BlueGate 1000

Administrator's Guide

May 8, 2001

Document Number: 010501-0619-BG-AdminGuide
Version: 2.0

Confidential and Proprietary Information

WIDCOMMinc.

Wireless Internet and Data Communication

9645 Scranton Road, Suite 205
San Diego, CA 92121
Phone: 858.453.8400
Fax: 858.453.5735
Email
Technical Support: support@widcomm.com
Information: info@widcomm.com

FCC Statement

Widcomm Inc., 9645 Scranton Road, Suite 205, San Diego, CA 92121, 858-453-8400. BlueGate , WDC-WBG-1000.

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and, (2) This device must accept any interference received including interference that may cause undesired operation.

Per CFR 47, PART 15, Paragraph 15.21: User changes or modifications not expressly approved by the party responsible for compliance could void the users authority to operate the equipment.

Application PKLWBG-1000

Additional Information for the FCC approval of Widcomm Inc.'s BlueGate 1000

RF Exposure Statement

IMPORTANT NOTE: To comply with FCC RF exposure compliance requirements the following antenna installation and device operating configurations must be satisfied:

The BlueGate 1000 unit must be placed on a desk or table such that a minimum normal operating distance of 20 cm is maintained from the body at all times.

Copyright and Trademark Notices

Table of Contents

List of Figures

1 Introduction

BlueGate™ 1000 provides access to a local area network (LAN) using wireless technology. It is Bluetooth specification (1.0B) certified.

BlueGate 1000 also supports Bluetooth™ specification 1.1 critical errata.

Devices that can access the network through BlueGate 1000 are Personal Digital Assistants (PDAs), computers, or other Bluetooth-enabled devices that support the industry standard LAN Access Profile (LAP) portion of Bluetooth specification (1.0B).

Configuration information is saved in internal non-volatile memory and preserved even when power is lost.

An on-board Web server is accessed to set up, diagnose, and configure BlueGate 1000.

Microsoft™ Internet Explorer™, version 5.0 or later, is used to access the internal Web server from a computer on the same network subnet.

From the IE browser you can access the internal Web server to:

- Configure BlueGate 1000 for proper network operation.
- Change the user-friendly device name of BlueGate 1000.
- Access network diagnostic tools.
- Access BlueGate 1000 network statistics.
- Upgrade BlueGate 1000 software.

2 Kit Contents

The BlueGate 1000 kit includes:

- A BlueGate 1000 network access point.
- An external power adapter.
- A standard Ethernet cable with an RJ-45 connector on each end.
- A compact disc that contains the BlueGate 1000 documentation and support software.
- A “Start Here” quick start guide.

Figure 1: BlueGate 1000 box and contents.

3 Installation

Before installing BlueGate 1000, you should be familiar with basic local area network (LAN) and Bluetooth (BT) concepts.

For a non-technical overview of key Bluetooth concepts refer to Appendix A—An Introduction To Bluetooth

1. Place BlueGate 1000 on a flat surface away from heat, moisture, open flames, microwave devices and 2.4 GHz telephones.
2. Use the Ethernet cable provided in the kit to connect BlueGate 1000 to the local area network.

   See Figure 2 for the location of BlueGate 1000's RJ-45 network connector.

   The Ethernet cable can be plugged into a network switch or network hub, or into a hardwired wall jack that connects to the network. Consult your network administrator if you are unsure of where or how to establish a physical connection to the network.

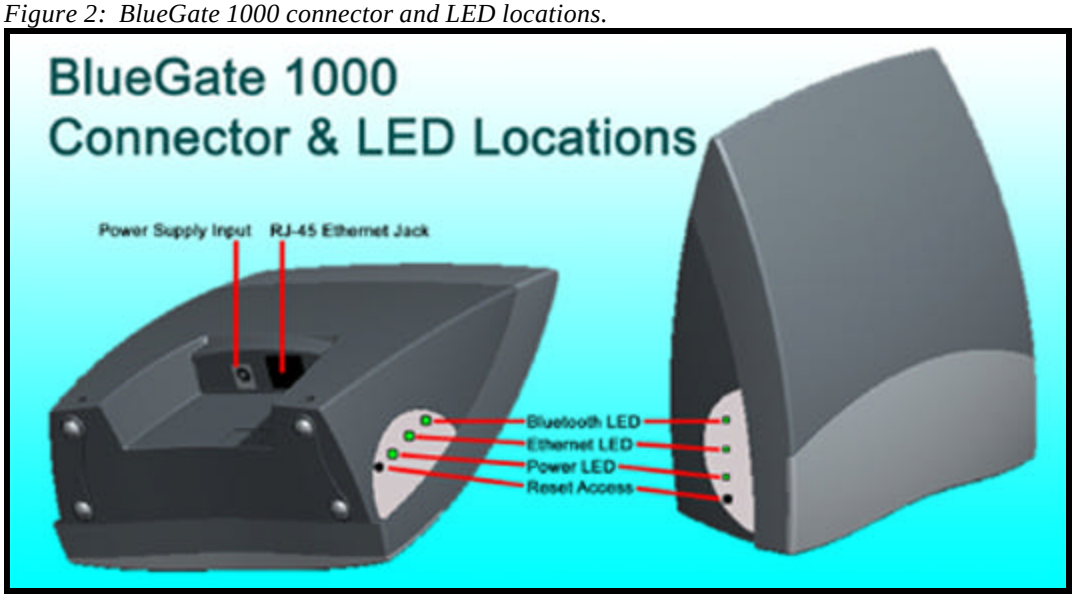
   Route the network cable away from other cables that may cause electrical interference. Avoid routing the cable through areas where it will be stepped on, tripped over, or damaged in any way.

NOTE: Telephone connections often use the RJ-45 connector; some wall plates, especially in office environments, have both telephone and network jacks in the same plate. When connecting through a wall plate of this type verify the physical connection between the jack and the network.

3. Plug the power supply into a wall outlet (120-220VAC, 60-50 Hz) and insert the small circular power plug into the power jack on the back of BlueGate 1000 (Figure 2). When power is applied the bottom light emitting diode (LED) will blink for 6 seconds and then stay on continuously.

If the LAN is 10Base-T or 100Base-T and a Dynamic Host Configuration Protocol (DHCP) server is available, BlueGate 1000 is ready to use.

Figure 2: BlueGate 1000 connector and LED locations.



4 Reset BlueGate 1000

BlueGate 1000 can be reset in several ways:

1. Click the Reset button on any internal Web page that it appears on.
2. Physically remove power from BlueGate 1000:
   - Unplug the power to the unit.
   - Wait 30 seconds.
   - Plug the power back in.
3. Press the hardware reset button for five seconds (see Figure 2).

NOTE: When the hardware-reset button is used to reset BlueGate 1000 the "Admin" user name and password are restored to the factory-default settings.

BlueGate 1000 can store up to seven user names and their associated passwords. The first name in the list is "Admin". The remaining user names/password entries are numbered User one through User six.

"Admin" holds the administrator's user name and password. The information that it contains can be re-configured (see Section 6.6.1.4).

The "Admin" factory default settings are:

- User name = "widcomm".
- Password = "admin".

NOTE: When BlueGate 1000 is reset in a DHCP environment it is possible that it will have a different IP address assigned to it by the server. See Section 5.1 for information on how to obtain the new IP address.

5 Access The Internal Web Server

BlueGate 1000 is setup and configured through an internal Web server.

Access to the internal Web server requires BlueGate 1000's IP address.

In a Dynamic Host Configuration Protocol (DHCP) environment the server assigns BlueGate 1000's IP address automatically.

A Java applet[1] that discovers BlueGate 1000's dynamically assigned IP address is included on the BlueGate 1000 compact disc (see Section 5.1).

In a non-DHCP environment BlueGate 1000 defaults to a static IP address that can be used to access the internal Web server (see Section 5.2).

Refer to Section 6.6 for specific configuration options and information on how to use them.

5.1 IP ADDRESS IN A DHCP ENVIRONMENT

To determine BlueGate 1000's IP address:

1. Create a directory named *C:\BGPolicy* on the system hard drive.
2. Copy *BGIPLookup.html*, *BGIPLookup.class*, *BGPolicy*, and *widcomm.jpg* from the root directory of the BlueGate 1000 compact disc to the new *C:\BGPolicy* directory.
3. Run Microsoft Internet Explorer, version 5.0 or higher, and open *BGIPLookup.html* from the *C:\BGPolicy* directory.
   If the Java Run-time Environment is not installed on your system, you will be prompted to download and install JRE from the Sun Microsystem's Web site (see Java Run-time Environment, Section 5.1.1). After completing the Java Run-Time Environment installation, return to this step to complete the process of getting an IP address.

NOTE: The Netscape browser is not supported in this release.

4. Enter the Media Access Control (MAC) address of BlueGate 1000 (located on the label on the bottom of the unit, see Figure 3) and click the "*Click here to Find IP Addr of BG WebServer*" button (DO NOT press enter).

The IP address of BlueGate 1000 is displayed in an Internet Explorer dialog box, (Figure 4, inset).

Click the **OK** button to close the dialog box and automatically open BlueGate 1000's internal Web page in Internet Explorer.

NOTE: The Java applet uses a UDP broadcast packet to interrogate BlueGate 1000 for its assigned IP address. UDP packets are not routed; be sure there is not a router between BlueGate 1000 and the computer.

[1] An applet is a JAVA-based program that is downloaded by a browser.

5.1.1 Java Run-time Environment

If version 1.3 of the Java Run-time Environment (JRE) is not installed on your computer, *BGIPLookup.html* (see above) will prompt you to install it from Sun Microsystem's Web site.

To install and configure JRE:

1. Select "Yes" when prompted to download JRE and follow the on-screen instructions.
2. Close Internet Explorer.
3. Open `C:\ProgramFiles\JavaSoft\JRE\1.3\lib\security\java.security` in a text editor.
4. Insert a blank line after the line:
   `policy.url.2=file:${user.home}/.java.policy`
5. On the blank line enter:
   `policy.url.3=file:/C:/BGPolicy/BGPolicy`
   This line points to the BGPolicy file in the C:\BGPolicy directory.
6. Save the file.

The Java Run-Time environment installation is complete. Return to Step 3 on page 5 and complete the determination of BlueGate 1000's IP address in a DHCP environment

Figure 3: The serial number label, located on the bottom of BlueGate 1000.

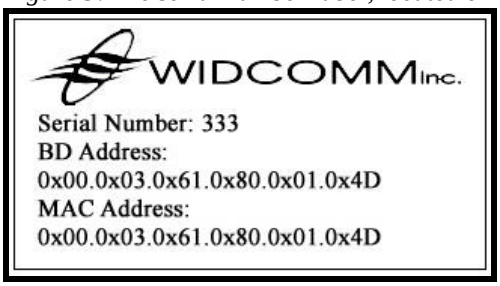
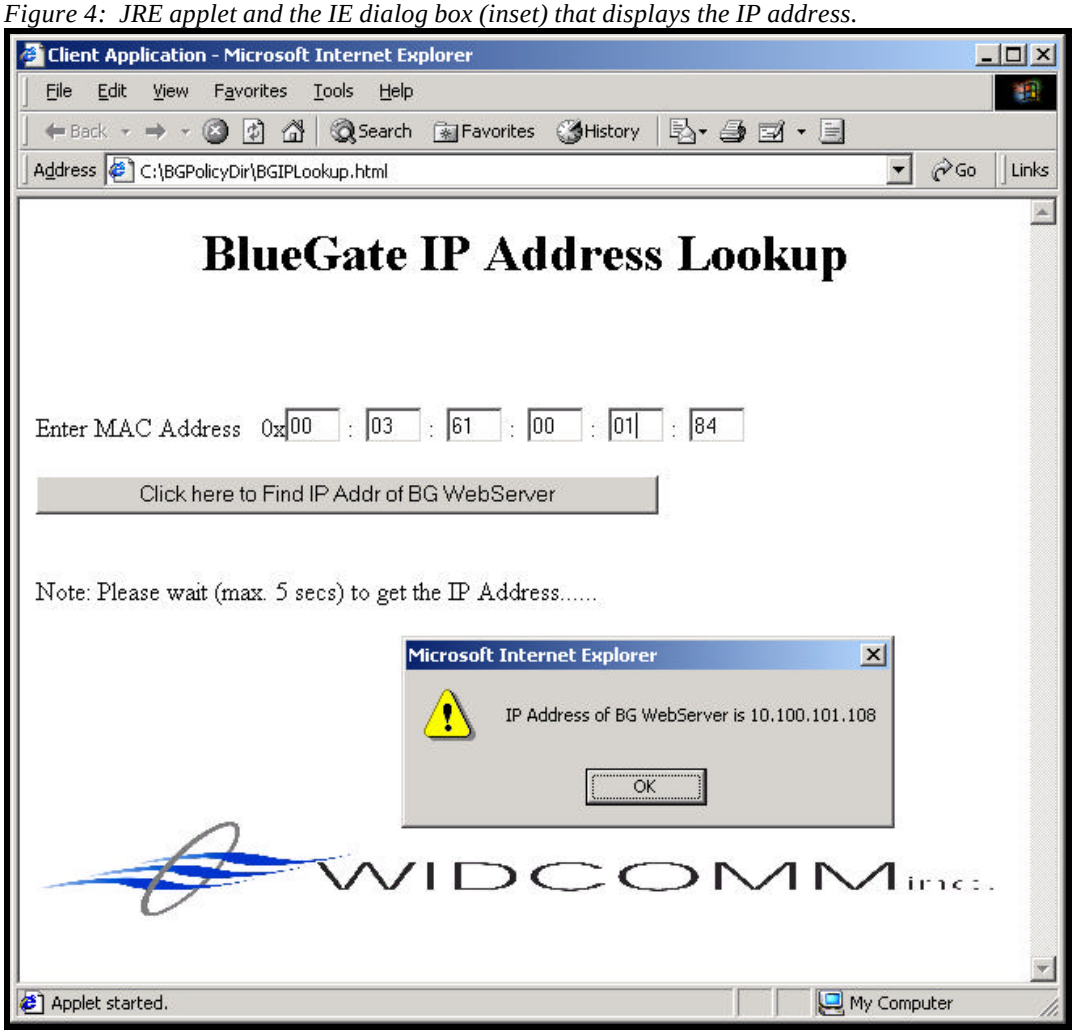


Figure 4: JRE applet and the IE dialog box (inset) that displays the IP address.



