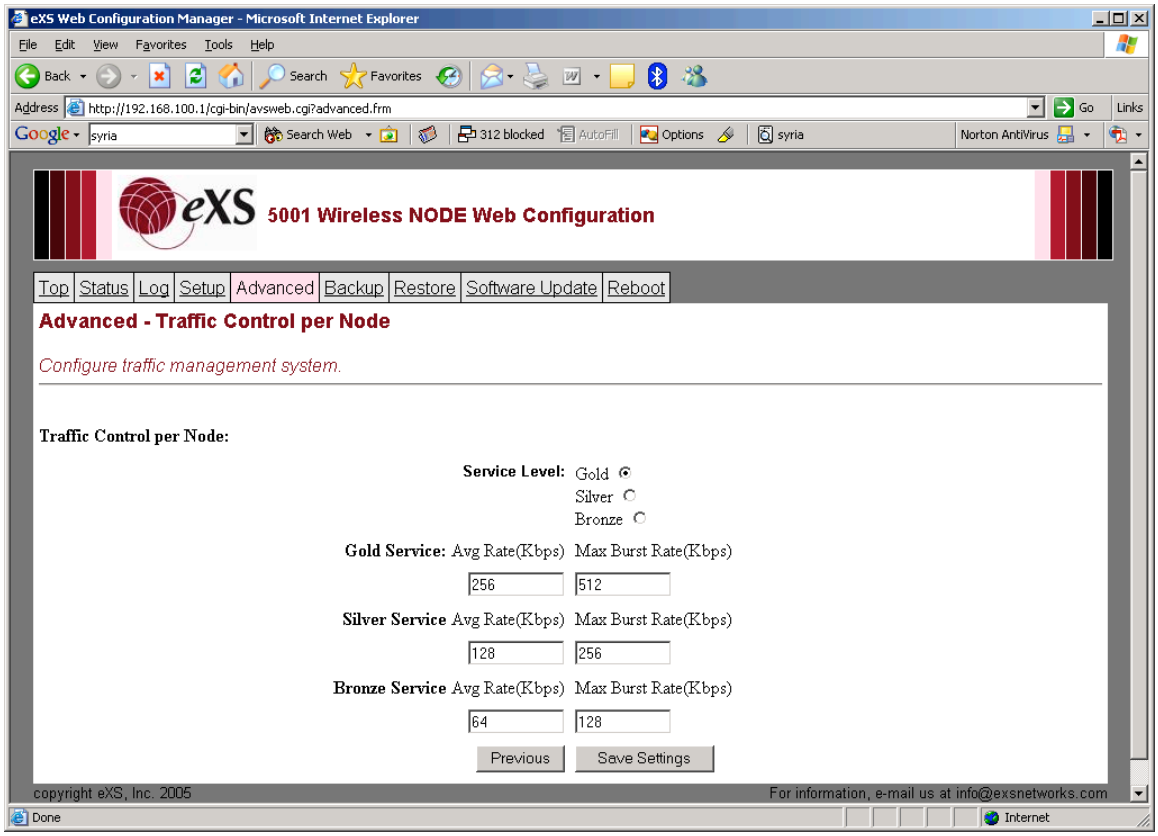

Figure 21

Backup

The *Backup* main menu item provides any easy way to retrieve the last committed configuration settings from the single NODE, namely the *config* file. This file is saved as a Linux "tar" formatted file, and you can save this file on your local PC in the same manner as you save files from other URL's using your web browser.

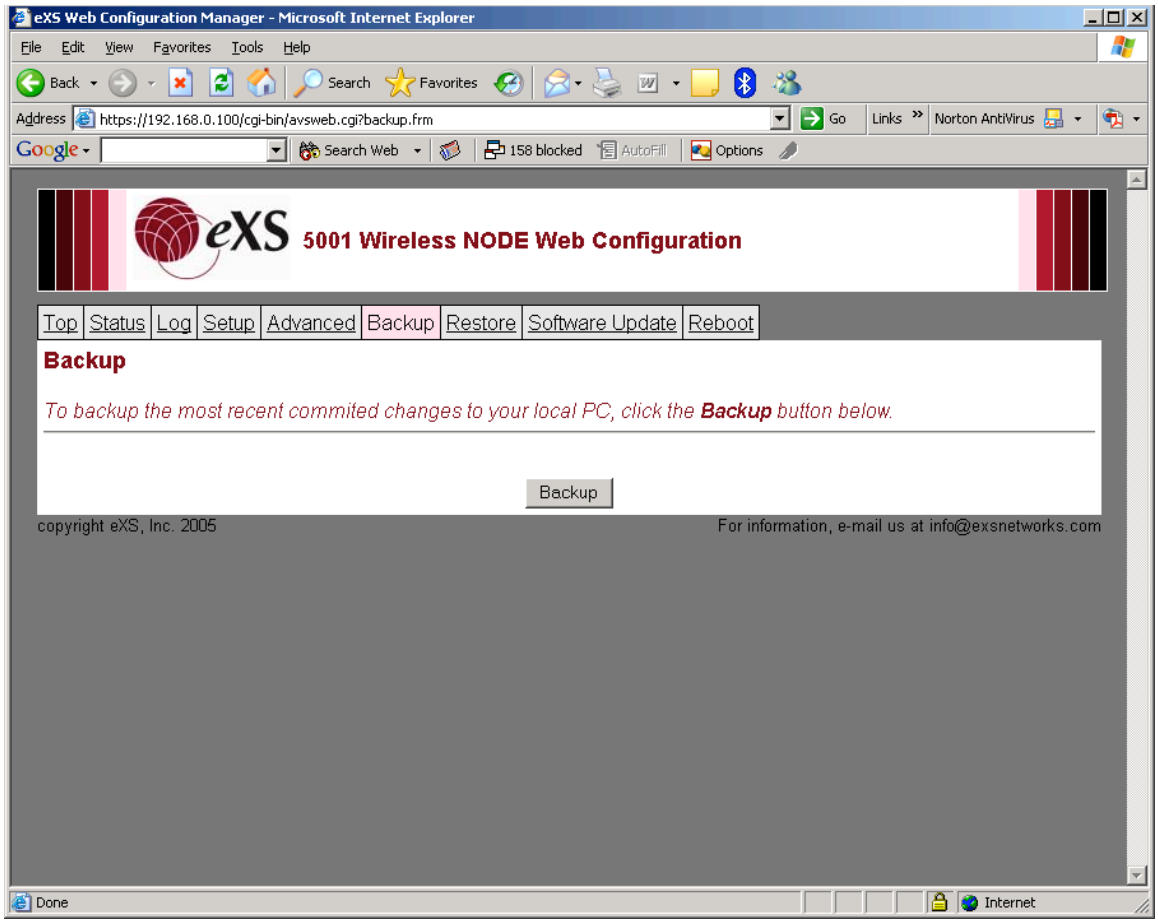

Figure 22

Restore

The *Restore* main menu item provides a way for you to restore the set of configuration variables on the NODE. There are three sources from which you can restore the variables, namely from the factory default settings, from the last committed changes or from a file.

