BLUEGIGA ACCESS DEVICES

USER GUIDE

Tuesday, 20 September 2011

Version 4.3

TABLE OF CONTENTS

1 Introduction

Bluegiga Access Server product family offers cutting-edge wireless *Bluetooth*® routers, Access Points and management tools - enabling you to create efficient and scalable networks. The open and adaptable platform enables you to meet your applications' and customers' needs.

Bluegiga Access Server AX4 is a powerful Linux based wireless connectivity platform targeted for eHealth, point-of-sale, proximity marketing, captive portal, and long range *Bluetooth* connectivity applications. The AX4 integrates three high performance *Bluetooth* class 1 radios, 802.11b/g radio and optional 2G or 3G modem.

Bluegiga Access Point 3241 is designed for various health and medical applications, *Bluetooth* proximity marketing, industrial telemetry applications, point of sales systems and digital pens. It provides with +20dBm *Bluetooth* output power and a low noise amplifier 1000 meters long range between other Access Point 3241 or *Bluetooth* device with matching output power and receiver sensitivity. Improved receiver sensitivy extends range also with class 2 *Bluetooth* devices like mobile phones.

Bluegiga Access Point 3201 is a size-optimized access device targeted at business applications. The product is designed to fit into wireless *Bluetooth* applications where network performance, reliability, scalability and easy management are important design drivers.

Access Point 3201 is an evolution from Bluegiga's extremely reliable and successful Access Server product family. Access Point product software and user interface make it compatible with Bluegiga Access Servers. Access Points can be remotely managed from a centralized location with Bluegiga Solution Manager (BSM), a web-based remote management and monitoring platform.

Access Server is a cutting edge wireless *Bluetooth* router. It supports multiple communication standards including ethernet, WiFi, and GSM/GPRS/3G enabling full media-independent TCP/IP connectivity. Access Server is easy to deploy and manage in existing wired and wireless networks without compromising speed or security. For rapid deployment, Access Server configurations can easily be copied from one device to another by using USB memory dongles. The device can be fully managed and upgraded remotely over SSH secured links. Large numbers of Access Servers can easily be controlled using Bluegiga Solution Manager (BSM).

Usage scenarios and applications:

- Medical and health device gateways
- Proximity marketing
- Point-of-sale and retail systems
- Telemetry and machine-to-machine systems
- Industrial *Bluetooth* gateways

Key features:

- Open Linux platform for adding local customer applications
- Turn-key applications for *Bluetooth* networking and *Bluetooth* proximity marketing
- Supported *Bluetooth* profiles: SPP, ObjP, FTP, PAN, LAP, DI, HDP
- Software-configurable range to up to 100 meters (up to 1000 meters with Access Point 3241 or Access Server AX4)
- External and internal antenna options
- Supports all key communication medias:
    - *Bluetooth*
    - Ethernet
    - WiFi, 2G/3G and NFC supported via USB (Access Server supports also via Compact Flash, AX4 has built-in support for WiFi and 2G/3G)
    - USB and RS232
- Fast and easy to install
- Uncompromised security: SSH, firewall, and 128 bit *Bluetooth* encryption
- *Bluetooth*, CE, FCC and IC certified
- Compliant with *Bluetooth* 1.1, 1.2 and 2.0 Specification (2.1 support with eHealth software)

2 Getting started with Bluegiga Access Device

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.

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

2.1 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 Devices 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 and AX4, also a direct ethernet cable works.

> ⚠ 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. Access Point and AX4, however, do 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.

2.1.1 Access Point connectors

The physical interface locations of Access Point 3201 and 3241 are shown below.

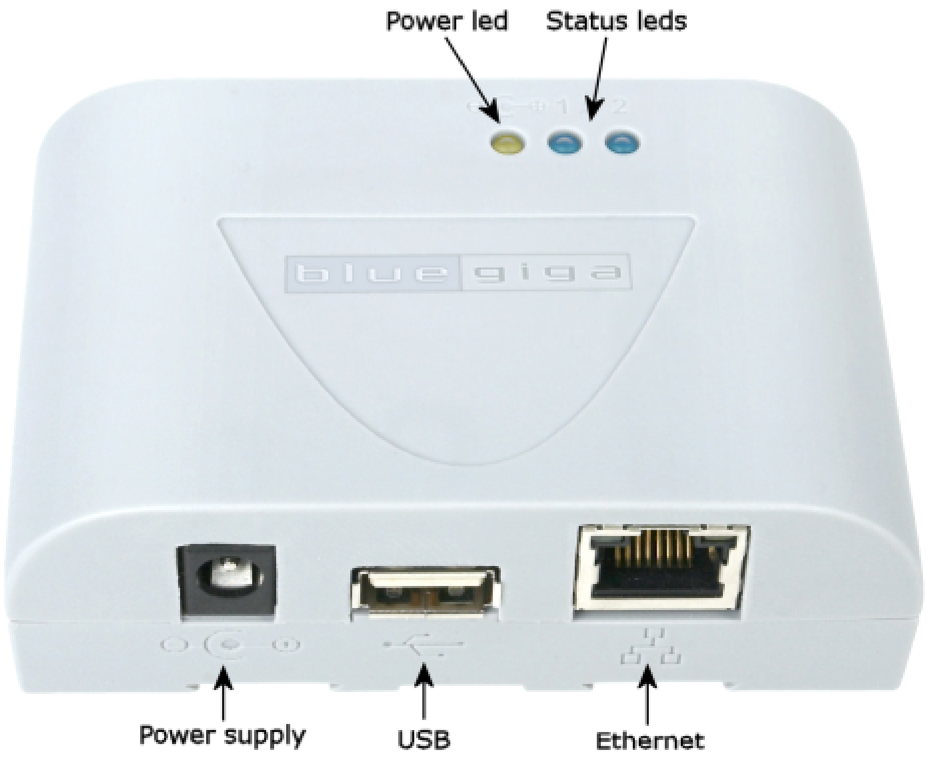


Figure 1: Physical interfaces of Bluegiga Access Point

In addition, Access Point 3241 has a hole in the bottom of the unit. Trough that hole user can press a button. If that button is pressed while the unit is powered on, configuration is reset to factory defaults.

> ⚠ There is no power switch in Access Point 3201 or 3241. 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 above is on when the power adapter is connected.

All the blue status leds are turned off and the status led number 1 blinks on four second intervals when the boot procedure is finished and the unit is ready to be connected. Led number 2 is *Bluetooth* led which blinks quickly every 30 seconds indicating *Bluetooth* service activity.

2.1.2 Access Server AX4 connectors

The physical interface locations of Access Server AX4 are described in figures below.

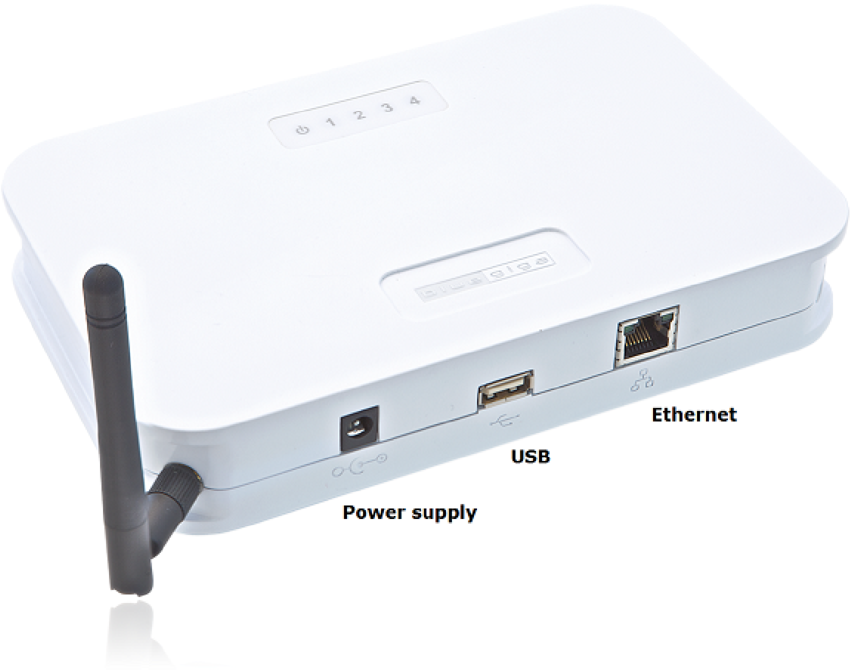


Figure 2: Physical interfaces of Bluegiga Access Server AX4

> ⚠ There is no power switch in Access Server AX4. 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 below is on when the power adapter is connected.

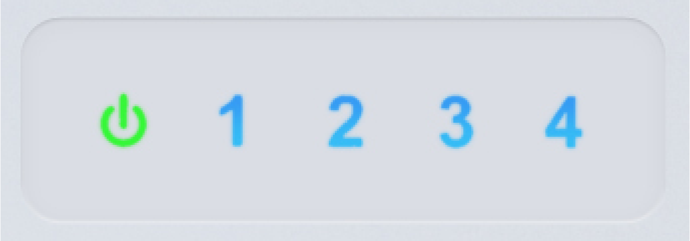


Figure 3: Access Server AX4 leds

All the blue status leds are turned off and the status led number 1 blinks on four second intervals when the boot procedure is finished and the unit is ready to be connected. Bluetooth led, (led number 4) blinks quickly every 30 seconds indicating *Bluetooth* service activity.

Access Server AX4 has microSD card slot, factory reset button and SIM card slot (for optional, integrated modem) under a cover in the bottom of the unit. See the picture below.

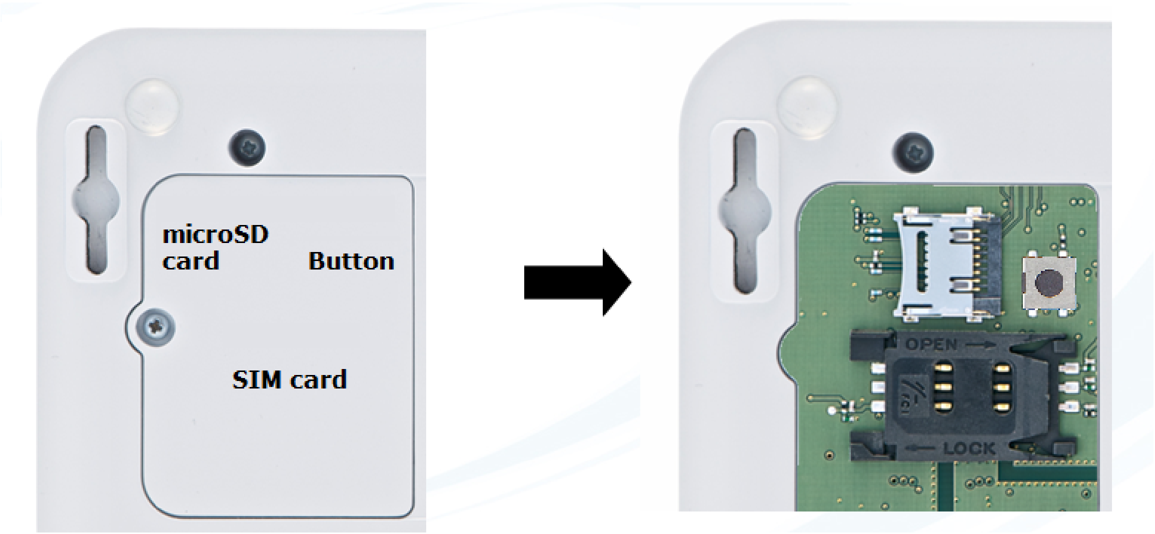


Figure 4: Connectors below Access Server AX4 bottom cover

2.1.3 Access Server connectors

The physical interface locations of Access Server 229x are described in figures below.

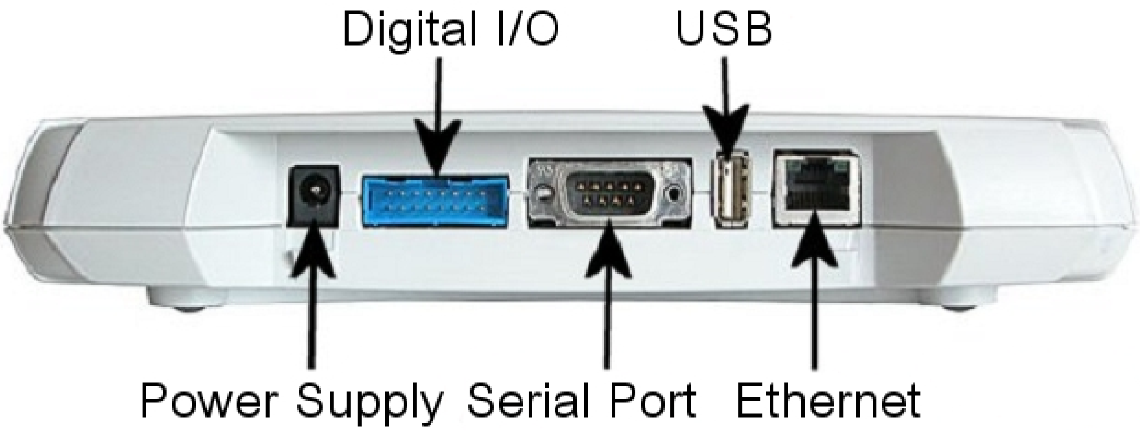


Figure 5: Physical interfaces of Bluegiga Access Server 229x

⚠ 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 above is on when the power adapter is connected.

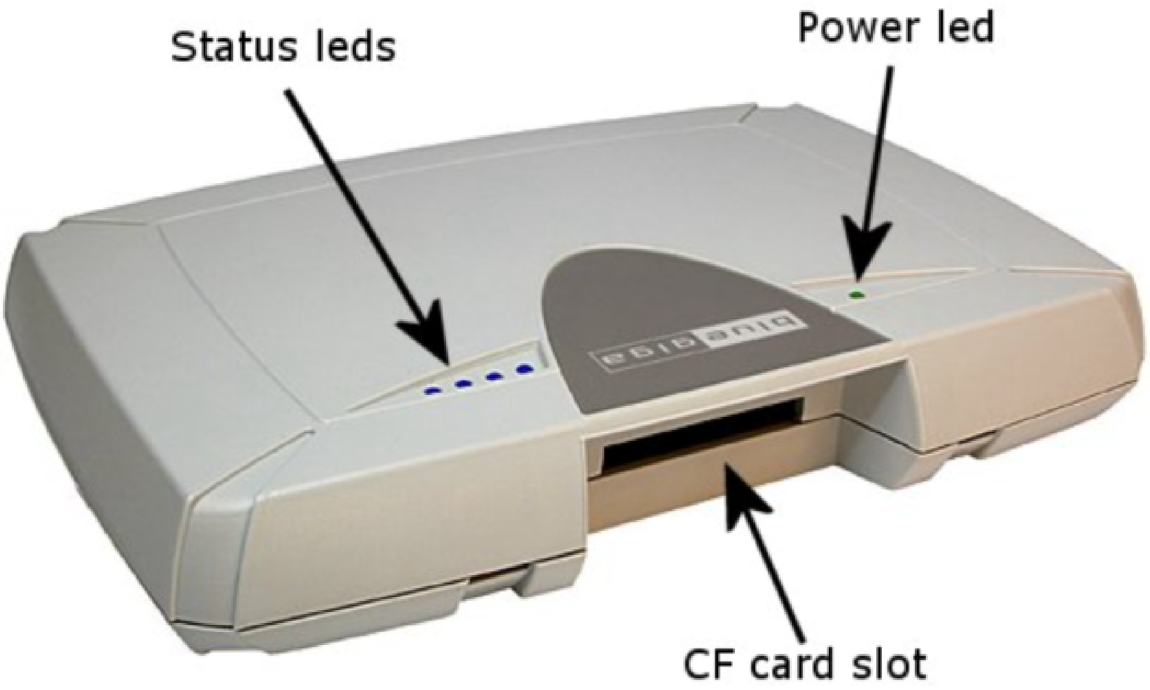


Figure 6: Leds and Compact Flash card slot of Access Server 229x

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

2.2 Connecting to Access Device

In order to manage your Bluegiga Access Device you need to be able to connect to it over the network. This can be done in two ways: either by having the Access Device directly connected to the PC via a crossover ethernet cable or by attaching the device to a switch in your local area network using a standard ethernet cable.