5.2 IP ADDRESS IN A NON-DHCP ENVIRONMENT

BlueGate 1000's internal Web pages can be accessed using a static IP address.

When DHCP is enabled (factory default), the DHCP attempt must first timeout before attempting to access BlueGate 1000's internal Web pages using the static IP address.

After the DHCP timeout (120 seconds), BlueGate 1000 uses the configured static IP address.

The factory-default static IP address is: 192.168.0.1.

To access BlueGate 1000's internal Web server using the static IP address, create a two-node private network between a single computer and BlueGate 1000:

1. Connect BlueGate 1000 and the computer (see Figure 5):
   - **Solution One:** use standard Ethernet cables to establish a connection through a switch or hub.
   - **Solution Two:** use a crossover cable to create a direct connection. (Figure 6 shows the connections for a crossover cable.)
2. Configure the computer:
   - Static IP address of 192.168.0.2.
   - Subnet mask of 255.255.255.0.
3. Run Internet Explorer, version 5.0 or higher, and enter http://192.168.0.1 in the address field.
4. Press ENTER or click Go.

NOTE: The default static IP address for BlueGate 1000 can be changed through the Configuration > Setup option on the internal Web pages. If BlueGate 1000's static IP address has been reconfigured, enter the current address.

Figure 5: Two-node private network options.

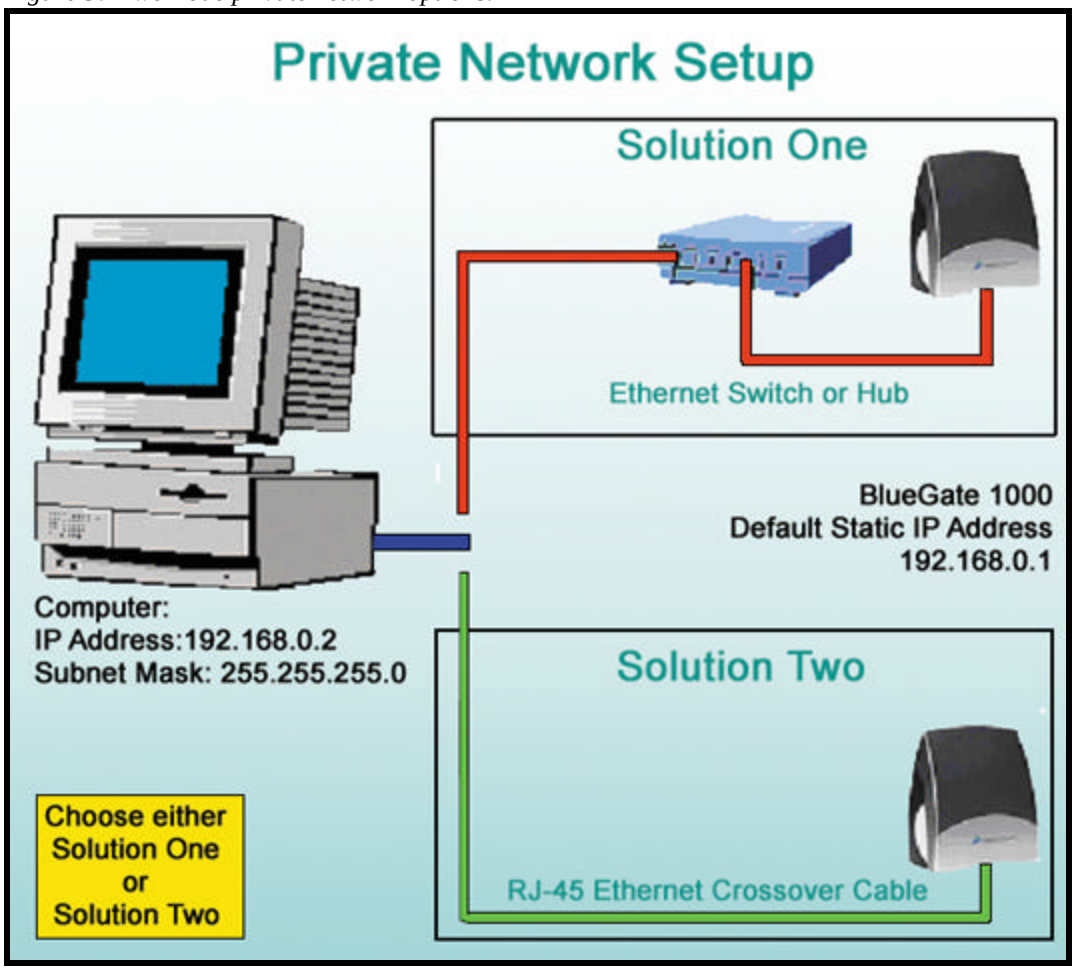
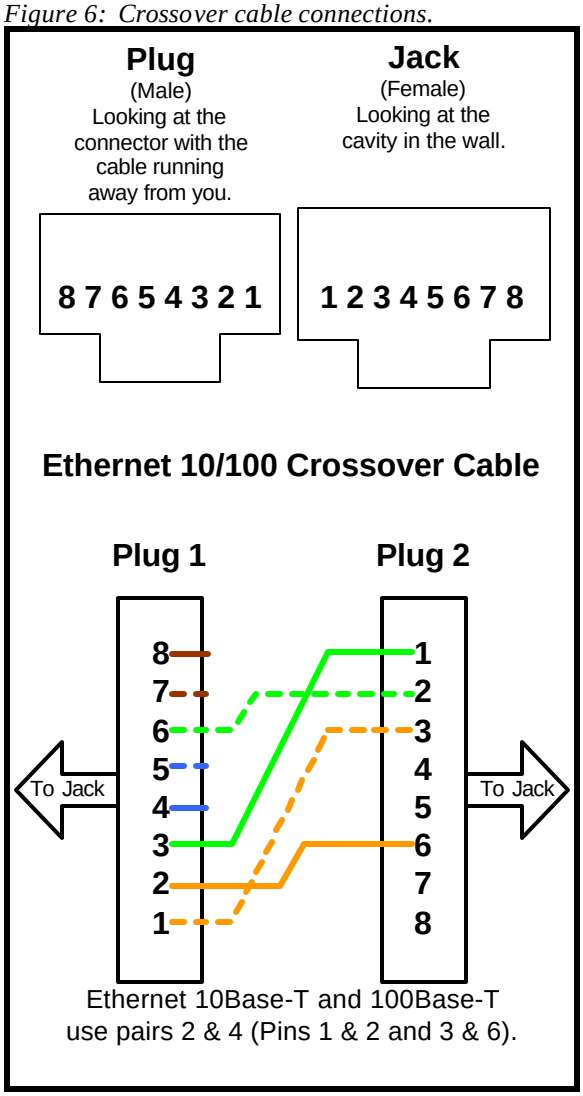


Figure 6: Crossover cable connections.



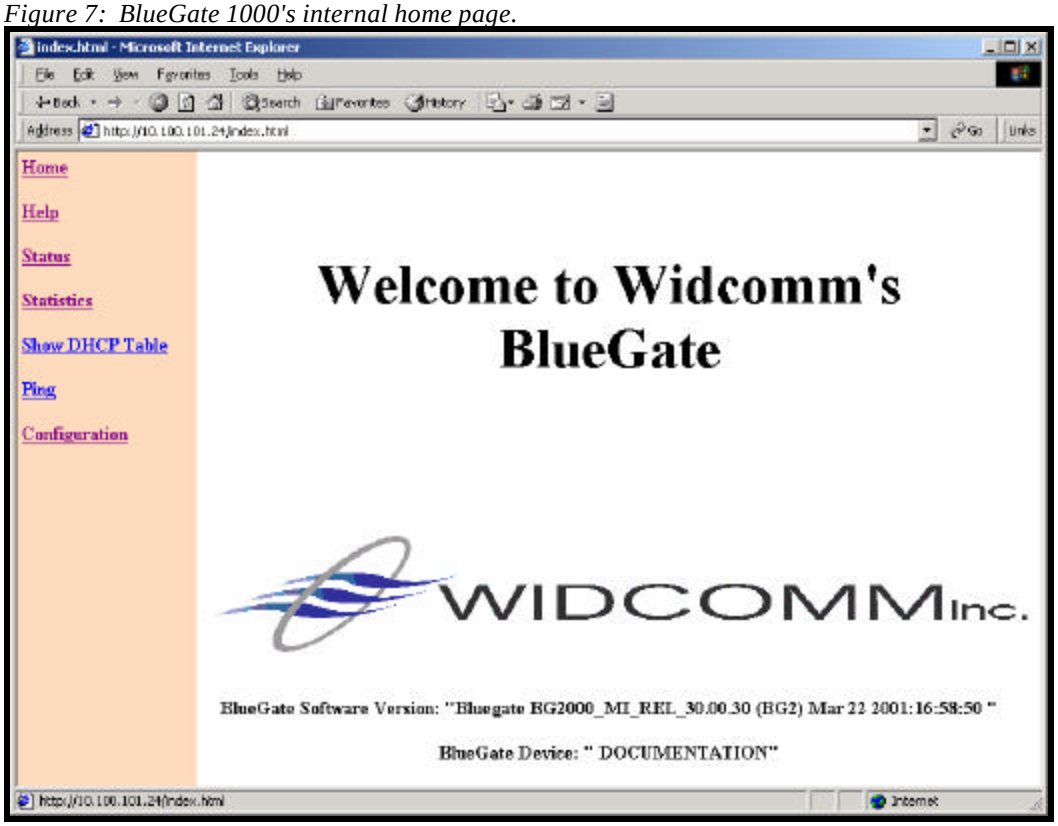
6 Internal Web Server

To access BlueGate 1000's internal Web server:

- In a DHCP environment:
  1. Run Internet Explorer and open the Java applet *BGIPLookup.html* (see section 5.1 for details)
  2. Enter BlueGate 1000's Media Access Control (MAC) address from the label on the bottom of BlueGate 1000.
  3. Click **OK** in the dialog box that returns the IP address. The internal home page opens automatically in Internet Explorer.
- In a non-DHCP (private network) environment (see section 5.2 for details about setting up a private network):
  1. Run Internet Explorer.
  2. Enter http://192.168.0.1 in the address area.
  3. Click **Go** or press the ENTER key. BlueGate 1000's internal home page opens in Internet Explorer.

In the figures in this section, the Java applet *BGIPLookup.html* was used to obtain the DHCP server-assigned IP address and open the internal home page.

Figure 7: BlueGate 1000's internal home page.



Click the *Home* hyperlink on the left edge of any internal Web page to return to the home page.

The remainder of this section describes the internal Web pages associated with the other hyperlinks in the left pane of Internet Explorer.

6.1 HELP

The *Help* hyperlink displays an internal Web page with links to on-line resources:

- BlueGate technical support.
- The WIDCOMM Web site.

6.2 STATUS

The *Status* hyperlink displays an internal Web page that provides access to additional pages that contain information related to the network and Bluetooth settings of BlueGate 1000.

The links at the top of the Status page display:

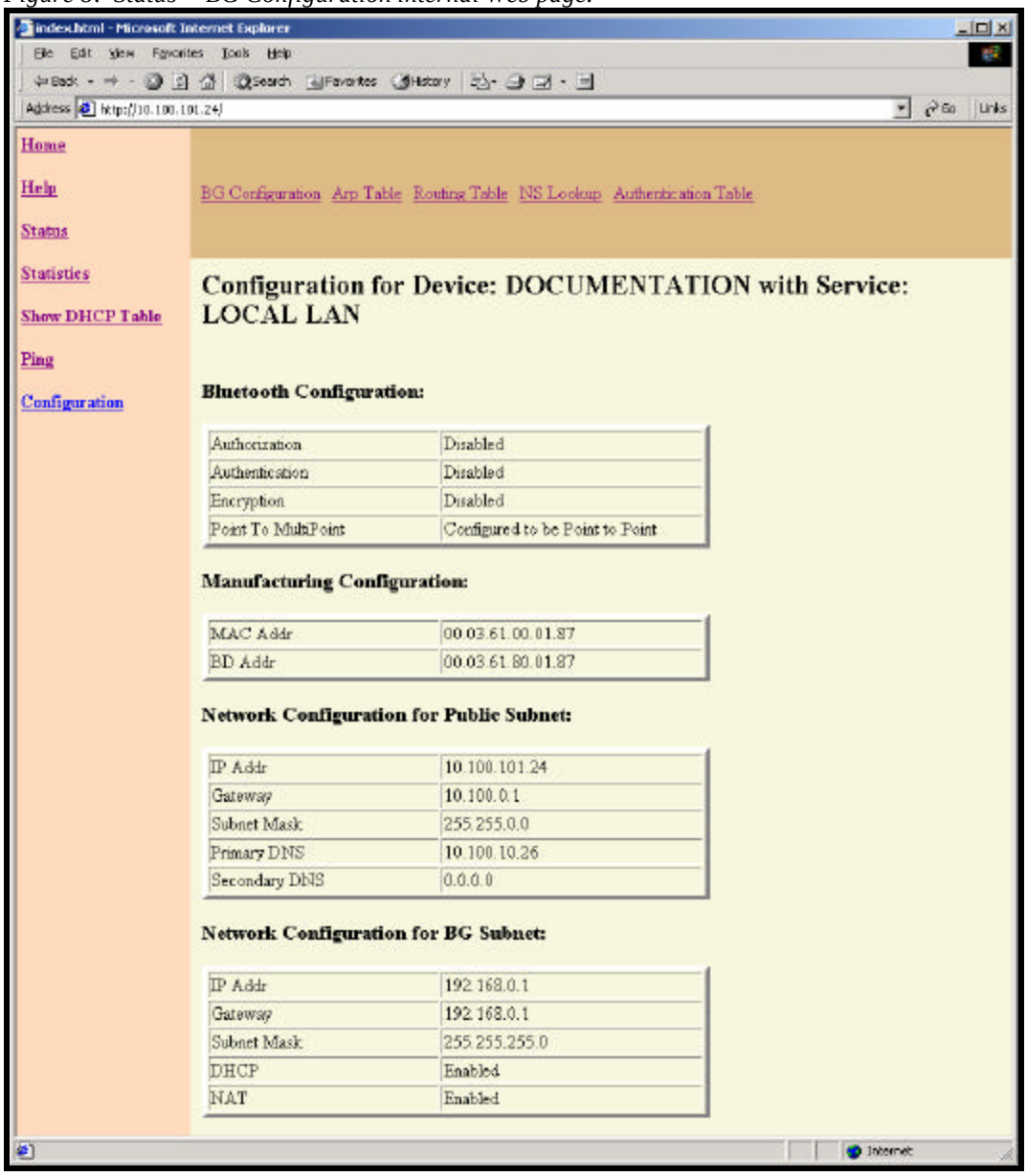
- **BG Configuration**—basic network and Bluetooth security settings.
- **ARP Table**—the active Address Resolution Protocol entries.
- **Routing Table**—the active routing entries.
- **NS Lookup**—a list of recently accessed IP addresses and the host names associated with them.
- **Authentication Table**—the Bluetooth authentication-level security table.

