Access Point and Access Server

Quickstart

Bluegiga Technologies

Access Point and Access Server: Quickstart

by Bluegiga Technologies

Table of Contents

List of Tables

Chapter 1. Getting Started

Access Point and Access Server can be controlled in four ways:

- by using Bluegiga Solution Manager (see BSM documentation for details)
- by using the WWW interface
- by entering commands and using applications at the shell prompt
- by sending and/or retrieving files to/from the device.

    Note: The default username is `root` and the default password is `buffy`.

1.1. Powering Up

To get started with Access Point or Access Server, connect it to your local area network (LAN) by using an ethernet cable, and connect the power adapter. The unit will power up and retrieve the network settings from your network's DHCP server.

Access Point and Access Server will also use Zeroconf (also known as Zero Configuration Networking or Automatic Private IP Addressing) to get a unique IP address in the 169.254.x.x network. Most operating systems also support this. In other words, you can connect your controlling laptop with a cross-over ethernet cable to Access Server, then power up Access Server, and the devices will automatically have unique IP addresses in the 169.254.x.x network. With Access Point, also a direct ethernet cable works.

    Note: If you need to configure the network settings manually and cannot connect Access Server first by using Zeroconf, you can do it by using the management console. For more information, see Section 1.3.1. Access Point, however, does not provide user access to the management console. You can configure static network settings by sending the settings in a management packet for example using a USB memory dongle. See User's and Developer's Guide for more information.

The physical interface locations of Access Point are described in Figure 1-1.
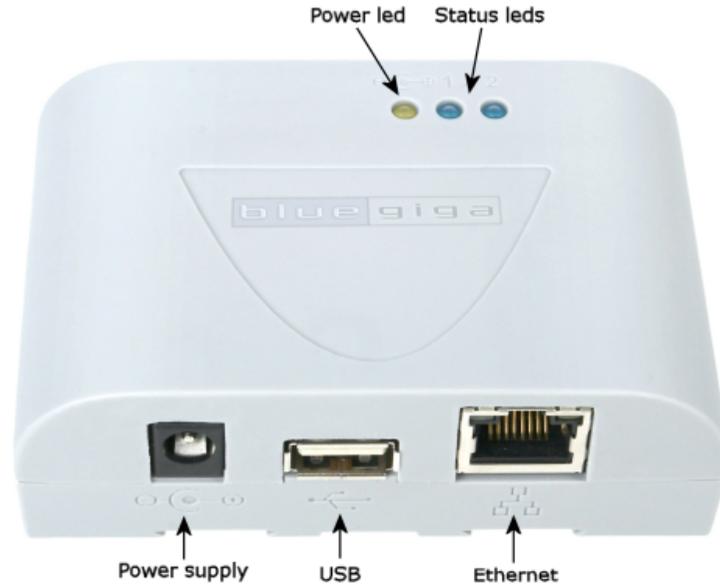
Figure 1-1. Access Point Interfaces

> **Note:** There is no power switch in Access Point. The adapter is the disconnection device; the socket-outlet shall be installed near the equipment and shall be easily accessible. Unplug and plug the power adapter to switch the power on and off. The power led in Figure 1-1 is on when the power adapter is connected.

The physical interface locations of Access Server are described in Figure 1-2 and Figure 1-3.
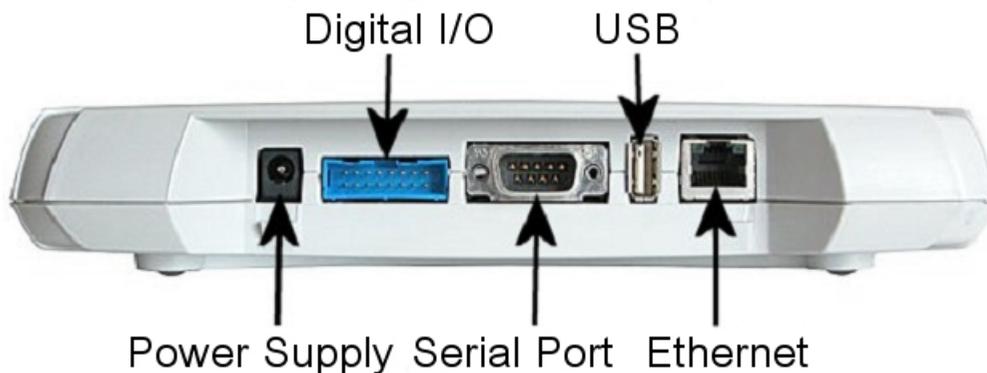
Figure 1-2. Access Server Connectors

> **Note:** There is no power switch in Access Server. The adapter is the disconnection device; the socket-outlet shall be installed near the equipment and shall be easily accessible. Unplug and plug the power adapter to switch the power on and off. The power led in Figure 1-3 is on when the power adapter is connected.
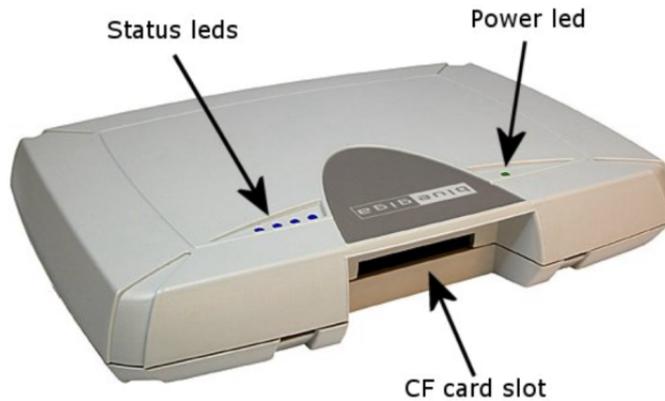
Figure 1-3. Access Server leds

All the blue status leds are turned off and the rightmost blue led (closest to the power led, led number 1 in Access Point) blinks on four second intervals when the boot procedure is finished and the unit is ready to be connected. Bluetooth led, (led number 2 in Access Point and blue led furthest away from power led in Access Server) blinks quickly every 30 seconds indicating Bluetooth service activity.

1.2. WWW Interface

Most Access Point and Access Server functionality can be controlled through the WWW interface by using any standard WWW browser.