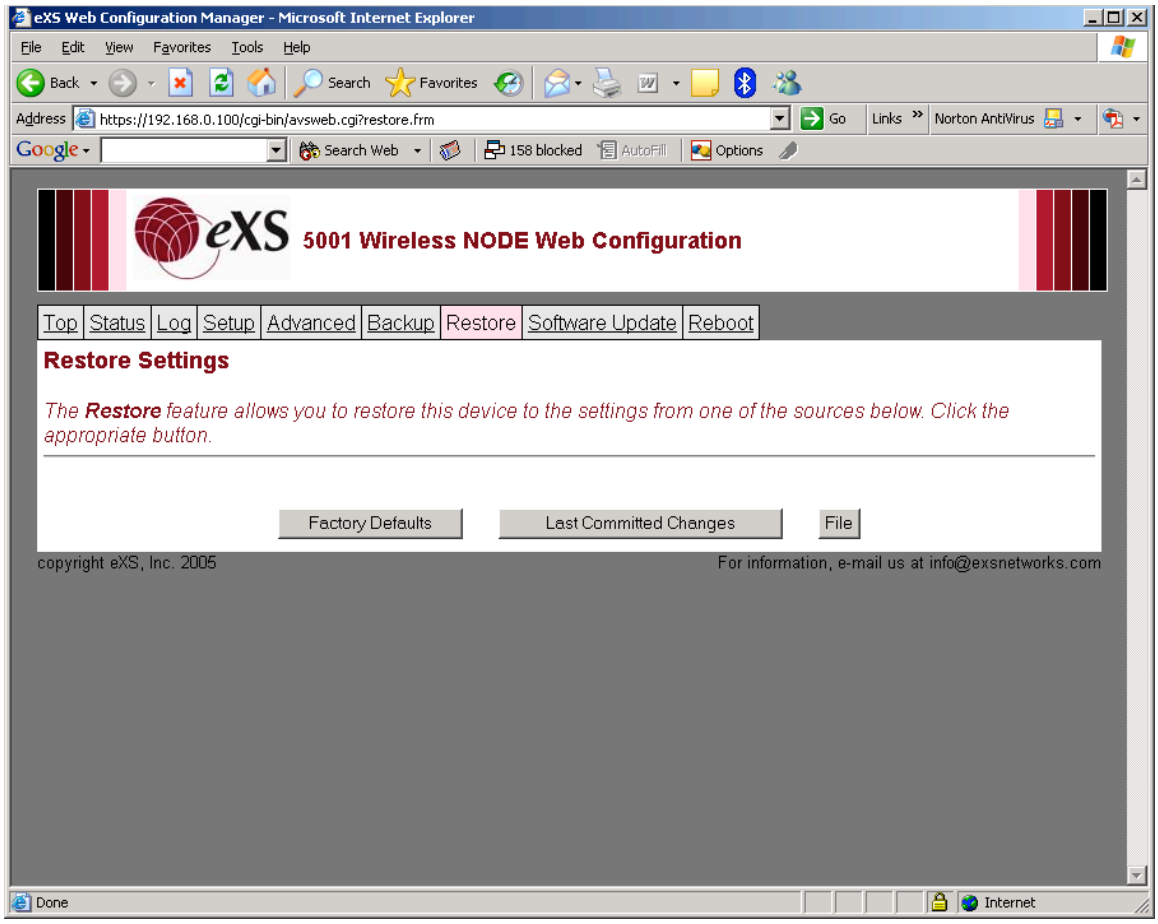

Figure 23

• *Factory Defaults* _ Restores the NODE configuration data variables to the factory default settings. These are the settings in the NODE when it's shipped.

• *Last Committed Changes* _ Restores the NODE configuration data variables to the last committed settings.

• *File* _ Restores the NODE configuration data variables from a file that was previously saved using the Backup feature of the web configuration manager application.

Select an option by clicking the appropriate button. The following subsections walk you through the Restore procedure of each.

Restoring from Factory Defaults

After you click the *Factory Defaults* button, the factory defaults settings are written to the temporary configuration data file and you are prompted to commit the changes. To make the factory defaults permanent, click the *Commit* button.

After you commit your changes, you are prompted to reboot the single board computer so the changes you made take effect.

Restoring from Last Committed Changes

After you click the *Last Committed Changes* button, the saved configuration file is activated a "commit" is not necessary.

Restoring from a Local File

After you click the *File* button, the following web page is displayed prompting you to choose the method for the NODE to use to retrieve the configuration data file. The file should be a backup file of the configuration data saved using the Backup feature. You can upload the file via your web browser on our local PC or you can download the file via the http or ftp protocol.

