Fire4 Systems
Network Products for Public Internet Access

Router & Wireless Products

Guide to Operation

Version 2.0 firmware

Router and Wireless Products for Public Internet Access with Customer Billing, Failure Monitoring and Remote Management

Ver2 - Rev. 0

FCC Statement

This device complies with Part 15 of the FCC rules. Operation is subject to the following conditions.

1. *The device may not cause harmful interference.*
2. *This device must accept any interference received, including interference that may cause undesired operation.*

Caution: Exposure to Radio Frequency Radiation.

The radiated output power of this device is below the FCC radio frequency exposure limits. Nevertheless, the device shall be used in such a manner that the potential for human contact during normal operation is minimized.

When connecting an external antenna to the device the antenna shall be placed in such as manner to minimize the potential for human contact during normal operation. In order to avoid the possibility of exceeding the FCC radio frequency exposure limits, human proximity to the antenna shall not be less than 8 inches during normal operation

Federal Communications Commission Notice

This equipment complies 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.

The equipment generates, uses, and can radiate radio frequency energy. If not installed and used in accordance with the instructions in this manual, it may cause harmful interference to radio, television or telecommunications reception, which can be determined by turning the equipment off and on. The user is encouraged to try and correct the interference by one or more of the following measures.

- *Reorient or relocate the receiving antenna*
- *Increase the distance between the equipment and the receiver*
- *Power the equipment via a different electrical circuit from that which the receiver is connected*
- *Consult the dealer who installed the equipment, or an experienced radio frequency technician*

Modifications

The FCC requires the user to be notified that any changes or modifications to this device that are not expressly approved by Fire4 Systems or its authorized distributors may void the users authority to operate the equipment

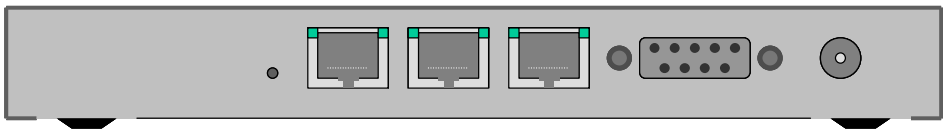
Contents

1. Connecting the Equipment

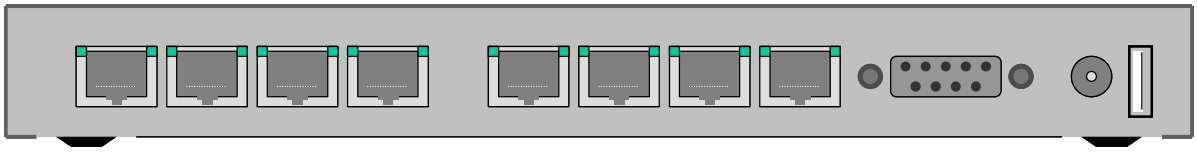
Equipment configuration is shipped with the ETH0 port (first or only Ethernet port) set as the uplink (connected to the Internet circuit) In the case of router equipment, ETH1 is the primary downlink port (DCHP server) and is used for client connection. All other Ethernet ports are secondary downlink ports. In the case of wireless equipment, the wireless interface is the primary downlink port (DCHP server) and is used for client connection.

Router Equipment

NX1

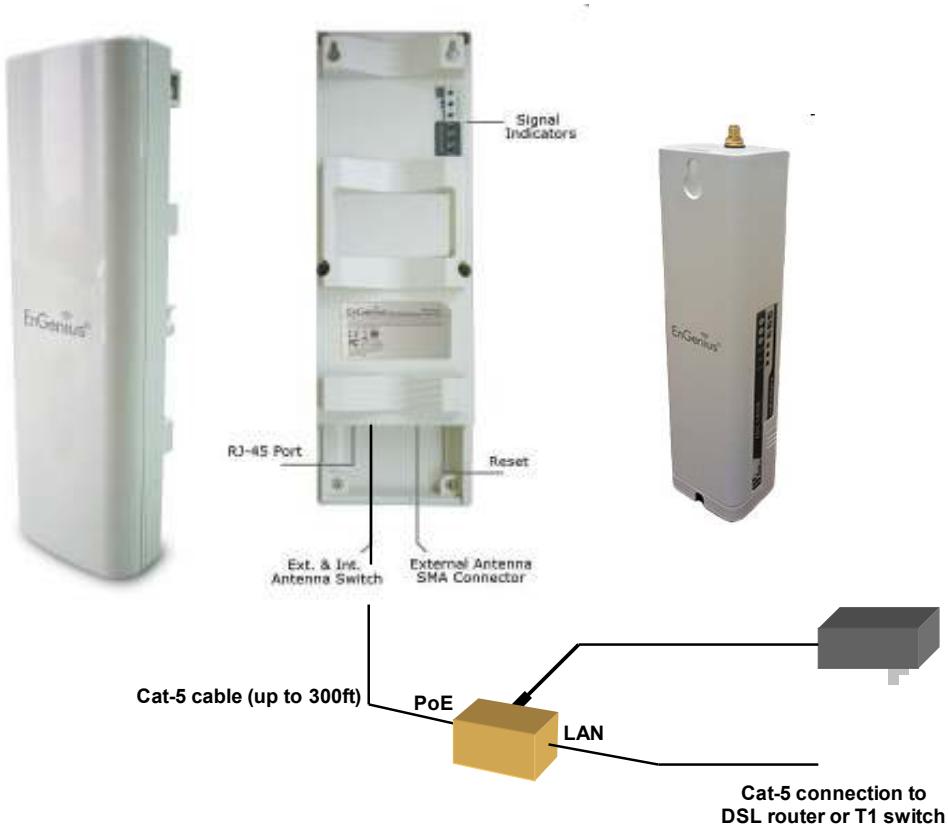


NX2



Router equipment has a 12 volt power connector. The external power supply plug is pushed into this connector.

Wireless Equipment



Power over Ethernet (PoE) supply configuration

The PoE unit shipped with the AP series equipment supplies power over the Ethernet Cat-5 cable. The Ethernet cable supplied with the AP unit should be plugged into the PoE supply to the connector marked DATA+POWER. A second Ethernet cable must be connected from the PoE supply terminal marked DATA to the network switch or DSL modem.

AP series equipments are shipped with a 25ft data cable, however this can be replaced or extended up to 300 feet between the AP unit and the DSL/cable modem or T1 hub.

2: The Equipment Configuration Process

The equipment is configured wirelessly using a notebook computer with a wireless card that conforms to the 802.11/g standard. Wireless equipment must be powered using the external Power over Ethernet (PoE) supply and the data cable must be connected to a DSL/cable modem or to a T1 circuit. Router equipment must be powered by the external 12 volt supply.

After powering the equipment unit allow 3 minutes for the unit to perform internal test routines before beginning the configuration process.

The equipment defaults to the following operating modes:

- The Ethernet circuit is configured to request an IP address via DHCP (DHCP client mode)
- For wireless devices: the wireless circuit is configured to request a pass code (commercial mode)
- For router devices: A secondary Ethernet circuits are configured to request a pass code (commercial mode)

If the equipment is to be used in the configuration described above then the only required setting is the change of administrative password (described later).

The computer (preferably notebook) should have MS Windows XP installed. Go to START, CONTROL PANEL then NETWORK CONNECTIONS. There will be two icons, one for the computers Ethernet port, and one for the wireless network interface.

Right click on the wireless network icon, then left click on SCAN FOR NETWORKS. One or more wireless network names will appear in the window. Look for the wireless name:

Hot Spot.

This is the wireless name of the equipment.

Click on this name then click on the button at the bottom right hand of the window, CONNECT.

The computers browser is used for configuration. Open the browser and type the URL:

https: // ap.fire4.com / admin

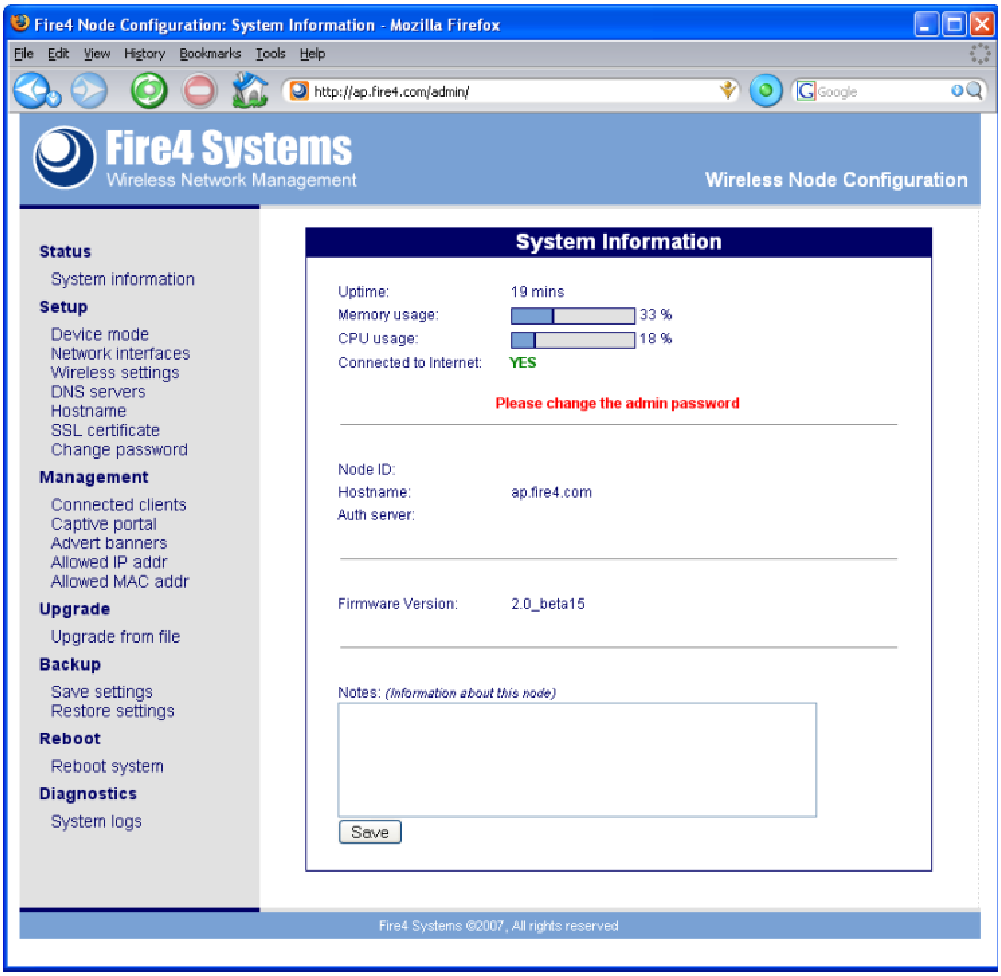
A box will open requesting the user name and password. The default username and password are:

- Username = **admin**
- Password = **admin**

When the password has been accepted then the configuration page will open. The computer is now logged in as the administrator of the equipment. The initial configuration page is shown in the figure below. This page has menu items down the left side of the page. This is called the **System Information** Page. If Manage Connections is clicked then this page will be displayed.

Remember that the password must be changed at the end of the configuration process.

Initial configuration page: System Information



The information displayed shows;

- Memory and CPU usage
- Internet connection status
- Node ID (required by the authentication server)
- Firmware version
- Information text box containing ASCII data

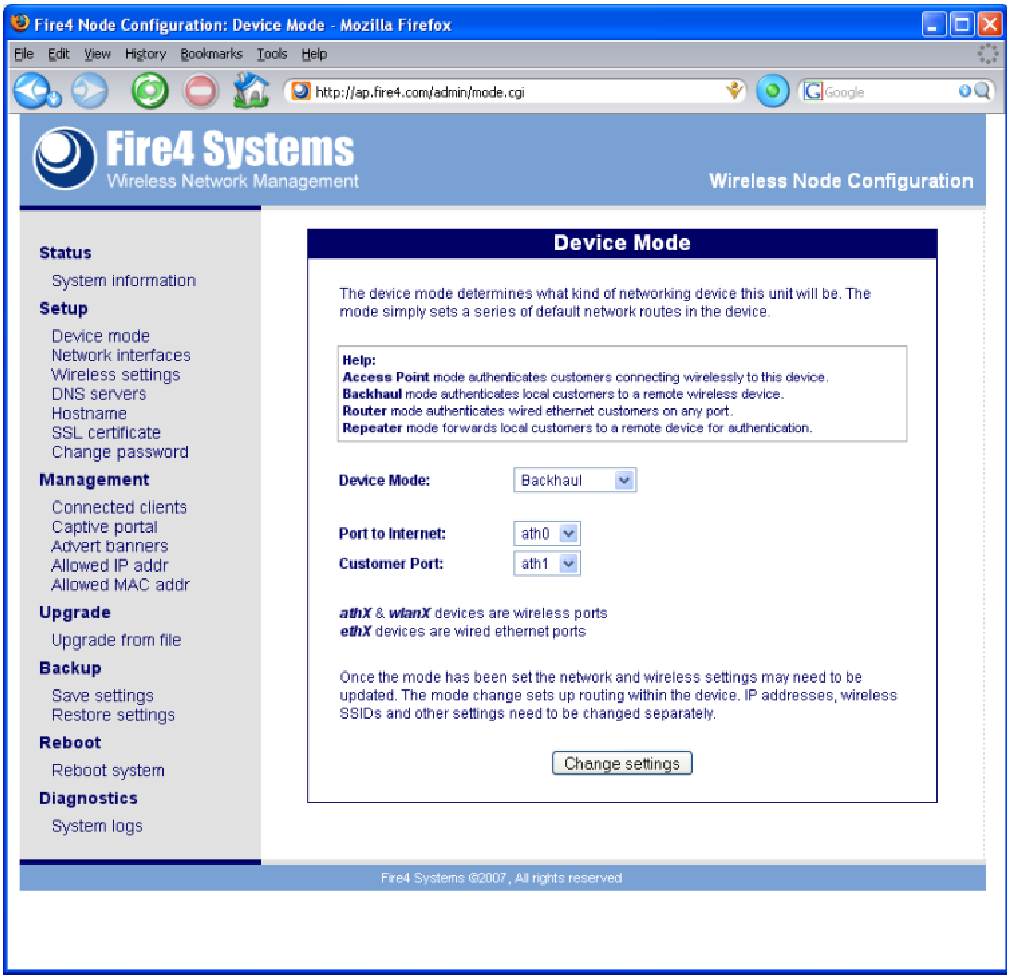
3: Configuring the Equipment Setup Functions

Once logged on to the equipment as the administrator then equipment configuration parameters can be modified. The **Setup** functions are configured first. The default configuration for the equipment operation mode is the Access Point mode. Four modes are available.