The wrapfinder application (see Figure 1-4), available for the Windows operating system from Bluegiga Techforum (http://techforum.bluegiga.com/) provides an easy-to-use interface for finding Access Points and Access Servers (with SW version 2.1.0 or later) in the local area network.
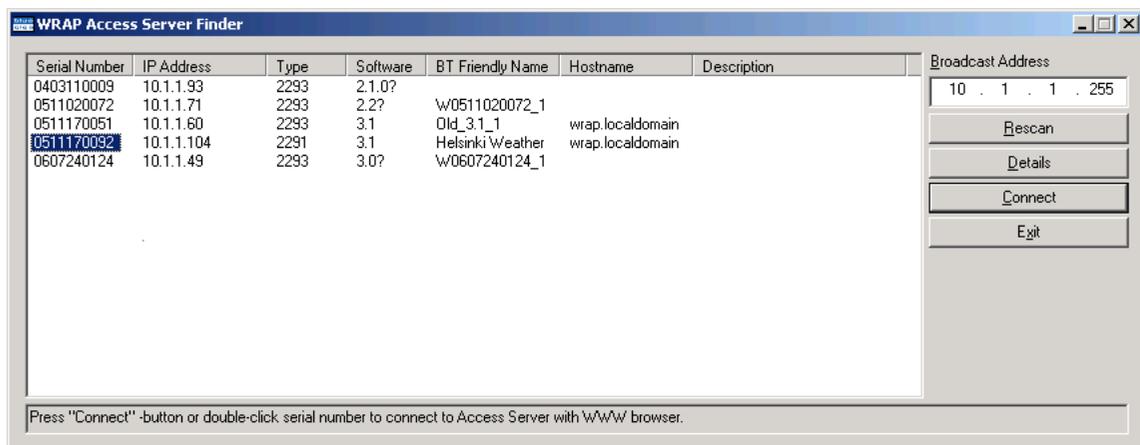
Figure 1-4. Access Server Finder Application

When wrapfinder is launched, it automatically identifies the broadcast address of the network it runs in and sends a special query packet (UDP broadcast) to units. The most important information in their responses is then shown in table format.

You can change the broadcast address used for finding Access Points and Access Servers. A new scan can be done by clicking Rescan.

Select a unit by clicking its serial number, and click Details to see more information (such as all Bluetooth addresses and friendly names). See Figure 1-5 for details.
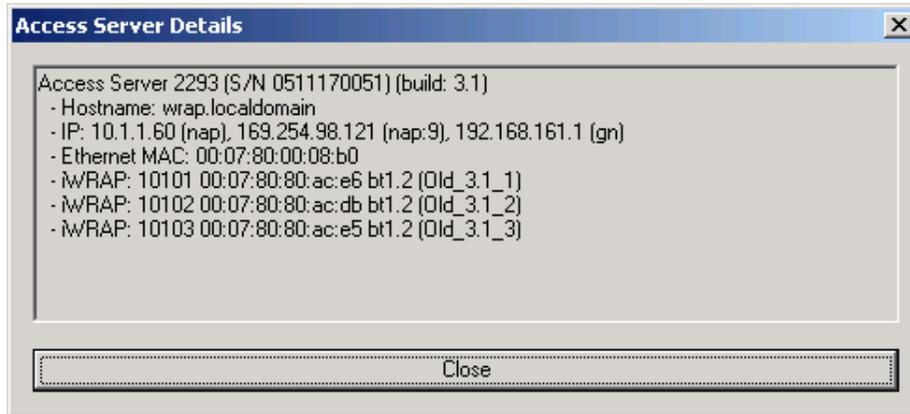
Figure 1-5. Details Dialog of Access Server Finder

Click Connect or double-click a serial number to connect to the selected Access Point or Access Server by using a WWW browser.

Click Exit to close the program.

> **Note:** To find Access Server's IP address without wrapfinder, see Section 1.3.2.

To access the WWW interface, enter the IP address of Access Point or Access Server to the browser's address field and press **Enter** (see Figure 1-6).

Figure 1-6. WWW Interface

From the top-level page, click Setup to log in to the configuration interface. The default user-name is `root` and the default password is `buffy` (see Figure 1-7).
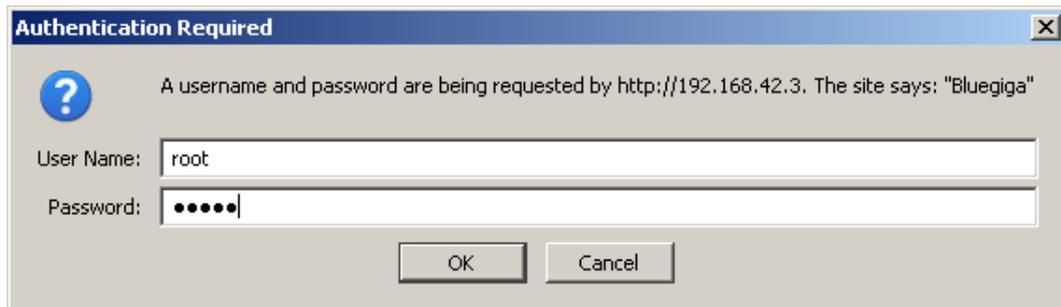
Figure 1-7. WWW Login Prompt for Access Server Setup