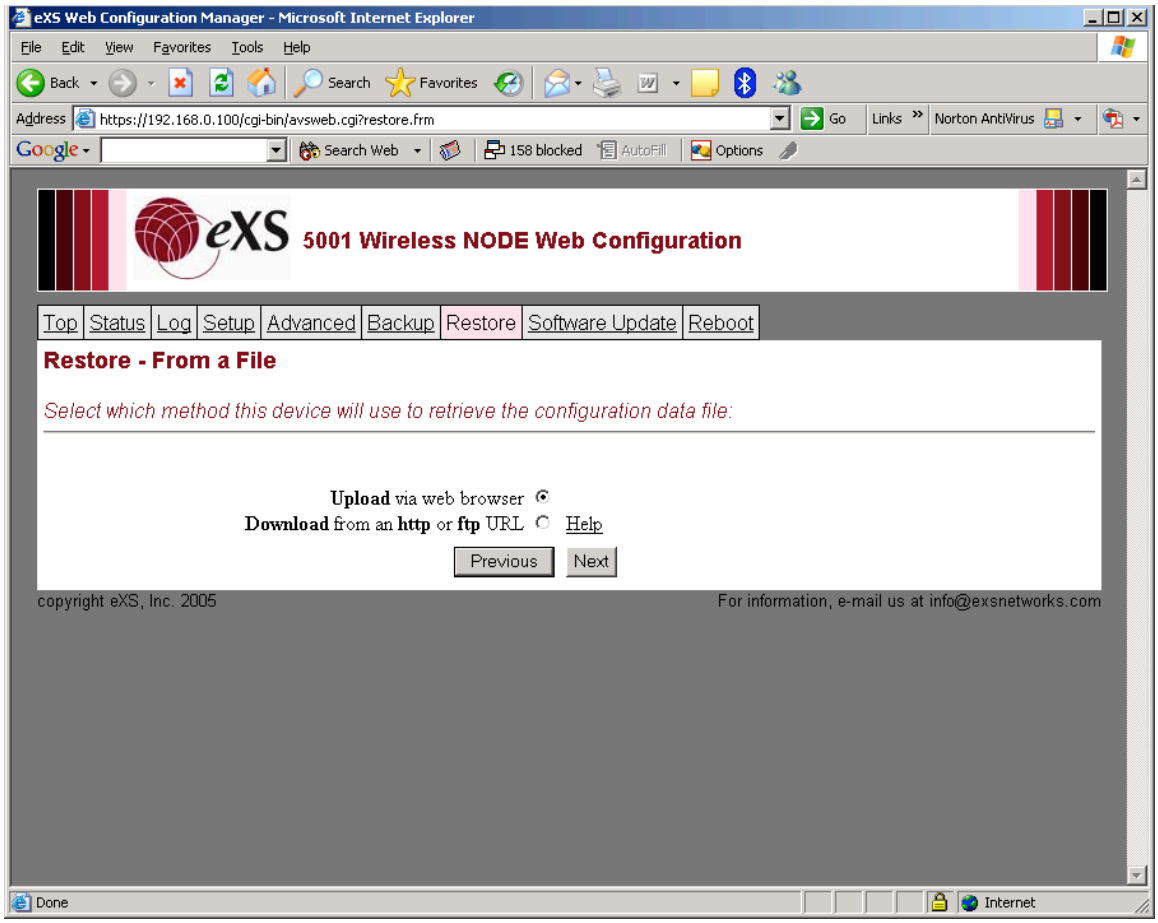

Figure 24

1. **Uploading via Web Browser**

   When prompted for the name of the file to upload, either enter the name of the file or click the Browse button to select the file name as shown in the following example web page.

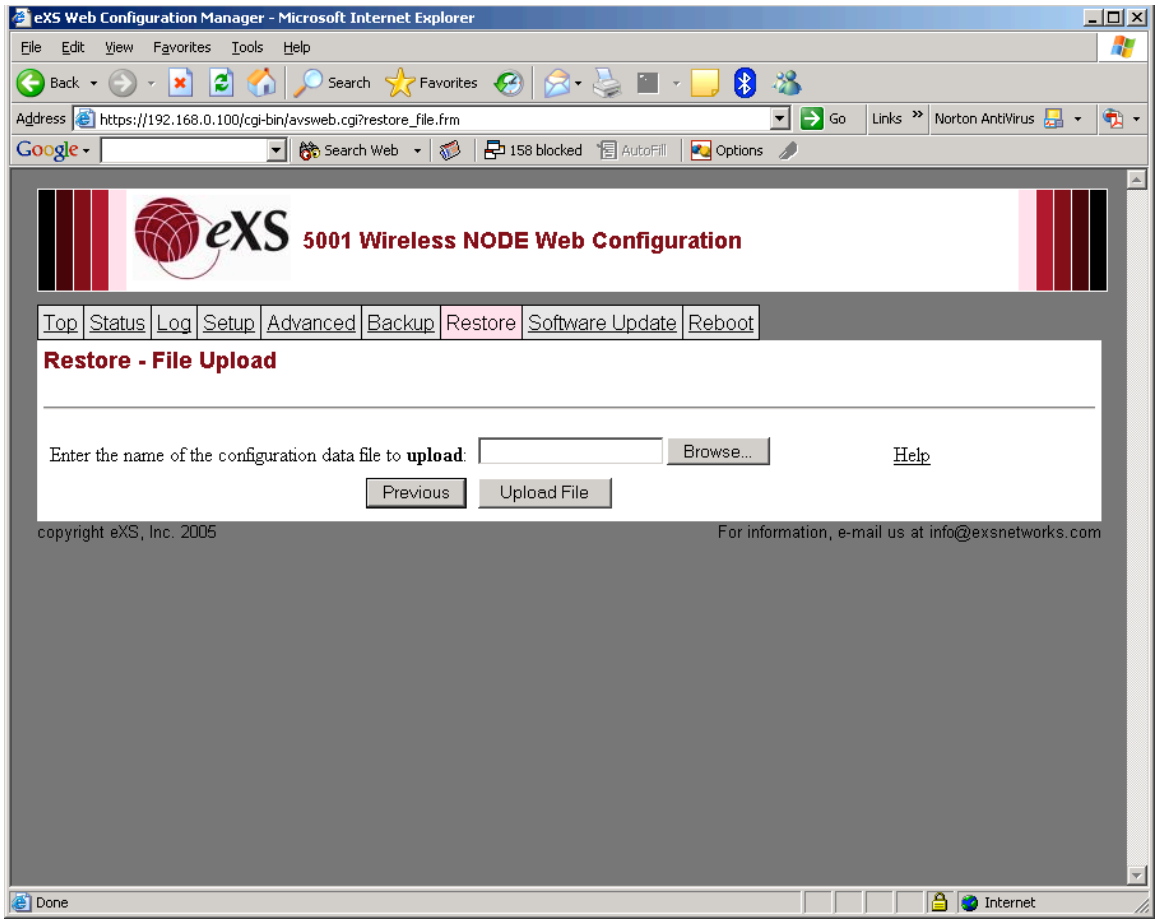

Figure 25

If the file is successfully uploaded, the page to validate the uploaded configuration data file is displayed as shown in the following figure. Click the *Validate* button to initiate the validation process.

If the file is a valid configuration data file, the file will be copied. You will be prompted to commit your changes to make them permanent. After you commit your changes, you will be prompted to reboot the single board computer.

2. **Downloading via the http or ftp Protocol**

   When prompted for the name of the file to download, enter the URL for the file using either the http or ftp protocol as shown in the following examples and web page.