6.2.1 BG Configuration

The Status > BG Configuration internal Web page (Figure 8) displays Bluetooth and network settings, including:

- Bluetooth security configuration settings:
  - Authorization.
  - Authentication.
  - Encryption.
- Manufacturing configuration settings:
  - MAC (Media Access Control) address.
  - BD Addr (Bluetooth Device address).
- Public network configuration settings:
  - IP (Internet Protocol) address.
  - Gateway.
  - Subnet Mask.
  - Primary DNS (Domain Name System) Server.
  - Secondary DNS Server.
- Private network configuration settings:
  - IP address.
  - Gateway.
  - Subnet Mask.
  - DHCP.
  - NAT.

Figure 8: Status > BG Configuration internal Web page.

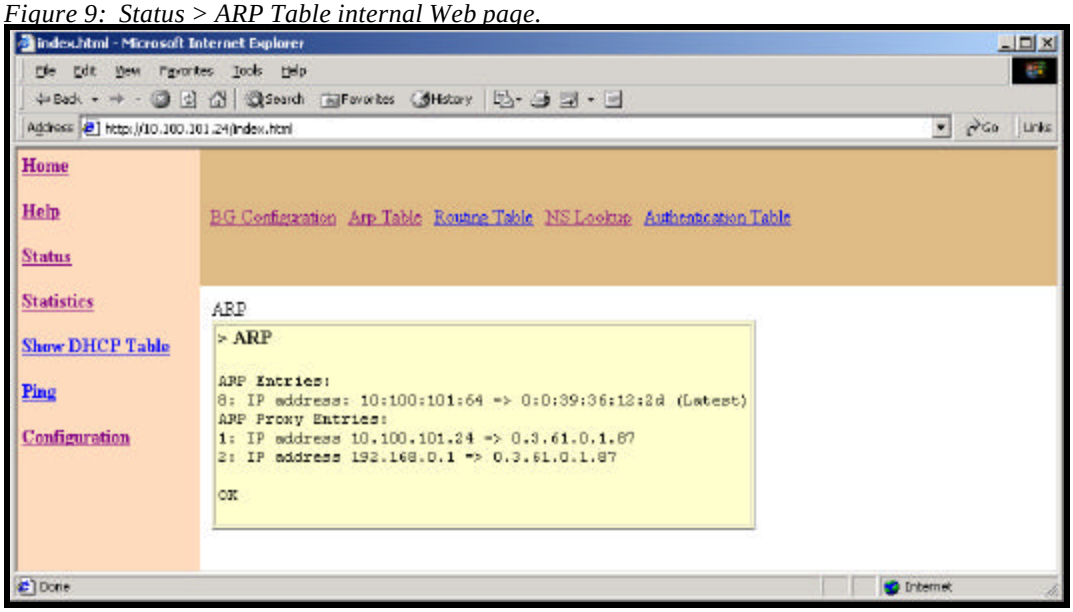


6.2.2 ARP Table

The Status > ARP Table internal Web page (Figure 9) displays the active Address Resolution Protocol (ARP) entries in BlueGate 1000, including:

- Entries for Ethernet devices communicating with BlueGate 1000.
- Proxy entries for Bluetooth devices.

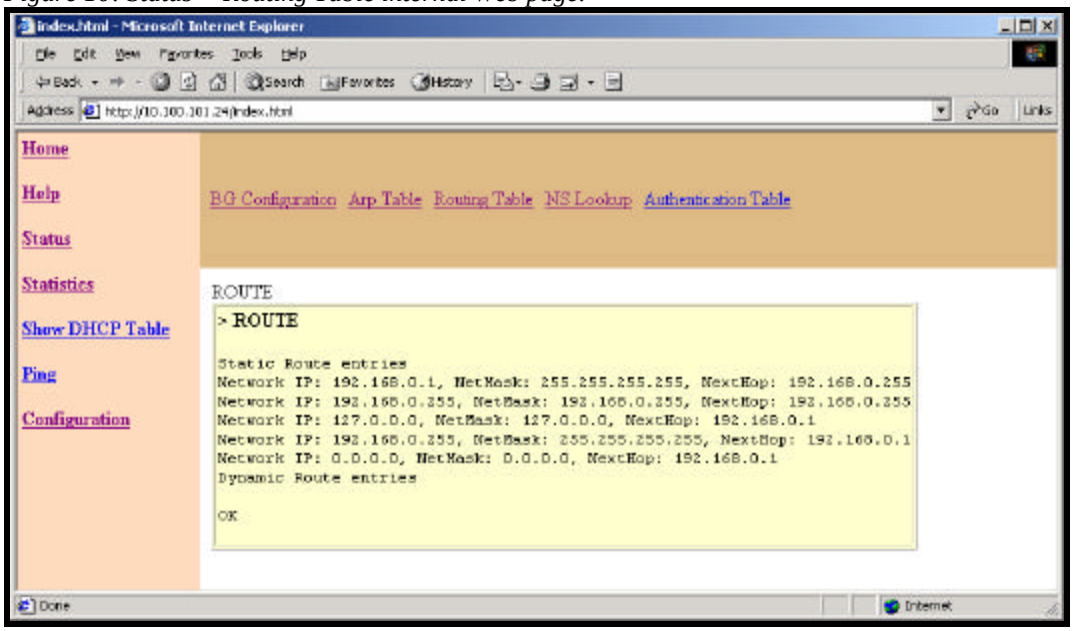
Figure 9: Status > ARP Table internal Web page.



6.2.3 Routing Table

The Status > Routing Table internal Web page displays the active routing entries for loop-back, gateway, and other network node…

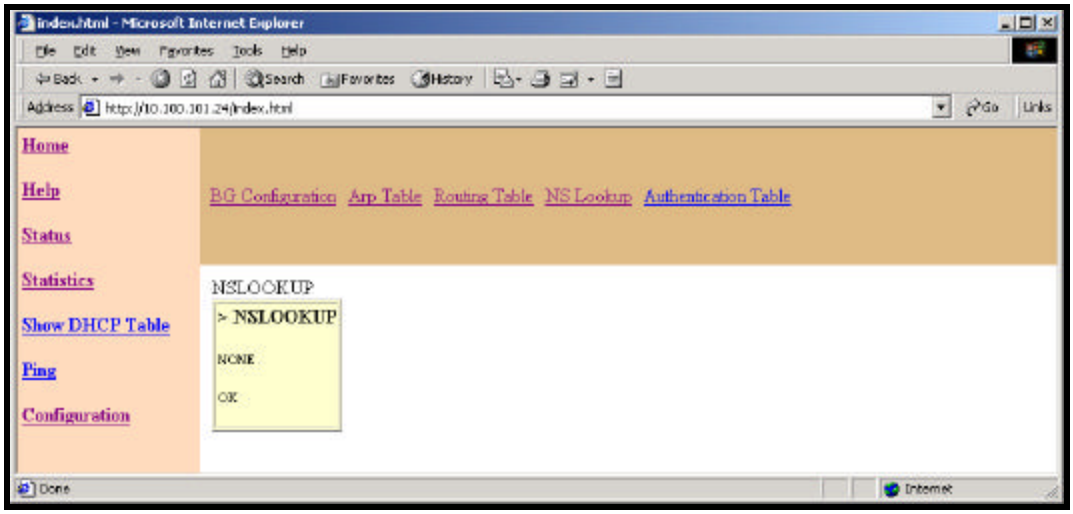
Figure 10: Status > Routing Table internal Web page.



6.2.4 NS Lookup

The Status > NS Lookup internal Web page displays recently accessed IP addresses and the host names associated with them.

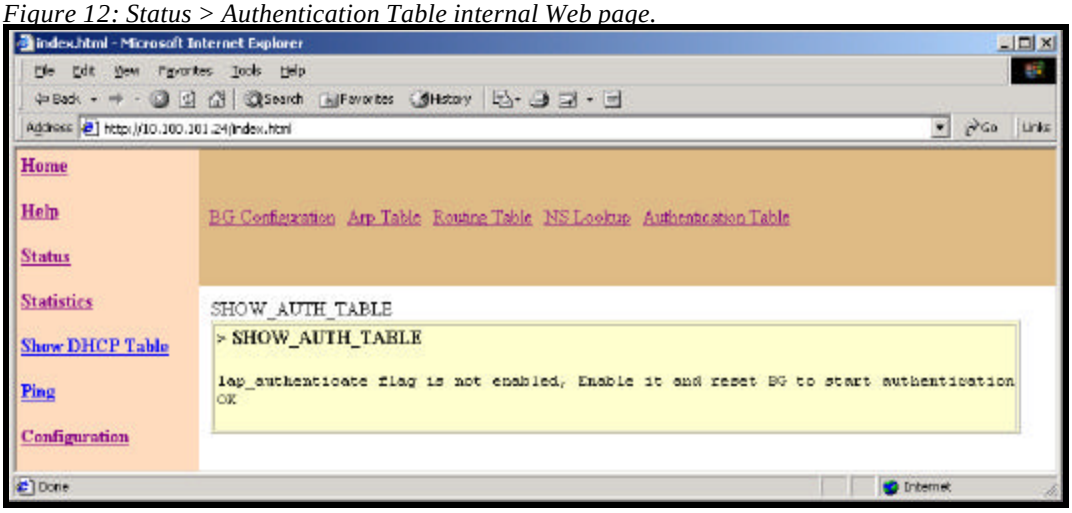
Figure 11: Status > DNS Lookup internal Web page.



6.2.5 Authentication Table

The Status > Authentication Table internal Web page displays the contents of the table used for Bluetooth security. This table contains the mapping between the Bluetooth device addresses (BD Addresses) and Bluetooth device attributes, including Pin Code and Link Key or individual PIN code if authentication is enabled separately for each device; otherwise it displays the fixed Pin Code if a fixed Pin Code is enabled for all devices.

Figure 12: Status > Authentication Table internal Web page.



6.3 STATISTICS

The statistics hyperlink displays an internal Web page that provides access to additional Web pages. The additional pages contain read only information related to the network and the Bluetooth settings of BlueGate 1000.

These functions display a snapshot of network statistics.

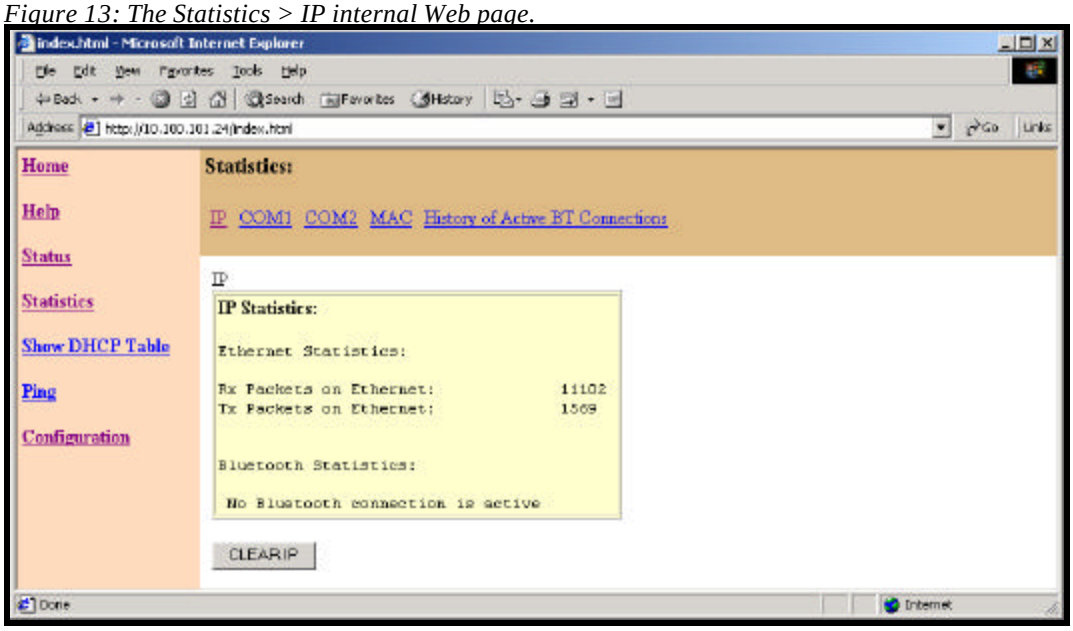
- **IP**—displays network packet counts.
- **COM1—**reserved for use by WIDCOMM technicians.
- **COM2—**reserved for use by WIDCOMM technicians.
- **MAC—**displays framing and error information related to the MAC layer.
- **History of Active BT Connections—**shows connection statistics.

6.3.1 IP

The Statistics > IP internal Web page displays the number of IP packets transmitted and received by BlueGate 1000 on the Ethernet and Bluetooth connections.

The CLEAR IP button resets the counters to zero.

Figure 13: The Statistics > IP internal Web page.