- Access point
- Backhaul (bridge or CPE)
- Repeater
- Router (non-wireless application)

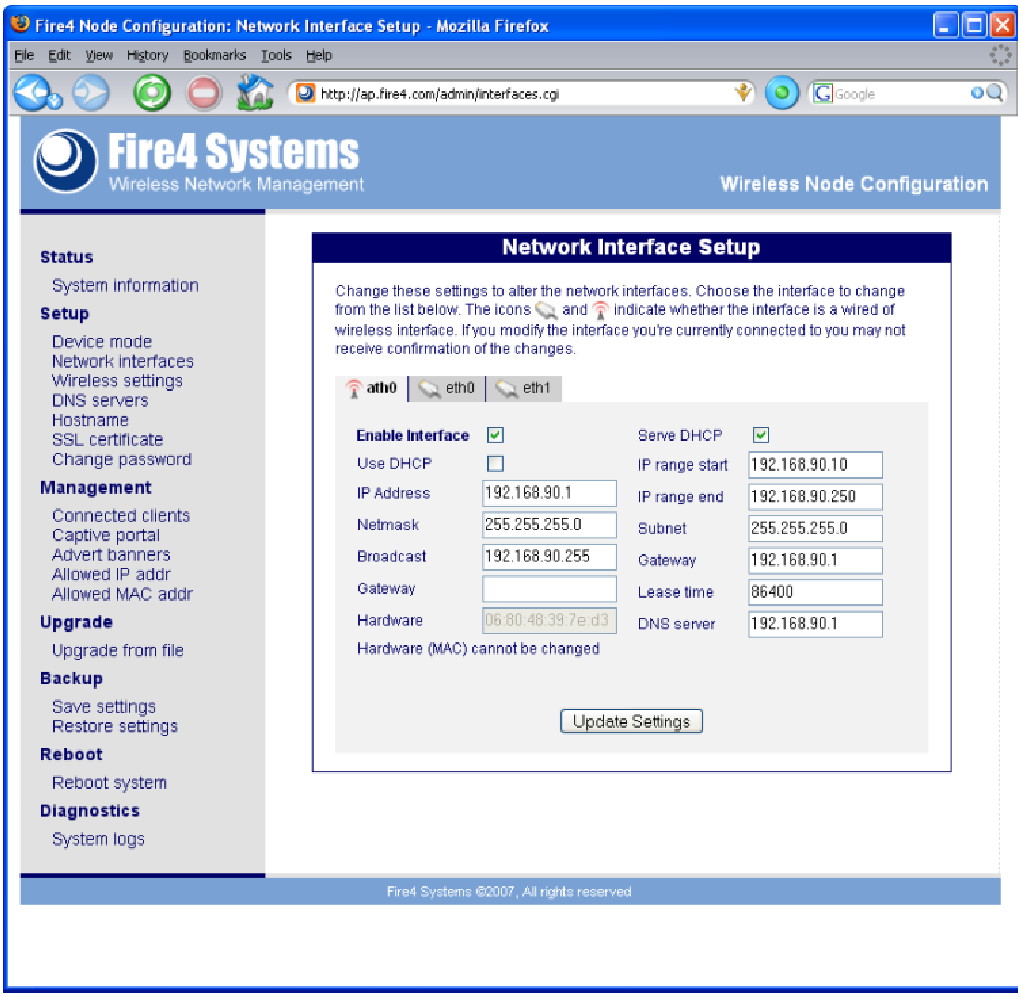
If one of the other modes listed is required then open the **Device Mode** menu option. Select the desired mode from the pull-down menu. Then specify which port will connect to the Internet, and which port will be the primary user access port.

Device Mode screen



If DSL modem or T1 switch provides DHCP services then no changes are required. If however the network requires that the wireless node has a fixed IP address then a change will have to be made. Select the **network interfaces** page. Eth0 is the default connection to the Internet. If a different port will be used to connect to the Internet then change this on the **Device Mode** page. Select the Eth0 tab and configure the IP parameters required by the network. The **network interfaces** screen is shown below.

Network Interfaces screen



Next the wireless interface parameters are configured using the **wireless interface setup** page. Remember that when these parameters are changed then the configuration computer will loose its connection and have to be re-connected.

For public access networks two parameters are important

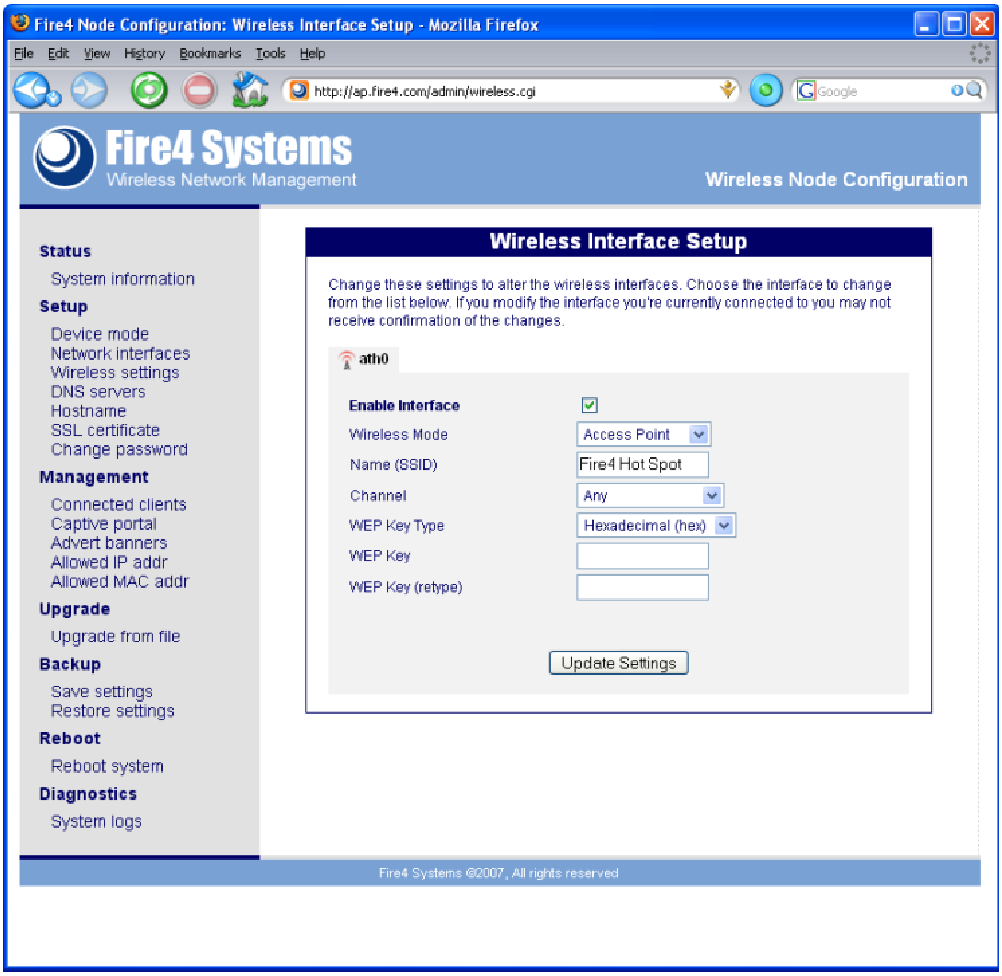
- The hot spot name (called the SSID)
- The channel or frequency used for transmission

WEP encryption is generally not used to public access networks, however a WEP key can be configured. The hot spot name should be selected to facilitate users identifying the wireless network (e.g. ***Keystone Marina Hot Spot***). Keep the name as short as possible.

Before installing the hot spot use a site survey tool such as Netstumbler to identify RF channels (frequencies) that are in use. The default channel for most access point equipment is ch#6 or ch#3 so avoid this channel. Usually channel 11 has less interference. Check RF signals and select the channel with the least amount of RF transmission.

The **wireless interface setup** page is shown overleaf.

Wireless Interface Setup page for access point



If the device mode is set in the backhaul (bridge or CPE) mode then the configuration of the wireless interface is different, the wireless interface is already configured as a CPE devices rather than an access point device.

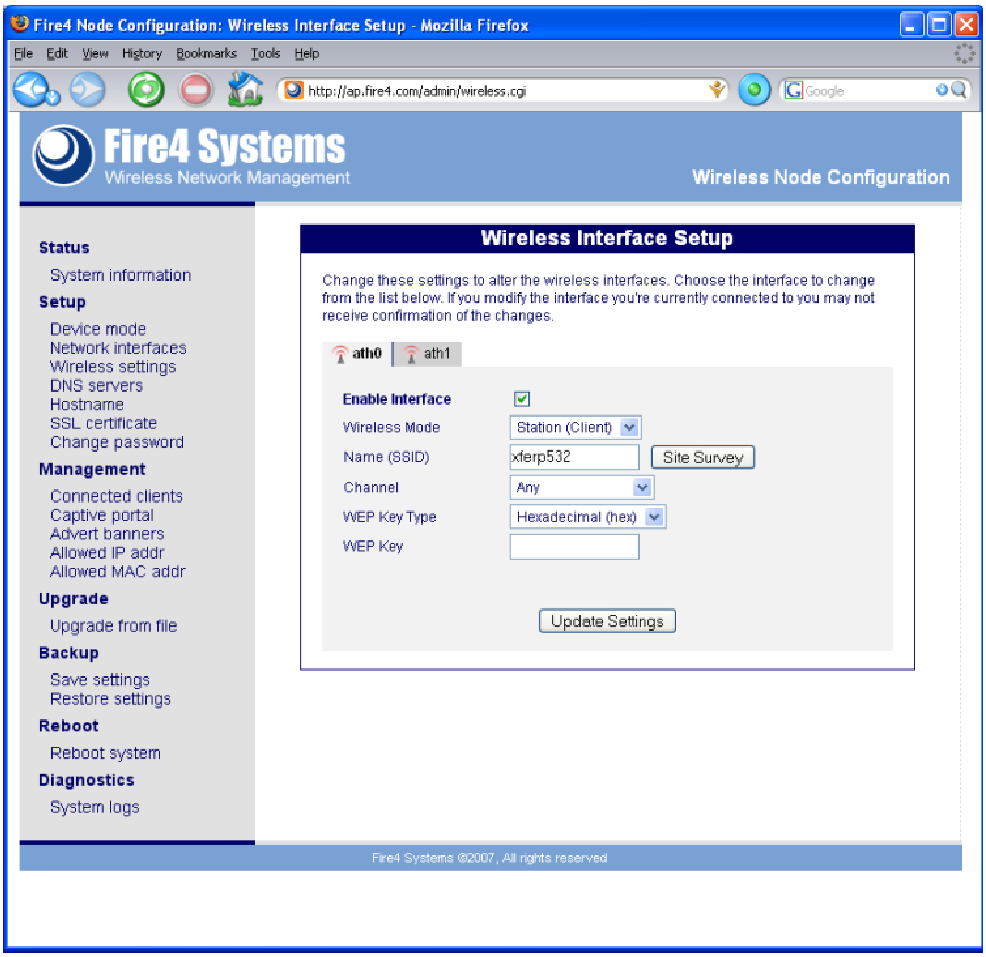
The wireless interface must be configured to connect to the remote access point that will provide network connectivity. The radio interface requires the name of the remote access point and this is found by pressing the site **survey button**. A window will open listing the remote devices that are available and the user can click on the remote network name to select it.

The remote network may be WEP encrypted and so the WEP key will be entered in the box.

If more then one wireless interface is installed in the unit then the default backhaul interface will be Ath0. Other wireless interfaces, Ath1, Ath2, etc can be configured as access point. The Wireless interface select for the backhaul function can be changed using the **Device Mode** screen.

The wireless interface setup for backhaul configuration is shown on the following page.

Wireless Interface Setup page for backhaul



Pressing the site survey button opens the window shown. The access points are ordered by signal strength.