   Syntax:

   http://<username>:<password>@<IP Address>/<full_directory_path>/<filename>

   _OR_
   ftp://<username>:<password>@<IP

Address>/<full_directory_path>/<filename>
Examples:

http://bob:wave@192.168.100.9/downloads/config.tar
ftp://bob:wave@192.168.100.9/home/bob/wdp80211/dot11Linux/loadimages/config.tar

In the examples above, the username is *bob*, and the password is *wave*. The IP address, 192.168.100.9, is the IP address of the PC. The remainder of the line is the full directory path and filename for the backup configuration data file. NOTE: In order for the NODE to use the FTP protocol to download the file from the PC, the PC must have an FTP server running.

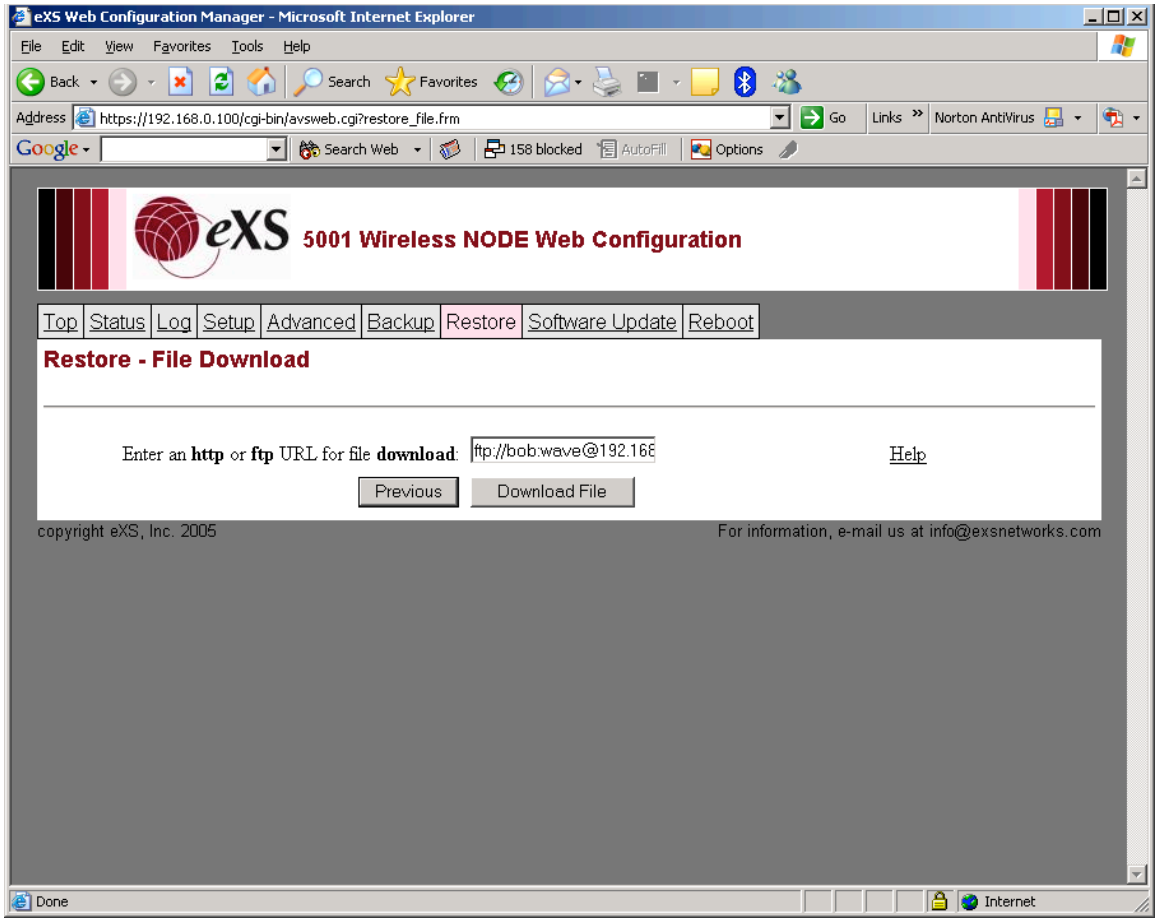

Figure 26

If the file is successfully downloaded, the page to validate the downloaded configuration data file is displayed. Click the Validate button to initiate the validation process.

If the file is a valid configuration data file, the file will be copied. You will be prompted to commit your changes to make them permanent. After you commit your changes, you will be prompted to reboot the NODE.

Software Update

The Software Update main menu item is a feature that allows you to remotely update all the NODE. The first page of the software update feature is shown in the following figure.