After logging in, you can configure several settings (see Figure 1-8). These are discussed in detail in Section 1.4.
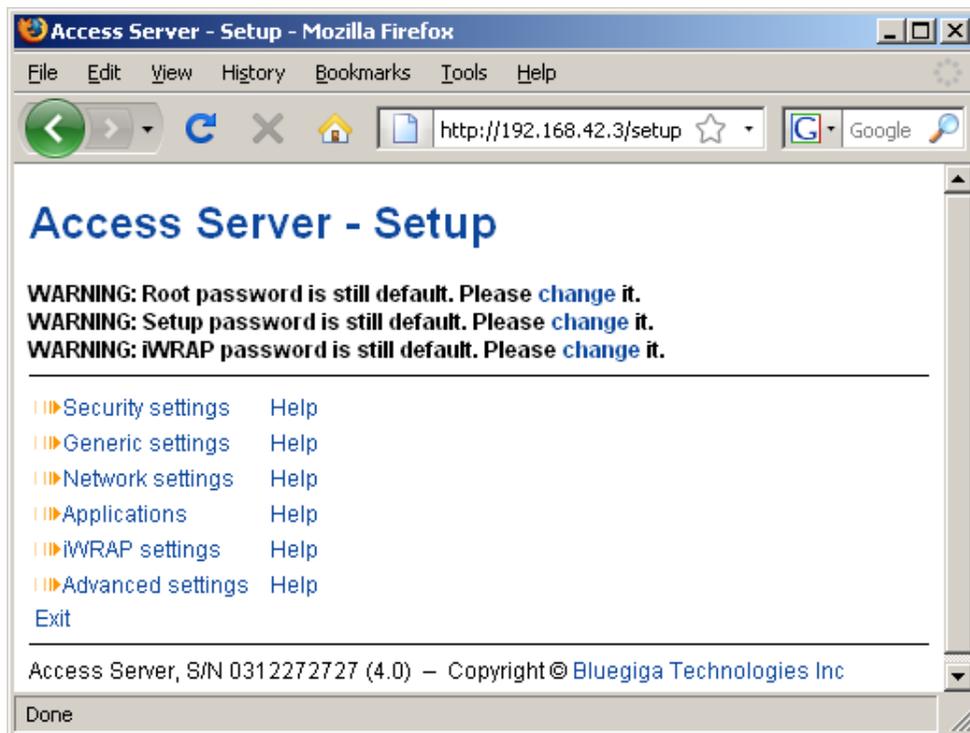
Figure 1-8. The WWW Configuration Interface

1.3. Shell Prompt Access

Shell prompt access may be needed for advanced controlling operations that cannot be per-formed by using the WWW interface. You can get to the shell prompt by using SSH. When you are connected to the same LAN network with your Access Server or Access Point, you can find its IP address using the wrapfinder application (see Section 1.2 for details).

You can use SSH to get shell prompt access also using Bluetooth LAN Access or PAN profile. Access Server and Access Point can be seen in Bluetooth inquiries as "Wserialno_n", where "serialno" is the serial number of the device and "n" is the number of the Bluetooth baseband in question (model 2293 has three Bluetooth basebands, any of which can be connected). After you have connected to the server (no PIN code, username or password is needed), establish an SSH connection to the device at the other end of the connection. You can use the wrapfinder application to find the IP address (see Section 1.2 for details).

> **Note:** Bluetooth LAN Access and PAN profiles are disabled by default. Use the WWW interface to enable them, if needed. The PAN profile can also be enabled by sending the `enable-pan.noarch.wpk` file (available on-line at http://bluegiga.com/as/current/enable-pan.noarch.wpk) to Access Server by using Bluetooth Object Push profile or by inserting a USB memory dongle with the file in its root directory to Access Server's or Access Point's USB port.
> **Note:** The default username is `root` and the default password is `buffy`.

1.3.1. Management Console (Access Server only)

If you do not have a Bluetooth LAN/PAN client and if Access Server is not connected to your LAN, or if you do not know the IP address given to Access Server, you can get the first shell prompt access by using the management console. The management console is only needed to change the network configuration settings if you cannot configure the network by using DHCP or Zeroconf. The management console is connected to Access Server with a serial cable. After you have configured the network settings by using the management console, all further controlling activities can be performed remotely using SSH sessions over ethernet or Bluetooth LAN/PAN connection.

To setup the management console, proceed as follows:

1. Have a PC with a free COM port.

2. Power off Access Server.

3. Configure your terminal application, such as HyperTerminal in Windows, to use the settings below for your computer's free COM port

Setting	Value
Speed	115200bps
Data Bits	8
Parity	None
Stop Bits	1
Flow Control	None

Table 1-1. The Management Console Port Settings

4. Connect the serial cable shipped with Access Server to your PC's free COM port.

5. Connect the serial cable to the management (user) port in Access Server (see Figure 1-2).

6. Power on Access Server.

7. Enter letter **b** in the terminal application during the first five seconds.

8. The management console is now activated and you can see the boot log in your terminal window.

> **Note:** The boot process may stop at the following U-Boot prompt:
>
> ```
> Hit any key to stop autoboot:  0
> U-Boot>
> ```
>
> If this happens, enter command **boot** to continue to boot Linux.

9. Wait for the device to boot up and end with the following prompt:

   ```
   Please press Enter to activate this console.
   ```

10. Press **Enter** to activate the console. You will be logged in as **root** in directory `/root`:

    ```
    [root@wrap root]
    ```

11. You can now control Access Server from the management console.

1.3.2. Accessing Remotely

When Access Server or Access Point is connected to a LAN, it tries to get the IP address by using DHCP and Zeroconf by default. You can then use the wrapfinder application to find the IP address (see Section 1.2).

With Access Server but not Access Point, if you cannot get the IP address by using the wrapfinder, another way to see the IP address is to connect with a management console (see the previous section), power on the unit and, after the system is up and running, give the **ifconfig nap** command. The `inet addr` field for the `nap` interface contains the IP address of Access Server. For example, in the following capture from the management console, the IP address is `192.168.42.3`.

```
[root@wrap /]$ ifconfig nap
nap       Link encap:Ethernet  HWaddr 00:07:80:00:BF:01
          inet addr:192.168.42.3  Bcast:192.168.42.255  Mask:255.255.255.0
          inet6 addr: fe80::207:80ff:fe00:bf01/64 Scope:Link
          UP BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:12635 errors:0 dropped:0 overruns:0 frame:0
          TX packets:8 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:1686246 (1.6 MiB)  TX bytes:1640 (1.6 KiB)
          Interrupt:24 Base address:0xc000
```

You can use this address to connect to Access Server remotely over SSH, SCP or SFTP.

> **Note:** The default username is **root** and the default password is **buffy**.

1.3.3. Transferring Files to/from Access Server

You can transfer files to and from Access Server and Access Point by using, for example:

- SCP (secure copy over SSH).
- SFTP (secure FTP connection over SSH).
- FTP (plain FTP connection).

> **Note:** FTP is disabled by default for security reasons. Use SFTP instead. FTP server is not installed by default. You can install it from software package `ftpd`. See User's and Developer's Guide for information about installing software components.
>
> **Tip:** If enabled, use the integrated FTP client on the Internet Explorer (type ftp://root:buffy@wrap-ip-address/ in the address bar).

- Bluetooth OBEX (Object Push and File Transfer Profiles) to/from directory `/tmp/obex` in Access Server or Access Point.