Click on the name of the SSID that the backhaul should connect to, then close the window. The SSID name will be transferred to the wireless interface set up screen.

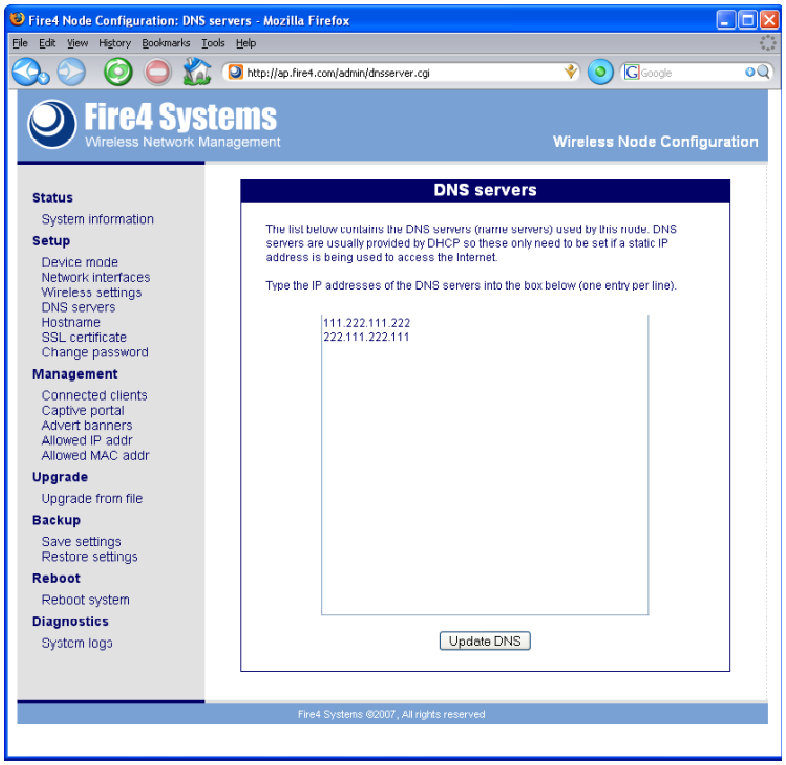
Enter the WEP key (if any) then click on the update settings button.

The backhaul radio will establish a connection with the remote access point and advise if this was successful, or if the connection was not obtained.

The setup section of the menu has screens for DNS servers, Hostname, and SSL certificate. These screens are not necessary for a hot spot configuration. The can be used if the access point is to be used with modified parameters for Internet connection and customer billing.

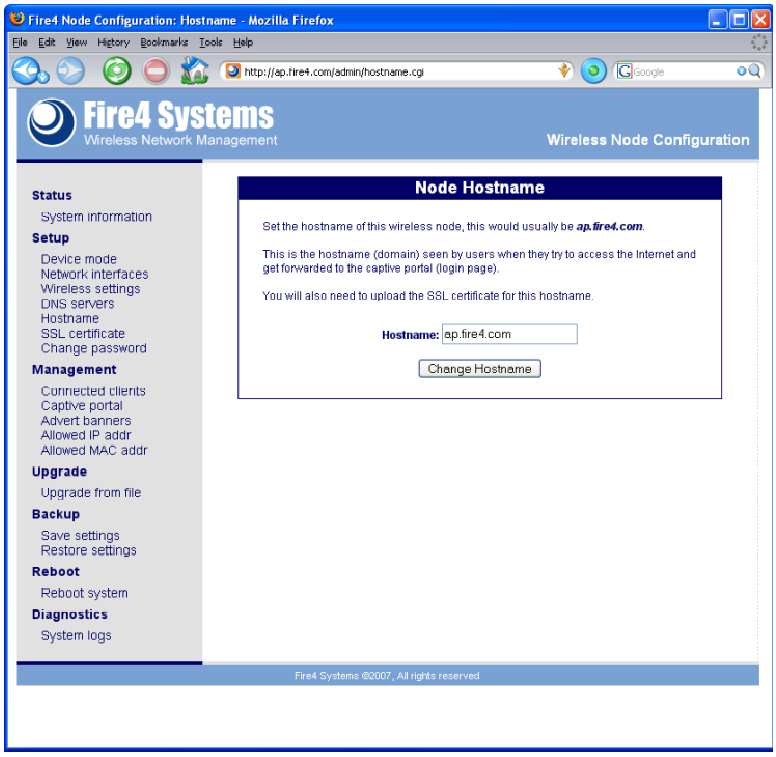
DNS Servers page

DNS server IP addresses can be added to the list shown in the box. This feature will be necessary if the network to which the access point is connected requires that the node use fixed IP address.



Node Hostname Page

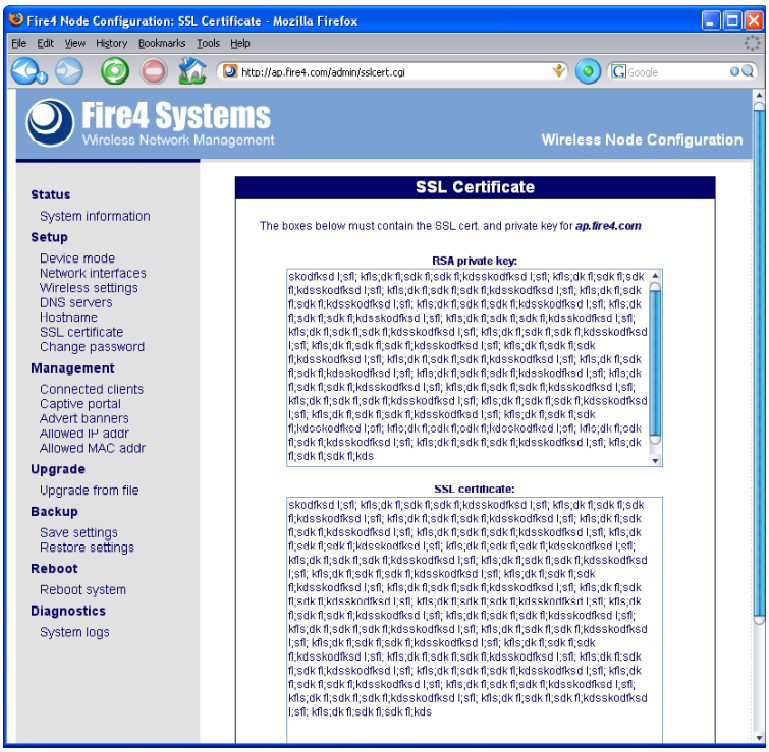
The node hostname is the server used for authentication. This name will not be changed if the customer is using the Avansu subscription services. If the customer decides to purchase an authentication and management server then this hostname will be modified to that of the new server.



SSL Certificate Page

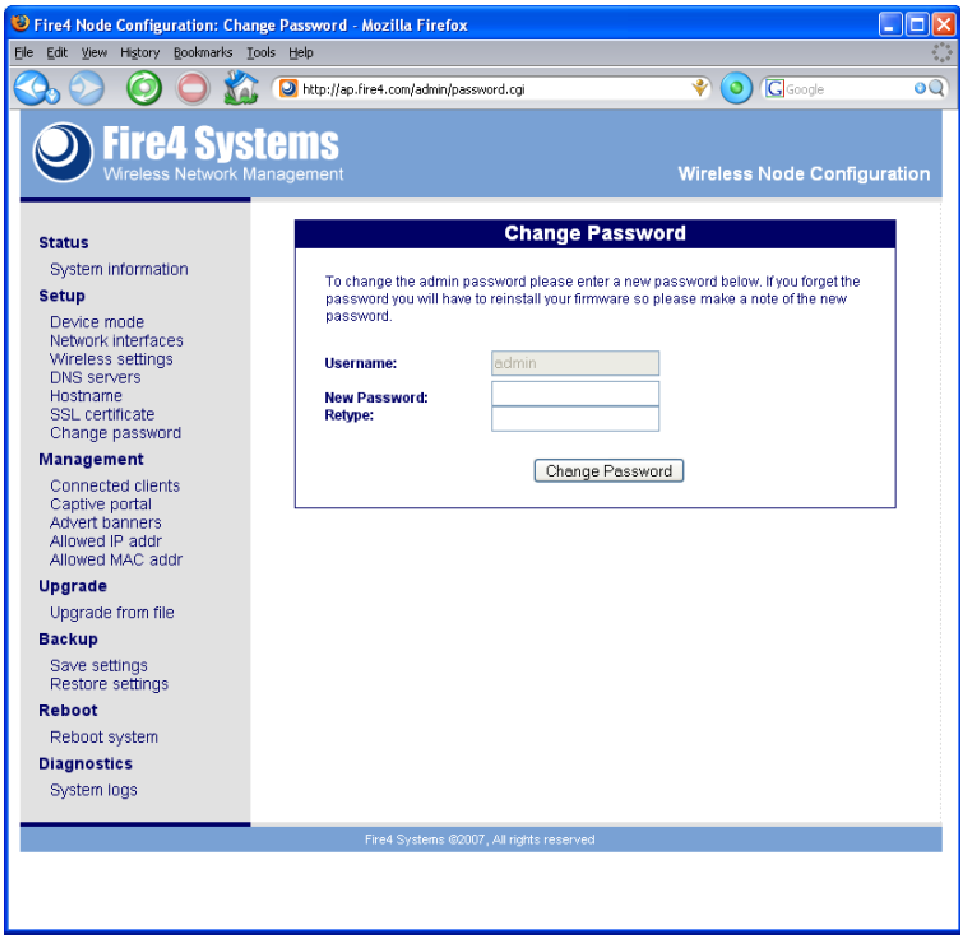
The SSL certificate is used for the secure server login: access codes are authenticated using the https server in the wireless node.

The SL certificate is provided for information purposes only.



Change Password page

Always change the password before completing the wireless node configuration. Make a note of your password: if the password is lost then the wireless device will have to be re-flashed with new firmware.



4: Configuring the Equipment Management Functions

The equipment management functions determine how the access point will be configured for hot-spot public Internet access. A number of options are available:

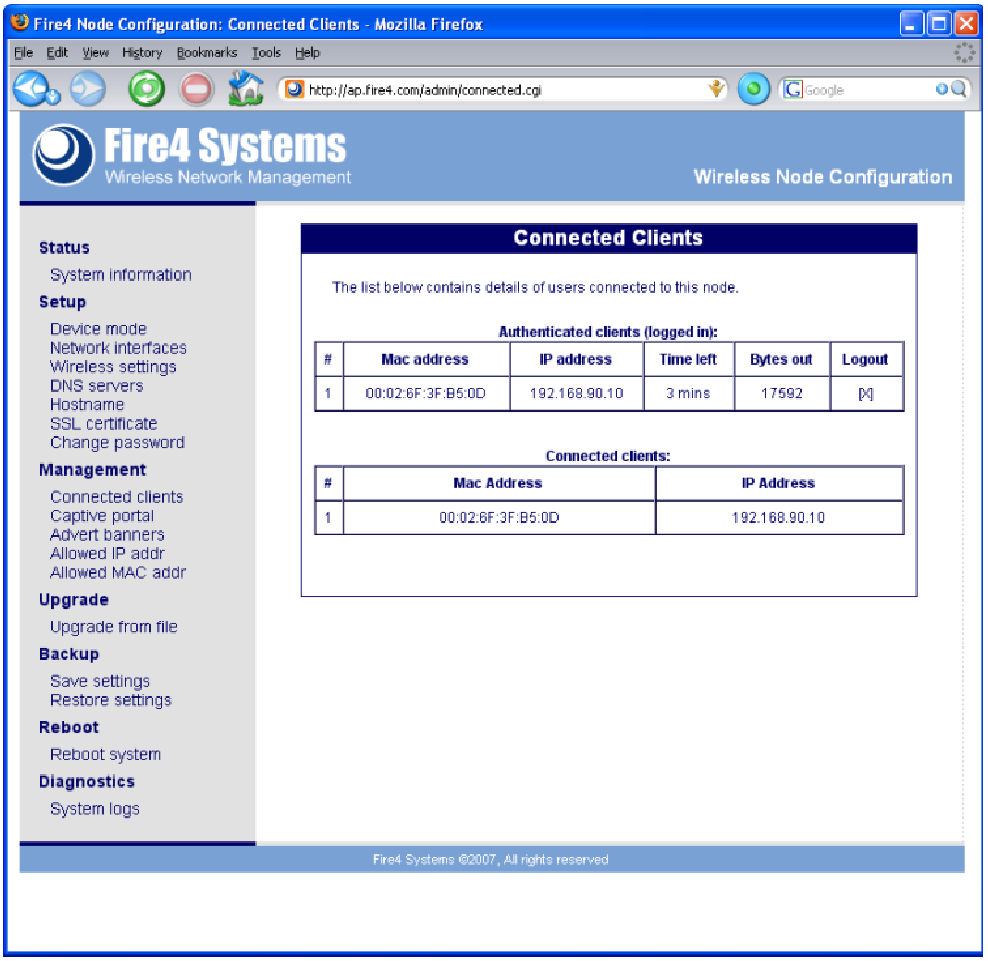
- Create a custom log in screen or select a log in screen from the library
- Set up log in screen advertising using banners
- Look at reports of users logged on to the hot spot
- Set IP and MAC address filters

The screens will be explained in the order that they are listed in the configuration screen menu.