In the latter case, before continuing please make sure that your Access Device is powered on and properly connected to your network. Notice that, by default all Access Devices are configured to acquire their IP configuration from a DHCP server which must be present in the LAN. On the other hand, when PC and Access Device are connected directly, both will use a random zeroconf address in the range 169.254.x.x/16 given the lack of DHCP server in the simple network, and provided that also the PC is configured for dynamic IP configuration. Anyway, also in this case the two devices will be in the same LAN and will be able to communicate together.

Bluegiga Access Device can be managed either through a web browser or from the command line using SSH by advanced users. Both methods require you to know the IP address of your device, and this can be found by following the methods described below.

2.2.1 Using UPnP

To use the Universal Plug'n'Play feature for connecting Bluegiga Access Device web interface you need to have Windows Vista or Windows 7 operating system. Go to **Start - Computer - Network**. Now you should be able to see Access Devices appearing under **Other devices** group:

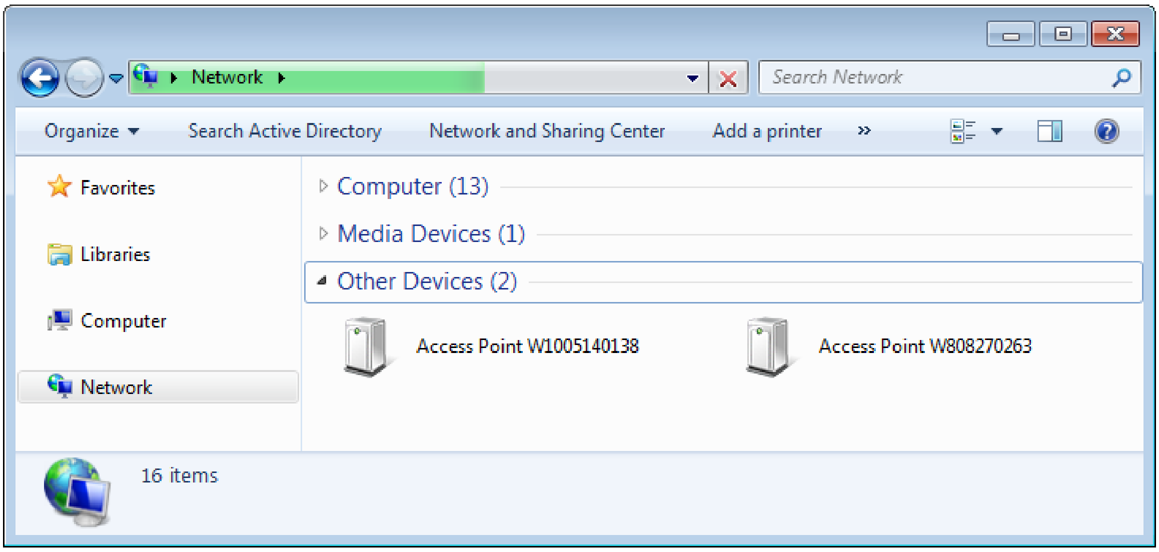


Figure 7: Windows 7 listing UPnP devices

Bluegiga Access Devices will have name "Access Point/Server Wserial number" where the serial number corresponds to the serial number in the sticker underneath the unit. To connect to Bluegiga Access Device web interface you can either double click the icon of the correct device or right click the icon and select **View device webpage**.

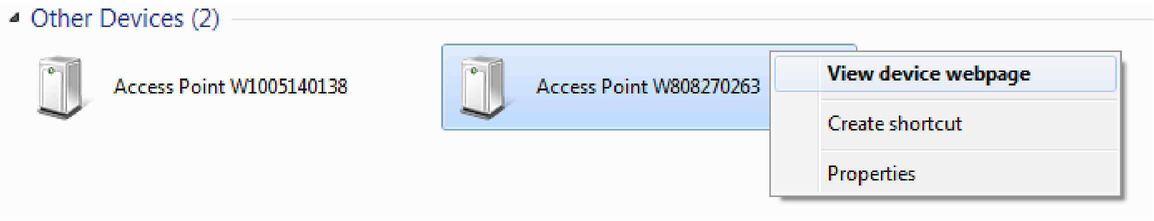


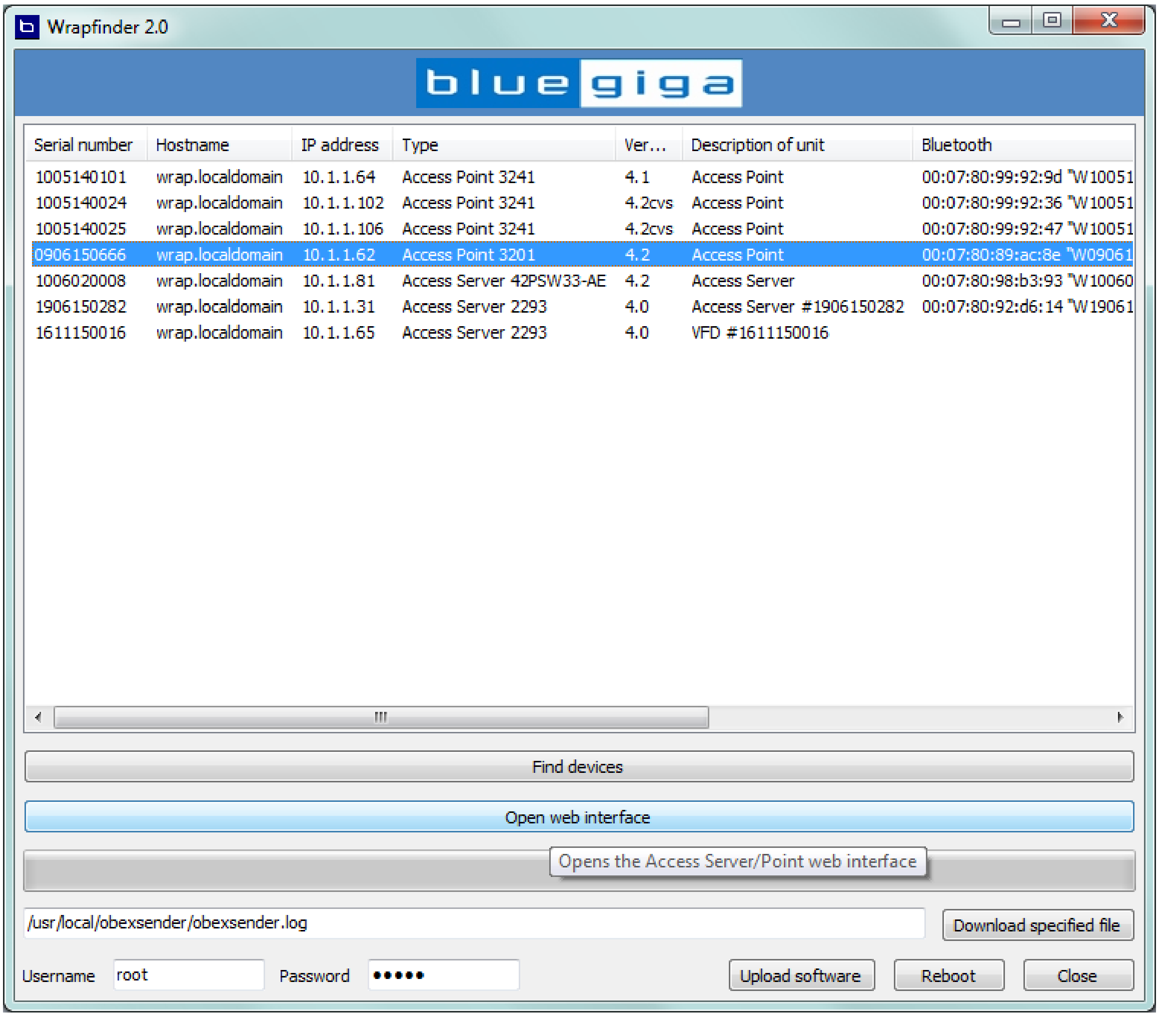
Figure 8: Connecting to web setup using UPnP

2.2.2 Using WrapFinder

A second way to discover the IP address of your Bluegiga Access Device is to use the **Bluegiga Wrapfinder 2.0** application. The **Bluegiga Wrapfinder** application is available from the Bluegiga Tech Forum. It allows you to scan and find all Bluegiga Access Devices that are present in your local network.

Once you have downloaded the Wrapfinder file from the Bluegiga Tech Forum you need to

1. Extract the .zip file to desired location
2. Launch *Wrapfinder2.exe*



Serial number	Hostname	IP address	Type	Ver...	Description of unit	Bluetooth
1005140101	wrap.localdomain	10.1.1.64	Access Point 3241	4.1	Access Point	00:07:80:99:92:9d "W10051
1005140024	wrap.localdomain	10.1.1.102	Access Point 3241	4.2cvs	Access Point	00:07:80:99:92:36 "W10051
1005140025	wrap.localdomain	10.1.1.106	Access Point 3241	4.2cvs	Access Point	00:07:80:99:92:47 "W10051
0906150666	wrap.localdomain	10.1.1.62	Access Point 3201	4.2	Access Point	00:07:80:89:ac:8e "W09061
1006020008	wrap.localdomain	10.1.1.81	Access Server 42PSW33-AE	4.2	Access Server	00:07:80:98:b3:93 "W10060
1906150282	wrap.localdomain	10.1.1.31	Access Server 2293	4.0	Access Server #1906150282	00:07:80:92:d6:14 "W19061
1611150016	wrap.localdomain	10.1.1.65	Access Server 2293	4.0	VFD #1611150016	

/usr/local/obexsender/obexsender.log

Username root Password ●●●●●

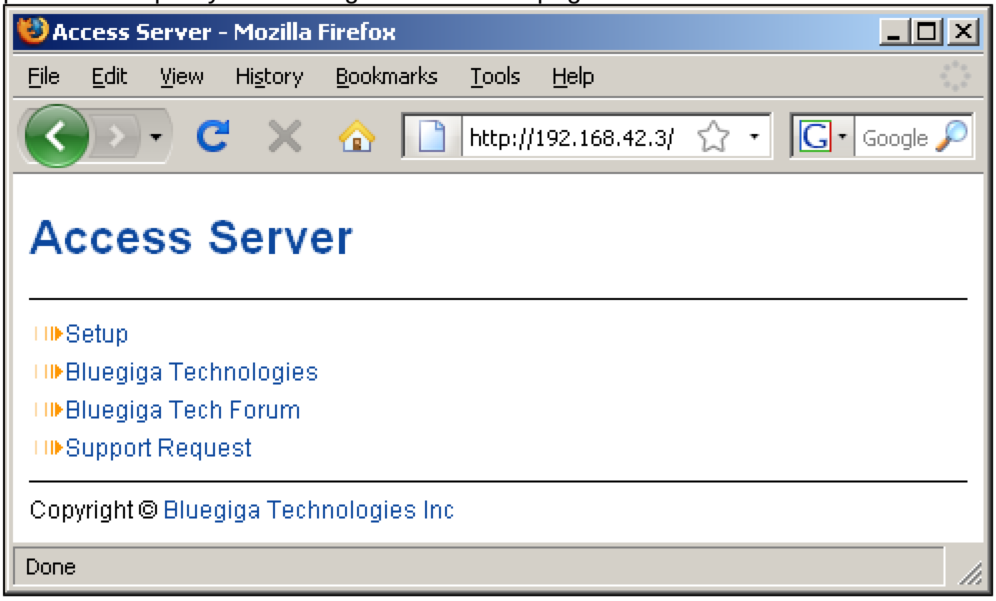
Figure 9: Wrapfinder 2.0 started listing Access Devices within local network

After you have started the Wrapfinder software you might be prompted by the firewall applications to allow the use of certain ports by Wrapfinder. There are cases in which it is wise to temporarily disable completely the software firewall running in the PC, if any. Once the Wrapfinder utility has started it automatically runs a search through the local network and lists all found Bluegiga Access Devices. You can refresh the search by clicking **Find Devices** -button. Sometimes on slow networks two consecutive presses are needed.

To access Bluegiga Access Device you can either double click it or select the one you want to connect to and click **Open web interface** -button.

2.3 Web interface

When you have accessed the Bluegiga Access Device web interface using either of the methods described in previous chapter you should get main WWW page shown below:


Access Server - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Google
Done

http://192.168.42.3/

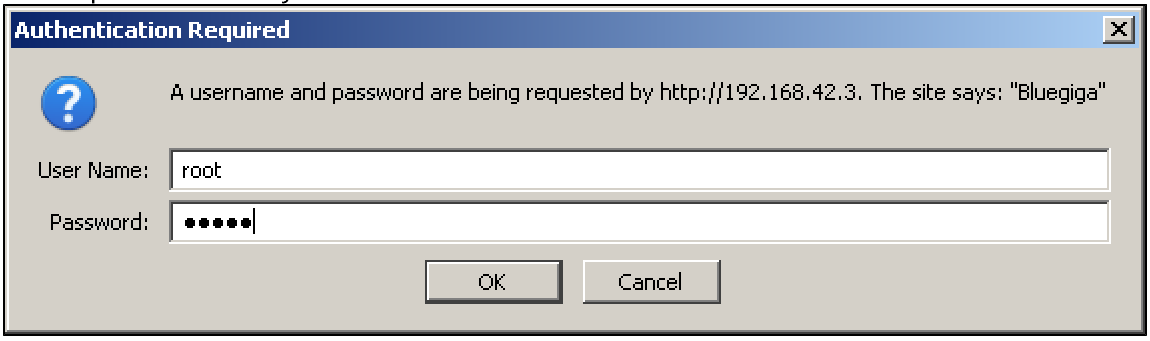
Access Server

- Setup
- Bluegiga Technologies
- Bluegiga Tech Forum
- Support Request

Copyright © Bluegiga Technologies Inc

⚠ If you see a login prompt instead of this page, you have already eHealth software bundle installed. See **eHealth software user guide** for more information.