- NFS (mount an NFS share from a remote computer as a part of Access Server's or Access Point's file system).

- SSHFS (mount an Access Server or Access Point directory over SSH as a part of any other Linux host file system).

  To download and install SSHFS, visit http://fuse.sourceforge.net/sshfs.html.

- CIFS (mount a Common Internet File System share from a remote computer as a part of Access Server's or Access Point's file system). A CIFS client, available in a separate software packet `cifs-client`, is required. See User's and Developer's Guide for information about installing software components.

- USB memory dongle (see User's and Developer's Guide for more information.

- Xmodem/Ymodem/Zmodem (use **rz/rx/rb/sz/sx/sb** commands from the management console). You can install these commands from software package `rzsz`. See User's and Developer's Guide for more information about installing software components.

  > **Note:** The management console is not available for Access Point, only for Access Server.

1.4. Introduction to Configuration

When Access Server or Access Point is installed and powered up for the first time, the default configuration settings are being used. With these settings, the unit automatically configures its network settings assuming that it is connected to a LAN network with a DHCP server running. Additionally, the unit also uses Zero Configuration Networking (also known as Automatic Private IP Addressing) to connect to the 169.254.x.x network, which can be used if the network has no DHCP server.

After booting up, the only Bluetooth profiles enabled are the Object Push and File Transfer Profiles, used to send files to/from Access Server.

More Bluetooth profiles can be enabled, and most of Access Server and Access Point settings can be configured by using the **setup** application. It has a WWW interface at http://wrap-ip/setup but it can also be run at the command line.

> **Note:** The default username is **root** and the default password is **buffy**.

1.5. Using the Setup WWW Interface

The easiest way to change Access Server or Access Point settings is to use the WWW interface. Accessing the WWW interface is instructed in Section 1.2.

A typical WWW configuration page is shown in Figure 1-9 (This page can be found at Setup ⟶ Security settings)
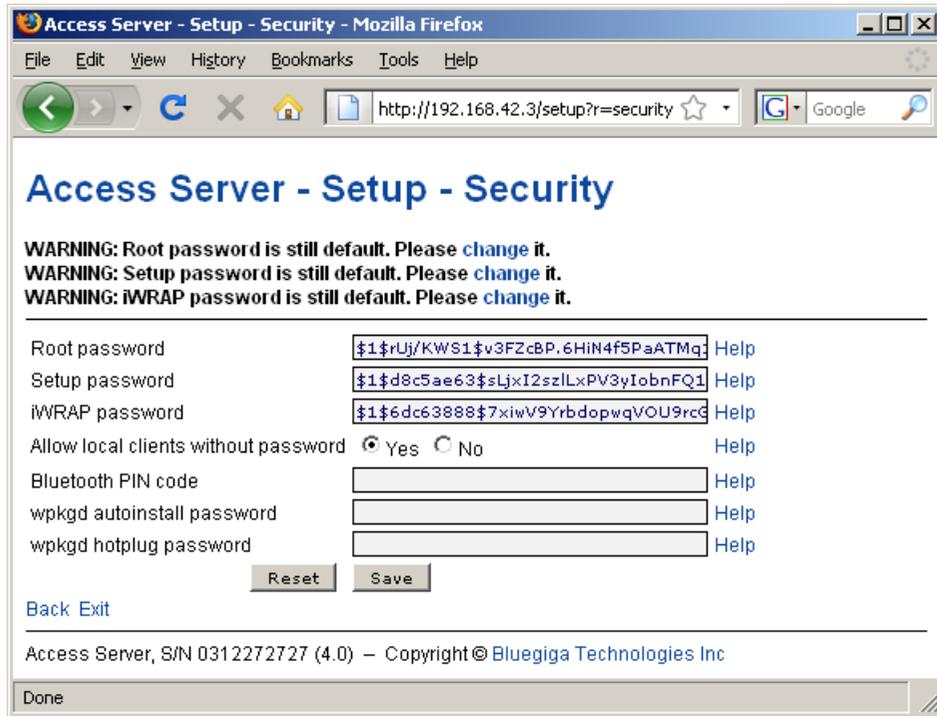
Figure 1-9. Example WWW Setup Page

The different parts of the WWW Setup page are discussed in the following list:

- Status area

  The status area serves three purposes:

  - It indicates that the changes are permanently saved when the user clicks the Save button (or when the user clicks a toggling Yes/No link).

  - It warns when default passwords are in use.

  - If invalid values were entered in one or more fields, an error message is shown in this area (see Figure 1-10).
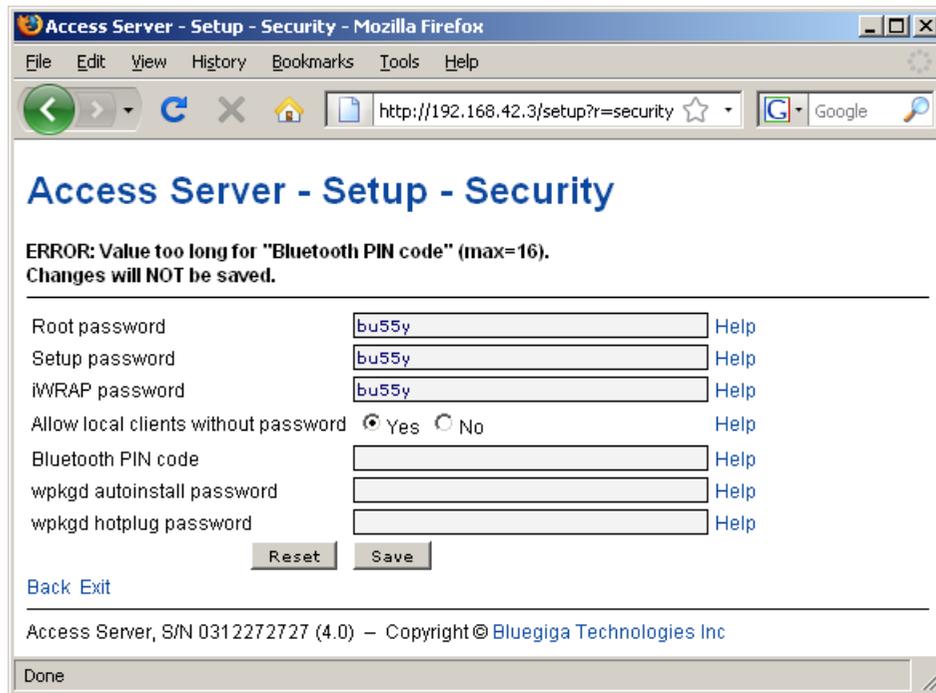
Figure 1-10. Trying to Save an Invalid Input

> **Note:** It is typically necessary to reboot Access Server or Access Point for the changes to take effect. This can be done through the WWW interface (Advanced settings menu).