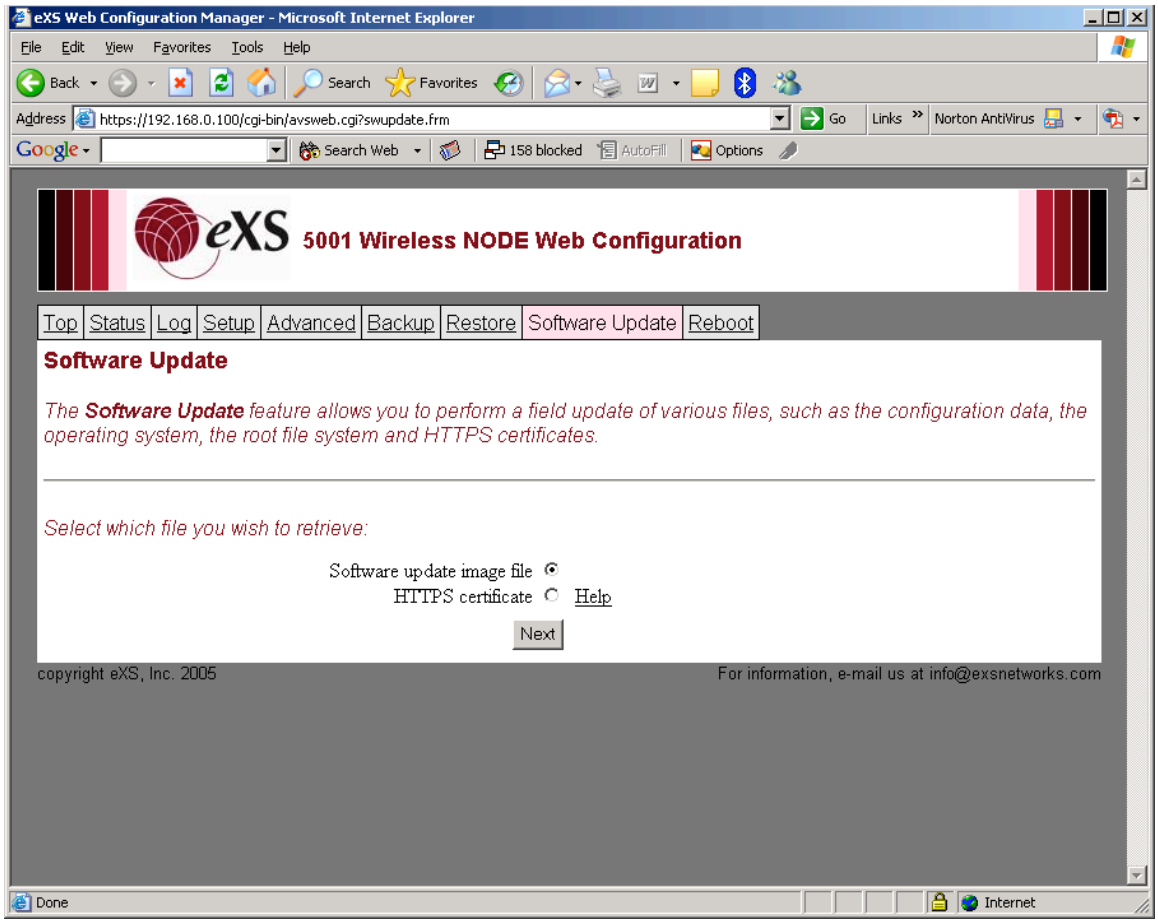

Figure 27

Using the Update Feature

The software update feature is accessed through the *Software Update* tab on the main menu of the web management application. After logging into the web management application and clicking the *Software Update* tab, the following web page is displayed. You can upload the swupdate.img file via your web browser on our local PC or you can download the file via the http or ftp protocol.

Uploading via Web Browser

When prompted for the name of the file to upload, either enter the name of the file or click the *Browse* button to select the file name as shown in the following example web page.

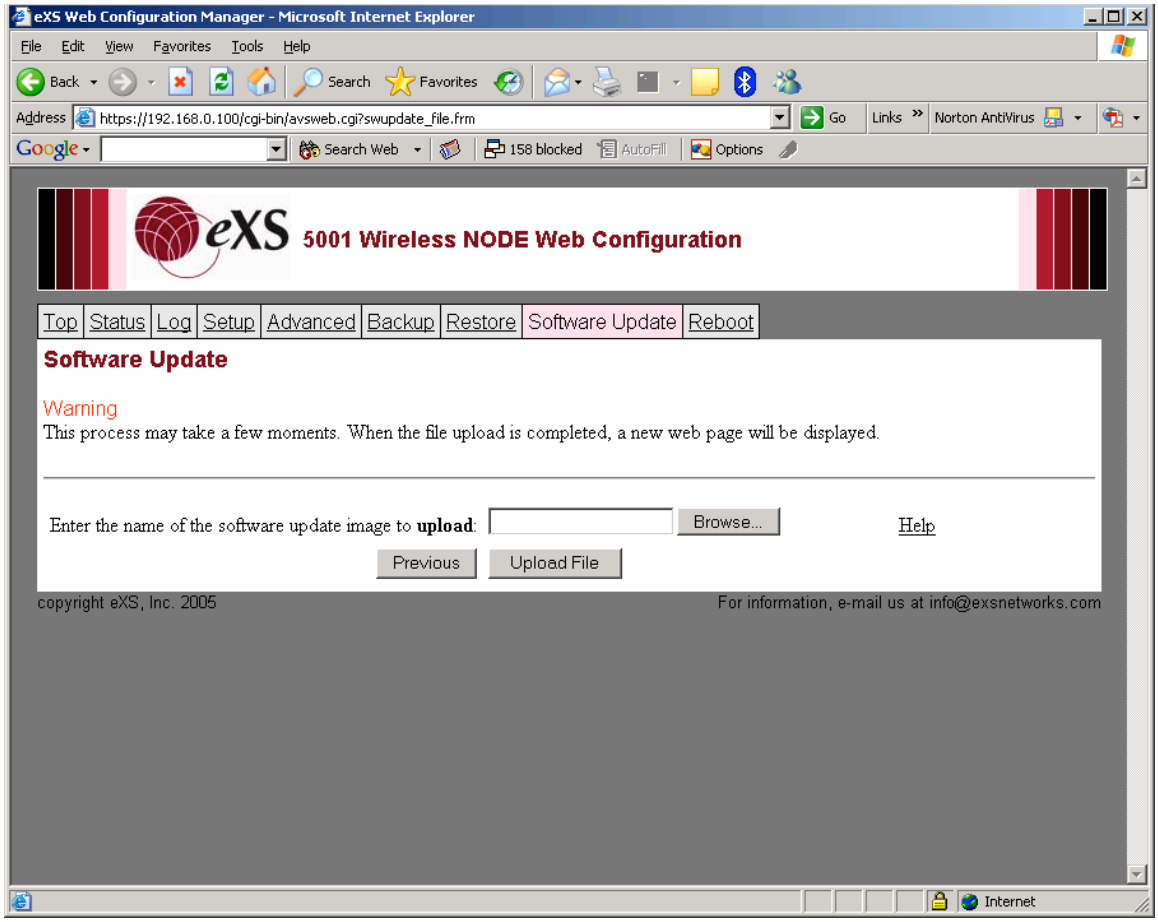

Figure 28

After you have entered the name of the file to upload, click the Upload File button. The upload will take a few moments before the next page in the software update process is displayed.

When the update file is acquired successfully. you will be asked to validate the file, press the *Validate and Update* button to proceed with the software update validation and update process.

After clicking on the *Validate and Update* button, the validation process checks the integrity of the uploaded binary image by verifying the checksum of the image. If the binary image is a valid image, the update procedure begins, namely the images are written to flash.

Once the flash writing process is completed (it will take a few moments), the NODE will automatically reboot. Once the reboot sequence is complete, you

may access the web configuration manager application again by clicking the *Go to Top* button.

Downloading via the http or ftp Protocol

When prompted for the name of the file to upload, enter the URL for the file using either the http or ftp protocol as shown in the following examples.