From the top-level page, click **Setup** to log in to the configuration interface. The default username is *root* and the default password is *buffy*:

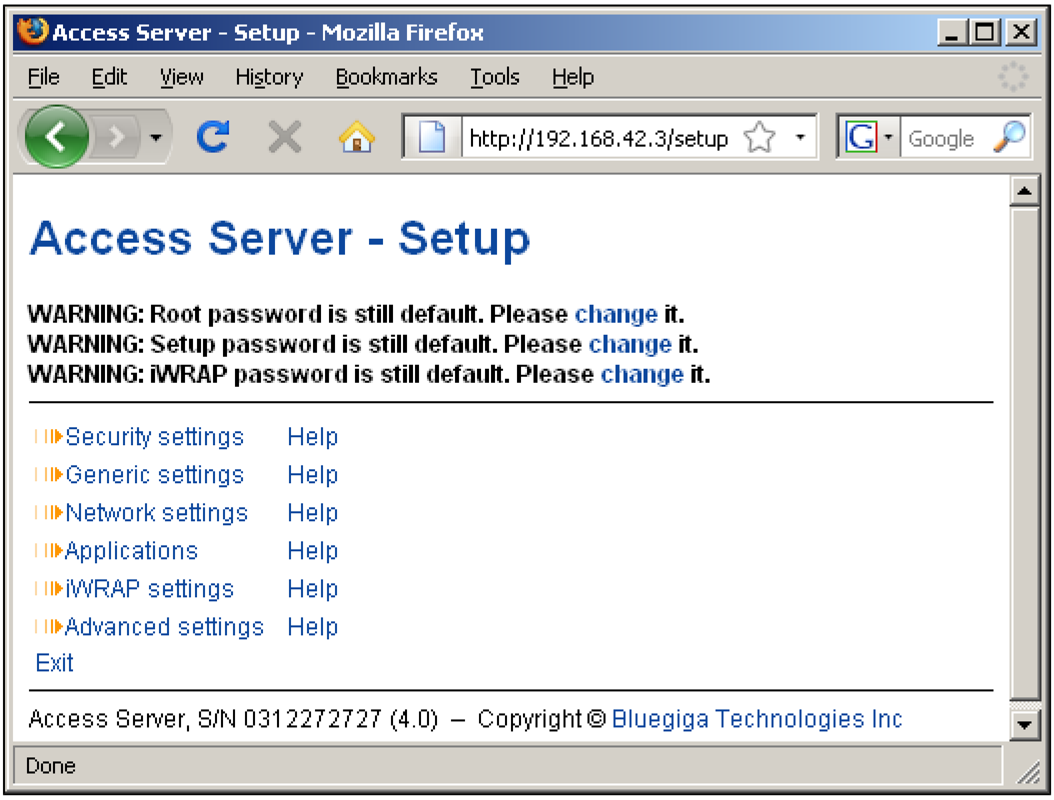


A username and password are being requested by http://192.168.42.3. The site says: "Bluegiga"

User Name: root

Password: •••••

After logging in, you can configure several system and application settings:


Access Server - Setup - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://192.168.42.3/setup
Google
Done

Access Server - Setup

WARNING: Root password is still default. Please change it.
WARNING: Setup password is still default. Please change it.
WARNING: iWRAP password is still default. Please change it.

Security settings	Help
Generic settings	Help
Network settings	Help
Applications	Help
iWRAP settings	Help
Advanced settings	Help
Exit	

Access Server, S/N 0312272727 (4.0) – Copyright © Bluegiga Technologies Inc

For details of WWW interface components, see **Default web interface and iWRAP Bluetooth user guide**.

2.4 Access Device software bundles

Access Device application use cases may require additional software packages to be installed for full functionality. For key applications, these are also available in software bundles. A bundle is a single update packet which contains all software packages for certain application. You can order Access Devices with a bundle of your choice pre-installed. Currently available bundles are listed below:

Table 1: Software bundles for Access Devices

Bundle name	Description	Notes
obexsenderbundle	ObexSender	Built in and installed by default if no other bundle was ordered. See separate ObexSender documentation.
ehealthbundle	eHealth software bundle	Only available for Access Point 3201 and 3241 in SW version 4.3. See separate eHealth user guide.
captiveportalbundle	Captive Portal bundle	See Captive Portal documentation.
oggplayerbundle	Ogg Player bundle	Available for testing purposes.

Bundles other than **obexsenderbundle** which comes inside system upgrade reflash packet are available on Access Device DVD in directory *wpk* or installable with command **wpkgd install *bundlename***. See Managing Software Components (wpkgd) for installation instructions.

3 Connecting Access Device to network

This chapter describes Access Device network interfaces and WiFi and modem configuration. For additional documentation, see separate "Networking Guide" document.

3.1 Network interfaces

The network interfaces used in Access Devices are described in table below:

Table 2: Access Device network interfaces and their description

Interface	Description
nap	Dynamic virtual ethernet ("cable") device. This is the device having an IP address. All the programs should use this device instead of eth0.
nap:9	Alias interface of nap device for zero configuration networking.
eth0	The real ethernet device, which is dynamically linked to the nap device. Do not use this device, use nap instead.
wlan0	Wi-Fi device. In the client mode (default), this device has its own IP address. In the access point mode, it is dynamically linked to the nap device (the default interface).
wifi0	Virtual control device for wlan0. Do not use this device.
gn	Virtual device for iWRAP *Bluetooth* PAN-GN connections.
bnep#	These devices are used for incoming and outgoing iWRAP *Bluetooth* PAN connections. These devices are created, deleted and linked (to nap or gn) dynamically.
ppp#	These devices are used for incoming and outgoing iWRAP *Bluetooth* LAP connections or for a modem Internet connection. In LAP use, these devices are created and deleted dynamically and traffic coming from them is masqueraded to the nap device. When modem is enabled, all traffic to ppp interfaces is also masqueraded.
lo	Local loopback interface.

3.2 Using 2G and 3G modems for Internet connectivity

Access Server and Access Point can be connected to Internet over 2G/3G using USB modems from several vendors. Access Server 229x can also connect to Internet using a GSM/GPRS Compact Flash card or an external modem connected to its serial port. The supported devices are listed in Tested 3rd Party Peripherals document.

Some Access Server AX4 models ship with integrated 2G or 3G modem.

Software packages required to use modem to connect to Internet are installed by default.

The operating system automatically identifies supported USB or Compact Flash modem devices and loads correct drivers when they are inserted.

You can enable the modem and configure its settings, such as the modem device and connection script details, by using the **setup** application or its WWW interface at **Setup - Network settings - Enable modem interface**

⚠ A reboot is needed for the new settings to take effect. From WWW Setup, you can do this at **Setup - Advanced settings - Reboot system (confirm)**.

When modem connection to Internet is enabled, by default Access Device tries to establish Internet connection with modem only once when the device boots up.

It is therefore recommended to enable option **Setup - Network settings - Modem settings - Force connection open**.

With this enabled, modem Internet connection is checked every 10 minutes with the **ping** command. If the check fails, modem connection is restarted.

> ⚠ Some modems power up in mass storage mode. Supported modems will be switched to modem mode automatically. Switching from mass storage mode to modem mode might take so long that first attempt to make a connection fails and there are no further tries if **Force connection open** option is turned off. Even if it is turned on, it can take up to 10 minutes before connection is properly established.

> ⚠ By default, **Force connection open** uses host 194.100.31.45 (bluegiga.com) for checking that the modem Internet connection is working. You might want to specify a reliable host closer to your system in **Setup - Network settings - Modem settings - IP address used in force check**. The test host must respond to ICMP ECHO_REQUEST packets generated by **ping** command, otherwise the modem connection is reset every ten minutes.

> ⚠ If you also want to use the ethernet connection, you must remove it from the default interface (*nap*) bridge and configure its network settings individually using the **setup** application while keeping the default interface network settings in their default (dynamic) state.

3.3 Using Wi-Fi

AX4 is delivered with integrated Wi-Fi. All Access Devices support several USB Wi-Fi dongles. The supported devices are listed in Tested 3rd Party Peripherals document.

> ⚠ Ad hoc mode is not supported.

> ⚠ WPA/WPA2 passphrase length must be 8..63 characters.

3.3.1 Using Wi-Fi as Client (Managed)

USB Wi-Fi client device support (including *wpa-supplicant* for WPA or WPA2 encryption support) is installed by default.

Enable Wi-Fi interface using the **setup** application or its WWW interface at **Setup - Network settings - Enable Wi-Fi interface**.

When the correct kernel modules are installed and Wi-Fi interface enabled, Access Device notices when a supported Wi-Fi card is inserted and tries to use it in the client mode, without encryption. So, if there is an open Wi-Fi access point in range, you will automatically connect to it.

To change Wi-Fi settings, use the **setup** application or its WWW interface at **Setup - Network settings - Wi-Fi settings**. *Wpa-supplicant* is used to manage Wi-Fi connections. Supported encryption methods are WEP and WPA/WPA2. Use the **Edit configuration file** menu option to change network SSID and encryption method.

Use following configurations to enable unencrypted, WEP or WPA/WPA2 encrypted connections:

- no encryption

```
network = {
    # no encryption
    ssid="Bluegiga"
    key_mgmt=NONE
}
```

- WEP

  ```
  network = {
      # WEP encryption
      ssid="Bluegiga"
      key_mgmt=NONE
      wep_key0="ASCII WEP key"
      #wep_key0=0123456789
      wep_tx_keyidx=0
  }
  ```

  - ASCII WEP key is given in quotes (e.g. "abcde" or "abcdeabcdeabc")
  - hex digits are given without quotes (e.g. 0123456789 or 01234567890123456789012345)

- WPA/WPA2

  ```
  network = {
      # WPA/WPA2 encryption
      ssid="Bluegiga"
      scan_ssid=1
      key_mgmt=WPA-PSK
      psk="WPA shared key"
  }
  ```

  - shared key length must be 8..63 characters

> ⚠ A reboot is needed for the new settings to take effect. From WWW Setup, you can do this at **Setup - Advanced settings - Reboot system (confirm)**

> ⚠ The current software version does not support Wi-Fi bridging in the client (managed) mode, which means that traffic from Wi-Fi cannot be forwarded to wired ethernet.

To debug Wi-Fi issues, you can collect and review Wi-Fi diagnostics information using **setup** application or its WWW interface at **Setup - Network settings - Wi-Fi settings - Collect Wi-Fi diagnostics**.

In addition, a standard set of command line wireless utilities is provided to fine-tune your Wi-Fi configuration:

- **iwconfig**
- **iwlist**
- **iwpriv**

For more information on these utilities, see: http://www.hpl.hp.com/personal/Jean_Tourrilhes/Linux/Tools.html

3.3.2 Using Wi-Fi as Access Point (Master)

Please refer to Tested 3rd Party Peripherals document to see which USB Wi-Fi dongles support access point mode. The required software packages are installed by default.

Enable Wi-Fi interface using the **setup** application or its WWW interface at **Setup - Network settings - Enable Wi-Fi interface**.

To change Wi-Fi settings, use the **setup** application or its WWW interface at **Setup - Network settings - Wi-Fi settings**.

To begin with, change the setting **Act as a Wi-Fi Access Point** to **yes**. *Hostapd* is used by default to manage Wi-Fi access point mode.

To change *hostapd* settings, use the **setup** application or its WWW interface at **Setup - Network settings Wi-Fi**

settings - Basic configuration. **Basic configuration** settings is used to change hostapd driver backend, SSID of your network, hardware mode, country code, Wi-Fi channel or maximum simultaneous client number. Default values should work with most of USB Wi-Fi dongles.

Depending on used encryption, use **Edit configuration file** menu option and change the following lines:

- No encryption
  Change nothing more.

- Typical WPA2 encryption (WPA2-CCMP (AES))

  ```
  wpa=2
  wpa_passphrase=verysecretpassphrase
  rsn_pairwise=CCMP
  ```

Other encryptions:

- WEP encryption

  ```
  wep_default_key=0
  wep_key0="mysecretkey
  ```

- WPA-TKIP

  ```
  wpa=1
  wpa_passphrase=verysecretpassphrase
  ```

- WPA2-TKIP

  ```
  wpa=2
  wpa_passphrase=verysecretpassphrase
  ```

- WPA-TKIP and WPA2-TKIP

  ```
  wpa=3
  wpa_passphrase=verysecretpassphrase
  ```

- WPA-CCMP (AES)

  ```
  wpa=1
  wpa_passphrase=verysecretpassphrase
  wpa_pairwise=CCMP
  ```

- WPA2-CCMP (AES)

  ```
  wpa=2
  wpa_passphrase=verysecretpassphrase
  rsn_pairwise=CCMP
  ```

- WPA-CCMP and WPA2-CCMP (AES)

  ```
  wpa=3
  wpa_passphrase=verysecretpassphrase
  wpa_pairwise=CCMP
  rsn_pairwise=CCMP
  ```

3.4 Shell prompt access

Shell prompt access may be needed for advanced controlling operations that cannot be performed 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 uPnP or **wrapfinder** application (see Getting started with Bluegiga Access Device).

You can use SSH to get shell prompt access also using Bluetooth LAN Access or PAN profile. Access Devices 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 and AX4 have 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. Again, you can use the **wrapfinder** application to find the IP address.

⚠ 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://update.bluegiga.com/as/4.3/misc/enable-pan.noarch.wpk) to Access Device by using Bluetooth Object Push profile or by inserting a USB memory dongle with the file in its root directory to Access Device's USB port.

3.4.1 Management console (Access Server 229x 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

Table 3: Management console serial port settings

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

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.

> ⚠ 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.

3.4.2 Transferring files to/from Access Device

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**.
- 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.
- USB memory dongle.
- Xmodem/Ymodem/Zmodem (use **rz/rx/rb/sz/sx/sb** commands from the management console). You can install these commands from software package *rzsz*.

> ⚠ The management console is only available for Access Server 229x.

4 Using services

This chapter contains documentation of the default system services available in Access Devices.

4.1 Default services

Access Device services are started automatically at system power-up or when another server daemon needs them. You can check which servers are currently installed and/or configured to start at system power-up with command **chkconfig --list** or navigating in WWW Setup to **Setup - Applications - Default startup applications**.

The servers and their purposes are described briefly below:

Server	Description
bluetooth	Bluegiga iWRAP *Bluetooth* Server, which is described its own user guide.
connector	Bluegiga Connector, which automatically opens and maintains connections to specified *Bluetooth* devices. This server is configurable using the **setup** application and its WWW interface.
crond	A daemon to execute scheduled commands. This server is configurable through the */var/spool/cron/crontabs/root* file or the **crontab** command in the same way as any Linux crond.
dhcpd	This server is a DHCP daemon for providing automatic network configuration for clients in the network. Notice that, by default, this server is only enabled for the *gn* interface, used by iWRAP *Bluetooth* PAN Generic Networking profile. You can enable it for *nap* interface by using command **chkconfig dhcpd on** or from WWW Setup at **Setup - Applications - Default startup applications**. You will then need to configure static network settings at **Setup - Network Settings - Default interface settings** and ensure you have matching DHCP server settings in file */etc/udhpcd-nap.conf*.
finder	Bluegiga WRAP Finder Service. See Finder - Bluegiga Access Device Finder
httpd	Web server. Another Web server, **lighttpd**, is available as a separate software component, also installed and used by **captiveportalbundle** and **ehealthbundle**.
inetd	Internet services daemon. Notice that this server is disabled by default. Use the WWW interface of **setup** application or the **chkconfig inetd on** command to enable it. To configure **inetd**, edit its configuration file */etc/inetd.conf*.
ntpd	Network Time Protocol (NTP) daemon.
obexsender	Bluegiga ObexSender server. See separate documentation for detailed information.
pppd	Point to Point Protocol daemon. Modem network connections are established using **pppd**, and iWRAP *Bluetooth* server uses it with Lan Access Profile.
serialport	Bluegiga iWRAP *Bluetooth* Serial Port Profile server. iWRAP Bluetooth user guide for more information.
sshd	SSH daemon.
syslogd	System logging daemon. This server can be configured by using the **setup** application or its WWW interface.
telnetd	Telnet protocol server. Notice that this server is disabled by default for security reason. Use the **setup** application or the **chkconfig telnetd on** command to enable it.
udhcpcd	DHCP client daemon for automatic network configuration.
watchdog	Bluegiga user level watchdog.
wpkgd	Bluegiga package management system daemon.
zcip	Zero configuration networking service.