The first screen shows clients connected to the hot spot access point. Two tables show clients that have obtained an IP address, and clients that have provided a valid access code and been authenticated.

The authenticated clients table shows the duration of the connection. The administrator can for a user logout by clicking on the box.

Connected Clients screen



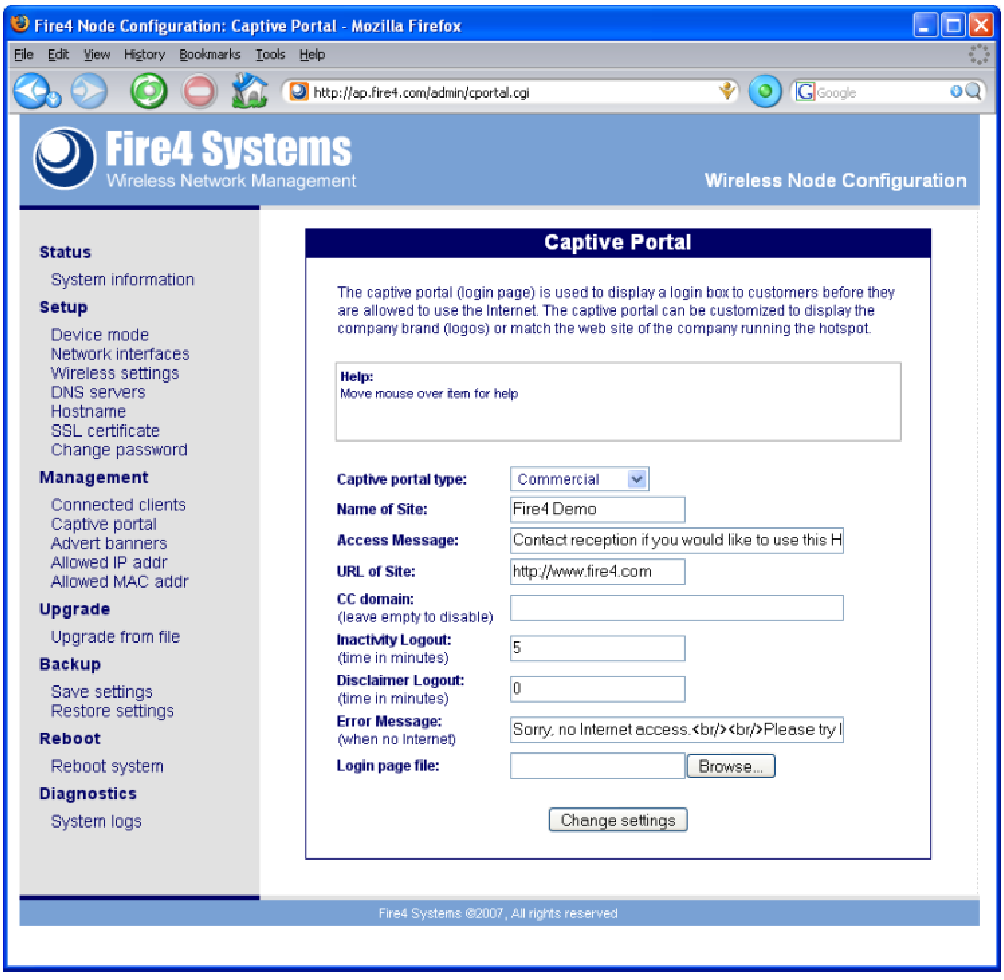
The **Captive Portal** screen provides the tools to configure all aspects of the hot spot user interface and billing. When a user gets an IP address from the hot-spot and then tries to access a web site, the user is redirected first to the log in page. This log in page is called the captive portal. There are three modes:

- Open: the access point operates like any other access point
- Disclaimer: a disclaimer log-in page is displayed. The disclaimer text can be modified and the log-in page can be configured for banner advertising. The disclaimer mode also has a timer that can determine how long the user can be connected to the network before being disconnected. A useful feature for coffee bars.
- Commercial: the user needs an access code to log in. This can be purchased via a scratch card, provided by the hot-spot operator, or the page can be configured for credit card billing. The log-in page can also display banner advertising.

Some of the commercial mode features require that the hot-spot operator subscribed to the Avansu billing site services. Each wireless node has a unique name and this can be entered on the captive portal page.

The hot-spot operator can design a login page and install it using the captive portal page. Developed notes are available for hot spot operators who wish to design log-in pages.

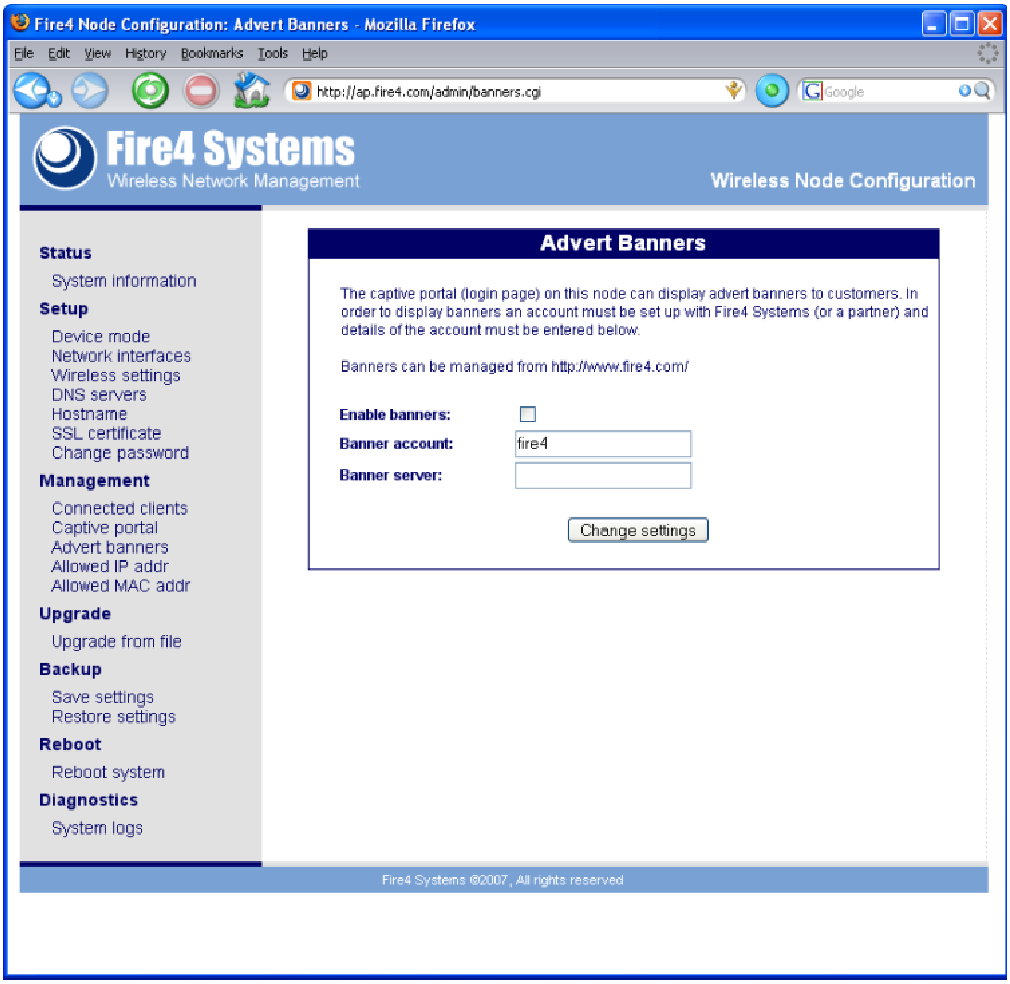
Captive Portal screen



A custom design log in page can include advertising banners. Banner advertising is enabled using the Advert Banners screen shown below. The server name is specified for the location of the banners.

Creation of custom log-in pages with banner advertising is described in a technical note available from Fire4 Systems. Fire4 Systems can also provide a login page creation service and can set up banner advertising for customers. Please call Fire4 Systems for a quote for this work.

Advert Banners screen



Examples of customized log in pages with banner advertising are shown on the following page.

The login page (sometimes called a splash page) should be created in HTML using the format described in the technical note. Banner references should be added at this time. The HTML page must be zipped together with all graphic files to generate the file that is then uploaded to the access point.

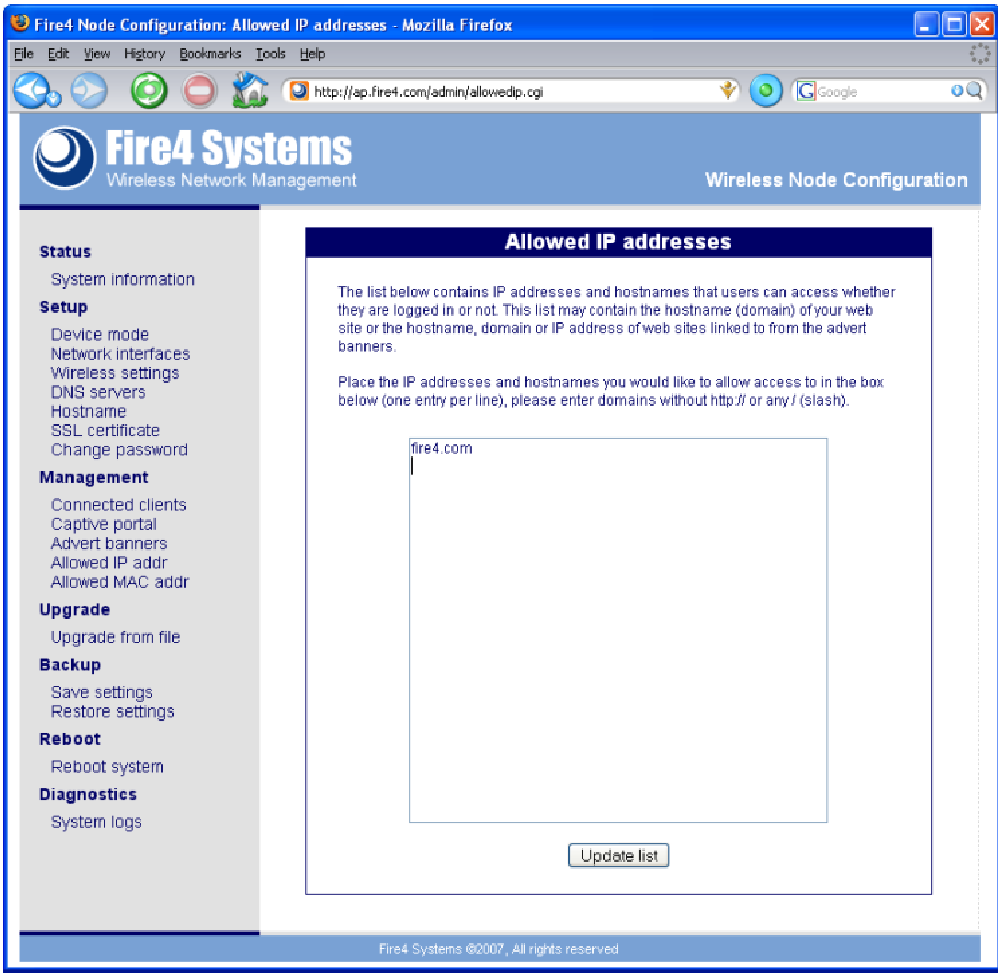
When the new login page is uploaded then the access point must be restarted to load the new login page.

If errors appear in the log in page it will be necessary to repeat this process, possibly several times, until, the login page design is satisfactory.

Login page example

If the hot spot operator wishes users the click through banners free of charge to advertisers web sites then the URL of each banner must be entered in the allowed IP list. See the screen on the following page. Allowed IP addresses can be written as URL's also.