- Number or text entry fields

Most of the configurable settings are text (or number) entry fields. For some fields, such as the IP address or netmask, there are restrictions on the input format. Setup validates the input at save time and accepts valid data only. The fields with errors are shown to the user so that mistakes can be fixed (see Figure 1-10).

- Help link

Click the Help link to retrieve the setup page again with requested help information displayed. For an example, see Figure 1-11.
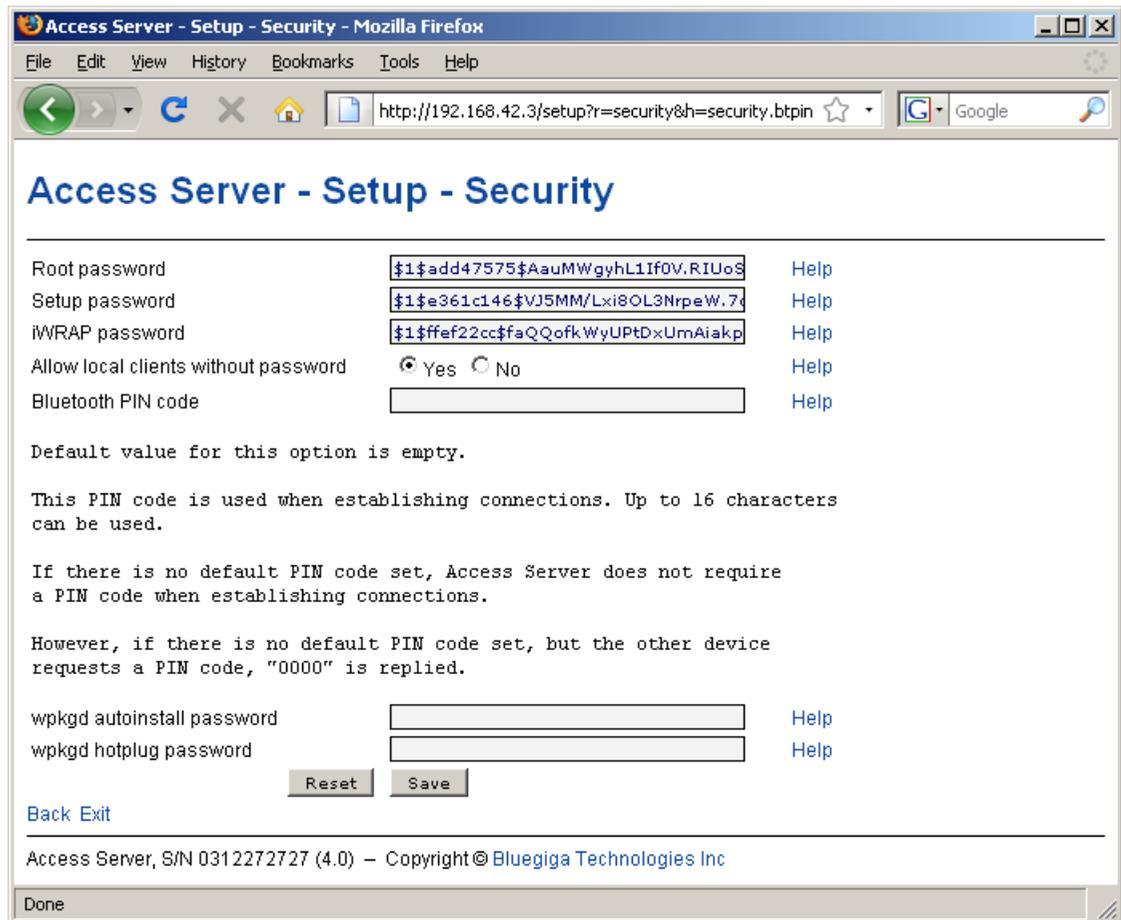
Figure 1-11. Help Links in WWW Setup
> **Note:** If you have made changes to the settings on the page before clicking Help and not saved them yet, a warning message is displayed. See Figure 1-12

- Yes and No radio buttons

These buttons are typically used to configure a setting that can be either enabled or disabled, and this setting has no effect on the visibility of other settings.

- Reset button

Reset button resets the fields to the values currently in use at Access Server or Access Point. In other words, the Reset button discards unsaved changes.
> **Note:** The Reset button does *not* make a "factory reset".

- Save button

Save button sends the WWW page to the setup application for validation. If the values in the fields are valid, they are permanently saved and the page is refreshed with the Changes have been saved. message at the top. The accepted values are shown in the page fields.

If there were errors in the fields, these are shown as in Figure 1-10.
> **Note:** It is typically necessary to reboot Access Server or Access Point for the changes to take effect. This can be done through the WWW interface (Advanced settings menu).

- Back link

Press the Back link to return to the previous level of the Setup menu hierarchy.
Note: Pressing the Back link does *not* save changes in the fields on the current page. Therefore, if there are changes not saved, a warning message is displayed, see Figure 1-12.
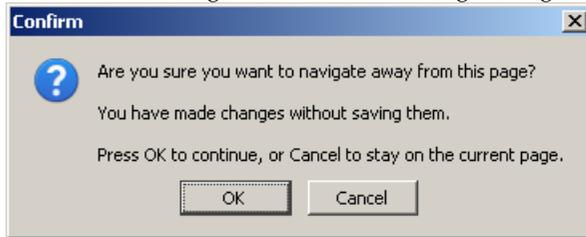
Figure 1-12. Warning Message of Changes not Saved

• Exit link

Exit link quits the setup application and returns to the Access Server's main WWW page.
Note: Pressing the Exit link does *not* save changes in the fields on the current page. Therefore, if there are changes not saved, a warning message is displayed, see Figure 1-12.