4.2 Managing software components (wpkgd)

To maximize memory available for customer applications, Access Devices ship with minimal amount of software components installed.

To see the installed software components and their version numbers, navigate to **Setup - Advanced - System Information - List installed software components** or give command **wpkgd list** at the shell prompt. See Available Software Packages for more information of software components installed by default and available separately.

Software component package naming

Software components are delivered in package files which are named in format *name-[version].[architecture].wpk*. For example: *smsgw-20100420-1.lt.wpk* is **smsgw** software component, version number 20080910-1, for **lt** architecture. You can only install a software package of a specific architecture to hardware that supports the architecture. The architectures and the supporting hardware are listed in following table

Table 4: Supported hardware architectures and software package naming

Architecture	Supporting Hardware
noarch	Any Access Device
hp	Access Server AX4
lt	Access Point 3201 or Access Point 3241
if	Access Server 229x with serial number 0607240000 or higher
df	*Not supported since software version 4.0*. Access Server 229x with serial number 0607239999 or lower (old non-RoHS Access Servers)

Installing software components

There are number of ways to install software components:

1. The easiest way to install a software component is to upload it from WWW Setup at **Setup - Advanced settings - Upload a software update**.
2. You can install software components by inserting a USB dongle with the WPK file containing the software installation packet in its root directory.
3. You can install software components by transferring the WPK file to */tmp/obex* directory on Access Device using SCP or *Bluetooth* Object Push. WPK files are automatically searched and installed from */tmp/obex*.
4. If you can access the command prompt of your Access Device and your device has access to Internet, you can manage software components using network update operations described in the section below.

The WPK files of additional software components provided by Bluegiga can be found in following locations:

- http://update.bluegiga.com/as/4.3/hp for Access Server AX4 software
- http://update.bluegiga.com/as/4.3/lt for Access Point 3201 or 3241
- http://update.bluegiga.com/as/4.3/if for Access Server 229x
- http://update.bluegiga.com/as/4.3/misc for software packages (utility WPK's) for all architectures
- *wpk*-directory in Bluegiga SDK DVD-ROM or ISO image
- After Bluegiga SDK is installed, in corresponding application and library directories under */home/user/asdk/*-directory

Uninstalling software components

You can uninstall software components from the shell prompt. To list installed software components use command **wpkgd list**. To uninstall a component, use command **wpkgd erase [component]**. See the **wpkgd** command without parameters for more information.

Network update operations

When Access Device is connected to the Internet, you can use the **wpkgd** command at the shell prompt to easily manage installed software components:

wpkgd install *pkg* installs the newest available software component called *pkg* for your architecture. The software is retrieved from the Bluegiga software update repository. Example:

```
[root@wrap root]$ wpkgd install smsgw
Downloading http://update.bluegiga.com/as/4.3/lt/smsgw-20100420-1.lt.wpk
Package "smsgw" installed
```

⚠ Currently the command **wpkgd install *pkg*** may report that software is installed even if the installation has failed because of failing dependencies. It is therefore worth ensuring that the installation has been successful, by using command **wpkgd search *pkg***

wpkgd erase *pkg* removes a software component called *pkg*. Example:

```
[root@wrap root]$ wpkgd erase smsgw
Purging smsgw (0100420-1)...
```

wpkgd update updates all installed software components.

wpkgd update *pkg* updates the software component called *pkg*.

wpkgd list lists installed and available software components and their version numbers.

wpkgd list-updates lists updates available for installed software components.

wpkgd search *keyword* searches for software component packages with name matching *keyword*.

wpkgd clean cleans network cache.

4.3 Bluetooth

Access Devices ship by default with iWRAP *Bluetooth* software. It is documented in its own user guide.

eHealth software bundle installs newer DBUS *Bluetooth* software, which is documented in eHealth user guide.

4.4 Web server

The integrated web server in Access Device support HTTP/1.0 methods GET and POST, and has light user authentication capabilities. The content can be either static or dynamic - the WWW server is CGI/1.1 compatible.

The web server is always running and the content (http://wrap-ip-address/) is located in the `/var/www/html/` directory in Access Device's file system.

The web server is configured to protect the WWW Setup interface with a username and password. The default username and password can be changed in **WWW Setup Security settings Setup password**. For further information about using the web server for your own applications, see the web examples in SDK.

Note
eHealth and Captive Portal bundles install more advanced **lighttpd** web server, which can be installed from its own software package also.

4.5 System time

Access Device has Real Time Clock (RTC) which is backed up with a battery so it runs even when device is powered down. Access Device is also keeping the system time in sync with Internet time servers.

4.5.1 Real time clock (RTC)

The system clock is read from the battery operated real time clock during boot. The system time is automatically written to the real time clock when the system is rebooted using the **reboot** command. This can also be done using the **hwclock --systohc --utc** command. Give command **hwclock --help** for more information about the **hwclock** utility.

Tip
Easiest way to set correct time is to use `setup` application or its WWW interface by navigating to **Setup Network settings Update current time now by NTP**. It will also save the time to the battery operated real time clock.

4.5.2 Network time

The **ntpd** service uses the standard Network Time Protocol (NTP) to keep Access Device system time automatically in sync using a random selection of eight public stratum 2 (NTP secondary) time servers. You can configure the NTP server to retrieve the correct time from a single time server by using the setup application or its WWW interface, at **Setup Network Settings Update current time now by NTP**. The service is also configured to answer NTP requests from other devices.

The NTP server configuration can also be altered by editing its configuration file */etc/ntpd.conf*.

Tip
Access Device can provide RFC 868 time service with **inetd** daemon. You need to enable **inetd** daemon at **WWW Setup Applications Default startup applications** and enable the time service by editing its configuration file */etc/inetd.conf*.

4.5.3 Time zones

The default time zone in Access Server and Access Point is UTC. You can change it by installing correct *tzdata*wpk* management packet, available from http://update.bluegiga.com/as/4.3/timezone/ or Bluegiga Software Development Kit DVD-ROM. eHealth software bundle contains improved WWW interface to select correct time zone.

4.6 Using remote file shares

4.6.1 Using NFS mount

First, create a mountpoint with command **mkdir -p /mnt/nfs**. To use the NFS mount, issue a command such as **mount -o nolock <ipaddr-of-server>:/sharename /mnt/nfs**. After this, you can access the share in directory */mnt/nfs*.

When the share is not needed, unmount it with command **umount /mnt/nfs**

4.6.2 Using CIFS mount

To use a CIFS mount (for example a shared folder in Windows), you need the *cifs-client* software component installed in Access Device.

First, create a mountpoint with command **mkdir -p /mnt/cifs**. Mount the directory by using command **mount.cifs <ipaddr-of-server>/sharename /mnt/cifs -o user=username,nounix**. You will then be prompted for password of the username you specified. After entering the correct password, you can access the share in directory */mnt/cifs*.

When the share is not needed, unmount it with command **umount /mnt/cifs**

4.6.3 Mounting at boot time

System startup script *rc.local* which is editable in **WWW Setup - Advanced Settings - System startup script** can be used to automatically mount remote file shares at bootup. Add the mountpoint creation and actual mount commands in that script. If your CIFS share needs a password, it can be added to mount options, for example **-o user=username,pass=password,nounix**.

4.7 Factory reset and complete system upgrade (reflash)

Bluegiga Access Devices can be returned to default settings using three ways:

1. Configuration reset using factory reset button (Access Point 3241 and Access Server AX4 only), useful for example for restoring default network settings
2. Complete system upgrade using "reflash" WPK package (over WWW interface, SSH or with USB memory dongle), recommended when you want to install latest software
3. Kernel, filesystem and configuration restore with special "Factory Reset" USB memory dongle, useful if system has been corrupt and does not boot properly for methods above to work

4.7.1 Resetting default system configuration with factory reset button

Access Point 3241 and Access Server AX4 can be resetted to its default configuration by keeping the button in the bottom of the device pressed while it is powered up. The device will then boot, reset system configuration settings and restore default configuration files and reboot itself. You can also run command **configreset** from shell prompt to perform same reset (especially in Access Server 229x which does not have a button).

> ⚠ Factory reset with button press does not uninstall applications or recover deleted application files. To perform this, a factory reset with reprogramming is required, see below.

4.7.2 Complete system upgrade (reflash)

The latest software updates and instructions are available at http://techforum.bluegiga.com

> ⚠ Upgrading with a reflash package, which will erase all existing information, reset all passwords to their defaults and regenerate SSH keys.
> If you have your own applications running in the Access Device you plan to upgrade, stop and backup their data first.

The easiest way to install the latest software version is to do it with a USB memory dongle:

1. Find the correct software upgrade packet for your Access Device's architecture (see Managing Software Components (wpkgd) for information of architectures) and copy the correct *reflash-[version].[architecture].wpk* file to an empty USB memory dongle.
2. Power down Access Device.
3. Insert the dongle in Access Device.
4. Power up Access Device.
5. Wait with the dongle inserted for Access Device to boot and the blue leds to start blinking from side to

side.

> ⚠ Do not power down Access Device while blue leds are blinking from side to side or if all of them are turned on.

Installation takes 5-15 minutes (in AX4 less than 5), be patient.

6. Check that only led labeled "1" in Access Point or AX4 (blue led closest to the power led in Access Server 229x) turns on and off every 4 seconds. You will then also see Bluetooth led, (led labeled "2" in Access Point, "4" in AX4 and blue led furthest away from power led in Access Server 229x) to blink quickly every 30 seconds indicating iWRAP Bluetooth service activity.
7. You have now successfully upgraded Access Device.

If you hear beeps (in case of Access Server) and all blue leds start blinking on and off at the same time, you have tried to upgrade with a wrong *reflash-[version].[architecture].wpk* packet. You can confirm this from a log file in the root directory of your USB dongle. The log file is a *txt* file named using the software upgrade packet's filename and system timestamp. Please check again which file you should have used with help from Managing Software Components (wpkgd) and try again.

In some rare occasions the update process of an old Access Server may hang. If after 15 minutes all blue leds are still on, please power down Access Server, remove duplicate install protection file called *reflash-[version].[architecture].wpk.dupe* from USB dongle and restart the installation process.

Instead of using a USB dongle, you can install software upgrade by uploading the packet with WWW Setup at **Setup Advanced settings Upload a software update**.

You can also install software upgrade by uploading it to directory */tmp/obex* using SSH (SCP).

4.7.3 Kernel, filesystem and configuration restore with "Factory Reset" memory dongle

Access Device can be reprogrammed with the latest software version, erasing all data and recovering a system that does not boot up normally.

> ⚠ The latest software updates and instructions are available at http://techforum.bluegiga.com/.

The easiest way to install the latest software version is to do it with a USB memory dongle:

1. Copy `kernel.*` and `root.*` files to an empty USB memory dongle. You can find these files inside *factoryreset.zip* available at http://techforum.bluegiga.com/, or in directory *dev/shm/phantom* inside *reflash*.wpk* packets (just rename the packets to **.tgz* files and unpack with for example **tar** or **WinZip**)
2. Insert the dongle in Access Device.
3. Power up Access Device.
4. Wait with the dongle inserted as long as all blue leds are on. You will need to wait for 5 minutes when reprogramming Access Point and 10 minutes when reprogramming Access Server (less than 5 minutes when reprogramming Access Server AX4).
5. Check that only led labeled "1" in Access Point or AX4 (blue led closest to the power led in Access Server) turns on and off every 4 seconds. You will then also see Bluetooth led, (led labeled "2" in Access Point, led labelled "4" in AX4 and blue led furthest away from power led in Access Server) to blink quickly every 30 seconds indicating Bluetooth service activity.
6. You have now successfully reprogrammed Access Device.

5 Using utilities

Access Device ship with many standard Linux utilities pre-installed.

Most of the utilities are part of BusyBox; see Enabled Busybox Applets for complete list of enabled BusyBox commands.

For a complete list of all installed and available utilities and software packages, see Available Software Packages.

5.1 Wrapid - Bluegiga Access Device System Information

You can get detailed information of Access Device hardware and software at **WWW setup Advanced settings Hardware information**. At shell prompt, running command **wrapid** outputs the same information.

If you need to use a hardware information detail for example in your own shell scripts, you can ask it directly with **wrapid** command. Run it with parameter *--help* for list of queries it supports (hardware serial number, software version number and so on).

5.2 Changing the Bluetooth Range and EDR Performance

The *Bluetooth* transmit power of Access Device is configurable.

By default, class 1 settings for maximum range are used. With this setting, when maximum transmit power is being used, EDR packets are disabled. Next setting down is EDR, which limits transmit to the maximum that allows EDR packets, thus providing maximum EDR range. This setting can be configured with **btclass EDR** command. The settings can be changed further down to class 2 (10 meter range) settings with the **btclass 2** command, or even lower with the **btclass 3** command. Default class 1 settings can be restored with the **btclass 1** command.

You can also find these commands in **Setup Advanced settings Bluetooth commands** menu in the WWW Setup interface.

After **btclass #** is given, it is recommended to reboot Access Device once to restart all *Bluetooth* services properly.

> ⚠ It is recommended to stop all applications using *Bluetooth* before issuing the **btclass** command.

5.3 Badctl - Bluegiga Access Device Control

Badctl is used to read the reset button state and control internal devices like modem, Wi-Fi and external USB port. This tool switches power on/off and does power cycle for internal components. Currently **badctl** supports AP 3241 (button, USB) and AX4 (button, modem, Wi-Fi, USB).

```
$ badctl --help
usage: badctl DEVICE [COMMAND]

Manage Bluegiga Access Device and read state of button

available devices:
 modem internal GPRS/3G modem
 wifi internal Wi-Fi
 usb external USB port
 button state of button

commands (all devices except button):
 on switch power on
 off switch power off
 reset do power cycle

exit status (commands):
 0 executed successfully (OK)
 1 problems during running command
 2 unable to open device /dev/led

exit status (state of button):
 0 button is not pressed
 1 button is pressed
```

5.4 Finder - Bluegiga Access Device Finder

5.4.1 Finder Service and Command

The Finder service is a small service, which listens for UDP broadcast queries from Access Device Finder applications and responds to those queries with identification information (IP address, model, serial number, etc.).