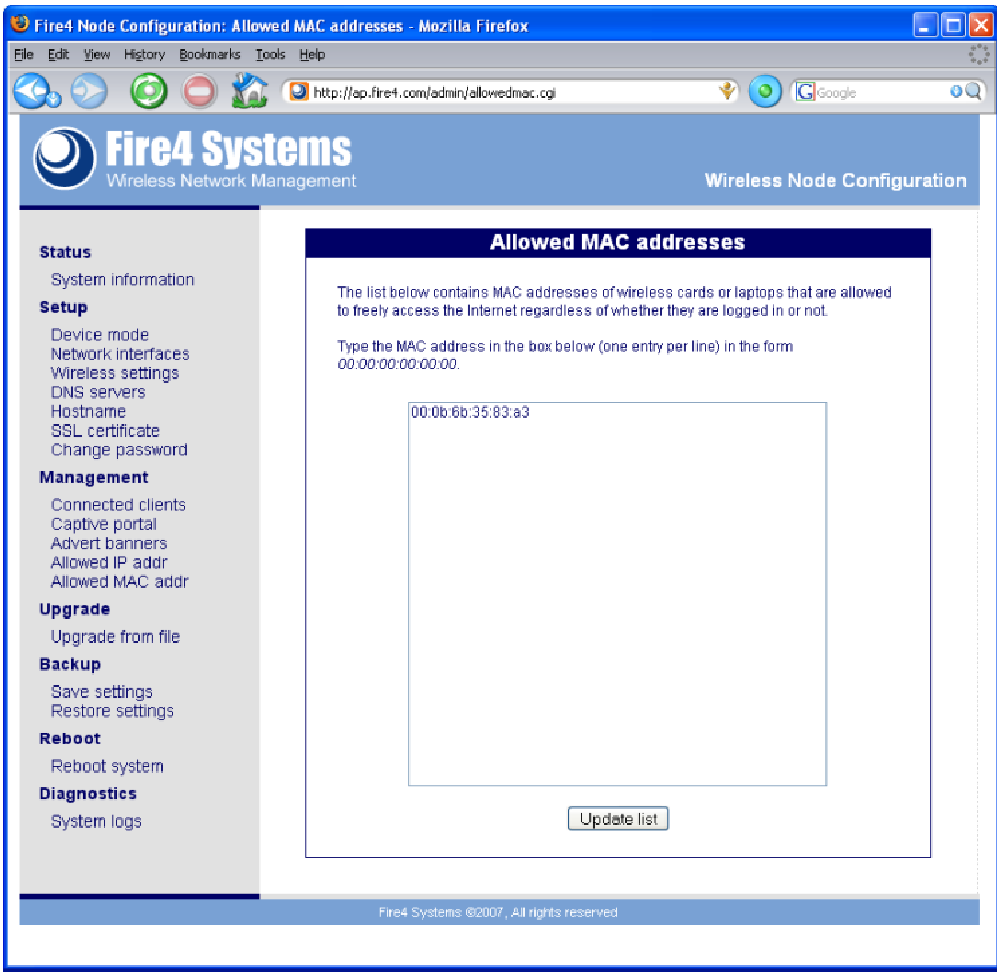
Allowed IP Addresses screen



MAC addresses can also be permitted to bypass the authentication system. This facility is useful for various applications.

- Service personnel computers can be authorized for any access point in the network to facilitate maintenance
- The hot spot operator can authorize his business computers to use the wireless network without authorization
- Authorization of a remote wireless repeater when it is configured in a router mode (the repeated provides DHCP services). When the repeater is configured to forward DHCP requests (using WDS services) then this feature is not required.

Allowed MAC Addresses screen



Configuration characteristics may change slightly between different wireless and router hardware platforms.

5: Additional Features: Upgrade, Backup, Reboot and Diagnostics

The node firmware can be upgraded by downloading the firmware file from the Fire4 Systems website to the computer being used for node configuration. Firmware upgrades will be announced on the website as they become available.

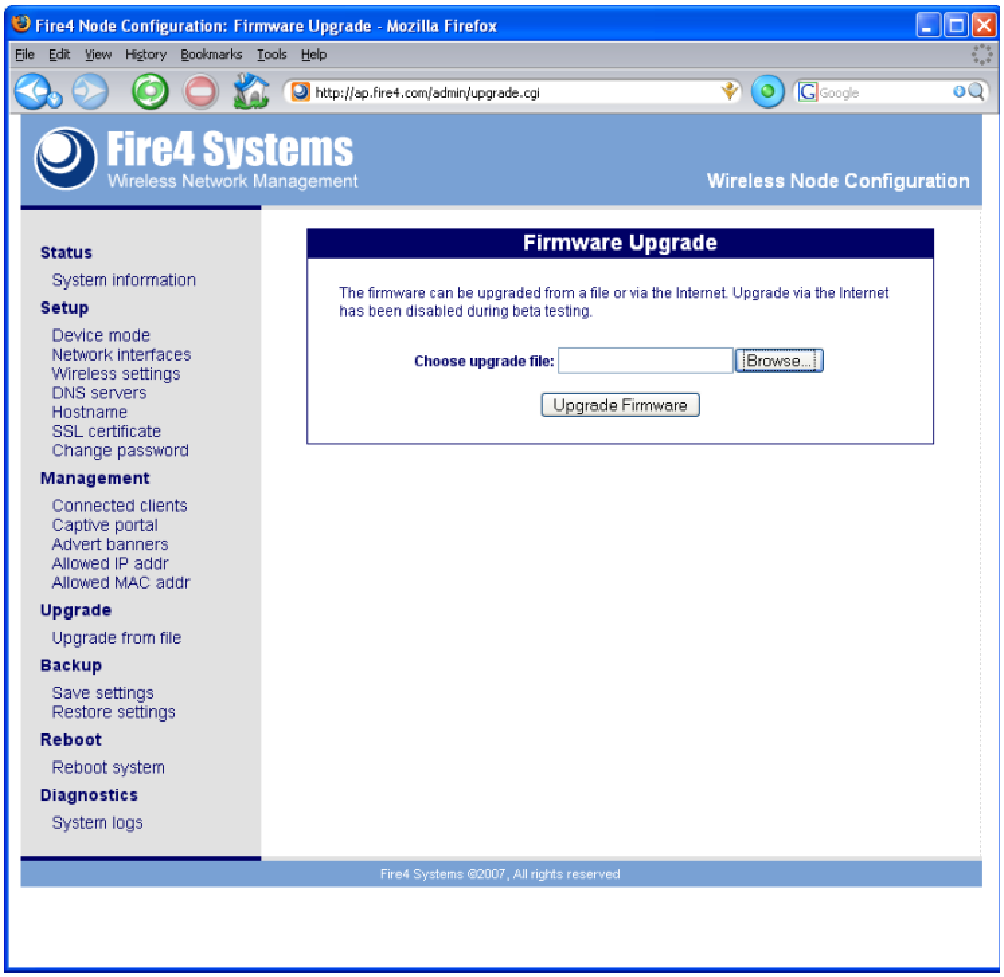
Remember that different hardware platforms have individual firmware files. Ensure that you are downloading the correct firmware file for your equipment.

When the firmware file has been downloaded to the computer then log in to the access point as ADMIN. When the status page opens click on **Upgrade from file** in the menu. Click on browse to find the correct upgrade file on the configuration computer. When located click on Upgrade Firmware.

The upgrade process will take several minutes. Do not disconnect power to the device during this process or the program storage memory may be corrupted.

A message will indicate when the upgrade process is complete and then the unit must be rebooted to work with the new firmware.

Firmware Upgrade screen

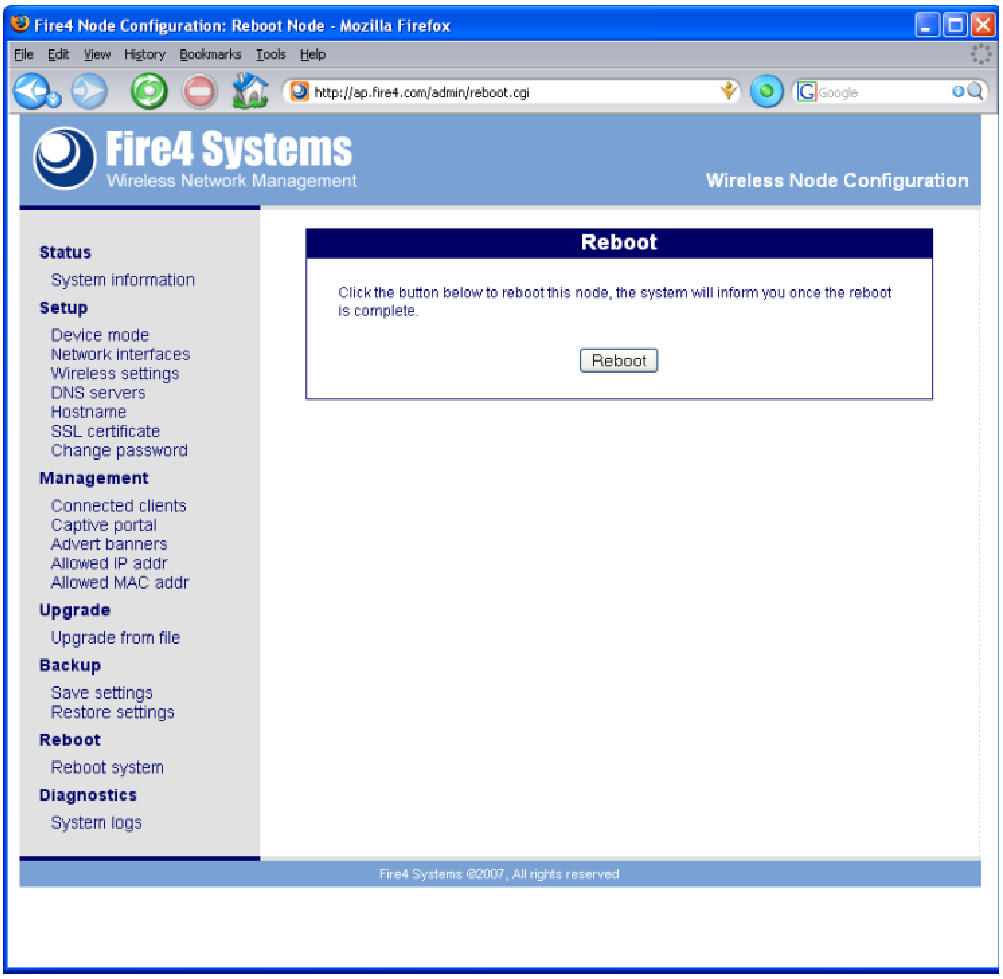


To reboot the device select **Reboot System** from the menu. The screen will open like that shown on the following page.

Click on the **Reboot** button to restart the device. This process is identical to cycling the power to the device. The firmware is reloaded from the flash memory

and all interface ports are initialized using the data stored in the configuration file. The reboot procedure will be required after several of the commands in the menu. Each command will indicate if the unit should be rebooted on completion of the command so that the command takes effect.

Reboot System screen



All the device configuration parameters are stored in a configuration file. The configuration file is very important and should be saved by using the **Save Settings** procedure when a device has been configured.

The configuration file is identical to any device that has the Avansu firmware installed, even if the device hardware is completely different. Therefore a configuration file saved on any device can be restored on any other device, to transfer the configuration characteristics.

This feature is extremely useful for any type of maintenance procedure. If a device has failed in the field then it can be replaced an the configuration file restored to the device to make it operational quickly.

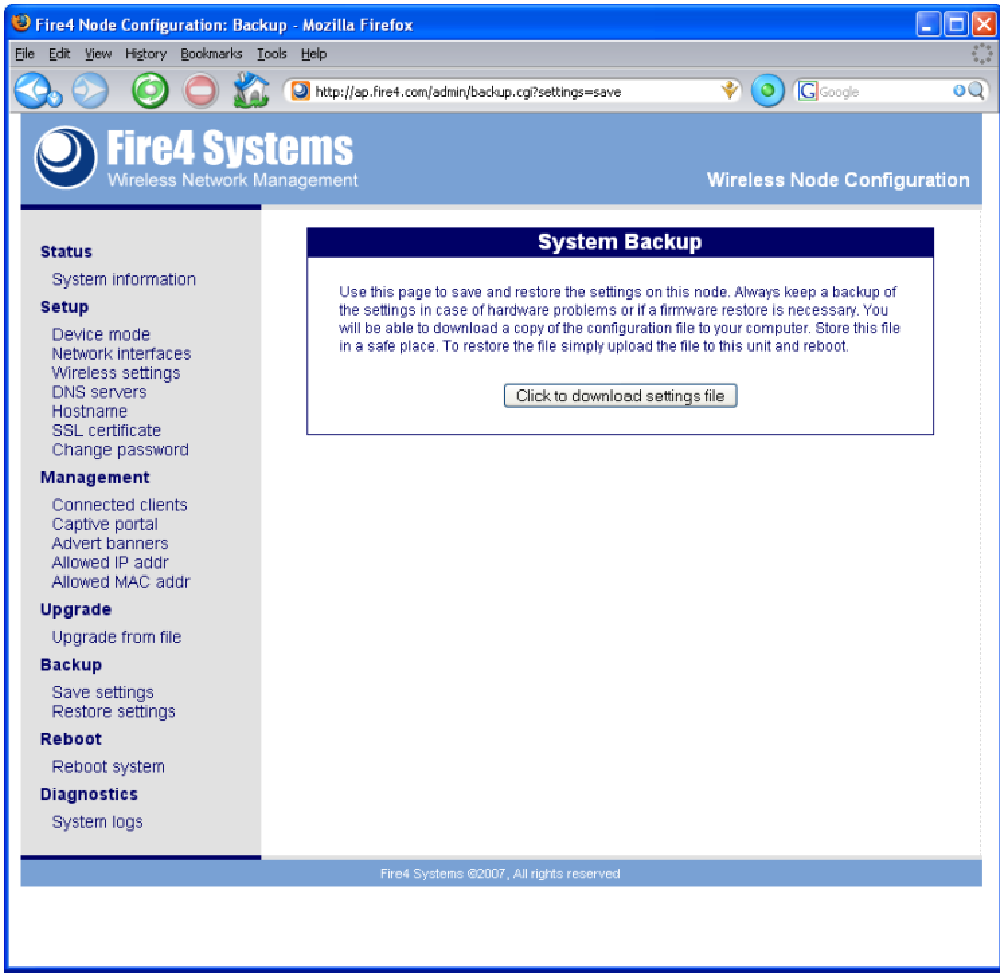
The backup and restore procedure can also be initiated remotely by a central network manager. A field technician therefore does not require technical knowledge about the device configuration. The field technician is only required to exchange units and power up the replacement. After then the network manager

can make the device operation from a central location.