Syntax:

http://<username>:<password>@<IP Address>/<full_directory_path>/swupdate.img
_OR_
ftp://<username>:<password>@<IP Address>/<full_directory_path>/swupdate.img

Examples:

http://bob:wave@192.168.100.9/downloads/swupdate.img
ftp://bob:wave@192.168.100.9/home/bob/wdp80211/dot11Linux/loadimages/swupdate.img

In the examples above, the username is *bob*, and the password is *wave*. The IP address, 192.168.100.9, is the IP address of the PC. The remainder of the line is the full directory path and filename for the *swupdate.img* file. NOTE: In order for the NODE to use the FTP protocol to download the *swupdate.img* from the PC, it must have an FTP server running.

After you have entered the URL using the either the HTTP or FTP protocol, click the Download File button. The download will take a minute or so before the next page in the software update process is displayed. The following page will be displayed after a successful download.

As the above page indicates, the update file was acquired successfully. Press the *Validate and Update* button to proceed with the software update validation and update process. After clicking on the *Validate and Update* button, the validation process checks the integrity of the downloaded binary image by verifying the checksum of the image. If the binary image is a valid image, the update procedure begins, namely the images are written to flash.

Once the flash writing process is completed (it will take a few moments), the NODE will automatically reboot. Once the reboot sequence is complete, you may access the web configuration manager application again by clicking the Go to Top button.

Troubleshooting the Software Update Process

If an error is displayed during the software update procedure, the most common reasons for error are as follows, particularly if using the FTP protocol:

- The FTP server is not running on the PC,
- The FTP server was not configured correctly on the PC.
- The directory permissions in the full path were not set up.
- The URL entered in the Update URL field contains a typographical error.
- The image you are attempting to download is not the swupdate.img file.

Reboot

The *Reboot* main menu item initiates a soft reboot of the single NODE. The reboot page is shown below.

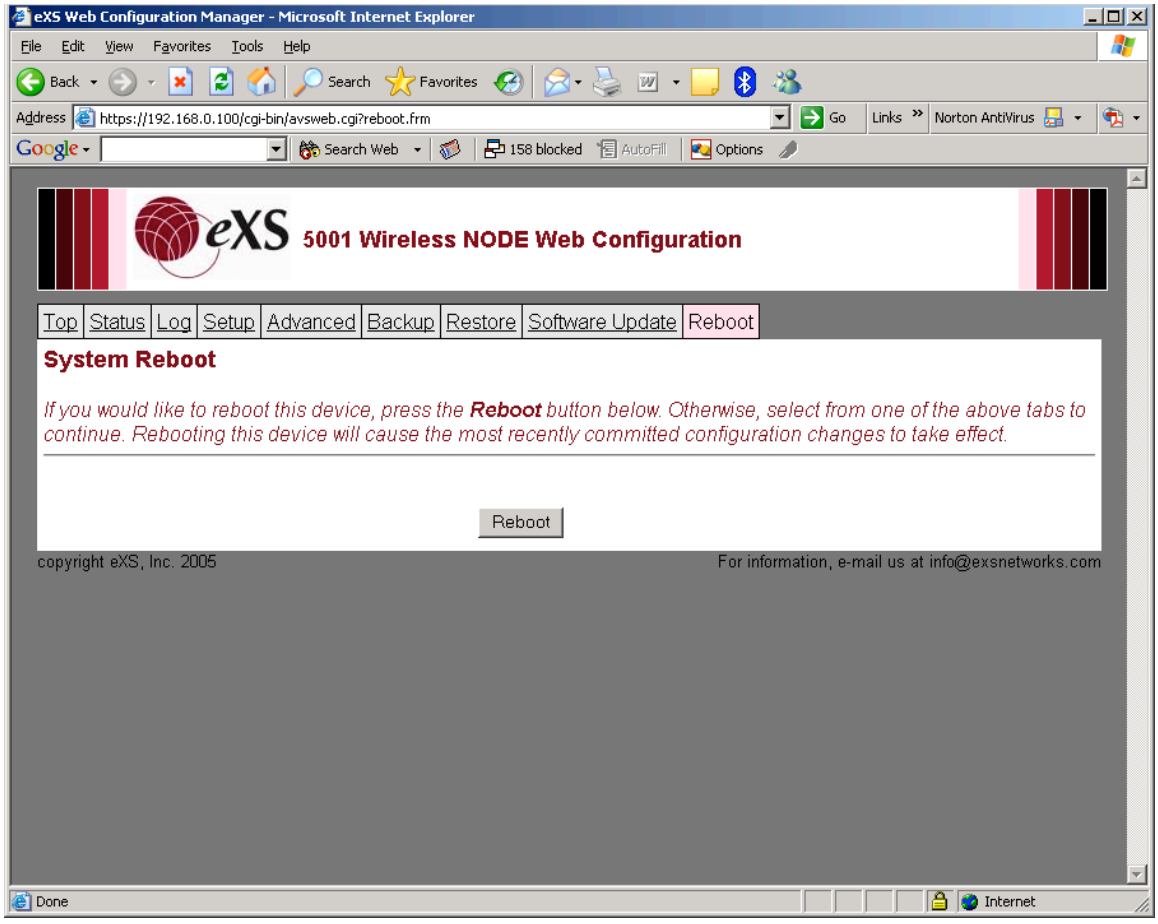

Figure 29

Multi-Layered Mesh Network

When configuring a multi-layered mesh, it is recommended that you configure each layer with a different subnet. This is to avoid having duplicate IP addresses on the assigned to end users and to the gateways linking 2 different level of the mesh hierarchy.

Copyright Information

To contact *e*XS Inc.:

*e*XS California, Inc.

1900 Alameda de las Pulgas, Suite 110, San Mateo CA 94403-1222 USA

email: info@eXSzone.com

Limited Warranty

The following is a summary of Warranty information. It will be superseded by Distributor Agreements, purchase order agreements or other appropriate written agreements between parties.

HARDWARE

*e*XS warrants to the end user ("Customer") that this hardware product will be substantially free from material defects in workmanship and materials, under normal use and service, for the following length of time from the date of purchase from eXS or its authorized reseller: One (1) year.

*e*XS's sole obligation under this express warranty shall be, at *e*XS's option and expense, to repair the defective product or part, deliver to Customer an equivalent product or part to replace the defective item, or if neither of the two foregoing options is reasonably available, refund to Customer the purchase price paid for the defective product. All products that are replaced will become the property of *e*XS. Replacement products or parts may be new or reconditioned. *e*XS warrants any replaced or repaired product or part for ninety (90) days from shipment, or the remainder of the initial warranty period, whichever is longer.