The **finder** command can be used to query Finder service information from Access Devices in the network. With no parameters, **finder** sends the query using the broadcast address of the default interface (nap). Broadcasting to networks of other interfaces can be done with --interface parameter, such as the zero configuration interface nap:9 in the following example:

```
[root@wrap root]$ finder --interface nap:9

Access Point 3241 (S/N: 1012010002) (build: 4.3)
   - Description: Access Point
   - Hostname: wrap.localdomain
   - IP: 10.1.1.111 (nap), 169.254.175.252 (nap:9), 192.168.161.1 (gn)
   - Ethernet MAC: 00:07:80:01:3a:46
   - iWRAP: 10101 00:07:80:99:91:ff bt2.0 (W1012010002_1)

Access Server 2293 (S/N: 1611150016) (build: 4.0)
   - Description: VFD #1611150016
   - Hostname: wrap.localdomain
   - IP: 169.254.202.147 (nap:9), 192.168.161.1 (gn), 10.1.1.65 (wlan0)
   - Ethernet MAC: 00:07:80:81:65:76
```

With parameter --send finder will send info once to a specified host, for example to inform the host that the device has booted.

5.4.2 Finder Protocol

Finder protocol is used to find Access Servers or Access Points using a UDP broadcast message. Finder server is listening in port 9990 for broadcast and unicast messages. The reply is unicasted to sender.

In Access Server and Access Point a finder message can be sent with command **finder**. See **finder --help** for usage. The finder server is enabled by default.

Finder Search Message

Finder search message has four bytes:

```
0x62 0x66 0x62 0x66
```

Finder Reply Message

Finder reply message has four header bytes:

```
0x66 0x62 0x66 0x62
```

Following the header bytes there is zero or more value tuples. Each tuple has format:

Field Name	Length	Description
ID	1 byte	Tuple ID, see below
Length	1 byte	Data length, in bytes
Data	Length bytes	Value for ID

Following tuple IDs are defined:

Tuple ID	Description of Data
0x01, ProdId	Product identification string, ASCII.
0x02, Revision	Product revision string, ASCII.
0x03, HWSerial	Hardware serial number, ASCII.
0x04, IP	IP address of "nap" interface, 4 bytes.
0x05, EthMac	Ethernet MAC address, 6 bytes.
0x06, iWRAP	iWRAP information string, ASCII.
0x07, IPString	List of all IP addresses, ASCII.
0x08, Hostname	Hostname and domain, ASCII.
0x09, Description	Free description, ASCII.
0x0a, BuildTag	Software version, ASCII.
0x0b, ObexSender	Reserved for ObexSender use, ASCII.

5.5 Smsgw - Bluegiga SMS Gateway

Bluegiga SMS Gateway Server can be used for sending and receiving SMS messages with internal or external modems.

Bluegiga SMS Gateway Server is not installed by default. It can be installed from software component *smsgw*.

When Bluegiga SMS Gateway Server is installed, it is also enabled to start at boot by default. You can disable it later (for example if you need to use the same modem for Internet connection) either with command **chkconfig smsgw off** or using the **setup** application's WWW interface at **Setup Applications Default startup applications smsgw**. You cannot use the same modem for Internet connection and SMS gateway use at the same time.

By default, Bluegiga SMS Gateway Server assumes the modem can be accessed using `/dev/ttyUSB0` device. The device can be changed by using the **setup** application or its WWW interface, by changing the setting at **Setup Applications SMS gateway settings Modem device**.

Another mandatory setting is the SMSC (Short Message Service Center) number. Remember to change it to match your mobile operator.

> ⚠ A reboot is needed for the new settings to take effect. From WWW Setup, you can do this at **Setup Advanced settings Reboot system (confirm)**

> ⚠ The PIN code query of the SIM card at power-up must be disabled.

> ⚠ Bluegiga SMS Gateway Server requires exclusive access to the modem device. Otherwise it will fail to start and the "can't lock device devicename" error message is printed to the system log. Especially, if you are using Bluetooth Serial Port Profile, ensure it is configured to use another serial port device or disabled completely.

By default, Bluegiga SMS Gateway Server uses directory */tmp/sms/in* for storing incoming messages (each message received is stored in a separate file). It scans messages to be sent from directory */tmp/sms/out*. These settings can be changed by editing the configuration file at **Setup Applications SMS gateway settings Edit configuration file** (search for dirin and dirout entries).

> ⛔ Bluegiga SMS Gateway Server exits in case of error. As it has registered itself to Bluegiga User Level Watchdog, this will make device to reboot. This is a feature to recover from problems in modem communication, but as a side effect it can cause a reboot loop if there is a mistake in the configuration file. Be careful when editing it.

To send a SMS message, create a text file with extension *.sms*. The first line of that file must contain only the GSM number of the recipient. Next lines contain the message. After you have created the file, copy or move it to the outgoing directory (*/tmp/sms/out* by default) and the message will be sent automatically.

An example message:

```
+17815550199
Hello, world!
```

Once the message is sent, the file is deleted from the outgoing directory.

For further information on using **smsgw**, see the **makesms** example in SDK.

5.6 Watchdog - Bluegiga User Level Watchdog

Bluegiga User Level Watchdog daemon listens on UDP port 4266 for "id timeout" messages. "id" is an ASCII string, without spaces. If "timeout" equals to 0 (zero), the "id" is removed from the list of processes to wait. If "timeout" is greater than 0 (zero), the "id" is added or updated.

When there is no message for "id" received within the "timeout" seconds, the user level watchdog dies and the kernel watchdog reboots Access Device.

The **watchdog** command can be used to send messages to the watchdog daemon. This is done through command **watchdog id timeout**. For example, **watchdog test 5**.

6 Using 3rd Party Peripherals

6.1 Using USB, Compact Flash or microSD Memories

Access Device's persistent memory storage can be extended by using a USB storage device like a memory dongle or a portable hard drive or a Compact Flash memory card. These are also used by the **wpkgd** daemon - each time this kind of device is inserted, it is automatically mounted and scanned for management packets, which are processed and unmounted.

Access Server AX4 supports also microSD card. If one is inserted, it is automatically mounted at boot and is accessible in */mnt/sdcard*

To use the USB storage device or Compact Flash memory card for your own applications, the memory must be mounted manually by using command:

```
[root@wrap /]$ mount -t vfat device directory
```

The device parameter is a path to the USB dongle or Compact Flash memory card filesystem device. For the first memory device inserted after a reboot, it is */dev/sda1* if the device is partitioned (which often is the case), or */dev/sda* if the device has no partition table. If you insert more memory devices at the same time, new device file names are created: */dev/sdb1* for the second one, */dev/sdc1* for the third one, and so on. If you unmount and remove the first memory device before inserting the second one, new device file names are not created.

> ⚠ Always remember to unmount the memory dongle or memory card with command:
>
> ```
> [root@wrap /]$ umount directory
> ```

> ⚠ If you have inserted both a USB memory dongle and a Compact Flash memory card before powering up Access Server, Compact Flash card is found first (typically getting device file name */dev/sda1*) and the USB memory device is found next (*/dev/sdb1*).

The filesystem in USB dongle can get corrupted if you have a power failure while you are writing data to it. A utility called **fsck.vfat** can fix the problem. Therefore, if mount fails, you should run **fsck.vfat** and try mounting again:

```
[root@wrap /]$ fsck.vfat -a device
```

> ⛔ There is not enough memory to run fsck.vfat on storage devices bigger than 8GB.

> ⚠ If your application uses USB storage devices or Compact Flash memory cards for additional storage, you must ensure that these services do not start before these storage devices are properly mounted. You should therefore disable the automatic startup of application(s) in question either by changing their startup state to off in WWW Setup at **Setup Applications Default startup applications** or at shell prompt with command **chkconfig application off**. The system startup script */etc/rc.d/rc.local* should then be edited (**WWW Setup Advanced settings System startup script**) according to the following example for **obexsender**:
>
> ```
> #!/bin/sh
>
> # This script will be executed *after* all the other init scripts.
> # You can put your own initialization stuff in here if you don't
> # want to do the full Sys V style init stuff.
>
> mkdir -p /mnt/disk
> mount -t vfat /dev/sda1 /mnt/disk
> if [ $? != 0 ]; then
>     # run fsck.vfat only if mounting failed, then try to mount
> again
>     fsck.vfat -a /dev/sda1
>     mount -t vfat /dev/sda1 /mnt/disk
> fi
>
> # Script assumes you have disabled obexsender automatic startup as
> instructed,
> # so it is  started now.
> # Sleep is just to make sure filesystem is calm after mounting.
> sleep 20
> service obexsender start
> ```

6.2 Using USB sound cards

Access Devices features can be extended by adding external USB sound card. All devices providing generic USB audio device class are supported. Please refer Tested 3rd Party Peripherals to see what devices we have tested. Software currently supports only output.

USB sound card drivers are not installed by default. Those can be installed using software component *kernel-modules-sound*. If you like to have *ogg123* to play Ogg files, easiest way is to install *oggplayerbundle* that includes needed drivers, libraries and commands.

To use the USB sound card with Open Sound System (OSS) use command (*ogg123* uses OSS):

```
[root@wrap /]$ modprobe snd-pcm-oss
```

> ⚠ If you compile your own application using Advanced Linux Sound Architecture (ALSA), there is no need to load OSS emulation layer module.

Using *ogg123* is simple:

```
[root@wrap /]$ ogg123 file.ogg
```

> ⚠ Decoding high quality Ogg files real time is not possible in Access Devices.

6.3 Using USB webcams

Access Devices features can be extended by adding external USB webcam. All devices providing generic USB video class devices are supported. Please refer Tested 3rd Party Peripherals to see what devices we have tested.

USB webcam drivers are not installed by default. Those can be installed using software component *kernel-modules-media*.

To use the USB webcam we provide one software: *mjpg-streamer*. That software, needed libraries and drivers can be installed using single command:

```
[root@wrap /]$ wpkgd install kernel-modules-media libjpeg libv4l2
mjpg-streamer
```

Using *mjpg-streamer* is simple:

```
[root@wrap /]$ mjpg_streamer -o "output_http.so"
```

To view output, point your browser to http://<ip-address-of-access-device>:8080/?action=snapshot to view a single snapshot. For simple stream you need a MJPEG compatible browser e.g. Firefox. In that case use URL http://<ip-address-of-access-device>:8080/?action=stream.

7 Licenses, Warranty, Certification Information and WEEE Compliance

Bluegiga Technologies is hereby willing to license the enclosed WRAP product and its documentation under the condition that the terms and conditions described in the License Agreement are understood and accepted. The License Agreement is supplied within every WRAP product in hard copy. It is also available on-line at http://www.bluegiga.com/terms_and_conditions. The use of the WRAP product will indicate your assent to the terms. If you do not agree to these terms, Bluegiga Technologies will not license the software and documentation to you, in which event you should return this complete package with all original materials, equipment, and media.

Some software components are licensed under the terms and conditions of an open source license. Details can be found from http://gpl.bluegiga.com/ or in directory /doc/license/ in SW CD-ROM or SDK DVD-ROM.

The Bluegiga WRAP Product Limited Warranty Statement is available on-line at http://www.bluegiga.com/terms_and_conditions.

7.1 Access Point Certification Information and WEEE Compliance

Access Point is CE approved and *Bluetooth* qualified v. 2.0 + EDR. It has been measured against the following specification standards: ETSI EN 300 328 v1.6.1 / EN 301 489-1/17 / EN 60950-1 / FCC parts 15.247, 15.209, 15.207, 15.109 and 15.107. Supported *Bluetooth* profiles are: GAP, SDAP, LAN client and server, SPP A and B, FTP client and server, ObjP client and server, PAN-PANU, PAN-GN and PAN-NAP.

Hereby, Bluegiga Technologies declares that this Access Point is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.

This device complies with Part 15 of the FCC Rules.

The device operation is subject to the following two conditions:

- This device may not cause harmful interference, and
- This device must accept any interference received, including interference that may cause undesired operation.

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 antenna
- Increase the distance between the equipment and receiver
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected
- Consult the dealer or an experienced radio or television technician for help

FCC RF Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm

between the radiator & your body. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

Notice for Canada

This Class B digital apparatus complies with Canadian ICES-003 and RSS-210.

Cet appareil numérique de classe B est conforme aux normes canadiennes NMB-003 et CNR-210.

This device complies with Industry Canada licence-exempt RSS standard.

Operation is subject to the following two conditions:

- This device may not cause harmful interference, and
- this device must accept any interference received, including interference that may cause undesirable operation.

Cet appareil est conforme avec Industrie Canada RSS standard exempts de licence.

Son Fonctionnement est soumis aux deux conditions suivantes :

- Le matériel ne peut étre source D’interférences et
- Doit accepter toutes les interférences reques, Y compris celles pouvant provoquer un fonctionnement indésirable.

RF exposure

Low power license-exempt radiocommunication

devices (RSS-210)

Operation is subject to the following two conditions:

- This device may not cause interference.
- This device must accept any interference, including interference that may cause undesired operation of the device.

The transmitter devices have been designed to operate with the antennas

integrated in the computer, and having a maximum gain of within 3 dBi.

Appareils de radio-communication basse tension sans licence

d'utilisation (CNR-210)

Le fonctionnement de ce type d'appareil est soumis aux deux conditions

suivantes :

- Cet appareil ne doit pas perturber les communications radio.
- Cet appareil doit supporter toute perturbation, y compris les perturbations qui pourraient provoquer son dysfonctionnement.

Les appareils émetteurs ont été conçus pour fonctionner avec les antennes

intégrées à l'ordinateur et avoir un gain d'antenne maximal de 3 dBi.

Exposure of humans to RF fields (RSS-102)

The computers employ low gain integral antennas that do not emit RF field in

excess of Health Canada limits for the general population; consult Safety Code 6,

obtainable from Health Canada's Web site at http://www.hc-sc.gc.ca/

The radiated energy from the antennas connected to the wireless adapters

conforms to the IC limit of the RF exposure requirement regarding IC RSS-102, Issue 4 clause 4.1.

Conformité des appareils de radiocommunication aux limites

d'exposition humaine aux radiofréquences (CNR-102)

L'ordinateur utilise des antennes intégrales à faible gain qui n'émettent pas un

champ électromagnétique supérieur aux normes imposées par Santé Canada

pour la population. Consultez le Code de sécurité 6 sur le site Internet de Santé

Canada à l'adresse suivante : http://www.hc-sc.gc.ca/

L'énergie émise par les antennes reliées aux cartes sans fil respecte la limite

d'exposition aux radiofréquences telle que définie par Industrie Canada dans la

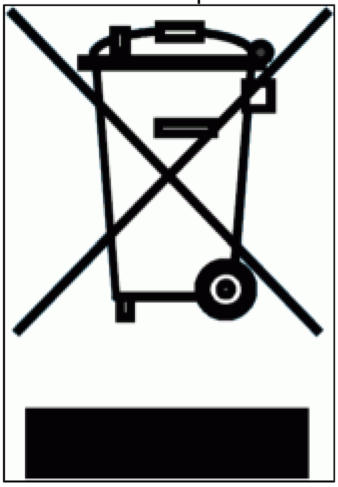
clause 4.1 du document CNR-102, version 4.