• Link to a configuration file

Some of the configurable settings are actually editable configuration files, such as `/etc/rc.d/rc.local` for Setup ⟶ Advanced setting ⟶ System startup script. Clicking the link will retrieve the file for editing in the browser window, or create a new file, if it does not exist. See Figure 1-13.
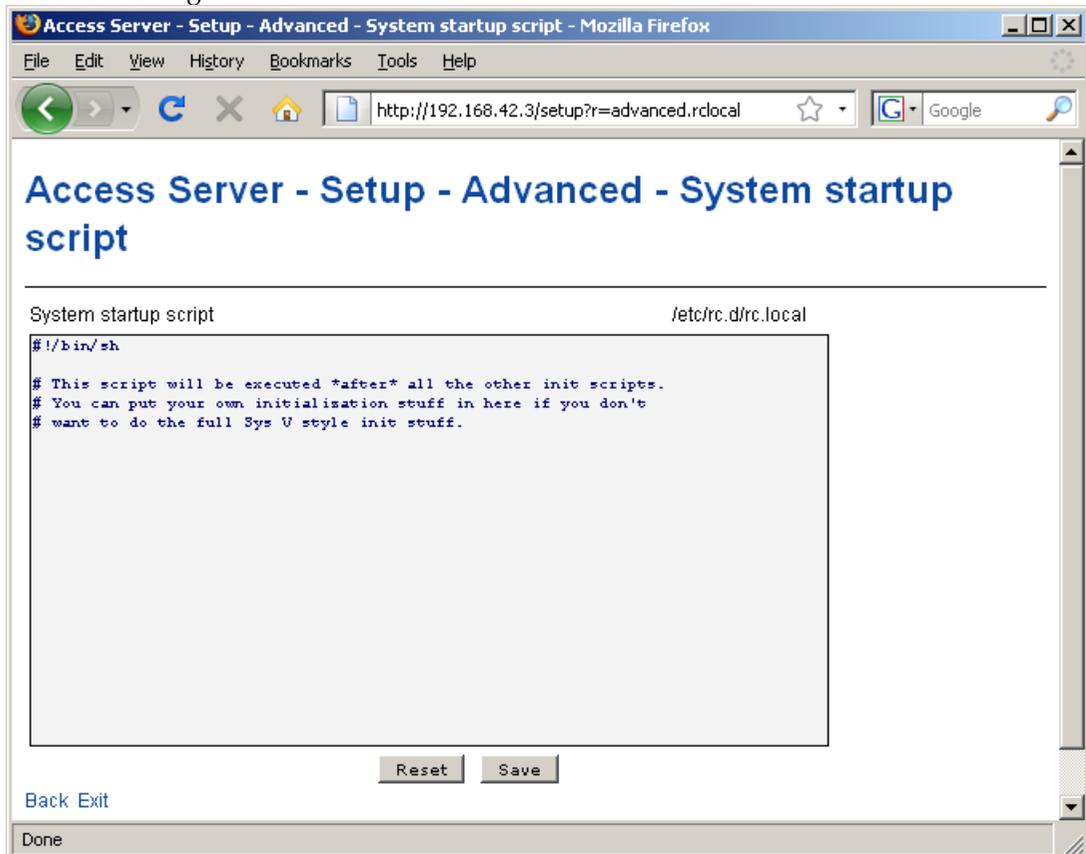
Figure 1-13. Editing Files in WWW Setup

> **Note:** You can edit any file through the WWW Setup. to edit files, navigate to Setup ⟶ Advanced setting ⟶ Edit other configuration files.

- Toggling Yes/No and on/off links

  Clicking the Yes/No link (see Figure 1-14) immediately changes the setting and saves the change. Typically these links are used to display or hide further settings.
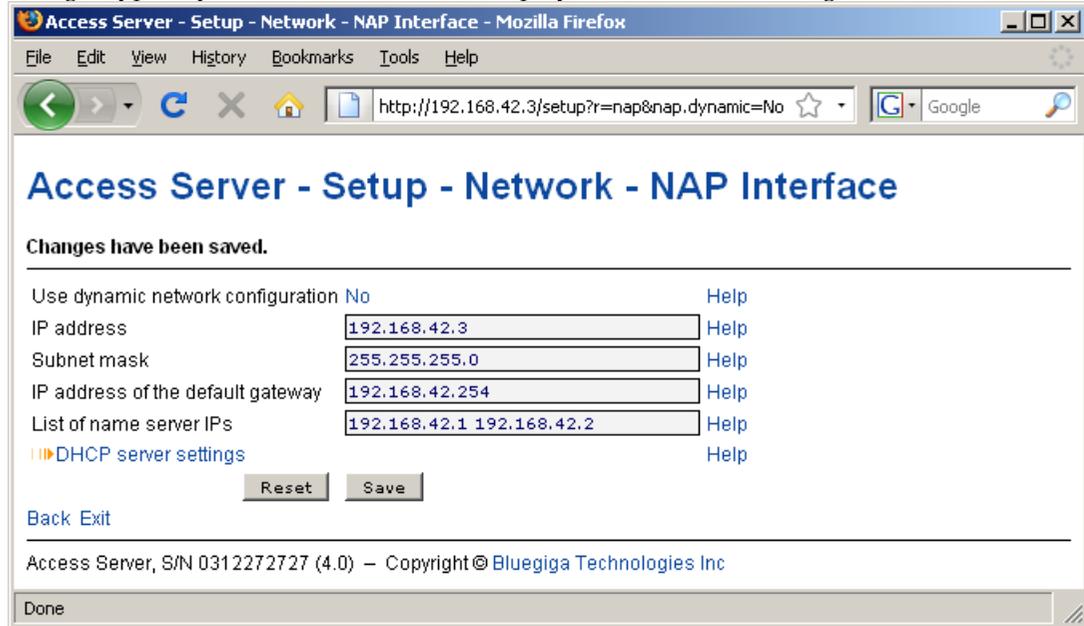
Figure 1-14. Yes / No links in WWW Setup