Furthermore, a device can be replaced by any other type of device in the field, even if the hardware is completely different. This feature greatly facilitates maintenance of a large wireless network.

The Save Setting display is shown below.

Save Settings screen



Click on the button to download the settings file from the wireless node to the local computer. A window will open to select the directory where the file should be saved. Create a director with the name of the hot-spot node so that the configuration file can be easily located at a later date.

It is wise to store all configuration files at a central location so that if a field technician requires information about any node in the network the appropriate configuration file can be sent via email.

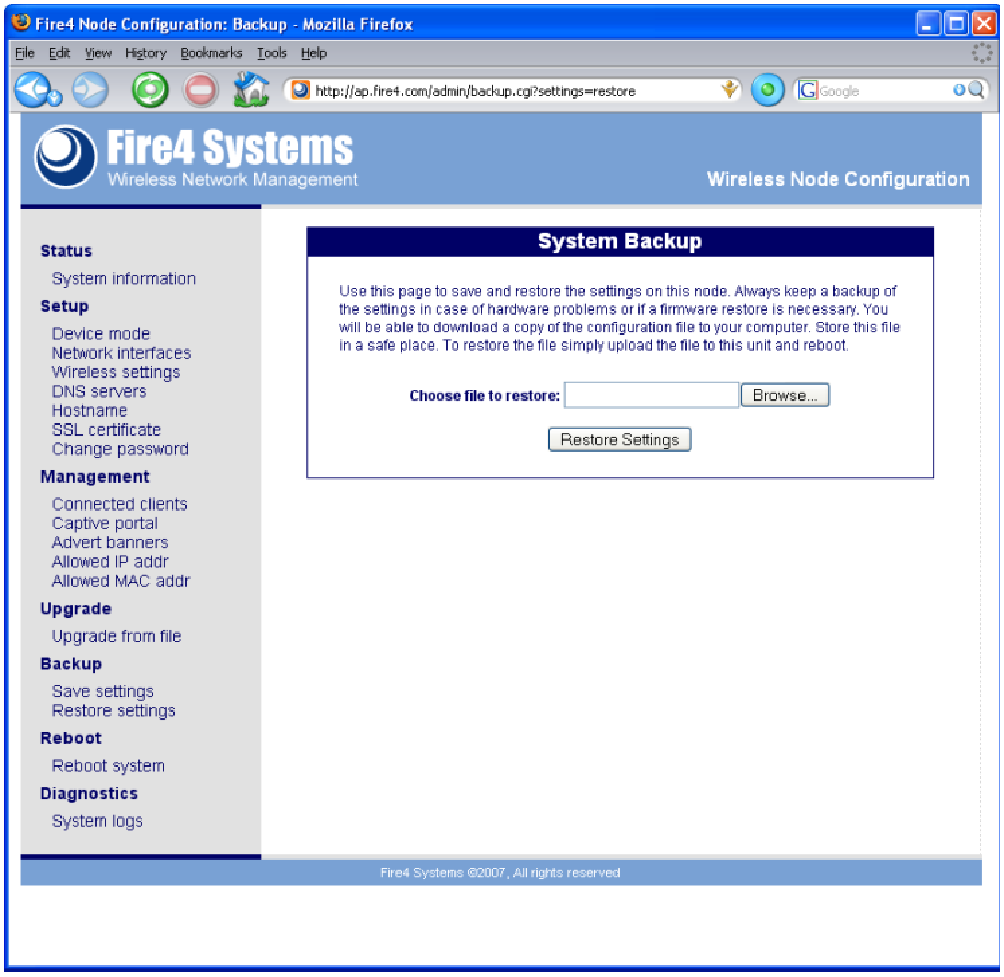
A configuration file is easily restored to the wireless device.

Click on the **Restore Settings** menu entry and the screen shown on the following page will open. Click on browse to locate the configuration file on the computer. When the file has been located then click on restore settings.

The device will take a few seconds to upload and store the configuration file. When this is completed the device must be rebooted to begin operation with the

restored settings.

Restore Settings screen



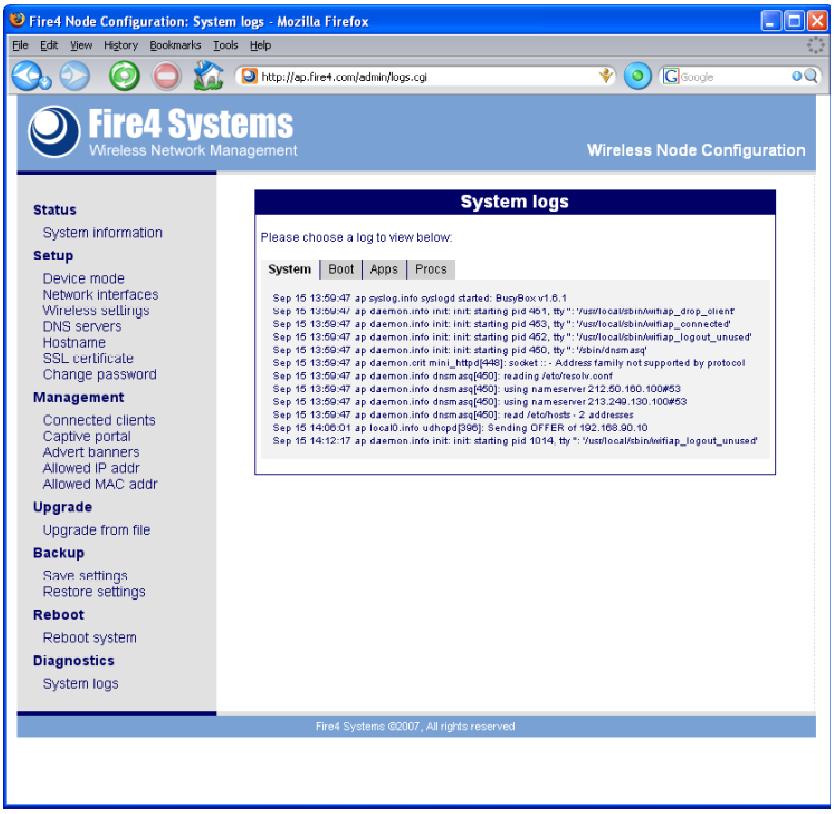
System logs are available that assist with diagnostic processes. If it is necessary to call the Fire4 Systems support personnel about some operational problem that has been encountered then the technician may require information presented on the diagnostics page.

Click on systems logs to open the diagnostic page. Four logs can be read by clicking on the appropriate tab in the box. These are:

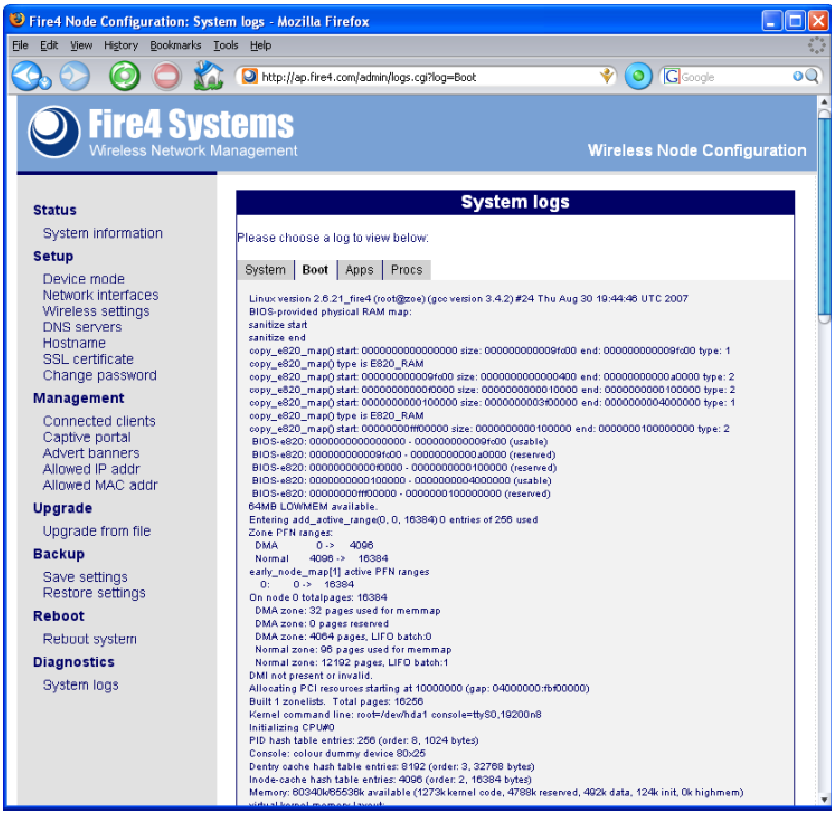
- System log: messages generated by the Linux kernel
- Boot log: messages generated during the system boot process
- Apps log: messages generated by firmware applications
- Procs log: messages generated by system processes

Examples of the log screens are shown on the following pages.