SOFTWARE

*e*XS warrants to Customer that each software program licensed from it, except as noted below, will, if operated as directed in the user documentation, substantially achieve the functionality described in the user documentation for a period of ninety (90) days from the date of purchase from eXS or its authorized reseller. No updates or upgrades are provided under this warranty. eXS's sole obligation under this express warranty shall be, at eXS's option and expense, to refund the purchase price for the software product or replace the software product with software which meets the requirements of this warranty as described above. Customer assumes responsibility for the selection of the appropriate programs and associated reference materials.

*e*XS makes no warranty or representation that its software products will meet Customer's requirements or work in combination with any hardware or software products provided by third parties, that the operation of the software products will be uninterrupted or error free, or that all defects in the software products will be corrected.

For any third party products listed in the eXS software product documentation or specifications as being compatible, eXS will make reasonable efforts to provide compatibility, except where the non-compatibility is caused by a "bug" or defect in the third party's product or from use of the software product not in accordance with eXS's published specifications or user manual.

THIS *e*XS PRODUCT MAY INCLUDE OR BE BUNDLED WITH THIRD PARTY SOFTWARE. THE WARRANTY PROVISIONS OF THIS DOCUMENT DO NOT APPLY TO SUCH THIRD PARTY SOFTWARE. IF A SEPARATE END USER LICENSE AGREEMENT HAS BEEN PROVIDED FOR SUCH THIRD PARTY SOFTWARE, USE OF THAT SOFTWARE WILL BE GOVERNED BY THAT AGREEMENT. FOR ANY APPLICABLE WARRANTY, PLEASE REFER TO THE END USER LICENSE AGREEMENT GOVERNING THE USE OF THAT SOFTWARE.

OBTAINING WARRANTY SERVICE

Customer must contact an *e*XS Corporate Service Center or an Authorized *e*XS Service Center within the applicable warranty period to obtain warranty

service authorization. Dated proof of purchase from *e*XS or its authorized reseller may be required. A User Service Order (USO), Return Material Authorization (RMA) or Service Repair Order (SRO) number will be issued. This number must be marked on the outside of the package sent to *e*XS's Corporate Service Center. The product must be packaged appropriately for safe shipment and sent prepaid. It is recommended that returned products be insured or sent by a method that provides for tracking of the package. Responsibility for loss or damage does not transfer to *e*XS until the returned item is received by *e*XS. *e*XS will retain risk of loss or damage until the item is delivered to Customer. The allocation of responsibility for loss or damage stated shall be subject to any mandatory legal requirements. *e*XS shall not be responsible for any software, firmware, information, or memory data of Customer contained in, stored on, or integrated with any products returned to *e*XS for repair, whether under warranty or not.

WARRANTIES EXCLUSIVE, WARRANTY DISCLAIMER

TO THE FULL EXTENT ALLOWED BY LAW, THE FOREGOING WARRANTIES AND REMEDIES ARE EXCLUSIVE AND ARE IN LIEU OF ALL OTHER WARRANTIES, TERMS OR CONDITIONS, EXPRESS OR IMPLIED, EITHER IN FACT OR BY OPERATION OF LAW, STATUTORY OR OTHERWISE, INCLUDING, WITHOUT LIMITATION, WARRANTIES, TERMS OR CONDITIONS OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, SATISFACTORY QUALITY, CORRESPONDENCE WITH DESCRIPTION, NON-INFRINGEMENT AND QUIET ENJOYMENT, ALL OF WHICH ARE EXPRESSLY DISCLAIMED. *e*XS NEITHER ASSUMES NOR AUTHORIZES ANY OTHER PERSON TO ASSUME FOR IT ANY OTHER LIABILITY IN CONNECTION WITH THE SALE, INSTALLATION, MAINTENANCE OR USE OF THIS PRODUCT.

*e*XS SHALL NOT BE LIABLE UNDER THIS WARRANTY IF ITS TESTING AND EXAMINATION DISCLOSE THAT THE ALLEGED DEFECT OR MALFUNCTION 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 OPEN, REPAIR OR MODIFY THE PRODUCT, OR ANY OTHER CAUSE BEYOND THE RANGE OF THE INTENDED USE, OR BY ACCIDENT, FIRE, LIGHTNING, POWER CUTS OR OUTAGES, OTHER HAZARDS, OR ACTS OF GOD.

LIMITATION OF LIABILITY

TO THE FULL EXTENT ALLOWED BY LAW, *e*XS ALSO EXCLUDES FOR ITSELF AND ITS LICENSORS AND SUPPLIERS ANY LIABILITY, WHETHER BASED IN CONTRACT OR TORT (INCLUDING NEGLIGENCE), FOR INCIDENTAL, CONSEQUENTIAL, INDIRECT, SPECIAL, OR PUNITIVE DAMAGES OF ANY KIND, OR FOR LOSS OF REVENUE OR PROFITS, LOSS OF BUSINESS, LOSS OF INFORMATION OR DATA, OR OTHER FINANCIAL LOSS ARISING OUT OF

OR IN CONNECTION WITH THE SALE, INSTALLATION, MAINTENANCE, USE, PERFORMANCE, FAILURE, OR INTERRUPTION OF ITS PRODUCTS, EVEN IF *e*XS OR ITS AUTHORIZED RESELLER HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, AND LIMITS ITS LIABILITY TO REPAIR, REPLACEMENT, OR

REFUND OF THE PURCHASE PRICE PAID, AT *e*XS's OPTION. THIS DISCLAIMER OF LIABILITY FOR DAMAGES WILL NOT BE AFFECTED IF ANY REMEDY PROVIDED HEREIN SHALL FAIL OF ITS ESSENTIAL PURPOSE.

Some countries, states, or provinces do not allow the exclusion or limitation of implied warranties or the limitation of incidental or consequential damages for certain products supplied to consumers or the limitation of liability for death or personal injury, so the above limitations and exclusions may be limited in their application to you. When the implied warranties are not allowed to be excluded in their entirety, they will be limited to the duration of the applicable written warranty. This warranty gives you specific legal rights which may vary depending on local law.

GOVERNING LAW

This Limited Warranty shall be governed by the laws of the State of California, U.S.A., and by the laws of the United States, excluding their conflicts of laws principles. The United Nations Convention on Contracts for the International Sale of Goods is hereby excluded in its entirety from application to this Limited Warranty.