6.3.2 COM1 & COM2

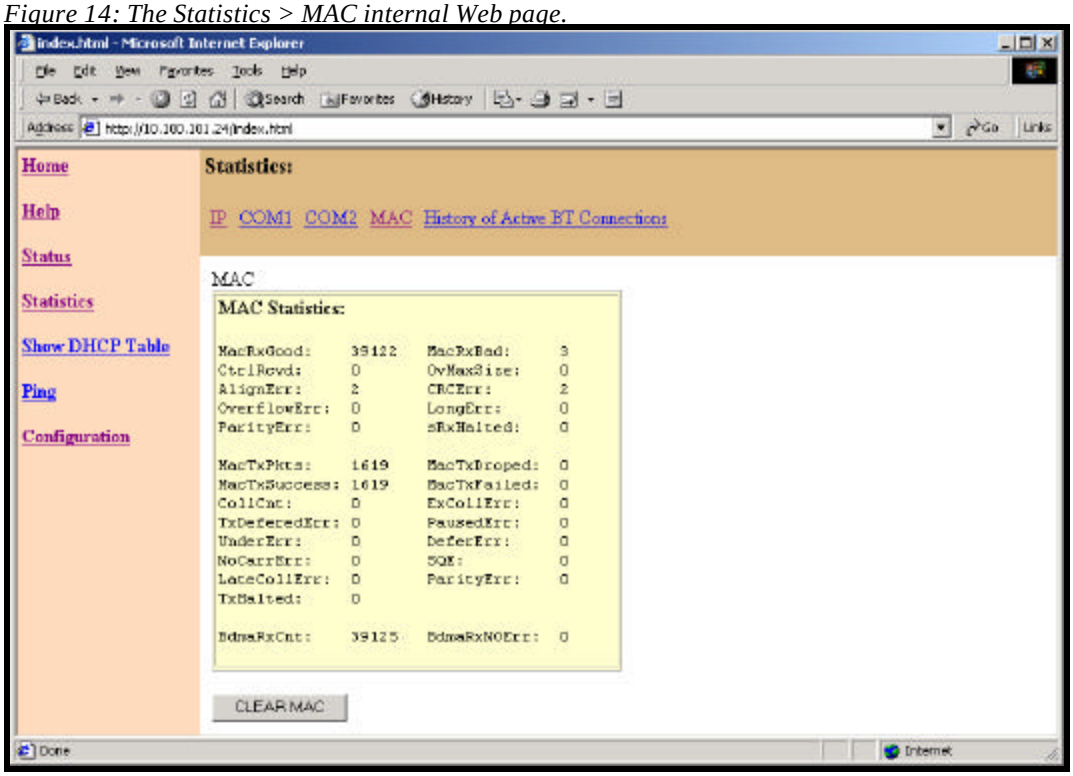
Reserved for use by WIDCOMM technicians.

6.3.3 MAC

The Statistics > MAC internal Web page displays statistics related to the MAC (Media Access Control) layer.

The CLEAR MAC button resets the counters to zero.

Figure 14: The Statistics > MAC internal Web page.

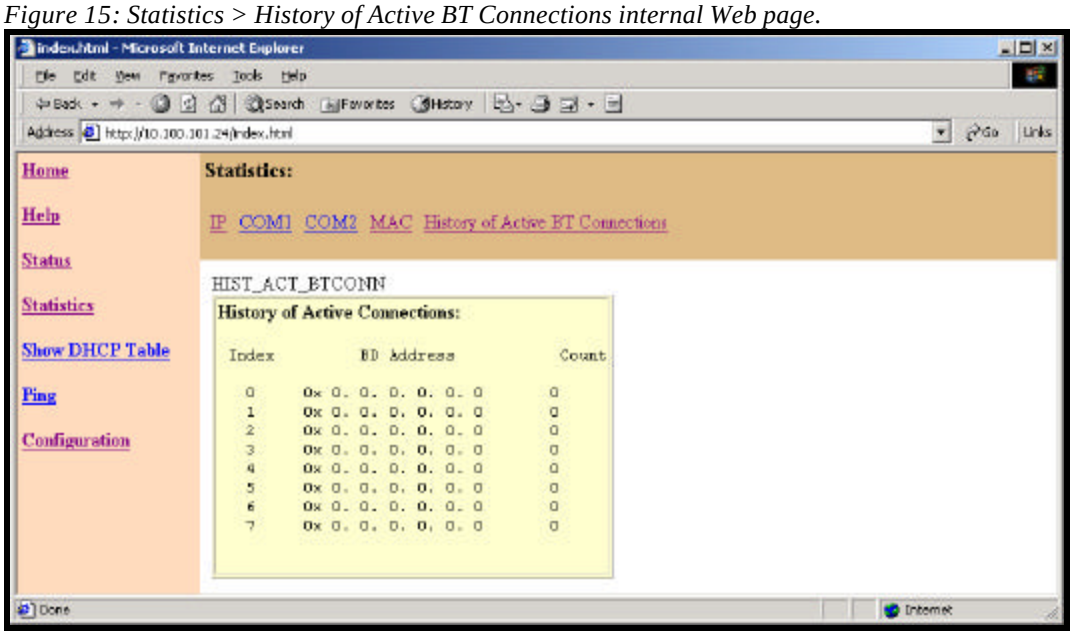


6.3.4 History of Active BT Connections

The Statistics > History of Active BT Connections internal Web page displays the number of times a connection was successful with a particular Bluetooth device address (BD Address).

The list displays only the eight most recently connected Bluetooth devices.

Figure 15: Statistics > History of Active BT Connections internal Web page.



6.4 SHOW DHCP TABLE

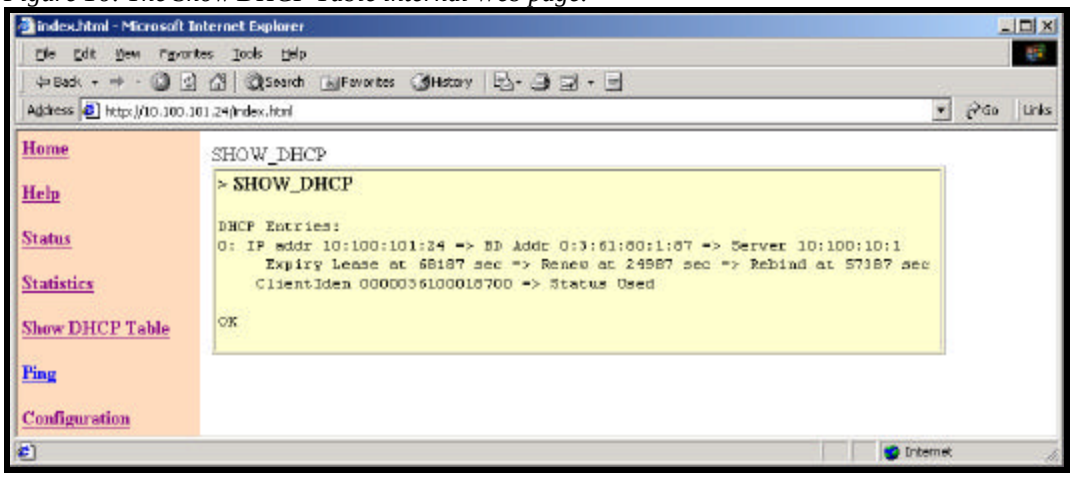
The Show DHCP Table hyperlink displays the IP addresses assigned by the DHCP server for use by BlueGate 1000 and its clients.

If Network Address Translation (NAT) is enabled this page displays a single entry that corresponds to IP address of BlueGate 1000.

If NAT is disabled this page displays multiple entries that correspond to BlueGate 1000 and the Bluetooth devices connected to it.

If DHCP is disabled no DHCP entries will exist, regardless of the NAT setting.

Figure 16: The Show DHCP Table internal Web page.



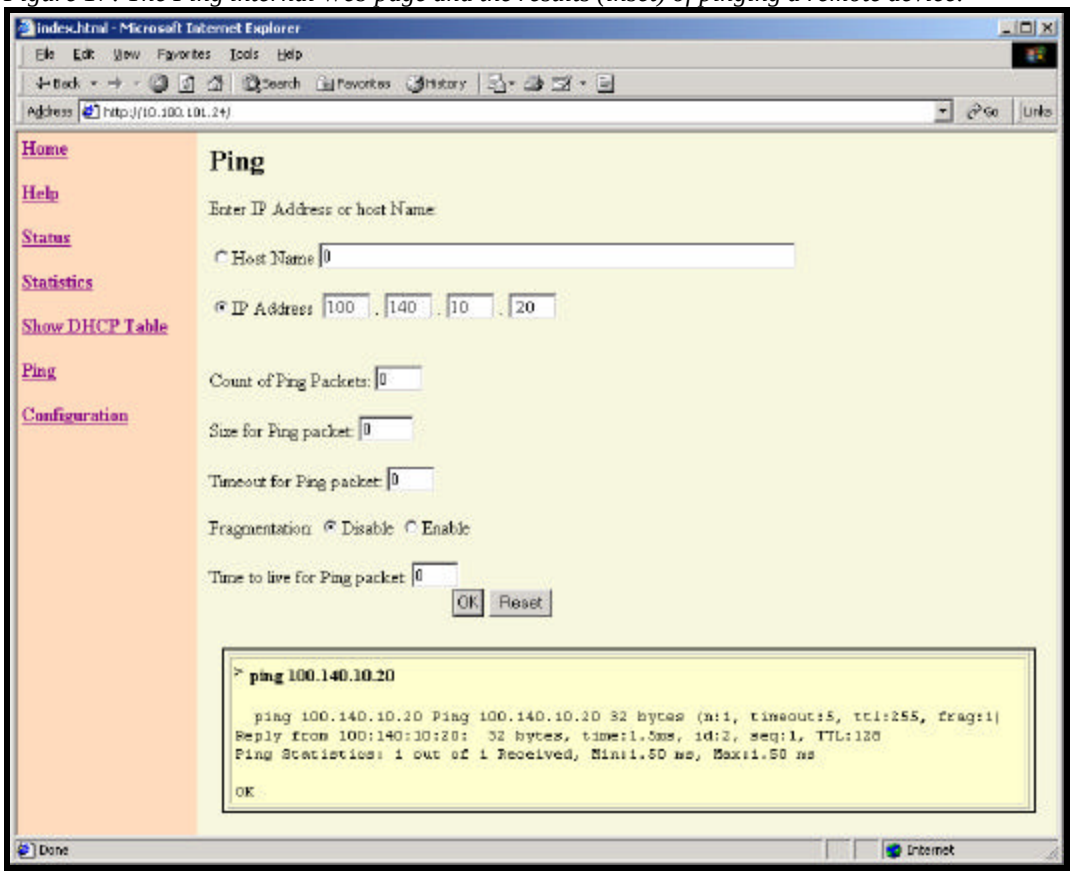
6.5 PING

The Ping hyperlink displays an internal Web page that provides a way to send network packets to a designated network device. The remote device echoes the packets, in the process providing information about the performance of the network connection.

The **OK** button executes the ping operation.

The **Reset** button resets all fields to zero.

Figure 17: The Ping internal Web page and the results (inset) of pinging a remote device.



6.6 CONFIGURE BLUEGATE 1000

The Configuration hyperlink provides access to the internal BlueGate 1000 configuration Web pages.

A logon screen (Figure 18) appears when "Configuration" is clicked.

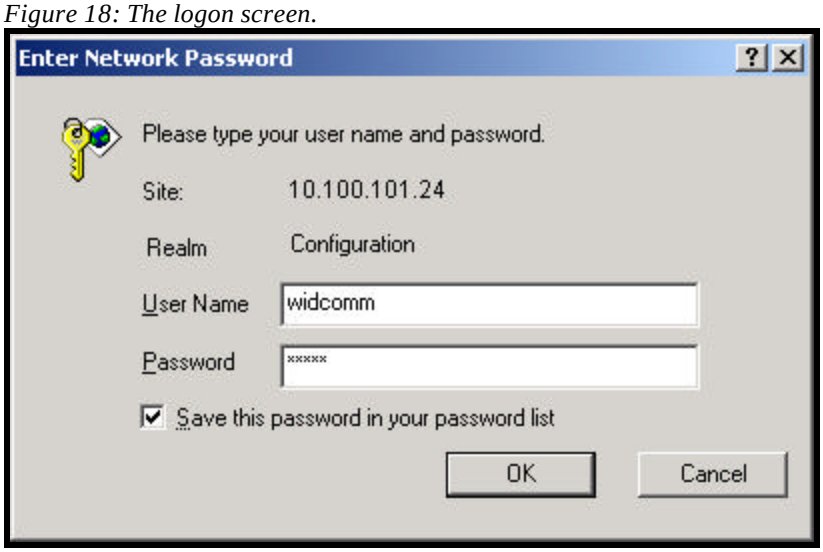
To logon:

1. Enter the user name "widcomm".
2. Enter the password "admin".
3. Click the **OK** button to display the Configuration main page.

NOTE: The administrator's user name and password are re-configurable (see section 6.6.1.4). If they have been changed, enter the appropriate user name and password. If the new user name and/or password has been lost or forgotten refer to section 4 for information about restoring the defaults.

Select the "*Save this password in your password list*" option if desired.

Figure 18: The logon screen.