> ⛔ Changes or modifications made to this equipment not expressly approved by Bluegiga Technologies Inc. may void the FCC authorization to operate this equipment.

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. End users must follow the specific operating instructions for satisfying RF exposure compliance. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

7.1.1 WEEE Compliance

The crossed-out wheeled bin means that within the European Union the product must be taken to separate collection at the product end-of-life. Do not dispose of these products as unsorted municipal waste.



7.2 Access Server Certification Information and WEEE Compliance

Access Server is CE approved and *Bluetooth* qualified v. 2.0 + EDR. It has been measured against the following specification standards: ETSI EN 300 328 v1.6.1 / EN 301 489-1/17 / EN 60950-1 / FCC parts 15.247, 15.209, 15.207, 15.109 and 15.107. Supported *Bluetooth* profiles are: GAP, SDAP, LAN client and server, SPP A and B, FTP client and server, ObjP client and server, PAN-PANU, PAN-GN and PAN-NAP.

Hereby, Bluegiga Technologies declares that this Access Point is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.

This device complies with Part 15 of the FCC Rules.

The device operation is subject to the following two conditions:

- This device may not cause harmful interference, and
- This device must accept any interference received, including interference that may cause undesired operation.

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 antenna
- Increase the distance between the equipment and receiver
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected
- Consult the dealer or an experienced radio or television technician for help

Changes or modifications made to this equipment not expressly approved by Bluegiga Technologies Inc. may void the FCC authorization to operate this equipment.

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. End users must follow the specific operating instructions for satisfying RF exposure compliance. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

Any transmitter installed in the CF card slot must not exceed 4 W of e.i.r.p. To check if a particular equipment complies with this restriction, you need to know its FCC ID number and visit the searching engine in the FCC web site in the following Internet address, where you can find the output power by the equipment in the grant of equipment: https://gullfoss2.fcc.gov/prod/oet/cf/eas/reports/GenericSearch.cfm

If this link does not work properly, please visit the FCC website (http://www.fcc.gov/) and follow the following steps to find the searching engine:

FCC website Office of Engineering Technology Equipment Authorization Electronic Filing Generic Search

Please notice that the output power listed in the grant uses different units depending on the type of the equipment, e.g.:

- The output power for 802.11a/b/g/h equipment or similar equipment approved under §15.247 or §15.407 is listed as Conducted RF power. §15.247 or §15.407 limit the e.i.r.p. to 4 W, so this restriction is fulfilled.
- The output power for Part 22 cellular equipment is listed as e.r.p. The relationship between e.r.p. and e.i.r.p. is the following one:
  e.i.r.p. = 1.64 x e.r.p.
- The output power for Part 24 PCS equipment is listed as e.i.r.p.
- For other type of equipment, please consult the distributor in order to assure the restriction is fulfilled.

Defininitions:
Effective Radiated Power (e.r.p.) (in a given direction): The product of the power supplied to the antenna and its gain relative to half-wave dipole in a given direction.
Equivalent Isotropically Radiated Power (e.i.r.p.) (in a given direction): The product of the power supplied to the antenna and its gain relative to an isotropic antenna.

The table below is excerpted from Table 1B of 47 CFR 1.1310 titled Limits for Maximum Permissible Exposure (MPE), Limits for General Population/Uncontrolled Exposure:

Frequency Range (MHz)	Power Density (mW/cm^2)
300 - 1500	f/1500
1500 - 100000	1.0

The equipment WRAP Access Server equipment transmits in the 2400 - 2483.5 MHz frequency range, so the applicable MPE limit is 1 mW/cm². The equipment can be provided with up to 4 Bluetooth modules WT11# (FCC ID: QOQWT11):

Under the conditions stated above MPE limits can be guaranteed as the calculation below shows:

Example 1. 15.247 or 15.407 Compact Flash Card with maximum allowed e.i.r.p. of 4 W

Using Equation from page 18 of OET Bulletin 65, Edition 97-01:

$S_{\text{Compact Flash card}} = \text{Prad (e.i.r.p.)}_{\text{Compact Flash card}} / 4R^2 = 4000 \text{ mW}/4(20 \text{ cm})^2$

$S_{\text{Compact Flash card}} = 0.795774 \text{ mW/cm}^2$

$S_{\text{Total}} = S_{\text{Bluetooth}} + S_{\text{Compact Flash card}} = 0.003481 \text{ mW/cm}^2 + 0.795774 \text{ mW/cm}^2$

$S_{\text{Total}} = 0.799255 \text{ mW/cm}^2 < 1 \text{ mW/cm}^2$

Example 2. Part 22 Compact Flash Card with maximum e.r.p. of 1.5 W (Category excluded of MPE evaluation according to §2.1091)

Using Equation from page 18 of OET Bulletin 65, Edition 97-01 and considering that e.i.r.p. = 1.64 x e.r.p.:

$S_{\text{Compact Flash card}} = \text{Prad (e.i.r.p.)}_{\text{Compact Flash card}} /4R^2 = 1500 \times 1.64 \text{ mW}/4(20 \text{ cm})^2$

$S_{\text{Compact Flash card}} = 0.489401 \text{ mW/cm}^2$

$S_{\text{Total}} = S_{\text{Bluetooth}} + S_{\text{Compact Flash card}} = 0.003481 \text{ mW/cm}^2 + 0.489401 \text{ mW/cm}^2$

$S_{\text{Total}} = 0.492882 \text{ mW/cm}^2 < 1 \text{ mW/cm}^2$

Example 3. Part 24 Compact Flash Card with maximum e.r.p. of 3 W (Category excluded of MPE evaluation according to §2.1091)

Using Equation from page 18 of OET Bulletin 65, Edition 97-01 and considering that e.i.r.p. = 1.64 x e.r.p.:

$S_{\text{Compact Flash card}} = \text{Prad (e.i.r.p.)}_{\text{Compact Flash card}} /4R^2 = 3000 \times 1.64 \text{ mW} / 4(20\text{cm})^2$

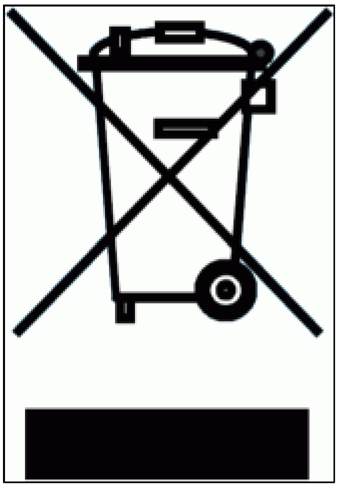
$S_{\text{Compact Flash card}} = 0.978803 \text{ mW/cm}^2$

$S_{\text{Total}} = S_{\text{Bluetooth}} + S_{\text{Compact Flash card}} = 0.003481 \text{ mW/cm}^2 + 0.978803 \text{ mW/cm}^2$

$S_{\text{Total}} = 0.982284 \text{ mW/cm}^2 < 1 \text{ mW/cm}^2$

7.2.1 WEEE Compliance

The crossed-out wheeled bin means that within the European Union the product must be taken to separate collection at the product end-of-life. Do not dispose of these products as unsorted municipal waste.



8 Appendices

8.1 Access Device directory tree

```
Access Device Directory Tree            Type Note
============================            ==== ====
/                                       f    whole filesystem is root writable
|-- bin                                 f
|-- dev                                 r
|   `-- shm                             r    ramdisk
|       |-- etc                         r    resolv.conf
|       |-- tmp                         r    /tmp
|       |   |-- obex                    r    obexserver dir
|       `-- var                         r    ramdisk part of /var
|           |-- lock                    r
|           |   `-- subsys              r
|           |-- log                     r
|           |-- run                     r
|           `-- empty                   r
|-- etc                                 f    system config and init scripts
|   |-- backup                          f    configreset files configuration
files
|   |-- configreset                     f    configreset scripts
|   |   |-- post.d                      f
|   |   `-- pre.d                       f
|   |-- init.d -> rc.d/init.d           l
|   |-- ppp                             f
|   |   `-- peers                       f
|   |-- rc.d                            f
|   |   |-- init.d                      f
|   |   `-- rc3.d                       f
|   |-- rc3.d -> rc.d/rc3.d             l
|   |-- rc.d                            f
|   |   |-- init.d                      f
|   |   |-- rc0.d                       f
|   |   |-- rc1.d                       f
|   |   `-- rc3.d                       f
|   |-- rc0.d -> rc.d/rc0.d             l
|   |-- rc1.d -> rc.d/rc1.d             l
|   |-- rc3.d -> rc.d/rc3.d             l
|   |-- ssh                             f
|   `-- sysconfig                       f
|-- home                                f
|-- lib                                 f    system libraries
|   |-- firmware                        f
|   |   |-- kaweth                      f
|   |   `-- zd1211                      f
|   |-- modules                         f
|   |       `-- [module directories]    f
|   |-- pppd                            f
|   `-- xtables                         f
|-- mnt                                 f    mount points
|   |-- disk                            f
|   `-- usb                             f
|-- proc                                p    proc filesystem
|-- root                                f    home directory of root
|-- sbin                                f
|-- sys                                 p    sys filesystem
|-- tmp -> dev/shm/tmp                  l    temporary data (ramdisk)
{code}
{code:none}
|-- usr                                 f
|   |-- bin                             f
|   |-- lib                             f
|   |   `-- gconv                       f
|   |-- libexec                         f
|   |-- local                           f    mount point for second flash
|   |-- sbin                            f
|   `-- share                           f
|       |-- tabset                      f
|       |-- terminfo                    f
|       |   |-- a                       f
|       |   |-- l                       f
|       |   |-- s                       f
|       |   |-- v                       f
|       |   `-- x                       f
|       `-- usb-modeswitch              f
`-- var                                 f
    |-- empty -> ../dev/shm/var/empty   f
    |-- lib                             f
    |   |-- btclass                     f
    |   |-- dpkg                        f
    |   |   `-- info                    f
    |   |-- obexsender                  f
    |   `-- setup                       f
    |-- lock -> ../dev/shm/var/lock     l
    |-- log -> ../dev/shm/var/log       l    log files
    |-- run -> ../dev/shm/var/run       l
    |-- spool                           f
    |   `-- cron                        f
    |       `-- crontabs                f
    |-- tmp -> ../dev/shm/var/tmp       l
    `-- www                             f
        |-- cgi-bin                     f
        `-- html                        f    WWW pages

Types
=====

f = FLASH filesystem, read/write, files will be saved on power-down
r = RAM filesystem, read/write, files will be lost on power-down
l = symbolic link
p = proc/sys filesystem, can be used to configure Linux
```

8.2 Tested 3rd Party Peripherals

USB peripherals tested with Access Devices

Working modems

All USB modems need *kernel-modules-modem* (installed by default) to work. VID:PID column reports values after USB modem has switched to modem-mode. Values reported by USB modem before switching to modem-mode are reported in brackets under usb-modeswitch column.

Name	Type	Port	Pluggable without extension cable	VID:PID	Usb-modeswitch needed	Notes
A-Link 3GU	3G	/dev/ttyUSB2	AS=no, AP=no, AX4=yes	1e0e:9200	yes (1e0e:f000)	
GPRS-MODEM	GPRS	/dev/ttyUSB0	AS=no, AP=no, AX4=yes	067b:0609	no	
Falcom SAMBA 75	GPRS	/dev/ttyACM0	AS=no, AP=no, AX4=yes	0681:0034	no	FCC ID: QIXSAMBA75 use ATD*99***1#
Global Wireless WM66-TF	3G	/dev/ttyUSB0	AS=no, AP=yes, AX4=yes	05c6:0015	yes (05c6:2000)	micro-SD reader does work, do not use or AS might not boot up
Huawei E160E	3G	/dev/ttyUSB0	AS=no, AP=yes, AX4=yes	12d1:1003	no	FCC ID: QISE160E, micro-SDHC reader wo connector for external antenna
Huawei EG162G	3G	/dev/ttyUSB0	AS=yes, AP=yes, AX4=yes	12d1:1001	no	tested by customer
Huawei E1552	3G	/dev/ttyUSB0	AS=no, AP=yes, AX4=yes	12d1:1001	yes (12d1:1446)	micro-SDHC reader wo
Huawei E169	3G	/dev/ttyUSB0	AS=yes, AP=yes, AX4=yes	12d1:1001	no	FCC ID: QISE169, micro-SD reader not supported, connector fo external antenna
Huawei E1690	3G	/dev/ttyUSB0	AS=no, AP=yes, AX4=yes	12d1:1001	yes (12d1:1446)	tested by customer
Huawei E1750	3G	/dev/ttyUSB0	AS=no, AP=yes, AX4=yes	12d1:1003	yes (12d1:1446)	micro-SDHC reader wo tested by customer
Huawei E1820	3G	/dev/ttyUSB0	AS=no, AP=yes, AX4=yes	12d1:1001	yes (12d1:14ac)	tested by customer
Huawei E180	3G	/dev/ttyUSB0	AS=no, AP=yes, AX4=yes	12d1:1003	no	micro-SDHC reader wo tested by customer
Huawei E220	3G	/dev/ttyUSB0	AS=no, AP=no, AX4=no	12d1:1003	no	FCC ID: QISE220
Mobidata GPRS	GPRS	/dev/ttyUSB0	AS=no, AP=no, AX4=yes	10c5:ea61	no	

MTX-H25	3G	/dev/ttyACM0	AS=no, AP=no, AX4=no	0681:0047	no	PID depends on configuration, mode mu be programmed before using in AS/AP (at^susb="Startup","Mc easiest to do with PC
Newolution Webbox	GPRS	/dev/ttyUSB0	AS=no, AP=no, AX4=no	0403:6001	no	
Nokia CS-15	3G	/dev/ttyACM0	AS=no, AP=yes, AX4=yes	0421:0611	yes (0421:0610)	FCC ID: PYARD-10, N CS-10 might work also
Sierra Wireless Compass 885	3G	/dev/ttyUSB3	AS=no, AP=yes, AX4=yes	1199:6880	no	FCC ID: N7NC885, micro-SDHC reader wc
SIMCom SIM5218	3G	/dev/ttyUSB2	AS=no, AP=no, AX4=no	05c6:9000	no	Module in evaluation ki tested.
Telewell GPRS	GPRS	/dev/ttyACM0	AS=no, AP=yes, AX4=yes	22b8:3802	no	
Telit UC864-G	3G	/dev/ttyUSB0	AS=no, AP=no, AX4=no	1bc7:1004	no	Module in evaluation ki tested. Some versions AX4 includes this.
Teltonika ModemUSB/G10	GPRS	/dev/ttyUSB0	AS=no, AP=no, AX4=yes	0403:6001	no	
Teltonika ModemUSB/H7.2, U3G15L	3G	/dev/ttyHS3	AS=no, AP=no, AX4=yes	0af0:6911	no	
ZTE K3565-Z	3G	/dev/ttyUSB2	AS=no, AP=yes, AX4=yes	19d2:0052	yes (19d2:2000)	micro-SDHC reader wc tested by customer
ZTE K3805-Z	3G	/dev/ttyACM1	AS=no, AP=yes, AX4=yes	19d2:0052	yes (19d2:1001)	tested by customer
ZTE MF100	3G	/dev/ttyUSB2	AS=no, AP=yes, AX4=yes	19d2:0017	yes (19d2:2000)	use **eject -s /dev/sg0** t get micro-SDHC reade work
ZTE MF636+	3G	/dev/ttyUSB2	AS=no, AP=yes, AX4=yes	19d2:0031	yes (19d2:2000)	micro-SDHC reader wc connector for external antenna

Non-working modems

Name	Type	VID:PID	Notes
Huawei E160X / Vodafone K3565	3G	12d1:1003	Should work but we tested SIM locked device.
NetComm USB56 Rave!	POTS	0483:7554	
NTTDocomo Foma L02A	3G	1004:610c	Contact Bluegiga to get this modem to work.
NTTDocomo Foma L05A	3G	1004:613a	Contact Bluegiga to get this modem to work.
Option Icon 225	3G	0af0:6971	does not support ppp
Sony-Ericsson WD400	3G	0fce:d0e1	tested with 4.0 software, might work with current one

Working Wi-Fi dongles

All USB Wi-Fi sticks support client (station) mode with WEP, WPA or WPA2 encryption. Also unencrypted mode is supported. Package *kernel-modules-wifi* is needed for USB sticks (installed by default). Some sticks (see table below under "Notes" column) need special *kernel-modules-wifi-experimental* package which however might occasionally present unstable behavior.