The on/off links in Setup ⟶ Applications ⟶ Default startup applications behave in a same way, making and saving the change immediately (see Figure 1-15).
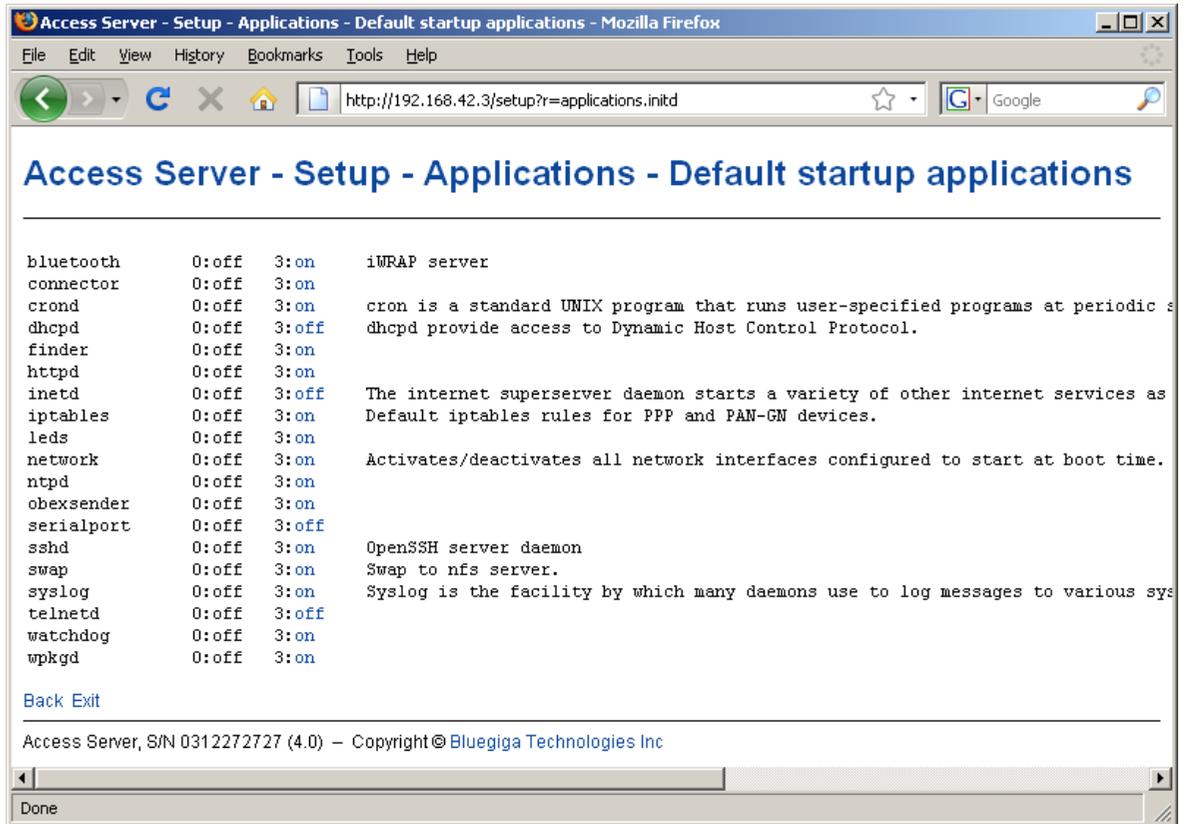
Figure 1-15. Selecting Default startup applications in WWW Setup

> **Note:** To configure the default startup applications from the command line, use the **chkconfig** command.

- Upload links

The WWW Setup has settings that allow user to upload files to Access Server or Access Point, for example Setup ⟶ Advanced ⟶ Upload a software update (see Figure 1-16).
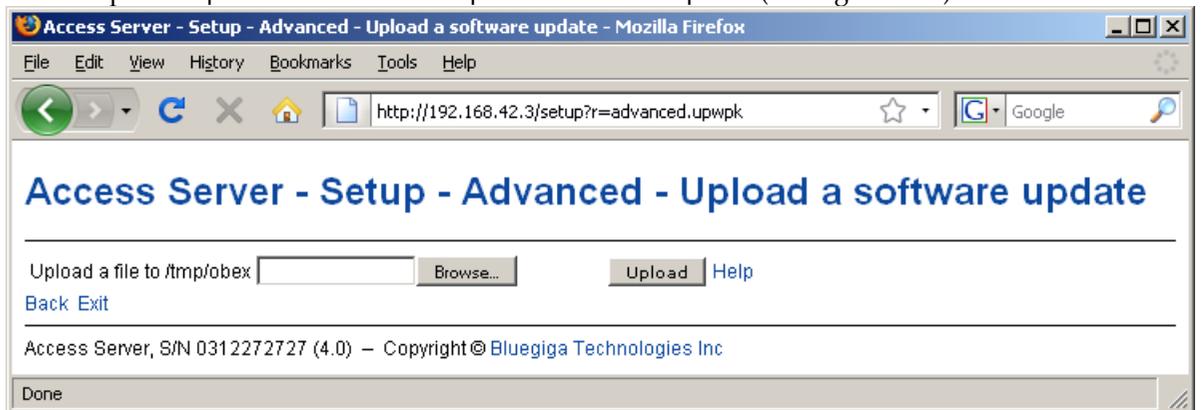
Figure 1-16. Uploading files through WWW Setup

Use the Browse... button to select the file to be uploaded, and send it to Access Server or Access Point by clicking Upload.