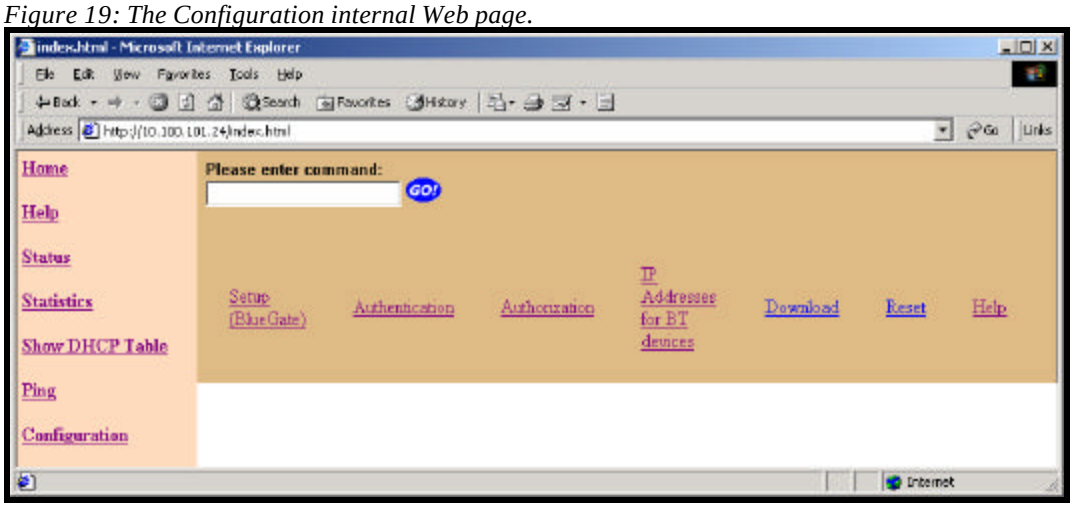


6.6.1 Main Page

The Configuration main Web page (Figure 19) contains:

- **Please enter command:**—an input field used to issue direct commands to the BlueGate 1000 software engine. See section 7 for command usage and syntax.
- **Setup (BlueGate)**—displays an internal Web page that provides a means to alter the configuration of BlueGate 1000.
- **Authentication**—displays an internal Web page used to configure security requirements for devices using BlueGate 1000.
- **Authorization**—displays an internal Web page used to setup the user names and passwords of authorized Bluetooth users.
- **IP Addresses for BT Devices**—displays an internal Web page that provides a means to enter IP addresses in three ranges.
- **Download**—displays an internal Web page that is used by customer support and other WIDCOMM technical personnel to download software to BlueGate 1000.
- **Reset**—Resets BlueGate 1000. This option does not display a separate Web page; instead a confirmation dialog box is displayed.
- **Help**—displays a list of commands that can be entered in the "*Please enter command:*" field. This option does not display a separate Web page; information is displayed in the white area of the main window.

Figure 19: The Configuration internal Web page.



6.6.1.1 Please Enter Command: Field

The *Please enter command* input field is used to issue direct commands to the BlueGate 1000 software engine. Type the command in the field and click "Go" or press ENTER.

The available commands are described in Section 7.

For a list of available commands type "help" or "?" in the *Please enter command* field and click "Go" or press the ENTER key.

6.6.1.2 Setup (BlueGate)

The Configuration > Setup (BlueGate) internal Web page (Figure 20) is used to configure BlueGate 1000.

Settings can also be modified one at a time with command line parameters using the *Please enter command* field. See Sections 6.6.1.1 and 7 for more information.

The available options are:

Bluetooth Settings

- User-friendly Device Name.
- Service Name.
- Encryption.
- Point-to-Multipoint
- Authorization.
- Authentication.

Network Settings

- IP address.
- Gateway.
- Subnet Mask.
- Primary/Secondary DNS Server.
- DHCP Enabled/Disabled.
- NAT Enabled/Disabled.

Make changes to the configuration of BlueGate 1000 by entering information in the fields and/or selecting radio buttons. Use the TAB key to move between fields.

Click the **Update** button to store the changes in BlueGate 1000's non-volatile memory.

The updated configuration is displayed in the white area of the Configuration > Setup Web page) and reflected on the Status > BG Configuration (Figure 8) Web page.

For the changes to take affect BlueGate 1000 must be reset (see Section 4).

NOTE: Setup changes do not take affect until BlueGate 1000 is reset.

6.6.1.2.1 Device Name

The device name is used to help identify BlueGate 1000 to other Bluetooth devices. It is limited in length to 100 characters.

To change the Device Name, highlight the existing text and type the new name.

Example : My BlueGate Network Access Point.

6.6.1.2.2 Service Name

The Service Name is the name for the LAN Access Profile service that BlueGate 1000 displays to remote devices. It is limited in length to 100 characters.

The default service for the LAN Access Profile is "*LOCAL LAN*".

To change the Service Name, highlight the existing text and type the new name.

Example : LAN Access.

6.6.1.2.3 IP Addr

IP Addr is the IP address of BlueGate 1000. This box contains two fields:

- **Active IP Addr**: the IP address in use by the BlueGate 1000.
  - If DHCP is enabled, this is the address assigned to BlueGate 1000 by the network DHCP server the last time BlueGate 1000 was started or reset.
  - If DHCP is disabled, this is the fixed IP address that was in non-volatile memory the last time BlueGate 1000 was started or reset.
- **Stored NV IP Addr**: the fixed IP address in BlueGate 1000's non-volatile memory. When DHCP is disabled this address is used by BlueGate 1000 as its IP address.
  To change the fixed IP address:
  - Highlight the existing address and type the new one in dotted decimal notation.
  - Click the Update button.
  - Reset BlueGate 1000.

Example: `192.168.0.50`

NOTE: Changes to values stored in NVRAM do not take affect until BlueGate 1000 is reset.

6.6.1.2.4 Gateway

Gateway is the IP address of the LAN gateway to which BlueGate 1000 will route packets destined for outside networks. This box contains two fields:

- **Active Gateway Addr**: the gateway address in use by BlueGate 1000.
  - If DHCP is enabled, it is the address provided to the BlueGate 1000 by the network's DHCP server the last time BlueGate 1000 was started or reset.
  - If DHCP is disabled, this is the fixed gateway address that was in non-volatile memory the last time BlueGate 1000 was started or reset.
- **Stored NV Gateway Addr**: the fixed gateway address stored in BlueGate 1000's non-volatile memory. If DHCP is disabled this address is used to determine BlueGate 1000's gateway address at startup.
  To change the gateway address:
  - Highlight the existing address and type the new one in dotted decimal notation.
  - Click the Update button.
  - Reset BlueGate 1000.

Example: `100.140.0.1`

6.6.1.2.5 Subnet Mask

The Subnet Mask is used to identify the subnet to which an IP address belongs. This box contains two fields:

- **Active Subnet Mask**: the subnet mask in use by BlueGate 1000.
  - If DHCP is enabled it is the subnet mask provided by the network DHCP server the last time BlueGate 1000 was started or reset.
  - If DHCP is disabled, this is the fixed subnet mask that was in non-volatile memory the last time BlueGate 1000 was started or reset.
- **Stored NV Subnet Mask**: the fixed subnet mask stored in BlueGate 1000's non-volatile memory. If DHCP is disabled this address is used to determine BlueGate 1000's subnet mask at startup.
  To change the subnet mask:
  - Highlight the existing subnet mask and type the new one in dotted decimal notation.
  - Click the Update button.
  - Reset BlueGate 1000.

Example: `255.255.255.0`

6.6.1.2.6 Primary DNS

Primary DNS is the IP address of the primary Domain Name System server. When a DNS server is provided with a "hostname", it returns the host's IP address. This box contains two fields.

- **Active Primary DNS**: the IP address of the primary DNS server in use by BlueGate 1000.
  - If DHCP is enabled, it is the primary DNS server provided the network DHCP server the last time BlueGate 1000 was started or reset.
  - If DHCP is disabled, this is the fixed IP address of the primary DNS server that was in non-volatile memory the last time BlueGate 1000 was started or reset.
- **Stored NV Primary DNS**: the IP address for primary DNS server stored in BlueGate 1000's non-volatile memory. If DHCP is disabled this address is used to determine the BlueGate 1000's primary DNS server at startup. To change the Primary DNS address:
  - Highlight the existing address and type the new one in dotted decimal notation.
  - Click the Update button.
  - Reset BlueGate 1000.

Example: `100.140.10.1`

6.6.1.2.7 Secondary DNS

Secondary DNS is the IP address of the secondary Domain Name System server. The secondary DNS server is used if the primary DNS server is either unavailable or unable to translate a submitted host name to an IP address. This box contains two fields.

- **Active Secondary DNS**: the IP address of the secondary DNS server in use by BlueGate 1000.
  - If DHCP is enabled, it is the secondary DNS server provided to by the network's DHCP server the last time BlueGate 1000 was started or reset.
  - If DHCP is disabled, this is the fixed IP address of the secondary DNS server that was in non-volatile memory the last time BlueGate 1000 was started or reset.
- **Stored NV Secondary DNS**: the IP address for the secondary DNS server that isstored in BlueGate 1000's non-volatile memory. If DHCP is disabled this address is used to determine BlueGate 1000's secondary DNS server at startup. To change the Secondary DNS address:
  - Highlight the existing address and type the new one in dotted decimal notation.
  - Click the Update button.
  - Reset BlueGate 1000.

Example: `100.140.10.1`

6.6.1.2.8 DHCP

DHCP (Dynamic Host Configuration Protocol) automatically assigns IP addresses on a network.

Enable/disable DHCP by clicking the appropriate radio button.

- When DHCP is enabled, BlueGate 1000's IP address is obtained from the DHCP server.
- When DHCP is disabled, fixed IP addresses are read from BlueGate 1000's on-board NVRAM.

NOTE: If DHCP is enabled BlueGate 1000 ignores the IP address(es) stored in its NVRAM.

6.6.1.2.9 NAT

NAT (Network Address Translation) is an Internet standard that allows a network to use one set of IP addresses for internal traffic and a different set of addresses for external traffic.

BlueGate 1000 handles address translations between the LAN (external) and the Bluetooth devices (internal) connected to BlueGate 1000.

Enable/disable NAT by clicking the appropriate radio button.

- If NAT is enabled, BlueGate 1000 automatically assigns an IP address to each connected Bluetooth device.
- If NAT is disabled *and*:
  - DHCP is enabled, Bluetooth devices get their IP address from the DHCP server.
  - DHCP is disabled, the IP address for each Bluetooth device must be configured in BlueGate 1000's NVRAM.

The table at the bottom of the Configuration > Setup (BlueGate) internal Web page shows the possible combinations of DHCP and NAT enabled/disabled.

6.6.1.2.10 Encryption

Encryption is the translation of data into a secret code. Encryption is a link-level security feature of Bluetooth; it requires no user input.

When enabled, encryption only applies to data transferred between Bluetooth devices—data transferred via the network is not encrypted.

To enable encryption, authentication must also be enabled. ***If authentication is not enabled, the encryption setting is ignored and the connection is not encrypted.***

Enable/disable Encryption by clicking the appropriate radio button.

NOTE: Do not enable Encryption if the connecting device does not support security.

6.6.1.2.11 Point-to-Multipoint

Point-to-Multipoint refers to the ability of a device to connect to more than one remote device at the same time.

BlueGate 1000's point-to-multipoint ability, when enabled, is limited to seven devices.

To enable/disable point-to-multipoint click the appropriate radio button.

6.6.1.2.12 Authorization

Authorization is part of the process of granting or denying access to a resource. A user name and password are required.

Computer security systems are frequently based on a two-step process:

- Authentication ensures that a user is who he claims to be.
- Authorization allows access to resources, based on the user's identity

If authorization is disabled, all users are allowed to connect to BlueGate 1000.

If authorization is enabled, only specific users can connect to BlueGate 1000.

See Section 6.6.1.4 for information on how to configure user authorization.

NOTE: Do not enable Authorization if the connecting device does not support security.

6.6.1.2.13 Authentication

Authentication is part of the process of granting or denying access to a resource.

Computer security systems are frequently based on a two-step process:

- Authentication ensures that a user is who he claims to be.
- Authorization allows access to resources, based on the user's identity.

Authentication, in this context, applies only to access to BlueGate 1000; it does not necessarily permit access to any higher-level network services.

If authentication is disabled, all Bluetooth devices are allowed to connect to BlueGate 1000.

If authentication is enabled:

- A single fixed Pin Code may be used for all devices.
- A different Pin Code may be used for each device.

See Section 6.6.1.3 for more information on how to configure authentication.

Enabling authentication generates a link key for each device. Link keys are based on the PIN code and the Bluetooth device address.

NOTE: Do not enable Authentication if the connecting device does not support security.

Figure 20: The Configuration > Setup (BlueGate) internal Web page.