Name	Speed	AP mode support	Pluggable without extension cable	VID:PID	Chipset	Notes
A-LINK WL54USB	b/g	no	AS=no, AP=yes, AX4=yes	0ace:1215	zd1211rw	internal antenna
A-LINK WL54USB-A	b/g	no	AS=no, AP=yes, AX4=yes	0ace:1215	zd1211rw	external antenna
A-Link WNU-A	b/g/n	no	AS=no, AP=no, AX4=yes	0cf3:9170	ar9170	older version with two external antennas tested
Asus WL168G V2	b/g	yes	AS=yes, AP=yes, AX4=yes	0b05:1723	rt2571	FCC ID MSQWL167G
Belkin F5D7050	b/g	yes	AS=no, AP=yes, AX4=yes	050d:705a	rt2571	FCC ID K7S-F5D7050B
D-Link DWA-140, H/W ver. B1	b/g/n	yes	AS=no, AP=yes, AX4=yes	07d1:3c09	rt2870	needs *kernel-modules-wifi-experimental*
D-Link DWL-G122, H/W ver. C1	b/g	yes	AS=no, AP=yes, AX4=yes	07d1:3c03	rt2571	FCC ID KA2WLG122C1
Edimax EW-7318Ug	b/g	yes	AS=no, AP=yes, AX4=yes	148f:2573	rt2571	
Edimax EW-7718UN	b/g/n	yes	AS=no, AP=yes, AX4=yes	148f:2870	rt2870	needs *kernel-modules-wifi-experimental*

Edimax EW-7718UN	b/g/n	yes	AS=no, AP=yes, AX4=yes	7392:7711	rt2870	needs *kernel-modules-wifi-experimental* , tested by customer
Linksys WUSB54GC-EU ver. 1	b/g	yes	AS=no, AP=yes, AX4=yes	13b1:0020	rt2571	FCC ID Q87-WUSB54GC, first version (silver)
Linksys WUSB54GC-EU ver. 3	b/g	yes	AS=yes, AP=yes, AX4=yes	1737:0077	rt2070	FCC ID Q87-WUSB54GCV3, third version (black), needs *kernel-modules-wifi-experimental*
Linksys WUSB200	b/g	yes	AS=no, AP=no, AX4=no	13b1:0028	rt2571	FCC ID Q87-WUSB200
Netwjork W311U	b/g/n	yes	AS=yes, AP=yes, AX4=yes	148f:3070	rt3070	needs *kernel-modules-wifi-experimental*
Netwjork W541U	b/g	yes	AS=no, AP=yes, AX4=yes	148f:2573	rt2571	
SignalKing SK-RT2571-X3	b/g	yes	AS=no, AP=yes, AX4=yes	148f:2573	rt2571	
Sunshine WLAN HWUG1	b/g	yes	AS=no, AP=yes, AX4=yes	148f:2573	rt2571	FFC ID NDD957318S607, external antenna
Telewell TW-WLAN 802.11n/g/b USB v2	b/g/n	yes	AS=yes, AP=yes, AX4=yes	148f:3070	rt3070	needs *kernel-modules-wifi-experimental*
TP-LINK TL-WN422G	b/g	no	AS=no, AP=yes, AX4=yes	0cf3:1006	ath9k	
Winxin WM802RTG	b/g	yes	AS=no, AP=yes, AX4=yes	18e8:6238	rt2571	external antenna, OEM module tested
Zyxel G-202	b/g	no	AS=no, AP=yes, AX4=yes	0586:3410	ar2524	

Non-working Wi-Fi dongles

Name	VID:PID	Chipset	Notes
A-Link WNU	0bda:8192	rtl8192	
Belkin F5D7050 v5000	050d:705e	rtl8187b	FCC ID: K7SF5D7050E
Buffalo WLI-USB-KB11	0411:0044	prism	FCC ID: NKRUSB400
D-Link DWA-131	07d1:3303	rtl8192	HW ver. A1, FW ver. 1.20 tested
EDUP 54M	0457:0163	sis163u	
Netgear WG111T	1385:4251	ar5523	FCC ID: PY3WG111T
Skycity SY-W8509	0bda:8176	rtl8192cu	
TP-LINK TL-WN620G ver 1.2	0cf3:0002	ar5523	
WLAN 54Mbps	0416:0035	winbond	

Working storage devices

All USB memory sticks, card readers and hard disks belonging to mass storage device class devices should work. USB CD/DVD drives are not working.

Working serial adapters

Most USB serial adapters should work without installation of any package. Below is list of adapters that we have tested.

Name	Port(s)	VID:PID	Notes
RS232-USB	/dev/ttyUSB0	067b:2303	Many different kind of "generic" adapters tested.
RS232-USB	/dev/ttyUSB0 /dev/ttyUSB1	0403:6001	
Sandberg 133-08B	/dev/ttyUSB0	067b:2303	
UC-232A	/dev/ttyUSB0	0557:2008	

Working NFC readers

Installation of package *kernel-modules-nfc* is needed.

Name	Standard	VID:PID	Notes
Sony RC-S330	Felica	054c:02e1	
Sony RC-S370	Felica	054c:02e1	

Working sound cards

All USB sound cards need *kernel-modules-sound* (not installed by default) to work. Other USB audio device class devices should work also but we have listed only ones we have tested.

Name	VID:PID	Notes
3D Sound SJ-588	1130:f211	
"No name black box"	0d8c:0102	6ch + SPDIF in/out + microphone in

Working webcams

All USB video class devices needs *kernel-modules-media* (not installed by default) to work. Other USB video class devices should work also but we have listed only ones we have tested.

Name	VID:PID	Notes
AVEO Technology USB Camera	1871:01f0	
Logitech Quickcam Ultra Vision	046d:08c9	

Non-working webcams

Name	VID:PID	Notes
Logitech QuickCam Web	046d:0850	

Working ethernet adapters

All listed USB ethernet adapters have build-in support and appear as second ethernet device (eth1).

Name	Speed	Pluggable without extension cable	VID:PID	Notes
A-Link NA110U2	10/100	AS=yes, AP=yes, AX4=yes	0b95:1720	
A-Link NA1GU	10/100/1000	AS=no, AP=no, AX4=no	0b95:1780	
Belkin F5D5055	10/100/1000	AS=yes, AP=no, AX4=yes	050d:5055	
Linksys USB200M	10/100	AS=yes, AP=yes, AX4=yes	13b1:0018	ver. 2.1 tested

Compact Flash peripherals tested with AS229x

Working modems

CF modems has built-in support.

Name	Type	VID:PID	Port	Notes
Anycom GS-320	GPRS	0279:950b	/dev/ttyS0	FCC ID: MSQAGC100
Audiovox RTM-8000	GPRS	0279:950b	/dev/ttyS0	FCC ID: QDJ-200205EDS01
Enfora GSM0110	GPRS	01e1:0300	/dev/ttyS0	FCC ID: MIVGSM0110

Non-working modems

Name	Type	VID:PID	Notes
Pretec OD-GRWXX-A	GPRS	02a5:0000	fails to connect

Non-working Wi-Fi cards

Please refer to User Guide of software release 3.2 to see which CF Wi-Fi cards were supported in that older version. Kernel used in newer versions doesn't support CF Wi-Fi cards in any usable level.

Name	VID:PID	Chipset	Notes
AmbiCom WL1100C-CF	d601:0002	prism	FCC ID: NI3IS20V35
Ambicom WL54-CF	02df:8103	libertas	FCC ID: P5T-WL54CF, chipset revision too old
Ambicom WL5400-CF	02df:8103	libertas	insertion reboots AS
Canon K30225	0004:2003	prism	OEM version tested
D-Link DCF-660W	d601:0005	prism	FCC ID: M4Y-08150
Linksys WCF12	028a:0673	prism	
Linksys WCF54G	0156:0004	?	
Pretec 802.11g	02df:8103	libertas?	
Pretec OC-WLBXX-A	0156:0002	prism	FCC ID: P5T-1100CCF
SMC EZ Connect SMC2642W V2 EU (11Mb/s)	d601:0005	prism	FCC ID: M4Y-08150
Socket Go Wi-Fi! P500	0104:5911	?	

Working storage devices

All CF memory cards should work.

Working GPS cards

CF GPS cards has built-in support.

Name	VID:PID	Port	Notes
Pretec CompactGPS	02a5:0000	/dev/ttyS0	9600bps
Rikaline GPS-6021-X6	0104:01e4	/dev/ttyS0	1200bps

8.3 Available Software Packages

Package	Description	Installed by default
badctl	Bluegiga utility for controlling Access Devices.	yes
bash	GNU Projects Bourne Again SHell, interactive shell with Bourne shell syntax.	no
bgtupnpd	Universal plug and play daemon	yes
bluetooth	Bluegiga iWRAP service.	yes
bluez-hcidump	Bluetooth packet analyzer.	no
bluez-libs	Bluetooth libraries needed by bluez-hcidump.	no
bstool	Bluegiga Bluetooth baseband control utilities including btclass command.	yes
btcli	Bluegiga iWRAP server command line interface utility.	yes
btd	Bluegiga HDP server	no
btlogger	Bluegiga example: a simple Bluetooth RFCOMM server.	no
btserver	Bluegiga example: an advanced iWRAP client.	no
busybox	Provides tens of general userland utilities.	yes
captivednsd	captivednsd, the Captive Domain Name Server, returns same authorative response to every query.	no
captiveportal	Bluegiga Captiveportal software.	no
captiveportalbundle	Bluegiga captive portal software bundle	no
ccrfiler	Bluegiga CCR filer application	no
chkconfig	Bluegiga utilities: chkconfig and service commands.	yes
cifs-client	Mount helper utility for Linux CIFS VFS client.	no
configreset	Bluegiga config reset script.	yes
connector	Bluegiga Connector, service which automatically opens and maintains connections to specified Bluetooth devices.	yes
curl-cacerts	CA certs for Curl.	no
curl	Command line tool for transferring files with URL syntax.	no
dataflasher	Bluegiga system update and bootloader configuration utility.	yes
dbus-cplusplus	C++ API for D-BUS.	no
dbus	DBUS	no
dbussetupd	Bluegiga setup and other utilities D-Bus bridge	no
dfu	Bluegiga Bluetooth baseband firmware upgrade tool.	yes
dnsmasq	Dnsmasq: A lightweight DNS forwarder and DHCP server.	no
dosfstools	DOS filesystem utils.	yes
dropbear	SSH server and client	no

duma	Detect Unintended Memory Access	no
dun	Bluegiga iWRAP service helper application.	no
ed	POSIX-compliant line editor.	no
ehealthbundle	Bluegiga eHealth bundle	no
ehealthxml	XMLs and defines used in SDK	no
evtest	evtest: Event device test program	no
expat	The Expat XML Parser	yes
finder	Bluegiga utility to find other Bluetooth Access Devices in the network.	yes
forkserver	Bluegiga example: the simplest Bluetooth RFCOMM server.	no
ftpd	Simple FTP server.	no
ftp	FTP client application.	no
gdbserver	Remote server for the GNU Debugger	no
ghealthposter	Google H9 data poster application	no
glibc-devel	The GNU C library.	no
glibc	The GNU C library.	yes
googleh9	Google H9 eHealth service	no
googlehealth	Google Health eHealth service	no
hdpd	Health Device Protocol daemon	no
helloworld	Bluegiga example: Hello world!	no
hostapd	Utility programs for WPA and RSN authenticator.	yes
httppost	Generic HTTP post JSON format eHealth service	no
http-upload-handler	HTTP upload handler	no
iptables	Administration tool for the Linux kernel IP packet filter.	yes
iptables-extra	Administration tool for the Linux kernel IP packet filter.	no
iptables-ipv6	Administration tool for the Linux kernel IP packet filter.	no
json-c	JSON-C library	no
jsoncpp	A simple API to manipulate JSON value, handle serialization and unserialization to string	no
json-dbus-bridge	D-Bus JSON bridge	no
kernel	Linux kernel.	yes
kernel-modules-bluegiga	Bluegiga hardware support kernel module	yes
kernel-modules-bluez	Linux kernel BlueZ modules.	no
kernel-modules	Linux kernel.	yes
kernel-modules-media	Linux kernel module providing support for webcams etc.	no
kernel-modules-modem	Linux kernel modules providing support for USB modems.	yes
kernel-modules-nfc	NFC drivers.	no

kernel-modules-ralink	kernel wifi modules for ralink RT2870/RT3070/RT3370/RT3572/RT8070	no
kernel-modules-realtek	Linux kernel module for Realtek USB Wi-Fi chipsets.	no
kernel-modules-sound	Linux kernel sound modules.	no
kernel-modules-wifi-experimental	kernel linuxwireless tree	no
kernel-modules-wifi	Wi-Fi drivers and firmwares	yes
kitt	Bluegiga utility for controlling LEDs (and buzzer).	yes
ledtest	Bluegiga example: LED control.	no
libao	A Cross-platform Audio Library	no
libbghw	Bluegiga hardware library.	yes
libbgnet	Bluegiga socket, iWRAP and watchdog access libraries.	yes
libbgobex	Bluegiga iWRAP OBEX libraries.	yes
libevent	Libevent library	no
libfcgi	FastCGI library	no
libfforwarder	Reliable file forwarder	no
libfreetype	A Free, High-Quality, and Portable Font Engine.	no
libgd	GD is an open source code library for the dynamic creation of images by programmers.	no
libjpeg	This package contains C software to implement JPEG image compression and decompression.	no
libnl	Library for applications dealing with netlink sockets.	yes
libogg	An implementation of the public domain Ogg bitstream format	no
libpcap	Provides portable framework for low-level network monitoring. Needed by tcpdump.	no
libpng	Libpng is the official PNG reference library.	no
libusb-1.0	Library for use by user level applications to access USB devices.	no
libusb	Library for use by user level applications to access USB devices.	yes
libv4l2	Library for use by user level applications to access v4l2 devices.	no
libvorbis	Vorbis is a general purpose audio and music encoding format	no
lighttpd-mod-alias	Secure, fast, compliant, flexible and small memory footprint http server.	no
lighttpd-mod-compress	Secure, fast, compliant, flexible and small memory footprint http server.	no
lighttpd-mod-evasive	Secure, fast, compliant, flexible and small memory footprint http server.	no
lighttpd-mod-evhost	Secure, fast, compliant, flexible and small memory footprint http server.	no
lighttpd-mod-expire	Secure, fast, compliant, flexible and small memory footprint http server.	no