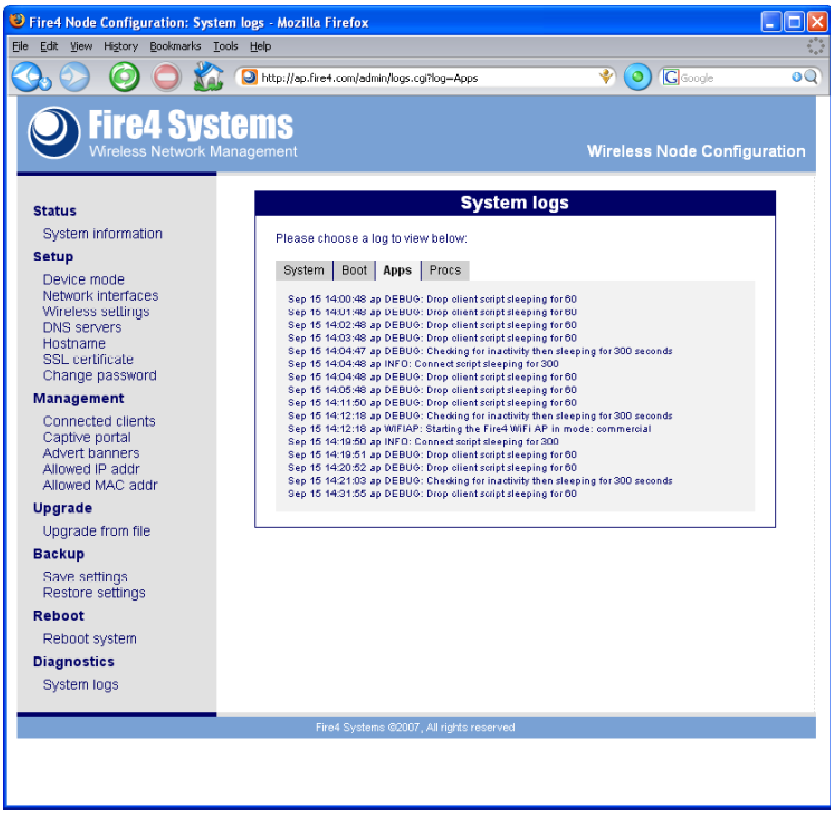
System Log screen



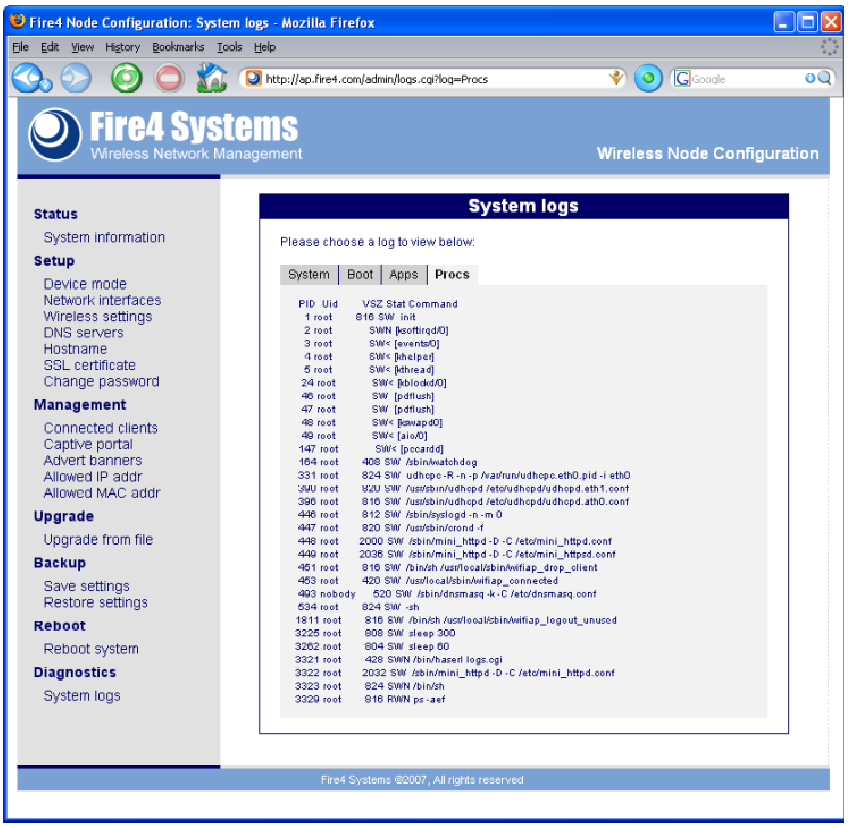
Boot Log screen



Apps Log screen



Procs Log screen



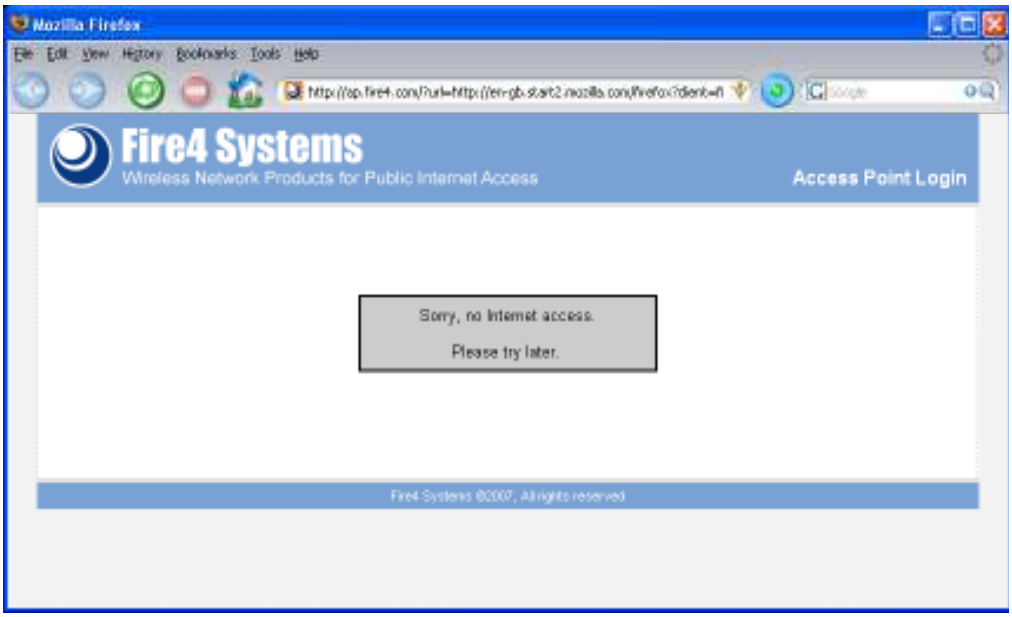
6: User Log-in Procedure

The user with a notebook computer and wireless interface will see the hot-spot SSID and request to connect (get an IP address). Any type of computer can connect to a hot-spot. Windows vista however requires careful configuration as it will block access to wireless networks without specific user authorization.

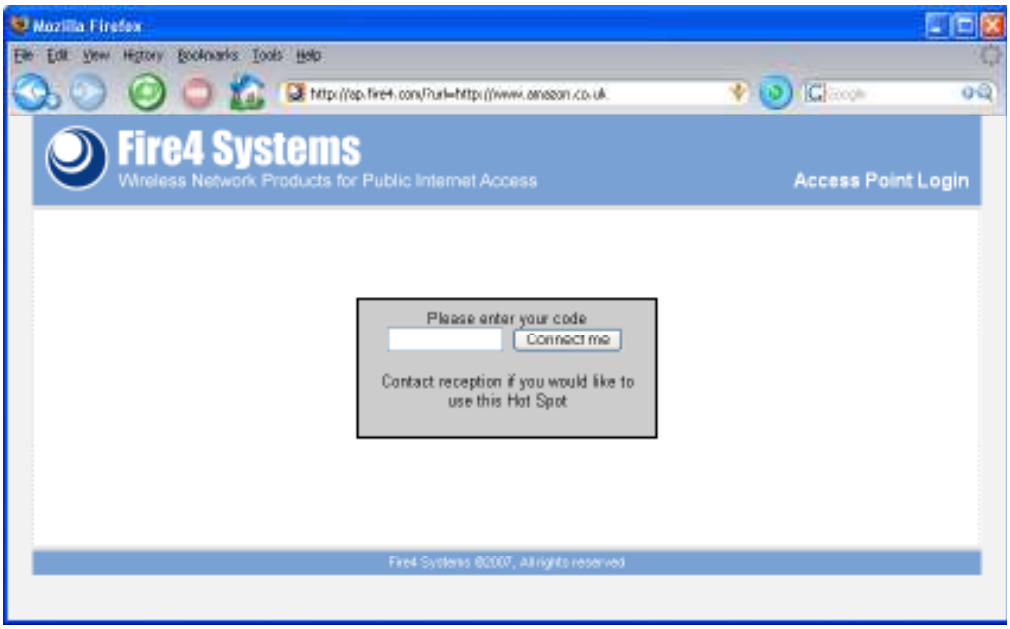
The next step is to open a browser window, which will attempt to connect to the default web page. The access point will redirect the user to the log-in or splash page (the captive portal).

The standard log in page is shown below. Other log in pages can be selected or programmed.

If the access point is not connected to the Internet then the user will see the message shown in the screen.



If the access point is connected to the Internet then the user will see the screen shown below.

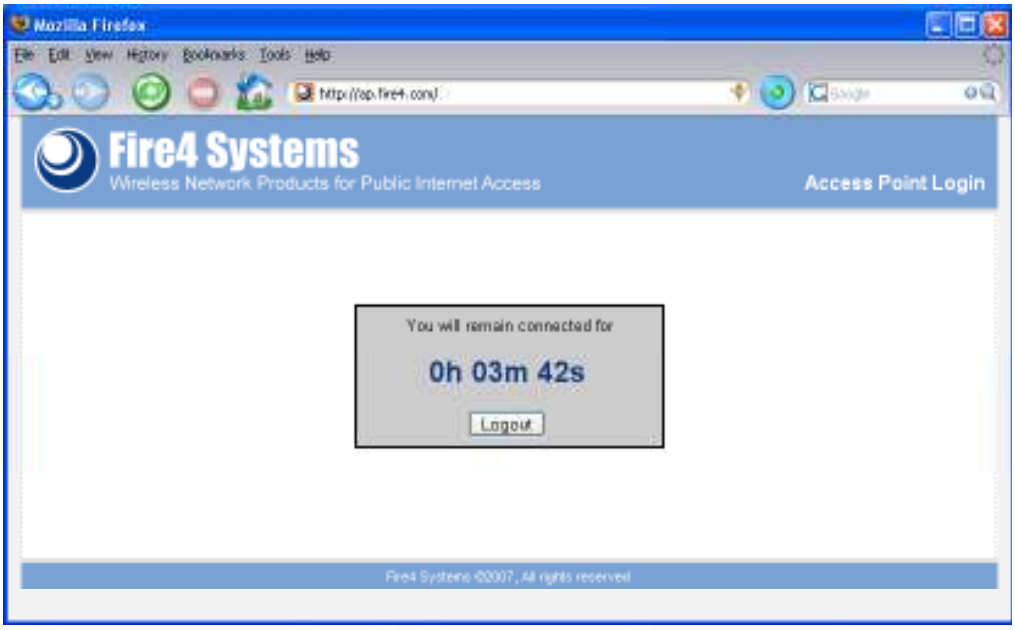


The user requires an access code to gain access to the Internet. The hot-spot operator can purchase pre-pay scratch cards from Fire4 Systems to sell to customers. The hot-spot operator can also download access codes to sell to users.

Other billing options are available. The hot-spot operator can configure the credit card processing display to charge users access via credit cards. Consult Fire4 Systems to configure credit card processing.

If the access code is not valid then the user will see an error message stating this. When the access code is valid then the user will see the screen shown where the time remaining for Internet access is displayed.

The user can now access the Internet for the duration of the code purchased.



By clicking on the continue button the window shown is opened permitting the user to have a convienent timer located on the computer desktop

7: Hot-Spot Billing Kit

The SK-01 hot spot billing kit contains the following items:

- 1 pack of 25 pre-pay cards: for access times of 1 hour, 6 hours, 1 day, 1 week
- 1 pack of 25 customer brochures: tri-folded for display
- 1 counter top display for brochures (manufactured in acrylic)
- 1 point of sale display for pre-pay cards (manufactured in acrylic)

The SK-01 kit items are shown in the figure.

Contents of the SK-01 hot-spot billing kit

Pre-pay access card

Customer brochure

Counter-top brochure display

Point-of-sale pre-pay card display

The point of sale display can be located behind the point of sale preventing access by the customer. The pre-pay cards are hung on the pegs provided.

The counter top display is used to present the hot-spot brochures that explain to potential users how the hot spot is accessed.

The kit items are available individually and the pre-pay cards and brochures are available in larger quantities, reducing the cost per unit.

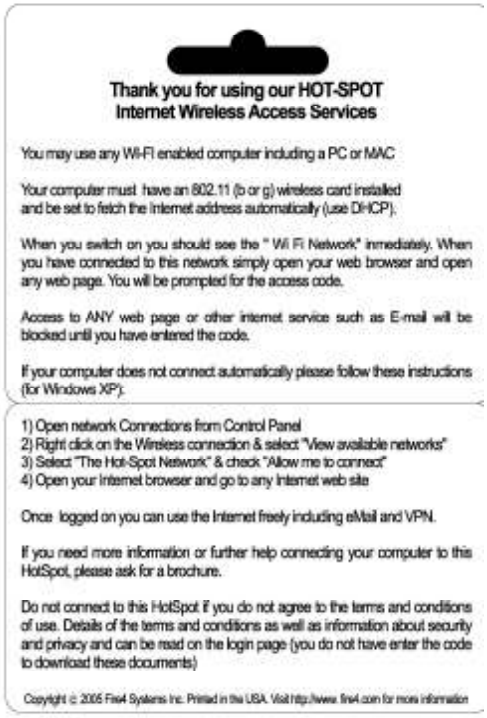
8: Internet Access Payment Using Pre-Pay Scratch-off cards

The pre-pay scratch card is identical to those sold for long-distance calling. The hot-spot owner determines the retail price of the scratch cards, no price is printed on the card. Cards are available with the following Internet connection times:

- 1 hour, continuous (runs to completion after the first log in)
- 6 hours, stop-start (user can stop time count (logout) and restart later)
- 1 day, continuous
- 1 week, continuous

The pre-pay card clearly states that the 'scratch' area must not be removed until the user can see the login screen on his or her computer. In some cases the users computer is not configured correctly to access wireless networks. If this is the case then the user should be refunded the price of the card when returned 'un-scratched'.

The pass-code is seen by scratching the area of the card indicated in the figure. The front and reverse of the card is shown.



Cards can be customized with the hot-spot owners graphic design. Consult Fire4 Systems regarding the cost of preparing a customized design and the minimum order volume required.

The hot spot operator can determine the following characteristics of the customized scratch card.

- Cards can be printed with up to four different time periods
- Each time period duration is determined when placing the order
- Each time period can be continuous or stop-start

9: Payment Using the On-Line Credit Card Billing System

Credit card billing require the hot-spot operator to obtain an account with a clearing bank.

The Avansu billing software is configured to work with either **authorize.net** or with **Pay-Pal**. Both options require the hot spot operator to be a resident of the USA or UK in order to obtain an account.

A third option, also with Pay-Pal, is available for hot-spot operators in other countries. In this case Pay-Pay will retain a percentage of the transaction to cover processing costs.

Please consult Fire4 Systems support staff to advise on creation of a credit casd subscription account.

10: Obtaining Billing System Supplies

Pre-pay access cards and brochures are consumed as part of the hot-spot business. Both pre-pay cards and brochures can be replenished in quantity packages. The larger quantity packages reduce the cost per unit. Replenishment packages are available as follows;

- Pre-paid "scratch" cards - packs of 50
- Pre-paid "scratch" cards - packs of 100
- Pre-paid "scratch" cards - packs of 250
- Pre-paid "scratch" cards - packs of 500
- Pre-paid "scratch" cards - packs of 1000
- Customer brochure - packs of 100
- Customer brochure - packs of 500

Please consult Fire4 Systems for pricing of these items. Hot-spot operators can also purchase customized graphic designs for both pre-pay cards and brochures. Please consult Fire4 Systems regarding scratch cards with custom graphics.