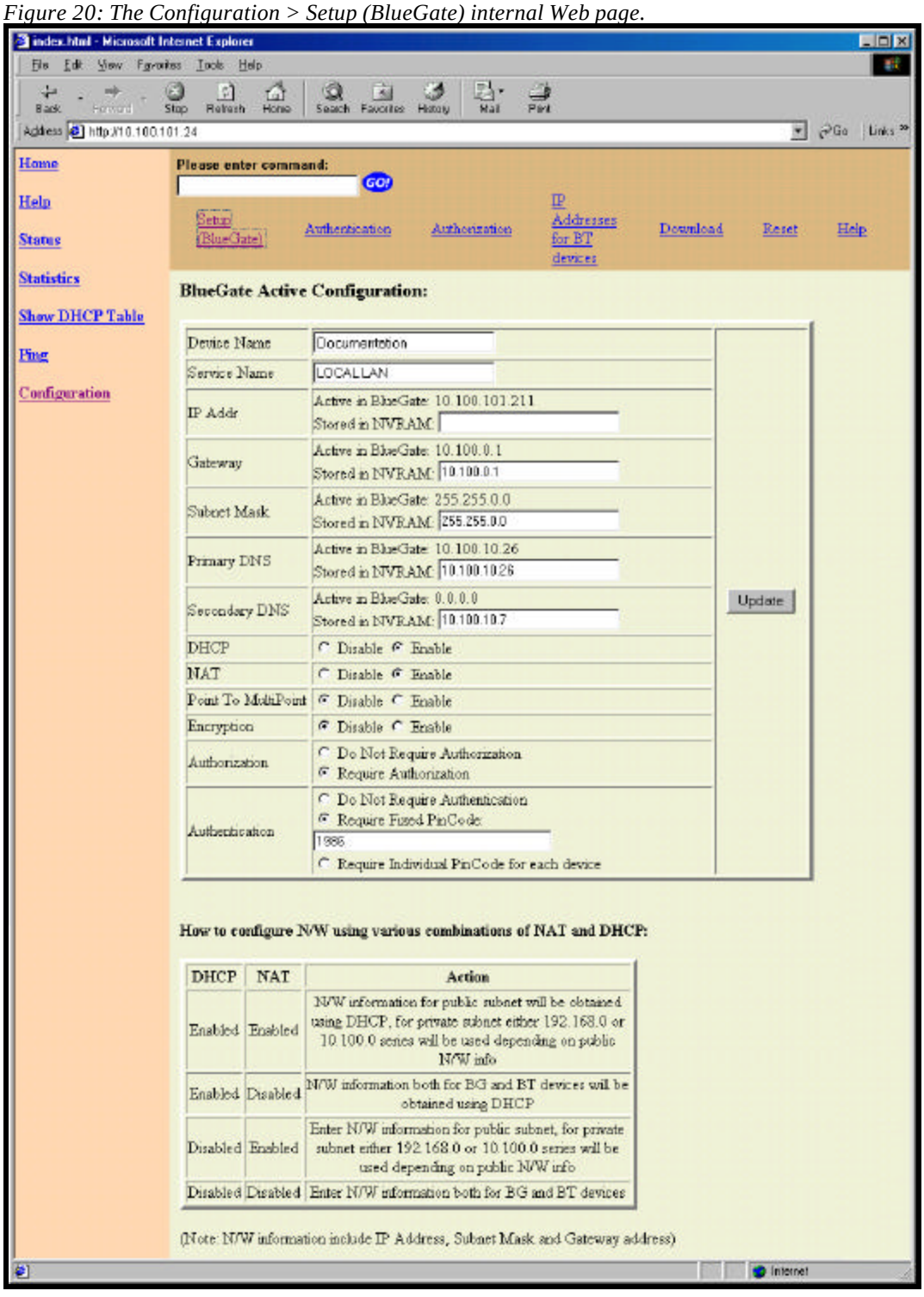
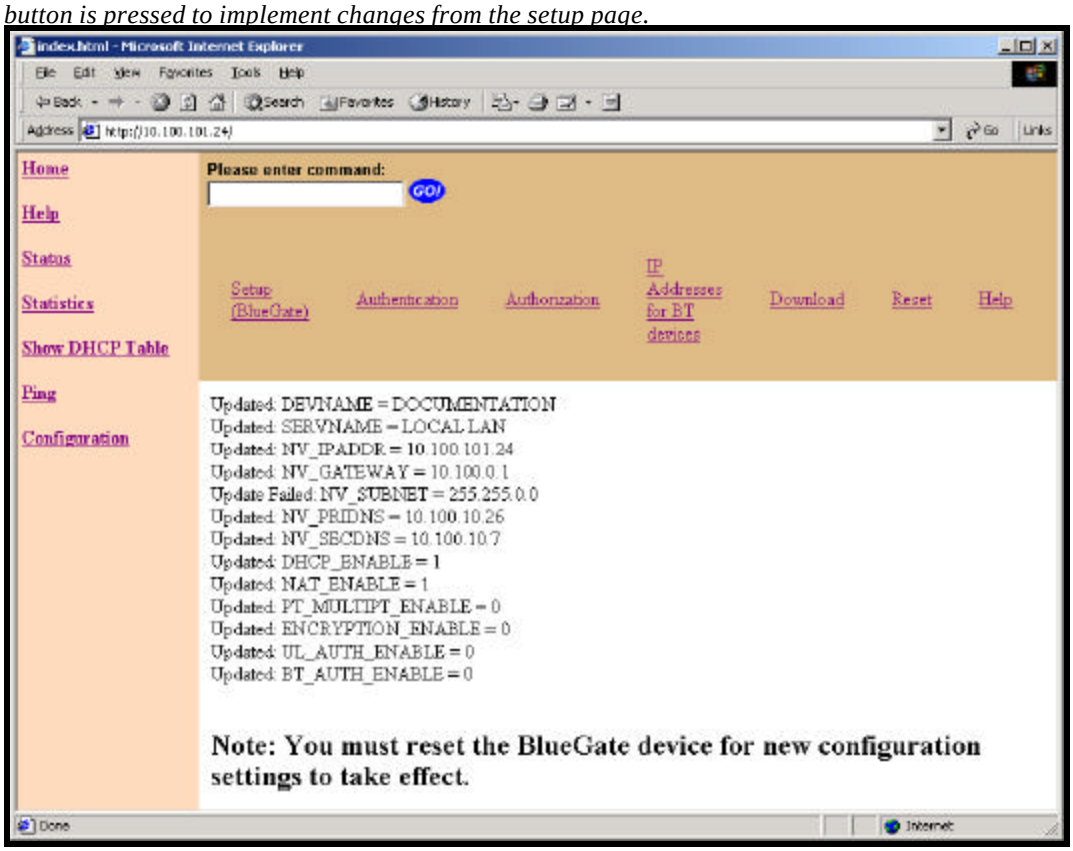


Figure 21: The Configuration > Setup (BlueGate) update page appears when the "Update" button is pressed to implement changes from the setup page.



6.6.1.3 Authentication

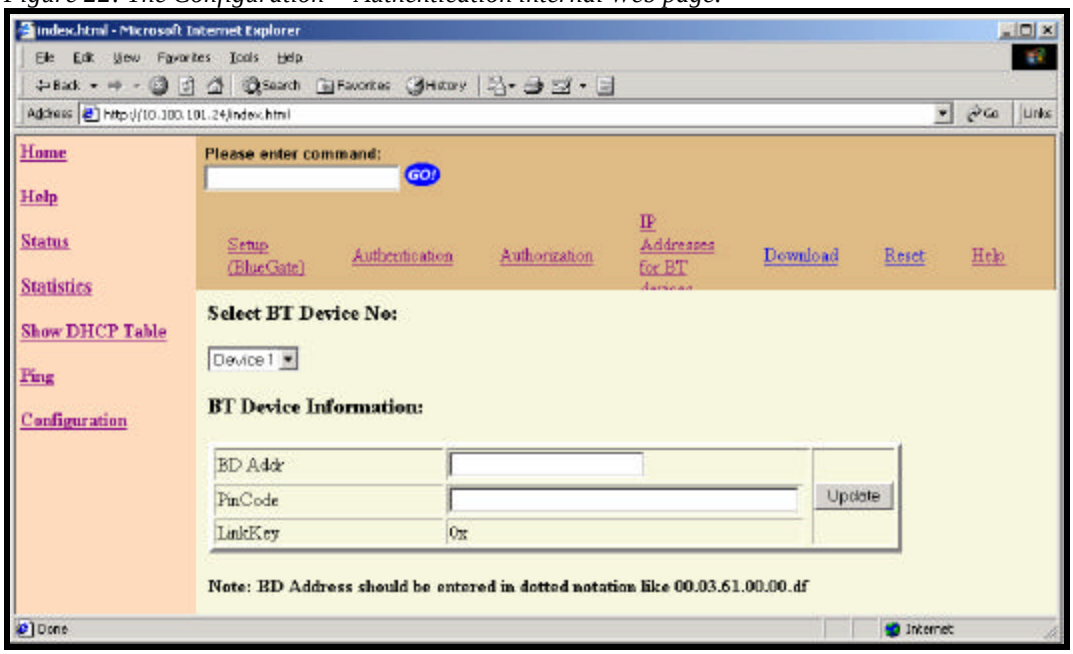
The Configuration > Authentication internal Web page provides a way to enter security settings for Bluetooth devices that use BlueGate 1000 to access the local area network.

A different Personal Identification Number (Pin Code) can be assigned to each of up to seven Bluetooth devices.

- To enter a Pin Code for an individual device.
  - Select the device number in the *Select BT Device No* drop-down menu.
  - Enter the Bluetooth Device Address in the *BD Addr* field.
  - Enter the Pin Code in the *PinCode* field.
  - Click the Update button.

NOTE: Individual PIN codes are only used if "*Require individual PinCode for each device*" is selected on the Configuration > Setup (BlueGate) internal Web page (see Section 6.6.1.2.13).

Figure 22: The Configuration > Authentication internal Web page.



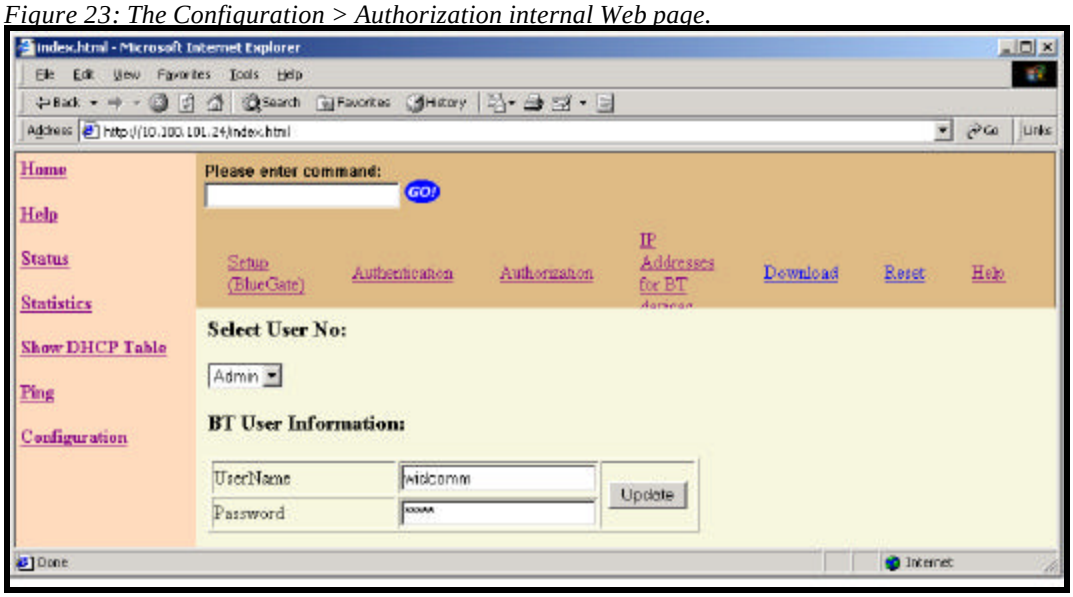
6.6.1.4 Authorization

The Configuration > Authorization internal Web page provides a way to enter user names and passwords for each authorized Bluetooth user. In addition to the administrator, up to seven users can be entered.

User names and passwords are case sensitive; if “Tony” is the valid password and “tony” is entered, access will be denied.

The first item in the drop-down list, “Admin”, contains the user name and password that is allowed to access the BlueGate 1000 internal Web server.

Figure 23: The Configuration > Authorization internal Web page.



6.6.1.5 IP Addresses for BT devices.

The Configuration > IP Addresses for BT devices internal Web page is used to specify three IP address ranges and the number of addresses in each range. Together, these addresses form an address pool from which BlueGate 1000's internal DHCP server allocates IP addresses to connecting Bluetooth devices.

Note: These IP addresses are only used when DHCP and NAT are both disabled (see Sections 6.6.1.2.8 and 6.6.1.2.9).

Valid IP addresses must be in the same subnet as BlueGate 1000.

To enter an IP address range:

1. Type the beginning IP address, in dotted decimal notation, in the *Range Starting From* field.
2. Enter the number of IP address to allocate in the *No. of IP Addresses in this range* field.
3. Click the Update button
4. Reset the BlueGate 1000 (see section 4).

Example:

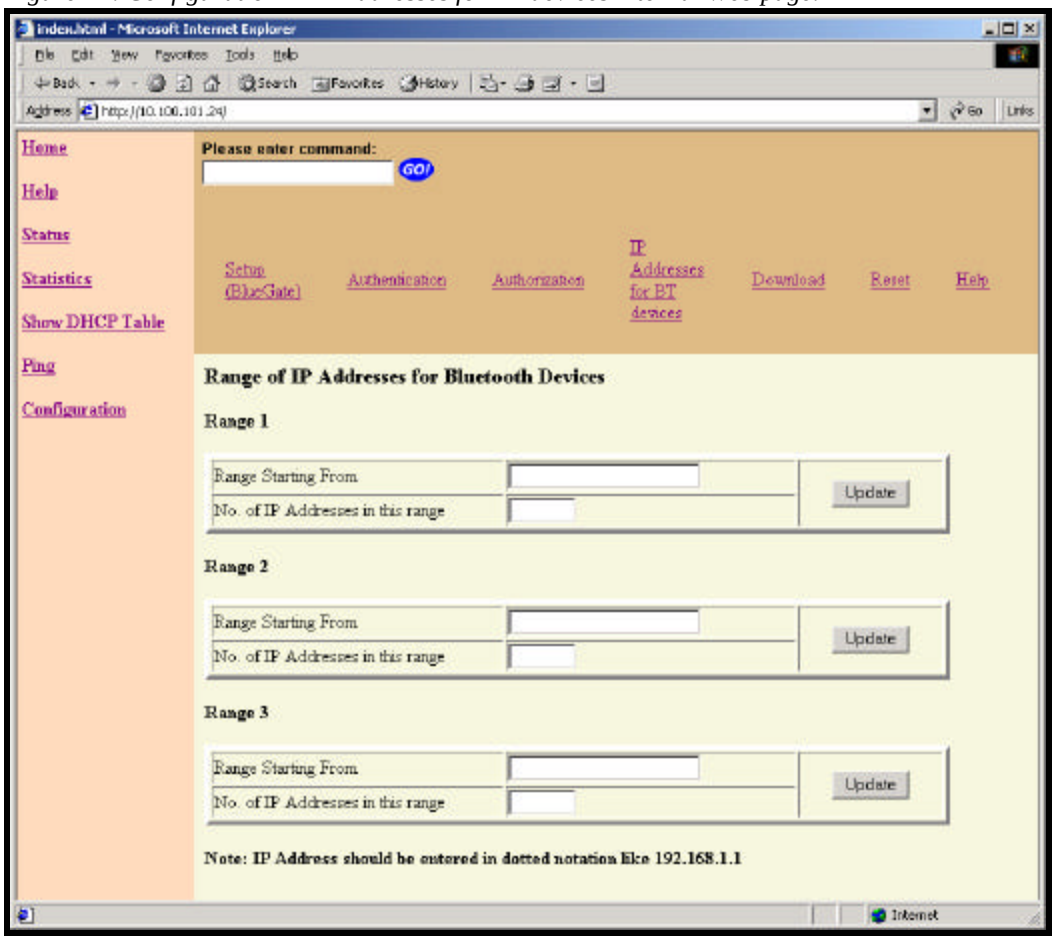
- *Range Starting From* = 192.168.1.20

  and

- *No. of IP Addresses in this range* = 5

  generates a pool of five IP addresses, beginning with 192.168.1.20 and ending with 192.168.1.24.