lighttpd-mod-extforward	Secure, fast, compliant, flexible and small memory footprint http server.	no
lighttpd-mod-fastcgi	Secure, fast, compliant, flexible and small memory footprint http server.	no
lighttpd-mod-flv-streaming	Secure, fast, compliant, flexible and small memory footprint http server.	no
lighttpd-mod-proxy	Secure, fast, compliant, flexible and small memory footprint http server.	no
lighttpd-mod-scgi	Secure, fast, compliant, flexible and small memory footprint http server.	no
lighttpd-mod-secdownload	Secure, fast, compliant, flexible and small memory footprint http server.	no
lighttpd-mod-setenv	Secure, fast, compliant, flexible and small memory footprint http server.	no
lighttpd-mod-simple-vhost	Secure, fast, compliant, flexible and small memory footprint http server.	no
lighttpd-mod-status	Secure, fast, compliant, flexible and small memory footprint http server.	no
lighttpd-mod-userdir	Secure, fast, compliant, flexible and small memory footprint http server.	no
lighttpd-mod-usertrack	Secure, fast, compliant, flexible and small memory footprint http server.	no
lighttpd-mod-webdav	Secure, fast, compliant, flexible and small memory footprint http server.	no
lighttpd	Secure, fast, compliant, flexible and small memory footprint http server.	no
limppu	More advanced demonstration application	no
lottery	Bluegiga example: lottery extension for obexsender service.	no
lzo	A real-time data compression library.	no
m2n	Bluegiga example: machine-2-network (M2N) with syslog.	no
mailhealth	Example Bluegiga eHealth to email backend	no
makesms	Bluegiga example: generating outgoing messages for Bluegiga SMS gateway.	no
make	The Make.	no
maradns	DNS server.	no
mg	Mg is a Public Domain EMACS style editor.	no
mjpg-streamer	Application to stream JPEG files over an IP-based network from the webcam.	no
mtd-utils	MTD utils.	no
ncurses	Library for displaying and updating text on text-only terminals.	no
net-snmp	Suite of applications used to implement SNMP v1, SNMP v2c and SNMP v3 using both IPv4 and IPv6.	no
nfs-utils	NFS server.	no
obexbrowser	Bluegiga iWRAP utility. A command line OBEX client interface.	no

obexget	Bluegiga iWRAP OBEX utilities: obexput and obexget commands for transfering files to/from remote devices with ObjP/FTP support.	yes
obexsender	Bluegiga proximity marketing service.	yes
obexsender-db	Bluegiga proximity marketing device database.	yes
obexserver	Bluegiga iWRAP service: ObjP and FTP server.	yes
oggplayerbundle	Bluegiga oggplayer bundle	no
openntpd	NTP (RFC-1305) client and server.	yes
openssh-sftp-server	sftp support for Dropbear SSH	no
openssh	SSH server and client	yes
openssl-progs	Toolkit implementing SSL v2/v3, TLS v1 and general purpose cryptography library.	no
openssl	Toolkit implementing SSL v2/v3, TLS v1 and general purpose cryptography library.	yes
openvpn	An open source VPN daemon.	no
oxpjsongen	Collects data from the OXP stack and places it in a json formatted file	no
oxpstack	Optimized exchange protocol (OXP) stack	no
pcsc-lite-ccid	SCard interface for communicating to smart cards and readers.	no
pcsc-lite	SCard interface for communicating to smart cards and readers.	no
perl	A programming language.	no
php-mod-gd	PHP: Hypertext Preprocessor.	no
php-mod-openssl	PHP: Hypertext Preprocessor.	no
php	PHP: Hypertext Preprocessor.	no
ppp	Point-to-Point Protocol userland driver.	yes
readline	GNU Readline library, providing set of functions for use by applications that allow users to edit command lines as they are typed in.	yes
rootfiles	Bluegiga Access Server and Access Point filesystem skeleton.	yes
rsync	Utility that provides fast incremental file transfer	no
rzsz	Provides X/Y/Zmodem file transfer tools.	no
sbc	SBC encoder and decoder.	no
screen	Screen is a full-screen window manager that multiplexes a physical terminal between several processes, typically interactive shells.	no
screen-utf8	Screen is a full-screen window manager that multiplexes a physical terminal between several processes, typically interactive shells.	no
searchclient	A simple demonstration application how to do inquiry	no
securitytool	Bluegiga security configuration tool	no
serialport	Bluegiga iWRAP service: SPP client/server.	yes

setup	Bluegiga Access Server and Access Point configuration utility and commands wrapid and supportinfo.	yes
setup-helloworld	Bluegiga example: extending setup application.	no
setup-json-bridge	Setup-Json-bridge	no
smsgw	Bluegiga SMS Gateway.	no
socat	SOcket CAT establishes byte streams and transfers data between them	no
sqlite	SQLite is a software library that implements a self-contained, serverless, zero-configuration, transactional SQL database engine.	no
strace	System call trace, i.e. a debugging tool.	no
sysfsutils	These are a set of utilites built upon sysfs, a new virtual filesystem in Linux kernel versions 2.5+ that exposes a systems device tree.	no
tcpdump	Utility to monitor network traffic.	no
termcap	Basic system library needed to access the termcap database.	yes
toolchain-native	Toolchain	no
tremor	Ogg Vorbis decoder, also known as Tremor.	no
tzdata	Timezone.	yes
usb-modeswitch	Mode switching tool for USB modems.	yes
vorbis-tools	Ogg Vorbis tools (ogg123).	no
watchdog	Bluegiga user level watchdog.	yes
webui	HDP (Health Device Profile) user interface demo	no
webui-locale-fi	Finnish localization for web user interface	no
webui-module-example	Example module for web user interface	no
wireless-tools	Package containing utilities to manage Wireless LAN specific parameters.	yes
wpa-supplicant	Utility programs for WPA and RSN supplicant.	yes
wpkgd	Bluegiga software component management service.	yes
www	Bluegiga example: demonstration of WWW server capabilities.	no
zlib	General purpose compression library.	yes

8.4 Enabled Busybox Applets

Command	Description
[	Check file types, compare values etc. Return a 0/1 exit code.
[[	Check file types, compare values etc. Return a 0/1 exit code.
addgroup	Add a group or add an user to a group.
adduser	Add an user.
adjtimex	Tune kernel clock.
ar	Create, modify, and extract from archives.
arp	Manipulate ARP cache.
arping	Send arp request to a neighbour host.
ash	The ash shell.
awk	Pattern scanning and processing language.
basename	Strip directory and suffix from filenames.
brctl	Manager ethernet bridges.
bunzip2	A block-sorting file decompressor.
bzcat	Decompresses files to stdout.
bzip2	A block-sorting file compressor.
cat	Concatenate files and print on the standard output.
chattr	Change file attributes on an ext2 fs
chgrp	Change group ownership.
chmod	Change file access permissions.
chown	Change file owner and group.
chroot	Run command or interactive shell with special root directory.
clear	Clear the terminal screen.
cmp	Compare two files.
comm	Compare two sorted files line by line.
cp	Copy files and directories.
cpio	Copy files to and from archives.
crond	A daemon to execute scheduled commands. This server is configurable through the *var/spool/cron/crontabs/root* file or the **crontab** command in the same way as any Linux crond.
crontab	Maintain crontab files for individual users.
cryptpw	Output crypted string.
cut	Remove sections from each line of files.
date	Print or set the system date and time.
dd	Convert and copy a file.

delgroup	Delete group from system or user from group.
deluser	Delete user from system.
depmod	Program to generate modules.dep and map files.
df	Report file system disk space usage.
diff	Find differences between two files.
dirname	Strip non-directory suffix from file name.
dmesg	Print or control the kernel ring buffer.
dnsdomainname	Show the system's DNS domain name
dpkg	A medium-level package manager for (.deb) packages.
dpkg-deb	Debian package archive (.deb) manipulation tool.
du	Estimate file space usage.
dumpleases	Display DHCP leases granted by udhcpd.
echo	Display a line of text.
egrep	Print lines matching a pattern.
eject	Eject device (needed by some modems to switch mode).
env	Print the current environment or run a program after setting up the specified environment.
expr	Evaluate expressions.
false	Do nothing, unsuccessfully.
fgrep	Print lines matching a pattern.
find	Search for files in a directory hierarchy.
flock	(Un)lock file descriptor, or lock.
free	Display amount of free and used memory in the system.
fuser	Identify processes using files or sockets.
getty	Open a tty, prompt for a login name, then invoke /bin/login.
grep	Print lines matching a pattern.
gunzip	Expand files.
gzip	Compress files.
halt	Stop the system.
head	Output the first part of files.
hexdump	Ascii, decimal, hexadecimal, octal dump.
hostid	Print the numeric identifier for the current host.
hostname	Show or set the system's host name.
httpd	Web server. Another Web server, **lighttpd**, is available as a separate software component.
hwclock	Query and set the hardware clock (RTC).
id	Print user identity.
ifconfig	Configure a network interface.

inetd	Internet services daemon. Notice that this server is disabled by default. Use the WWW interface of **setup** application or the **chkconfig inetd on** command to enable it.
init	Process control initialization.
insmod	Simple program to insert a module into the Linux kernel.
ip	Linux ipv4 protocol implementation.
ipaddr	Displays addresses and their properties, adds new addresses and deletes old ones.
iplink	Network device configuration.
iproute	Advanced ip routing and network device configuration tools..
iptunnel	Tunnel over IP.
kill	Terminate a process.
killall	Kill processes by name.
klogd	Kernel log daemon.
less	Opposite of more.
ln	Make links between files.
logger	A shell command interface to the syslog system log module.
login	Sign on.
losetup	Set up and control loop devices.
ls	List directory contents.
lsattr	List file attributes on an ext2 fs.
lsmod	Program to show the status of modules in the Linux kernel.
lsusb	Displays information about USB buses in the system and the devices connected to them.
lzcat	Uncompress to stdout.
makemime	Create multipart MIME-encoded message from files specified.
md5sum	Compute and check md5 message digest.
mdev	System device manipulation tool.
microcom	Copy bytes for stdin to TTY and from TTY to stdout. Minimal TTY terminal.
mkdir	Make directories.
mknod	Make block or character special files.
mkpasswd	Crypt (password) using crypt system call.
mkswap	Set up a Linux swap area.
mktemp	Make temporary filename (unique).
modprobe	Program to add and remove modules from the Linux kernel.
more	View file or standard input one screenful at a time.
mount	Mount filesystems.
mv	Move (rename) files.
nc	Open a pipe to ipaddress:port or file.
netstat	Display networking information.

nice	Run a program with modified scheduling priority.
nohup	Run a command immune to hangups, with output to a non-tty.
nslookup	Query Internet name servers interactively.
passwd	Update a user's authentication tokens(s).
patch	Apply a diff file to an original.
pgrep	Display process(es) selected by regex.
pidof	List PIDs of all processes with names that match one specified.
ping	Send icmp echo_request to network hosts.
ping6	Send icmp echo_request to network hosts.
pkill	Send a signal to process(es) selected by regex.
poweroff	Stop the system.
printf	Format and print data.
ps	Report a snapshot of the current processes.
pwd	Print name of current/working directory.
rdate	Get the time via the network.
readlink	Display value of a symbolic link.
realpath	Return the canonicalized absolute pathname.
reboot	Reboot the system.
renice	Alter priority of running processes.
reset	Reset the screen.
resize	Resize the screen.
rm	Remove files or directories.
rmdir	Remove empty directories.
rmmod	Remove a module from the Linux kernel.
route	Edit the kernels routing tables.
sed	Stream editor for filtering and transforming text.
sendmail	Send an email.
seq	Print a sequence of numbers.
sh	Shell, the standard command language interpreter.
sha1sum	Compute and check sha1 message digest.
sleep	Delay for a specified amount of time.
sort	Sort lines of text files.
strings	Print the strings of printable characters in files.
stty	Change and print terminal line settings.
su	Run a shell with substitute user and group ids.
sulogin	Single user login.
swapoff	Stop swapping to file/device.

swapon	Start swapping to file/device.
sync	Flush file system buffers.
sysctl	Read/write system parameters.
syslogd	System logger.
tail	Output the last part of files.
tar	Create, extract, or list files from a tar file.
tcpsvd	Create TCP socket, bind it to ip:port and listen for incoming connection. Run PROG for each connection.
telnet	User interface to the telnet protocol.
telnetd	Telnet daemon.
test	Check file types and compare values.
tftp	TFTP client.
tftpd	TFTP server.
time	Run a program with arguments specified. When command finishes, command's resource usage information is displayed.
top	Provide a view of process activity in real time.
touch	Change file timestamps.
tr	Translate or delete characters.
traceroute	Print the route packets trace to network host.
true	Do nothing, successfully.
tty	Print the file name of the terminal connected to standard input.
ttysize	Print dimension(s) of standard input's terminal, on error return 80x25.
udhcpc	DHCP client.
udhcpd	DHCP daemon for providing automatic network configuration for clients in the network.
udpsvd	Create UDP socket, bind it to ip:port and wait for incoming packets. Run PROG for each packet, redirecting all further packets with same peer ip:port to it.
umount	Unmount file systems.
uname	Print system information.
uniq	Report or omit repeated lines.
unlzma	Uncompress file.
unzip	List, test and extract compressed files in a zip archive.
unxz	Decompress file.
uptime	Tell how long the system has been running.
usleep	Sleep some number of microseconds.
uudecode	Decode a binary file.
uuencode	Encode a binary file.
vi	Screen-oriented (visual) display editor.
wc	Print the number of newlines, words, and bytes in files.

wget	The non-interactive network downloader.
which	Shows the full path of (shell) commands.
whoami	Print effective userid.
xargs	Build and execute command lines from standard input.
xzcat	Decompress to standard output.
yes	Output a string repeatedly until killed.
zcat	Expand and concatenate data.
zcip	Manage a ZeroConf IPv4 link-local address.

9 Contact information

Sales:	sales@bluegiga.com
Technical support:	support@bluegiga.com http://techforum.bluegiga.com
Orders:	orders@bluegiga.com
WWW:	http://www.bluegiga.com http://www.bluegiga.hk
Head Office / Finland:	Phone: +358-9-4355 060 Fax: +358-9-4355 0660 Sinikalliontie 5 A 02630 ESPOO FINLAND
Head address / Finland:	P.O. Box 120 02631 ESPOO FINLAND
Sales Office / USA:	Phone: +1 770 291 2181 Fax: +1 770 291 2183 Bluegiga Technologies, Inc. 3235 Satellite Boulevard, Building 400, Suite 300 Duluth, GA, 30096, USA
Sales Office / Hong-Kong:	Phone: +852 3182 7321 Fax: +852 3972 5777 Bluegiga Technologies, Inc. 19/F Silver Fortune Plaza, 1 Wellington Street, Central Hong Kong