*e*XS Inc., a BVI company with US correspondence offices at :

1900 Alameda de las Pulgas, Suite 110, San Mateo, CA 94403-1222 USA

Appendix: Radio Characteristics

Transmit Output Power

Test conditions: supply voltage=3.3v ambient temperature=25^{O}C

Frequency Range (Bands)	Modulations Rates (Mbps)	Minimum Output Power (dBm)	Typical Output Power (dBm)	Maximum Output Power (dBm)
Transmit Power Output low band (802.11b)	1	14	15.5	20.5
	2	14	15.5	20.5
	5.5	14	15.5	20.5
	11	14	15.5	20.5
Transmit Power Output low band (802.11g)	6	15.5	17	21.5
	9	15.5	17	21.5
	12	14	15.6	20
	18	14	15.6	20
	24	13	14.3	19
	36	13	14.3	19
	48	10	11.6	16
	54	10	11.6	16
Transmit Power Output high band (802.11a)	6	15	16.1	21
	9	15	16.1	21
	12	14	15.6	20
	18	14	15.6	20
	24	13	14.8	19
	36	13	14.8	19
	48	8.5	10.9	15
	54	8.5	10.9	15

The above numbers are for reference only

Maximum Output Power Settings, United States

Products sold for use in the United States shall not exceed the output power settings values in the following table:

Channel No.	**Frequency**	**Mode**	**Power, dBm**
6	2437	802.11b	27
All other channels		802.11b	21
6	2462	802.11g	26
all other channels		802.11g	18
32-48	5180-5240	802.11a	15.8
52-64	5260-5320	802.11a	15.5
149-165	5745-5805	802.11a	19

Receiver Sensitivity

Test conditions: supply voltage=3.3v ambient temperature=25^{O}C

Frequency Range (Bands)	Modulations Rates (Mbps)	Minimum Receiver Sensitivity (dBm)	Typical Receiver Sensitivity (dBm)
Receiver Sensitivity low band (802.11b) (8% Packet Error Rate)	1	-92	-94
	2	-90	-92
	5.5	-89	-91
	11	-85	-87
Receiver Sensitivity low band (802.11g) (10 % PER)	6	-89	-91
	9	-87	-89
	12	-86	-88
	18	-83	-85
	24	-79	-81
	36	-75	-77
	48	-70	-72
	54	-68	-70
Receiver Sensitivity high band (802.11a) (10 % PER)	6	-88	-90
	9	-86	-88
	12	-85	-87
	18	-82	-84
	24	-78	-80
	36	-74	-76
	48	-69	-71
	54	-67	-69

PER = Packet Error Rate.

The above numbers are for reference only

Appendix: User Information

After an installation, the network customer should be given written instructions appropriate to the country. The instructions in this Section are appropriate for the USA.

Professional Installation

This device must be professionally installed & maintained.

The end user cannot change frequency, transmitter power or any other RF parameters of this device.

Operation

This device complies with Part 15, Class B (residential and business) of the FCC Rules and Regulations (CFR47). 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.

CAUTION: changes or modifications not expressly approved by the party responsible for compliance and installation could void the user's authority to operate the equipment.

The transmitter must not be co-located or operated in conjunction with any antenna, amplifier or transmitter except those used by the professional installer.

Interference

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 or more of the following measures:

Reorient or relocate the receiving radio or TV antenna.

Increase the separation between the equipment and receiver.

Connect the equipment into an outlet on an AC circuit different from that to which the receiver is connected.

Consult the dealer or an experienced radio/TV technician for help.

Radiation Exposure

This equipment complies with FCC safe radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance of 20cm (8 inches) between the radiator (the antenna) and your body.

Appendix: FCC Rules

The following is a brief summary of the US Federal Communications Commission (FCC) Rules and Regulations, which is under the Code of Federal Regulations (CFR) in the USA. These are Rules that are most useful in planning a US installation.

A current copy of the FCC Rules is available at:
http://ftp.fcc.gov/oet/info/rules/

Part 15.203: Antenna Requirement

The installer shall be responsible for ensuring that the proper antenna is employed so that the limits in Part 15 are not exceeded.

The eXS Price List includes the antennas and the PoE power adapter that were used in the FCC testing and certification. The FCC Rules require that ONLY these units be installed, unless the antenna is of a lesser gain but same type as the approved antenna.

Part 15.407: Technical Requirements (UNII)

5.15-5.25 GHz, maximum power to antenna connector is 50 mW (17 dBm).

5.15-5.25GHz is restricted to INDOOR operation.

5.25-5.35GHz, max power to antenna is 250 mW (24 dBm). If directional antenna is greater than 6 dBi, maximum power shall be decreased by 1 dB for every dB the antenna exceeds 6 dBi.

5.725-5.825GHz, max power to antenna is 1 Watt (30 dBm). If the directional antenna exceeds 6 dBi, the maximum power shall be reduced by 1 dB for each dB the antenna exceeds 6 dBi. However, fixed point-to-point devices may employ antennas with directional gain up to 23 dBi without any corresponding reduction. Point-to-point excludes point-to-multipoint and omni-directional systems, or equivalent.

On February 18, 2005, the FCC postponed the Transmit Power Control (TPC) and Dynamic Frequency Selection (DFS) requirements. If there are no further postponements, they will require that after January 20, 2007, devices cannot be imported or marketed that do not meet TPC and DFS. [Subpart 15.37(L)].

TPC and DFS requirements ONLY apply to devices operating 5.25-5.35GHz.

Furthermore, Transmit Power Control (TPC) is NOT required for systems radiating less than 500 mW (27 dBm) E.I.R.P. in the 5.25-5.35GHz band (which is generally true for the *e*XS 5001A).

Part 15.407: RF Transmission Auto-control

This device is in compliance with FCC 15.407(c). It automatically discontinues transmission in case of either absence of information to transmit or operational failure.

Data transmission is always initiated by software. The data is either subscriber data or small amounts of network control and signaling information. The data passes down to the Media Access Control logical layer to the RF transmitter. The RF transmitter is ON only when passing these data packets out to the antenna. The transmission turns OFF at the end of each individual packet. If there is an operational failure, no data packets are transmitted.

Appendix: Malaysian Rules

The Malaysian Communications and Multimedia Commission (MCMC) Guidelines for WLAN devices are:

Frequency Band	**EIRP (dBm)**	**EIRP (mW)**
2.400 – 2.500 GHz	27	500
5.250 - 5.350 GHz	30	1000
5.725 – 5.875 GHz	30	1000

The *e*XS 5001A is a "Second Schedule" "Short Range Communications Device" according to the "Notification of Issuance of Class Assignments", 1 November 2004. The *e*XS 5001A has been approved by SIRIM.