- Browsing files

  Some WWW Setup pages allow users to browse the file system or part of it, such as Setup ⟶ Advanced settings ⟶ Browse all files (see Figure 1-17).
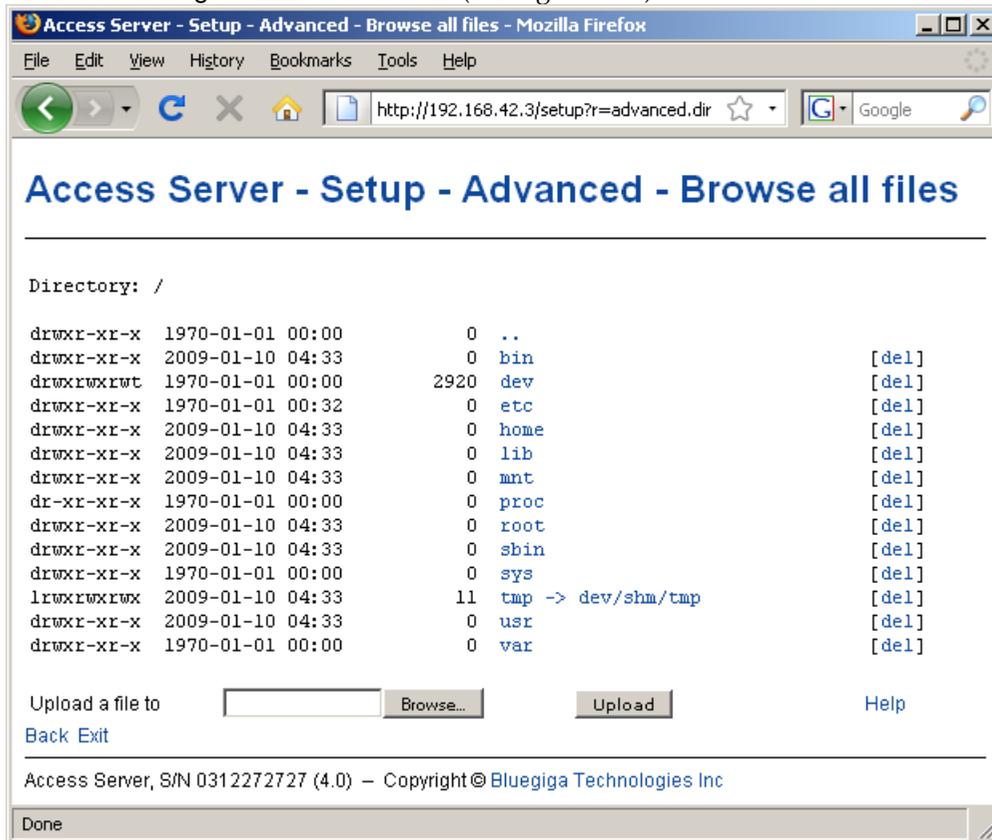
Figure 1-17. Browsing files via WWW Setup

Click the directory names to navigate in the file system.

Click a file name to view its contents.

> **Note:** Currently it is only possible to view contents of text files. It is not possible to download files, either.

Click del to delete a file or an empty directory.

Warning

You will not be asked for confirmation for the deletion.

The WWW Setup also has menu items that run commands in Access Server or Access Point, and show the output in the browser window. Some commands, such as rebooting the unit, require your confirmation before execution.

1.6. Using the setup Command Line Application

The basic configuration settings can also be changed by using the **setup** application at the command line interface.

The **setup** application displays the settings in a hierarchical menu (see Figure 1-18). Navigating the menu is accomplished by entering the number or letter corresponding to the setting to be viewed and/or changed and pressing **Enter**. Pressing only **Enter** either accepts the previous value of the setting or returns to the previous level in the menu hierarchy.
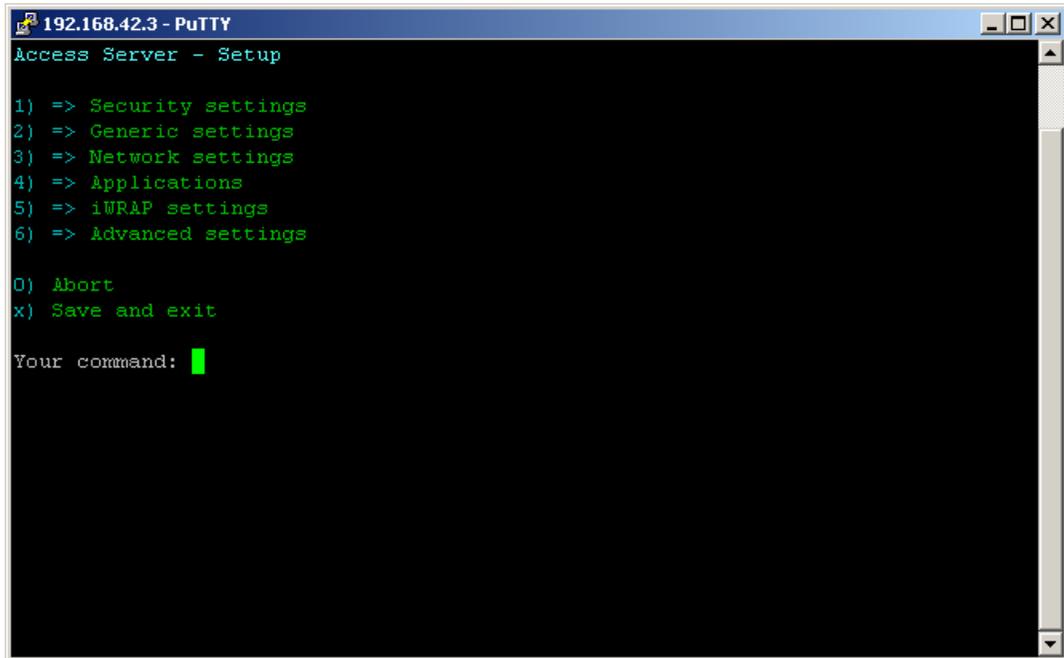
Figure 1-18. Using the setup Command Line Application

> **Note:** Ensure that your terminal application does not send line ends with line feeds. If your terminal sends both CR and LF when you press **Enter**, you cannot navigate in the **setup** application.

If you use the command line setup application, files are edited by default with the **vi** editor. If you want to use another editor, you can specify it in VISUAL environment variable.

You can not enable or disable default startup applications using the command line setup application. Use command **chkconfig *application on|off*** instead.

1.7. Resetting a Configuration

You can reset the default configuration with the **setup -r** command. The command requires rebooting of Access Server or Access Point. When the system starts up, the default configuration settings are restored. If you have only changed the configuration by using the **setup** application, the following commands at the Access Server's or Access Point's command prompt will suffice:

```
[root@wrap /]$ setup -r
[root@wrap /]$ reboot
```

> **Note:** This does not reset the edited files to factory defaults; it only affects the settings changed through the WWW Setup or the **setup** command line application. It does not uninstall extra applications installed by the user or reset Default startup applications settings, either. See Bluegiga Tech Forum (http://techforum.bluegiga.com/) for more information on how to perform a full factory reset.

1.8. Exporting and Importing Configurations

You can export configuration settings (expect for passwords and the list of default startup applications) by using the following command:

```
[root@wrap /root]$ setup -o > settings.txt
```

The saved settings can later be restored by using the following commands:

```
[root@wrap /root]$ setup -m settings.txt
[root@wrap /root]$ reboot
```