Figure 24: Configuration > IP Addresses for BT devices internal Web page.



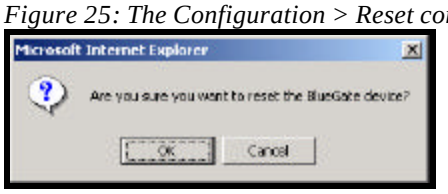
6.6.1.6 Download

This internal Web page is reserved for use by WIDCOMM support personnel.

6.6.1.7 Reset

To reset BlueGate 1000 click the Reset hyperlink.
An Internet Explorer confirmation dialog box appears (Figure 25).
Click OK in the dialog box to reset BlueGate 1000.

Figure 25: The Configuration > Reset confirmation dialog box.



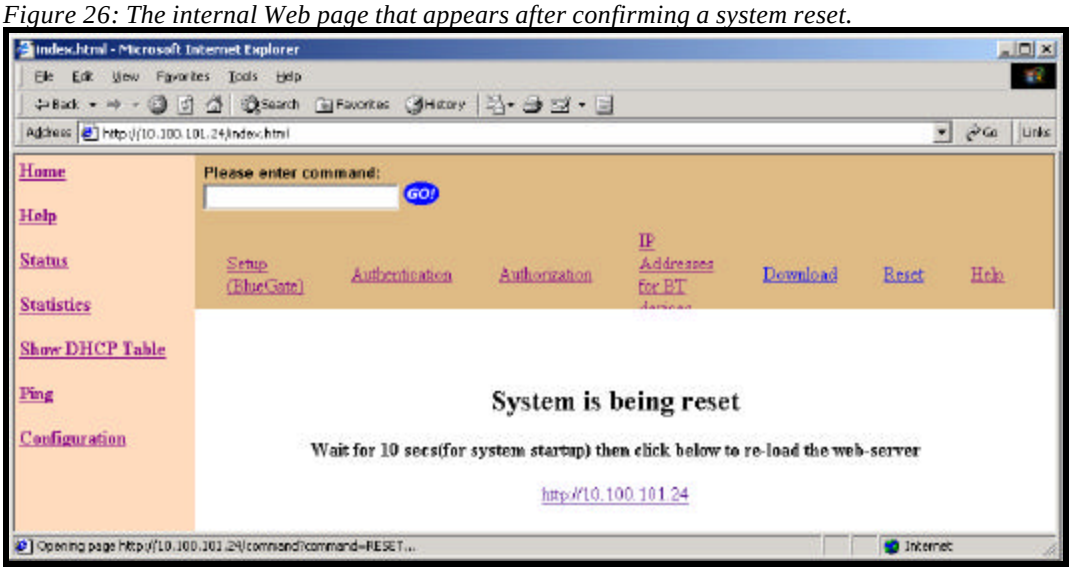
The internal Web page shown in Figure 26 appears. Click the IP address hyperlink after ten seconds to return to BlueGate 1000's internal home page.

When BlueGate 1000 is reset it disconnects from the DHCP server.

The server may assign a different IP address to BlueGate 1000 when it reconnects. If this happens run the Java applet *BGIPLookup.html* to discover the new IP address assigned to BlueGate 1000.

NOTE: See Section 4 for additional information about resetting BlueGate 1000.

Figure 26: The internal Web page that appears after confirming a system reset.

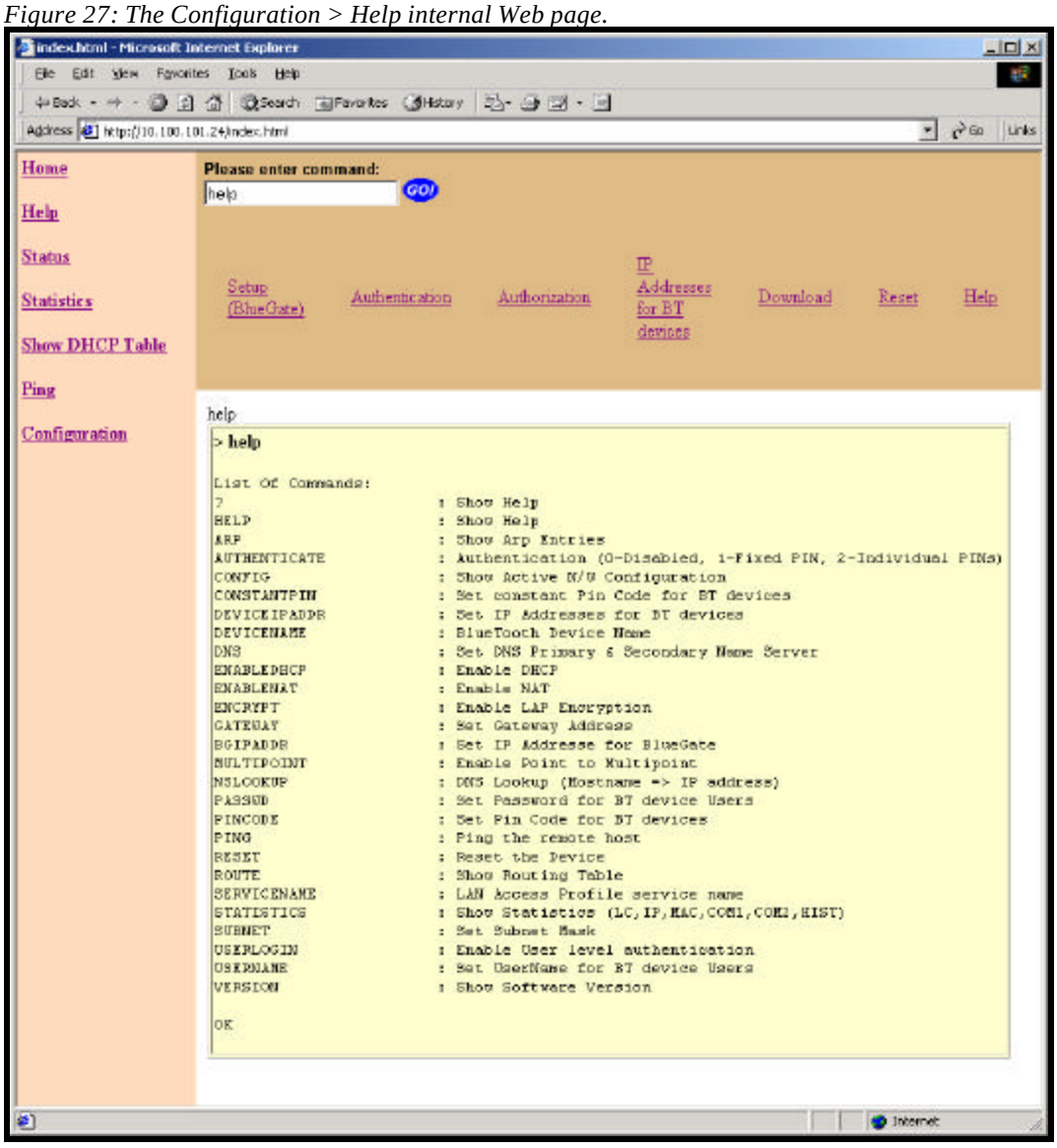


6.6.1.8 Help

The Configuration > Help internal Web page displays a list of commands that can be entered directly into the "*Please enter command*" field.

For information about how to use these commands see Section 7.

Figure 27: The Configuration > Help internal Web page.



7 Command Line Entry

Commands may be entered directly into the *Please enter command* field.

Many of the available commands accept parameters. When a command is entered without parameters, the current setting(s) for that command are displayed; exceptions to this general rule are noted on a command-by-command basis in the remainder of this section.

All commands in this section are also available via the hyperlinks on BlueGate 1000 internal Web pages.

When a command and its associated parameters are entered, a confirmation dialog box appears in the information pane of the Internet Explorer window.

NOTE: BlueGate 1000 must be reset for configuration changes to take affect.

7.1 ? OR HELP

Displays a list of the commands that may be entered in the *Please enter command* field and provides a brief description of each command.

7.2 ARP

Displays the active Address Resolution Protocol (ARP) table entries for BlueGate 1000.

7.3 AUTHENTICATE

Sets the authentication level.

Format: `AUTHENTICATE = n`
`n` is 0, 1 or 2:

- 0 disables authentication.
- 1 enables the use of a fixed Pin Code for all devices.
- 2 enables the use of an individual Pin Code for each device.

Example: `AUTHENTICATE = 0`

7.4 CONFIG

Displays the active configuration of BlueGate 1000.

7.5 CONSTANTPIN

Sets the fixed Pin Code to be used by all Bluetooth devices attempting to access BlueGate 1000. The Pin Code can be up to 16 characters long.

Format: `CONSTANTPIN = ASCII string`

- `ASCII string` is the actual Pin Code.

Example: `CONSTANTPIN = 2233`

NOTE: Do not use *CONSTANTPIN* if the connecting device does not support security.

7.6 DEVICEIPADDR

Sets the IP address ranges for Bluetooth Devices if DHCP is disabled.

Format: `DEVICEIPADDR = n,cnt,aa.bb.cc.dd`

- `n` is the range number: range1, range 2,or range 3.
- `cnt` is the number of IP addresses.
- `aa.bb.cc.dd` is the starting IP address in dotted decimal notation.

Example: `DEVICEIPADDR = 1,3,192.168.0.1` generates a pool of three IP addresses (192.168.0.1, 192.168.0.2, and 192.168.0.3) in range one on BlueGate 1000.

7.7 DEVICENAME

Sets the user-friendly device name of BlueGate 1000. The device name helps identify BlueGate 1000 to other devices; the name can be up to 100 characters in length.

Format: `DEVICENAME = ASCII string`

- `ASCII string` is the actual user-friendly name of the device.

Example: `DEVICENAME = My BlueGate Network Access Point`

7.8 DNS

Sets the Domain Name System (DNS) Primary & Secondary Server IP addresses.

Format: `DNS = n,aa.bb.cc.dd`

- `n` is 0 or 1
  - 0 sets the primary DNS server IP address.
  - 1 sets the secondary DNS server IP address.
- `aa.bb.cc.dd` is the IP address, in dotted decimal notation.

Examples: `DNS = 0,100.140.10.1` sets the Primary DNS server IP address to 100.140.10.1.

`DNS = 1,100.140.10.2` sets the Secondary DNS server IP address to 100.140.10.2.

7.9 ENABLEDHCP

Enables/disables Dynamic Host Configuration Protocol (DHCP).

Format: `ENABLEDHCP = n`

- `n` is 0 or 1:
  - 1 enables DHCP.
  - 0 disables DHCP.

Example: `ENABLEDHCP = 1`

7.10 ENABLENAT

Enables/disables the Network Address Translation (NAT).

Format: `ENABLENAT = n`

- `n` is 0 or 1:
  - 1 enables NAT.
  - 0 disables NAT.

Example: `ENABLENAT = 1`

7.11 ENCRYPT

Enables/disables LAN Access Profile (LAP) Encryption.

Format: `ENCRYPT = n`

- `n` is 0 or 1:
  - 1 enables Encryption.
  - 0 disables Encryption.

Example: `ENCRYPT = 1`

7.12 GATEWAY

Displays the IP address of the LAN gateway to which BlueGate 1000 is connected.

Format: `GATEWAY = aa.bb.cc.dd`

- `aa.bb.cc.dd` is the dotted decimal notated IP address of the LAN gateway.

Example: `GATEWAY = 192.168.1.1`

7.13 IPADDR

Sets the IP address of BlueGate 1000. It is only used when DHCP is disabled.

Format: `IPADDR = n,aa.bb.cc.dd`

- `n` must be 0.
- `aa.bb.cc.dd` is the dotted decimal notated IP address of BlueGate 1000.

Example: `IPADDR = 0,192.168.0.50`

7.14 MULTIPOINT

Enables/disables point-to-multipoint.

Format: `Multipoint = n`

- `n` is 0 or 1:
  - 1 enables point-to-multipoint.
  - 0 disables point-to-point.

Example: `Multipoint = 1`

7.15 NSLOOKUP

Displays the DNS lookup table i.e. mapping of HostName to IP addresses Format:

Format: `NSLOOKUP = valid hostname`

Example: `NSLOOKUP = www.yahoo.com`

7.16 PASSWD

Sets the password for the administrator and individual remote users. Password length is limited to 16 characters.

Format: `PASSWD = n,ASCII string`

- `n` is a number zero to six.
- `ASCII string` is the actual password.

Example: `PASSWD = 1,jsmith`

7.17 PINCODE

Sets the Individual PIN Code used to authenticate connecting Bluetooth devices. The individual PIN Code is limited in length to a maximum of 16 characters.

Format: `PINCODE = n,ASCII`

- `n` is device number, from one to seven.
- `ASCII string` is the actual Pin Code.

Example: `PINCODE = 1,2233`

7.18 PING

Pings the remote host. This command can be used to determine if a remote machine is "up."

"Ping" displays an error message if either the host name or IP address is not entered as a parameter.

Format: `PING hostname[or IPAddr] -nCOUNT -lSIZE -wTIMEOUT -f –iTTL.`

- `Hostname:` the user-friendly name of the remote device.
- `IP Addr`: the IP address of remote device, entered in dotted decimal notation.
- `-nCOUNT`: the number of Ping Packets to be sent (default = 1).
- `-lSIZE`: the size of each ping packet (default = 32 bytes).
- `-wTIMEOUT`: the length of time to wait for a response from the remote machine (default = 5 seconds).
- `-iTTL`: the lifetime, in seconds, of the ping packet. This value is contained in the IP Packet. After `TTL` seconds the packet is removed from the network (default = 255 seconds).
- `-f:` enables packet fragmentation if the packet size is greater than the maximum size allowed on the network.

The only required parameter in the PING command is either the IP address or the host name; all other parameters are optional.

Example: `PING 192.168.1.34 –n2` or `www.widcomm.com -n2` sends two ping packets to the remote device that has IP address 192.168.1.34. The omitted parameters assume their default values.

7.19 RESET

Resets BlueGate 1000.

7.20 ROUTE

Displays the Static and Dynamic route table entries for BlueGate 1000.

7.21 SERVICENAME

Sets the LAN Access Profile service name for BlueGate 1000.

The service name is limited in length to a maximum of 100 characters.

Format: `SERVICENAME = ASCII string`

- `ASCII string` is the actual service name.

Example: `SERVICENAME = LOCAL LAN.`

7.22 STATISTICS

Displays various statistics for BlueGate 1000.

Format: `Statistics=InterfaceName`

`InterfaceName` can be one of:

- `IP`: statistics for IP layer.
- `MAC`: statistics for Ethernet (MAC) layer.
- `COM1`: reserved for use by WIDCOMM personnel.
- `COM2`: reserved for use by WIDCOMM personnel.
- `HIST`: a history of active Bluetooth connections.

7.23 SUBNET

Sets the subnet mask of the LAN gateway to which BlueGate 1000 is connected.

Format: `SUBNET=aa.bb.cc.dd`

- `aa.bb.cc.dd` is the decimal notated IP address of the subnet mask of the LAN gateway.

Example: `SUBNET=255.255.0.0`

7.24 USERLOGIN

Format: `USERLOGIN = n`

- `n` is 0 or 1:
  - 1 enables authorization.
  - 0 disables authorization.

Example: `USERLOGIN = 1`

7.25 USERNAME

Sets the user name of the administrator and individual remote users of BlueGate 1000. The user name is limited in length to 16 characters.

Format: `USERNAME = n,ASCII string`

- `n` is a number between zero and six.
- `ASCII string` is the actual user name.

Example: `USERNAME = 1,falcon`

NOTE: The default user name and password for user zero (0) are "widcomm" and "admin".

7.26 VERSION

Displays the version number of the software.

8 Troubleshooting

8.1 General

BlueGate 1000 is factory configured to be ready to use out of the box.

The general steps for achieving LAN access via BlueGate 1000 are:

1. Verify that the client supports the *LAN Access Profile*; consult the user's manual for the product.
2. Configure the client to use the *LAN Access Profile*; consult the user's manual for your product.
3. Ensure that the Bluetooth security settings on the client are compatible with those that are configured on BlueGate 1000.
   In the case of the client, these may be device-wide setting (for example, a fixed PIN code for all connections), or it may be configurable on a service-by-service or profile-by-profile basis.
4. Perform a device inquiry from the client. Verify that BlueGate 1000 shows up.
   - Some client devices may display only the Bluetooth Device Addresses (BD Addr) of other units.
   - Some may display the user-friendly name (device name) of these devices.
   - Some may display both.
5. Select BlueGate 1000 and perform a service discovery on it.
6. Select the LAN Access Using PPP service.
7. Initiate a connection to the LAN Access Using PPP service on your BlueGate 1000.
8. Test the connection using ping, FTP, an Internet browser, or a similar network-enabled utility.

The remainder of this section deals with specific problems.

8.2 Administrative Password Lost

See Section 4 for information about how to restore the "admin" user name and password to the factory-default settings.

8.3 Bluetooth Device Address is Missing

Some clients may not display the user-friendly name returned during a device inquiry. Attempting to determine which device is which can be difficult without the user-friendly name; you must compare the BDA on each physical device to the on-screen list. BlueGate 1000's BDA is on the serial number tag on the bottom of the unit.

If the tag is missing, contact WIDCOMM BlueGate 1000 technical support at http//www.widcomm.com.

8.4 BT Light does not Blink

This is not necessarily a problem. On some BlueGate 1000 Beta units the BT light was not enabled. This does not affect the functioning of the unit.

8.5 Can't Log On As Administrator

See Section 4 for information about how to restore the "admin" user name and password to the factory-default settings.

8.6 CANNOT CONNECT TO THE LAN ACCESS PROFILE SERVICE

Device Inquiry and Service Discovery succeed but a connection cannot be established.

The client may be configured with security settings that are incompatible with those configured on BlueGate 1000. For example, if the PIN codes do not match, the connection will fail. Since fixed PIN codes are configured on both sides, there may never be a dialog box displayed to inform you that an authentication was performed.

The client may be configured to screen out certain classes of Bluetooth devices.

8.7 CANNOT DISCOVER SERVICES

Service Discovery on BlueGate 1000 device fails.

The client may be configured to screen out certain classes of Bluetooth devices.

8.8 CLIENT DISPLAYS A SECURITY DIALOG; CONNECTION FAILS

Device Inquiry and Service Discovery on BlueGate 1000 device succeed but attempts to connect result in a security dialog box on the client. No matter how the dialog is answered the connection fails.

- Check the client configuration: if the client has authentication turned ON and BlueGate 1000 has all security turned OFF, the connection will fail.
- Check the encryption settings on both client and server; if the client has encryption turned ON and BlueGate 1000 has encryption turned OFF (or vice-versa) the connection may fail.

8.9 DIFFERENTIATING BETWEEN MULTIPLE BLUEGATE 1000 DEVICES

Multiple BlueGate 1000 units are installed in the same Bluetooth Neighborhood; how can they be told apart?

- Check the tags on to the bottom of the BlueGate 1000 devices. Match the BD Address of BlueGate 1000 to the one displayed by the client.
- If the client software displays only the user-friendly name of the units:
  The factory-default user-friendly name of each BlueGate 1000 is the letters "BG" followed by the unit's serial number.
  A unit with the serial number of 9123 has a factory-default user name of ***BG9123***.

The serial number tag is located on the bottom of BlueGate 1000.

8.10 ETHERNET LIGHT IS OFF OR NOT BLINKING

BlueGate 1000's Power light is ON, but the "Ethernet" light is OFF.

- Ensure that the plugs on either end of the Ethernet cable are properly seated in the jack on BlueGate 1000 and the hub or wall jack.
- Make sure the Ethernet cable is plugged into the proper jack; telephone systems sometimes use the same type of jack.
- Verify that the Ethernet cable is good; replace it if necessary.
- Verify that the network is "up" if the symptom persists.

8.11 MAC Address is Missing or Not Valid

The MAC address of BlueGate 1000 is required to discover the network IP address assigned to BlueGate 1000.

The MAC address is on the serial number tag on the bottom of BlueGate 1000. If the tag is missing, contact WIDCOMM technical support (www.widcomm.com/support).

Make sure the MAC address was entered correctly.

Make sure that your local DHCP server is on-line and accessible.
If no DHCP server is available at power-up BlueGate 1000 defaults to a static IP address of 192.168.0.1.

Verify that there is not a network router between BlueGate 1000 and the computer running the Java applet (*BGIPLookup.html*). Contact the network administrator for assistance.
The Java applet uses a UDP broadcast packet to discover BlueGate 1000's assigned IP address. UDP packets are not routed; the PC running the applet must be on the same subnet as BlueGate 1000.

Appendix A—An Introduction To Bluetooth

This document provides a brief non-technical overview of Bluetooth.

For information on a specific topic click the appropriate link below:

Overview

The term “Bluetooth” refers to a worldwide standard for the wireless exchange of data between two devices.

In order to exchange data, two Bluetooth devices must establish a connection.

Before a connection is established, one device must request a connection with another. The second device accepts (or rejects) the connection.

The originator of the request is known as the *client*.

The device that accepts (or rejects) the request is known as the *server*.

Bluetooth devices can act as both client and server.

A client Bluetooth device runs a software program that requests a connection to another device as part of its normal operation. For example, the program may request a connection to a remote computer, a printer, or a modem.

Becoming a Bluetooth client normally requires an action by the device operator, such as an attempt to browse a remote computer, print a file or dial out on a modem.

Every Bluetooth device that provides a service must be prepared to respond to a connection request. Bluetooth software is always running in the background on the server, ready to respond to connection requests. <back>

Device Identity

Each Bluetooth device has a unique forty-eight-bit binary Bluetooth Device Address (BDA) burned into its Read Only Memory during the manufacturing process. This address cannot be changed by the end-user.

A devices' BDA is usually displayed in hexadecimal format, e.g, 00:D0:B7:03:2E:9F is a valid BDA.

Each Bluetooth device also has an operator-configurable user-friendly device name to help distinguish it from other Bluetooth devices in the vicinity. Valid user-friendly names include:

- Bob's PC.
- Randy's Laptop.
- John Q. Public's PDA.

User-friendly names make it easier to recognize the devices in the Bluetooth Neighborhood. However, because the name is easily changed, it is not reliable for security purposes. <back>

Security

Bluetooth offers five types, or levels, of security:

- None—all Bluetooth devices are allowed to connect.
- Authorization—the local device operator must authorize a remote device connection, usually by physically clicking an on-screen button.
- Authentication—remote devices must provide a password that matches that of the local device.
- Encryption—connections with remote devices can be encrypted for additional security.
- Service Level—individual local services may be disabled. Disabled services are not available to any remote device. Service Level security is only available on some types of devices. <back>

Authorization

Authorization provides name-level and device-level security.

An audible and/or visual warning notifies the local operator that a remote device is attempting to access the system.

The local operator can open a dialog box that provides:

- Name-level security information—the user-friendly name of the device attempting access.
- Device-level security information—the Bluetooth Device Address of the device attempting access.
- The type of access the requesting device is trying to achieve.

Based on the information provided in the dialog box, the operator may authorize or deny access by physically clicking an on-screen button.

If the initial notification is ignored access is denied after a preset timeout.

Authorization does not provide foolproof security since Bluetooth device names are re-configurable by the end-user.

Advantages of Authorization: Ease of use—requires a simple **YES**-or-**NO** response.

Disadvantages of Authorization: Weak security. <back>

Authentication

Authentication requires a passkey from the remote device attempting to access the local device.

An audible and/or visual warning notifies the local operator that a remote device is attempting to access the system.

The local operator can open a dialog box that provides:

- Name-level security information—the user-friendly name of the device attempting access.
- Device-level security information—the Bluetooth Device Address of the device attempting access.
- The type of access the requesting device is trying to achieve.
- A place for the local operator to enter a passkey.

The operator of the remote system must enter the identical passkey or access is denied.

If the initial notification is ignored access is denied after a preset timeout.

There is no limit to the number passkeys that may be assigned. Individual remote devices may be assigned different passkeys for each service provided by the local computer.

For example, John's PC, BDA 00:00:D0:11:22:33, may be assigned a passkey of "2468" and granted access to all services on the local computer, or John's PC can be assigned a different passkey for each service.

Advantages of authentication: Stronger security.

Disadvantages of authentication: Passkeys must be protected. <back>

Encryption

The Bluetooth specification allows for encrypted transactions using a key size of up to 128 bits.

Some Bluetooth devices do not support encryption. If a device or service is configured to use encryption and attempts a connection with a device that does not support encryption the connection may fail unexpectedly.

Advantages of encryption: Protects against radio frequency snooping.

Disadvantages of encryption: The receiving unit must also support encryption. <back>

Service Level

Each Bluetooth service can be selectively disabled. If all Bluetooth services are disabled the local computer is unable to accept connections from a remote computer.

The local machine can still initiate outgoing connections to other Bluetooth units, but incoming connections will not be allowed.

Advantages of service level security: Strong security.

Disadvantages of service level security: It is non-selective; it shuts out all incoming Bluetooth connections for a particular service. <back>

Link Keys

To avoid entering a passkey over-and-over for a known and trusted remote device, a link key can be created.

A link key is a number created from:

- The passkey.
- The Bluetooth device address of the remote device.
- An internally random-generated number.

There is no limit to the number link keys that may be created.

Devices that share a link key are “bonded.” Bonded devices are authenticated automatically, without operator intervention. <back>

Services

The software that allows a Bluetooth device to act as a server is known as a *service*. Enabled services are started automatically when the computer boots. The services then run as background tasks.

Typical Bluetooth services include:

- Local Area Network access.
- Dial-Up networking.
- File transfer between computers.
- Object exchange between computers.
- Serial port emulation.
- FAX device support.
- File system synchronization. <back>

NOTE: BlueGate only supports one service; Local Area Network access using PPP.

Device Inquiry and Service Discovery

To connect to a remote Bluetooth device, the remote device must:

- Be within radio range.
- Provide a Bluetooth service.
- Be accessible, from a security standpoint, by the local device. <back>

Device Inquiry

A Bluetooth device must be within radio range of a second Bluetooth device to establish a connection.

Every Bluetooth device keeps a list that contains the user-friendly name and device address of each remote device that is within its radio range.

As Bluetooth devices wander in and out of the Bluetooth Neighborhood the list must be updated. This is accomplished in two ways:

- The list is updated automatically when the local device periodically queries all other Bluetooth devices within range.
- The list can also be updated as necessary by selecting an on-screen option. <back>

Service Discovery

Even though a device is within radio range the local device will not be able connect to it if the remote device does not provide the requested service.

Service Discovery is the process of determining which Bluetooth services are available on the devices within radio range.

Connection requests are made for a specific service. If the desired service is the File Transfer Protocol (FTP) and the remote device does not offer that service, the connection will not be allowed. <back>

Security

The security parameters of the remote device must be set to allow the local device to establish a connection.

Even though there is a remote device in the Bluetooth Neighborhood that provides the desired service, the remote device security parameters may be set to allow only specific devices to connect. If the requesting device is not on that list, it will not be allowed to connect. <back>

A Typical Connection Scenario

In this simplified scenario Joe's PC is a Bluetooth-aware computer that needs access to the network:

1. Joe's PC performs a search of the Bluetooth Neighborhood (a Device Inquiry) and determines that there are four Bluetooth devices in the vicinity.
2. Joe's PC queries each of the four nearby devices to determine which services they provide (a Service Discovery). Ann's Computer offers the network access service.
3. Joe's PC sends a network connection request to Ann's Computer.
4. Ann's Computer evaluates the request and determines that Joe's PC is permitted to use the network connection service, PROVIDED THE CORRECT PASSWORD IS SUBMITTED.
5. Ann's Computer queries Joe's PC for the password (Authentication).
6. Joe's PC returns the correct password and the network connection is established.
7. Joe's PC uses the network access connection on Ann's Computer as if Joe's PC was connected directly to the network.

When Joe's PC no longer needs the network access service the connection between it and Ann's Computer is disconnected by the operator.

Some Bluetooth services disconnect automatically, others must be closed manually.
<back>