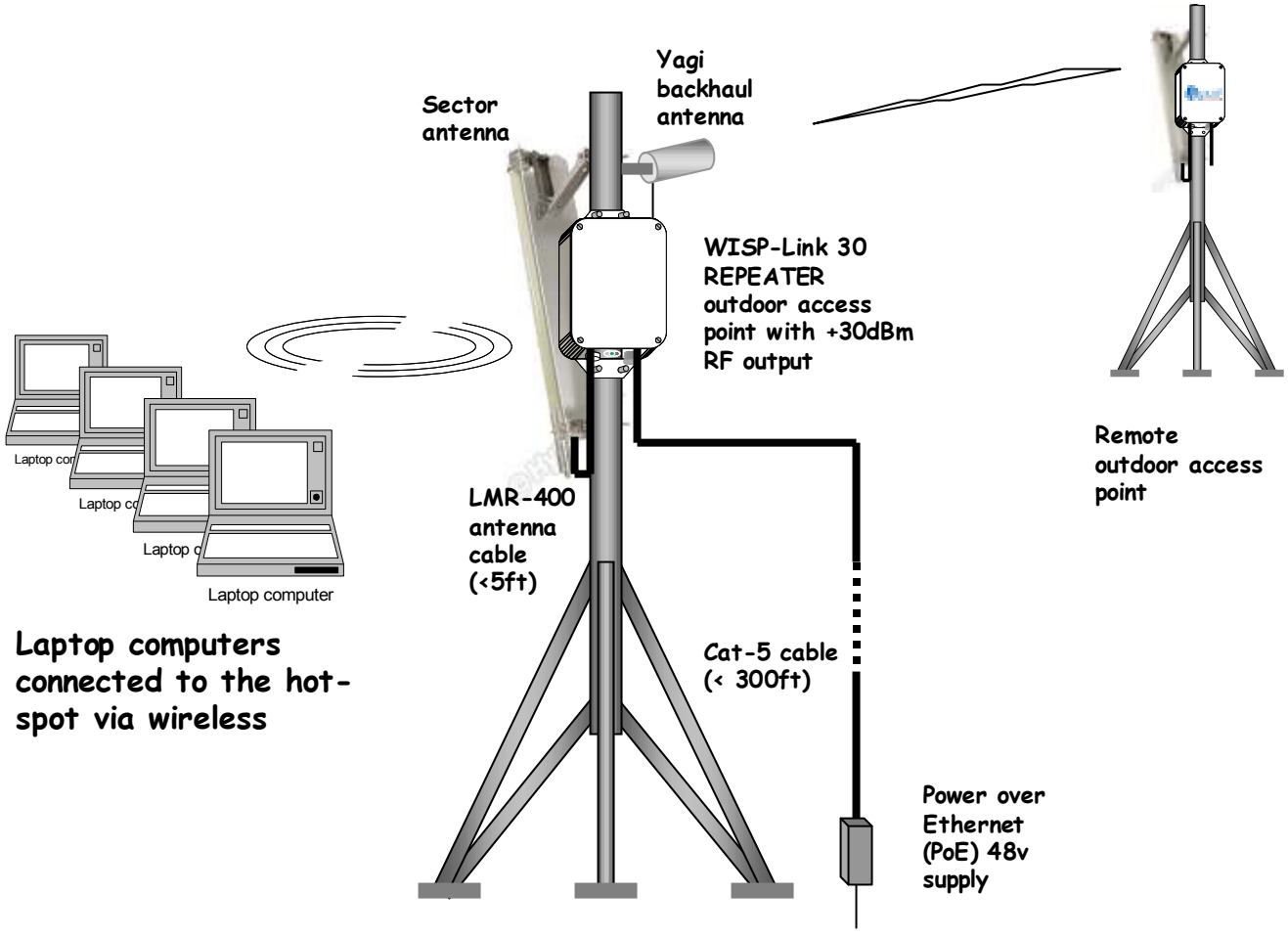
11: Extending the Hot-Spot Coverage Area: The Equipment Repeater

When the hot spot has been deployed it is possible that the area of coverage is not as great as the hot-spot owner had wished. Installing a repeater range extender can extend the range of the network.

The repeater is located within range of the equipment access point. The repeater RP-TNC antenna is connected to a directional backhaul antenna (Yagi, patch or parabolic). The directional antenna permits the relay to be located further from the equipment that would be possible using an omni-directional antenna. The relay sector or omni-directional antenna connects to the N connector. This antenna re-broadcasts the network connection outside the area of coverage of the equipment.

Several repeaters can be used simultaneously with the equipment access point.

Extending the network range using the Equipment Repeater



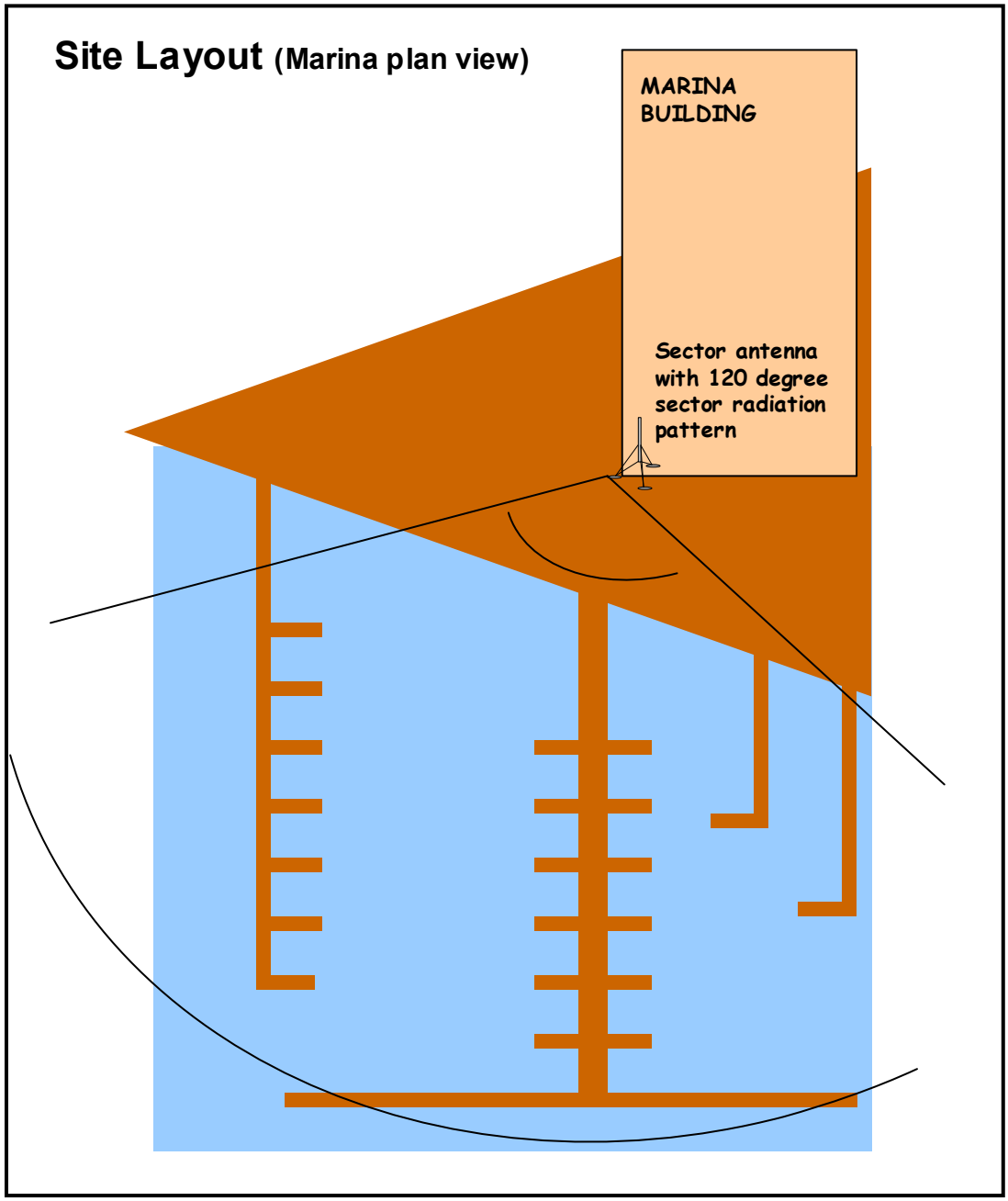
12: Example: A Marina Hot Spot Installation

The following project was prepared using the large-scale plan of the marina building. This information is insufficient to prepare comprehensive design, as the total area of the boat dockage space with distances has not been included.

A satellite photograph of the marina was obtained. It is presumed that the large building is the marina structure indicated in the FAX, and that the area to be covered by the hot spot is that shown within the circle. If this is not the case then additional information should be sent specifying the area of coverage with dimensions.

The building is specified as being 40ft tall. The antenna and outdoor access point should be mounted near the top on the corner of this building. The position of the antenna is shown in the diagram below.

The antenna is specified as a sector design with a horizontal angle of 120 degrees, the vertical angle will be approximately 30 degrees for a 9dBi antenna.



The antenna is mounted on the side of the building near to the top, a height of 35 ft. The vertical beam width is 30 degrees approximately for the 9 dBi gain antenna. Assuming that the area of coverage extends from the antenna for 400 ft, the antenna must be inclined downwards at an angle of 10 degrees. See the manual section describing antennas.

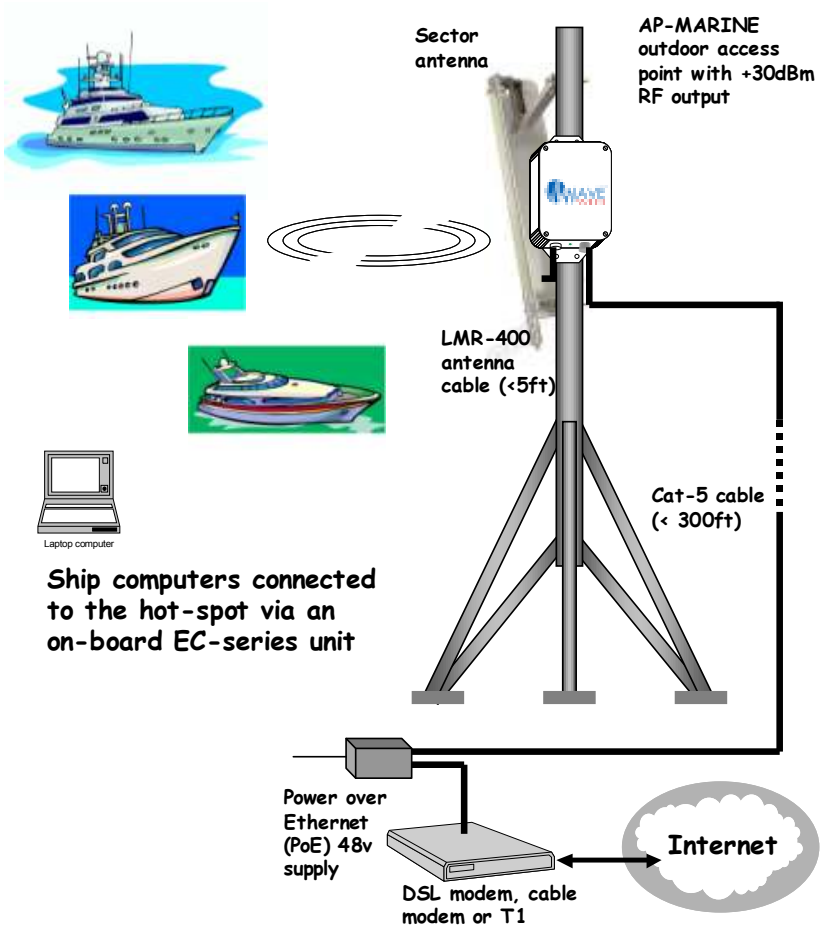
The access point configuration shown is an equipment single radio. One sector antenna provides coverage of the marina area. The equipment is also configurable for customer billing management. This means that the marina can sell scratch cards, and on-line billing is available where the marina received a percentage of the income.

The access point is specified has an RF power output of +30dBm. Assuming a power loss in the cables and connectors of +3dB, and specifying a sector antenna gain of 9dBi, then the total EIRP (Effective Isotropic Radiated Power) power output will be +36dBm. This is the maximum power output permitted by the FCC under part 15 of the regulations.

The access point is mounted close to the antenna. Long antenna cable runs are not permitted due to the high degree of signal attenuation at 2.4 GHz.

Cat-5 cable is routed through the wall and into the office to the location of the cable/DSL modem. A no-break supply should be used to power the cable/DSL modem, and the equipment PoE supply. The cat-5 cable can extend up to 300 ft.

The figure shows the installation arrangement. The equipment is mounted close to the antenna.



The equipment supports a customer-billing environment. The marina can bill customers via pre-pay scratch cards. The pre-pay scratch cards are presented at the point of sale display using the convenient card hanger. Customer brochures are also available as well as counter top brochure holders. The billing starter kit SK-01 should be purchased. Scratch cards and brochures can be purchased as supplies. The SK-01 starter kit includes the following components:

- 1 pack of 25 pre-pay cards: for access times of 1 hour, 6 hours, 1 day, 1 week
- 1 pack of 25 customer brochures: tri-folded for display
- 1 counter top display for brochures (manufactured in acrylic)
- 1 point of sale display for pre-pay cards (manufactured in acrylic)

The components contained in the starter kit can also be purchased separately. Brochures and cards can be purchased in packs of 25, 50, 100 and 250. Pre-pay cards can be purchased in any one of four access times. Other pre-pay card access times, and customized card graphic designs can be made to special order.

Appendix: LINUX Distribution

Fire4 Systems router and wireless equipment uses the Linux operating system version 2.6 as part of the software suite included with each Fire4 Systems product. The Linux V.2.6 operating system is distributed under the GNU (General Public License). Fire4 Systems abides by all the terms of the GNU. The Linux distribution installed in Fire4 equipment is available on a CD. The software distribution does not include proprietary applications programs developed by Fire4 Systems. Customers can request a copy of the Linux distribution CD. The customer will be charged $20 for packing and postage of the CD. For more information, please email Fire4 Systems at: info @ fire4 . com

GNU GENERAL PUBLIC LICENSE
Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA. Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Lesser General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program).
Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

> *a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.*
>
> *b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.*
>
> *c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)*

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

> *a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,*
>
> *b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,*
>
> *c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)*

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously

your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS