

Serial-to-WiFi AT Commands Sample Examples

To Create TCP and UDP Connection

User Guide

GS2K-SMP-EXP-UG-001207

Modules

GS2011M and GS2100M

GainSpan[®] 802.11b/g/n Ultra-Low Power Wi-Fi[®] Series Modules

Copyright Statement	<p>This GainSpan manual is owned by GainSpan or its licensors and protected by U.S. and international copyright laws, conventions, and treaties. Your right to use this manual is subject to limitations and restrictions imposed by applicable licenses and copyright laws. Unauthorized reproduction, modification, distribution, display or other use of this manual may result in criminal and civil penalties.</p> <p>GainSpan assumes no liability whatsoever, and disclaims any express or implied warranty, relating to sale and/or use of GainSpan products including liability or warranties relating to fitness for a particular purpose, merchantability, or infringement of any patent, copyright or other intellectual property right. GainSpan products are not authorized for use as critical components in medical, lifesaving, or life-sustaining applications</p> <p>GainSpan may make changes to specifications and product descriptions at any time, without notice.</p>
Trademark	<p>GainSpan is a registered trademark of GainSpan Corporation. All rights reserved. Other names and brands may be claimed as the property of others.</p>
Contact Information	<p>In an effort to improve the quality of this document, please notify GainSpan Technical Assistance at 1.408.627.6500 in North America or +91 80 42526503 outside North America.</p>

Table of Contents

Chapter 1 Serial-to-WiFi Connection Examples	15
1.1 Requirements	15
1.2 Infrastructure Mode	16
1.2.1 Joining Open or Secure Network (WPA2-PSK)	16
1.3 UDP	17
1.3.1 UDP Server	17
1.3.2 UDP Client	20
1.4 TCP	22
1.4.1 TCP Server	22
1.4.2 TCP Client	24
1.5 Limited AP Mode	26
1.5.1 Creating Limited AP Mode With No Security	26
1.5.2 Creating Limited AP WPA2-PSK Mode (Secure Network)	27
1.5.3 UDP Server	29
1.5.4 UDP Client	32
1.5.5 TCP Server	34
Chapter 2 Serial-to-WiFi Provisioning	41
2.1 Introduction	41
2.2 Setting Up Web Provisioning Using Limited AP Provisioning Mode	42
2.2.1 Wireless and Network Configuration	45
2.2.1.1 Select an Existing Network	45
2.2.1.2 Manual Configuration	49
2.2.2 Limited AP Settings	52
2.2.3 Operation Mode Selection	56
2.2.4 Administrator Settings	57
2.3 Setting Up WPS Based Provisioning	58
2.3.1 WPS Push Button Configuration (PBC) Mode	59
2.3.2 WPS Personal Information Number (PIN) Mode	63

About This Manual

This manual provides GS2000 based module evaluation kit sample examples for using Serial-to-WiFi AT commands to create TCP or UDP connections for Open and Secure networks.

Refer to the following sections:

- [Revision History, page 5](#)
- [Audience, page 6](#)
- [Standards, page 6](#)
- [Documentation Conventions, page 6](#)
- [Documentation, page 9](#)
- [References, page 11](#)
- [Contacting GainSpan Technical Support, page 12](#)
- [Returning Products to GainSpan, page 13](#)
- [Accessing the GainSpan Portal, page 14](#)

Revision History

This version of the *GainSpan GS2000 Based Module Sample Examples User Guide (for using Serial-to-WiFi AT Commands to Create TCP or UDP Connection)* contains the following new information listed in [Table 1, page 5](#).

Table 1 Revision History

Version	Date	Remarks
1.0	May 2014	Initial Release
1.0.1	September 2014	Added instructions on how to setup Infrastructure and Limited AP mode in a secure network environment. See 1.2.1 Joining Open or Secure Network (WPA2-PSK) , page 16 and 1.5.2 Creating Limited AP WPA2-PSK Mode (Secure Network) , page 27.

Audience

This manual is designed to setup, create, and run connection examples for UDP client/server and TCP client/server. This manual also provides instructions for provisioning the board, setting up Limited AP mode, and WiFi Protected Setup (WPS).

Standards

The standards that are supported by the GainSpan GS module supports IEEE 802.11b/g/n.

Documentation Conventions

This manual uses the following text and syntax conventions:

- Special text fonts represent particular commands, keywords, variables, or window sessions
- Color text indicates cross-reference hyper links to supplemental information
- Command notation indicates commands, subcommands, or command elements

[Table 2, page 6](#), describes the text conventions used in this manual for software procedures that are explained using the AT command line interface.

Table 2 Document Text Conventions






Convention Type	Description
command syntax monospaced font	This monospaced font represents command strings entered on a command line and sample source code. AT XXXX
Proportional font description	Gives specific details about a parameter. <Data> DATA
UPPERCASE Variable parameter	Indicates user input. Enter a value according to the descriptions that follow. Each uppercased token expands into one or more other token.
lowercase Keyword parameter	Indicates keywords. Enter values exactly as shown in the command description.
[] Square brackets	Enclose optional parameters. Choose none; or select one or more an unlimited number of times each. Do not enter brackets as part of any command. [parm1 parm2 parm3]
? Question mark	Used with the square brackets to limit the immediately following token to one occurrence.

Table 2 Document Text Conventions (Continued)

Convention Type	Description
<ESC> Escape sequence	Each escape sequence <ESC> starts with the ASCII character 27 (0x1B). This is equivalent to the Escape key. <ESC>C
<CR> Carriage return	Each command is terminated by a carriage return.
<LF> Line feed	Each command is terminated by a line feed.
<CR> <LF> Carriage return Line feed	Each response is started with a carriage return and line feed with some exceptions.
< > Angle brackets	Enclose a numeric range, endpoints inclusive. Do not enter angle brackets as part of any command. <SSID>
= Equal sign	Separates the variable from explanatory text. Is entered as part of the command. PROCESSID = <CID>
. dot (period)	Allows the repetition of the element that immediately follows it multiple times. Do not enter as part of the command. .AA:NN can be expanded to 1:01 1:02 1:03.
A.B.C.D IP address	IPv4-style address. 10.0.11.123 IPv6-style address.
X:X::X:X IPv6 IP address	3ffe:506::1 Where the :: represents all 0x for those address components not explicitly given.
LINE End-to-line input token	Indicates user input of any string, including spaces. No other parameters may be entered after input for this token. string of words
WORD Single token	Indicates user input of any contiguous string (excluding spaces). singlewordnospaces

Table 3, page 8, describes the symbol conventions used in this manual for notification and important instructions.

Table 3 Symbol Conventions

Icon	Type	Description
	Note	Provides helpful suggestions needed in understanding a feature or references to material not available in the manual.
	Alert	Alerts you of potential damage to a program, device, or system or the loss of data or service.
	Caution	Cautions you about a situation that could result in minor or moderate bodily injury if not avoided.
	Warning	Warns you of a potential situation that could result in death or serious bodily injury if not avoided.
	Electro-Static Discharge (ESD)	Notifies you to take proper grounding precautions before handling a product.

Documentation

The GainSpan documentation suite listed in [Table 4, page 9](#) includes the part number, documentation name, and a description of the document. The documents are available from the GainSpan Portal. Refer to [Accessing the GainSpan Portal, page 14](#) for details.

Table 4 Documentation List

Part Number	Document Title	Description
GS2K-QS-001205	GainSpan GS2000 Based Module Kit Quick Start Guide	Provides an easy to follow guide on how to unpack and setup GainSpan GS2000 based module kit for the GS2011M and GS2100M modules.
GS2K-EVB-FP-UG-001206	GainSpan GS2000 Based Module Programming User Guide	Provides users steps to program the on-board Flash on the GainSpan GS2000 based modules using DOS or Graphical User Interface utility provided by GainSpan. The user guide uses the evaluation boards as a reference example board.
GS2K-SMP-EXP-UG-001207	GainSpan GS2000 Based Module Sample Examples for using Serial-to-WiFi AT Commands to Create TCP or UDP Connection User Guide	Provides an easy to follow instructions on how to setup, create, and run connection examples for UDP client/server and TCP client/server. This manual also provides instructions for provisioning the board, setting up Limited AP mode, and WiFi Protected Setup (WPS), and Web provisioning over Ad-hoc.
GS-S2W-APP-PRG-RG-001208	GainSpan Serial-to-WiFi Adapter Application Programmer Reference Guide	Provides a complete listing of AT serial commands, including configuration examples for initiating, maintaining, and evaluating GainSpan WiFi series modules.
GS2K-SDK-DB-UG-001209	GS2000 Based Module Software Development Kit and Debugging User Guide	This manual provides SDK user installation instructions, IAR IDE workbench application, and I-Jet hardware used for JTAG Serial-to-WiFi (S2W) and TLS application development and debugging.
GS2K-EVB-HW-UG-001210	GainSpan GS2000 Based Module Evaluation Board Hardware User Guide.	Provides instructions on how to setup and use the GS2000 based module evaluation board along with component description, jumper settings, board specifications, and pinouts.

Table 4 Documentation List (Continued)

Part Number	Document Title	Description
GS2011M-DS-001211	GainSpan GS2011M Low Power WiFi Module Data Sheet	Provides information to help WiFi system designers to build systems using GainSpan GS2011M module and develop wireless applications.
GS2100M-DS-001212	GainSpan GS2100M Low Power WiFi Module Data Sheet	Provides information to help WiFi system designers to build systems using GainSpan GS2100M module and develop wireless applications.
GS2K-HTTP-EAP-UG-001213	GainSpan GS2000 Based Module Configuration Examples for using Serial-to-WiFi AT Commands to Create HTTP, HTTPS, and EAP Connection User Guide	Provides an easy to follow instructions on how to setup, create, and run connection examples for HTTP, HTTPS, and EAP.
GS2011MxxS-DS-001214	GainSpan GS2011MxxS Low Power WiFi Module Data Sheet	Provides information to help WiFi system designers to build systems using GainSpan GS2011MxxS module and develop wireless applications.
GS2K-SDK-BLDR-UG-001223	GainSpan GS2000 Based Module Software Developer Kit (SDK) Builder User Guide	Allows OEMs and system developers to configure and generate custom firmware binary images for GainSpan low power embedded GS2000 based WiFi modules. The SDK Builder supports the GainSpan GEPS software released, including the corresponding WLAN firmware.
GS2K-SDK-QS-001225	GainSpan GS2000 Based Module Software Development Kit Quick Start Guide	Provides an easy to follow guide that will walk you through easy steps to setup, evaluation, develop, and debug the full capabilities and features of the GS2011M or GS2100M embedded platform software.

Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. You can send your comments by logging into [GainSpan Support Portal](#). If you are using e-mail, be sure to include the following information with your comments:

- Document name
- URL or page number
- Hardware release version (if applicable)
- Software release version (if applicable)

References

The GainSpan references listed in [Table 5, page 11](#) are available on the GainSpan Portal. Refer to [Accessing the GainSpan Portal, page 14](#) for details.

Table 5 Other Documents and References

Title	Description
Schematics	GS2000 Based Module Evaluation Board schematics supporting: <ul style="list-style-type: none">• GS2011M• GS2100M
Module Firmware and Programming Utilities	<ul style="list-style-type: none">• Serial-to-WiFi (S2W) based firmware• Temperature and Light Sensor (TLS) based firmware<ul style="list-style-type: none">– For use with GS2011M EVK only• Firmware Release Notes• GSFlashprogram utility for programming the modules
Smart Phone Applications	<ul style="list-style-type: none">• Smart Phone applications for iOS and Android to evaluate and demonstrate the Temperature and Light Sensor (TLS) firmware.<ul style="list-style-type: none">– For use with GS2011M EVK only
Software Utilities	Serial terminal program to evaluate and demonstrate Serial-to-WiFi (S2W) applications

Contacting GainSpan Technical Support

Use the information listed in [Table 6, page 12](#), to contact the GainSpan Technical Support.

Table 6 GainSpan Technical Support Contact Information

North America	1 (408) 627-6500 - techsupport@gainspan.com
Outside North America	Europe: EUsupport@gainspan.com
	China: Chinasupport@gainspan.com
	Asia: Asiasupport@gainspan.com
Postal Address	GainSpan Corporation 3590 North First Street Suite 300 San Jose, CA 95134 U.S.A.

For more Technical Support information or assistance, perform the following steps:

1. Point your browser to <http://www.gainspan.com>.
2. Click **Contact**, and click **Request Support**.
3. Log in using your customer **Email** and **Password**.
4. Select the **Location**.
5. Select **Support Question** tab.
6. Select **Add New Question**.
7. Enter your technical support question, product information, and a brief description.

The following information is displayed:

- Telephone number contact information by region
- Links to customer profile, dashboard, and account information
- Links to product technical documentation
- Links to PDFs of support policies

Returning Products to GainSpan

If a problem cannot be resolved by GainSpan technical support, a Return Material Authorization (RMA) is issued. This number is used to track the returned material at the factory and to return repaired or new components to the customer as needed.



NOTE: Do not return any components to GainSpan Corporation unless you have first obtained an RMA number. GainSpan reserves the right to refuse shipments that do not have an RMA. Refused shipments will be returned to the customer by collect freight.

For more information about return and repair policies, see the customer support web page at: <https://www.gainspan.com/secure/login>.

To return a hardware component:

1. Determine the part number and serial number of the component.
2. Obtain an RMA number from Sales/Distributor Representative.
3. Provide the following information in an e-mail or during the telephone call:
 - Part number and serial number of component
 - Your name, organization name, telephone number, and fax number
 - Description of the failure
4. The support representative validates your request and issues an RMA number for return of the components.
5. Pack the component for shipment.

Guidelines for Packing Components for Shipment

To pack and ship individual components:

- When you return components, make sure they are adequately protected with packing materials and packed so that the pieces are prevented from moving around inside the carton.
- Use the original shipping materials if they are available.
- Place individual components in electrostatic bags.
- Write the RMA number on the exterior of the box to ensure proper tracking.



CAUTION! Do not stack any of the components.

Accessing the GainSpan Portal

To find the latest version of GainSpan documentation supporting the GainSpan product release you are interested in, you can search the GainSpan Portal website by performing the following steps:



NOTE: You must first contact GainSpan to set up an account, and obtain a customer user name and password before you can access the GainSpan Portal.

1. Go to the [GainSpan Support Portal](#) website.
2. Log in using your customer **Email** and **Password**.
3. Click the **Getting Started** tab to view a Quick Start tutorial on how to use various features within the GainSpan Portal.
4. Click the **Actions** tab to buy, evaluate, or download GainSpan products.
5. Click on the **Documents** tab to search, download, and print GainSpan product documentation.
6. Click the **Software** tab to search and download the latest software versions.
7. Click the **Account History** tab to view customer account history.
8. Click the **Legal Documents** tab to view GainSpan Non-Disclosure Agreement (NDA).

Chapter 1 Serial-to-WiFi Connection Examples

This chapter describes the Serial-to-WiFi procedures on how to setup, test, and evaluate UDP (client/server) and TCP (client/server) connection examples on GainSpan® GS2011M or GS2100M modules.

- [Requirements, page 15](#)
- [Infrastructure Mode, page 16](#)
- [UDP, page 17](#)
- [TCP, page 22](#)
- [Limited AP Mode, page 26](#)

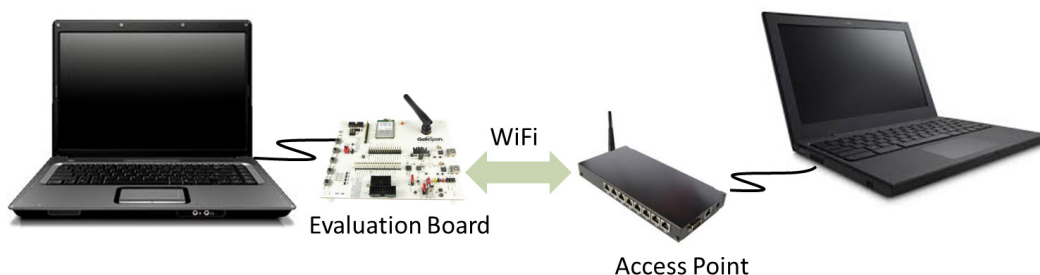
1.1 Requirements

The Serial-to-WiFi application firmware binaries must be loaded onto the GainSpan GS2011M or GS2100M module. For details on how to install the firmware and binaries. Refer to *GainSpan Serial-to-WiFi Adapter Application Programmer Reference Guide*.

1.2 Infrastructure Mode

Figure 1, page 16 illustrates Infrastructure Mode setup.

Figure 1 Infrastructure Mode Setup



1.2.1 Joining Open or Secure Network (WPA2-PSK)

The instructions below outline how to join an Open or Secure Infrastructure network.

1. If a network has security enabled, set the security password using the AT command below. If joining an Open network, skip **Step 2** below.
2. Set the WPA2-PSK Passphrase.

```
AT+WWPA=<PASSPHRASE>
```

3. Set device to infrastructure mode. This step is optional, since default mode is infrastructure mode.

```
AT+WM=0
```

4. Enable DHCP, if disabled previously.

```
AT+NDHCP=<disable=0/enable=1> (default is enable)
```

5. Join the infrastructure network.

```
AT+WA=<SSID>[ , [<BSSID>] [ , <Ch>] ]
```

Example

```
AT+WWPA=test12345
AT+WM=0
AT+WA=GainSpanDemo, , 11
```



NOTE: The TCP/UDP example is common to whether you associate with an open or secure network.

1.3 UDP

1.3.1 UDP Server

This section describes how to setup the UDP Server on the GainSpan GS2011M or GS2100M evaluation board using the AT commands.



NOTE: A socket test tool is used for this example. You can use a socket test tool like “Sockettest.” This can be downloaded from <http://sockettest.sourceforge.net>.

Run a terminal emulation program (like Tera Term) on the computer that is connected to the evaluation board and enter the following commands (see [Figure 2, page 18](#)):

1. Disassociate from the current network (if applicable).

```
AT+WD
```

2. Enable DHCP, if disabled previously.

```
AT+NDHCP=<disable=0/enable=1>
```

3. Associate to an Access Point (AP): AT+WA=<SSID>[, [<BSSID>] [, <Ch>]]

```
AT+WA=GS_Limited_AP, , 11
```

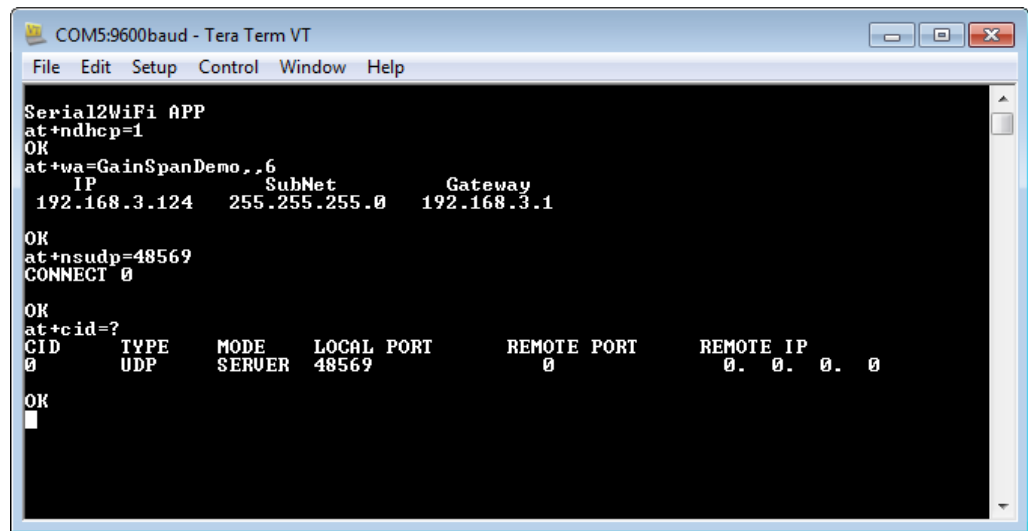
4. Start a UDP server on a specific port number: AT+NSUDP=<port>

```
AT+NSUDP=48569
```

5. Upon successful creation of the UDP server, you will see a “CONNECT <CID>” message, where CID is the newly allocated connection identifier. Check for the new CID by issuing the command: AT+CID=?

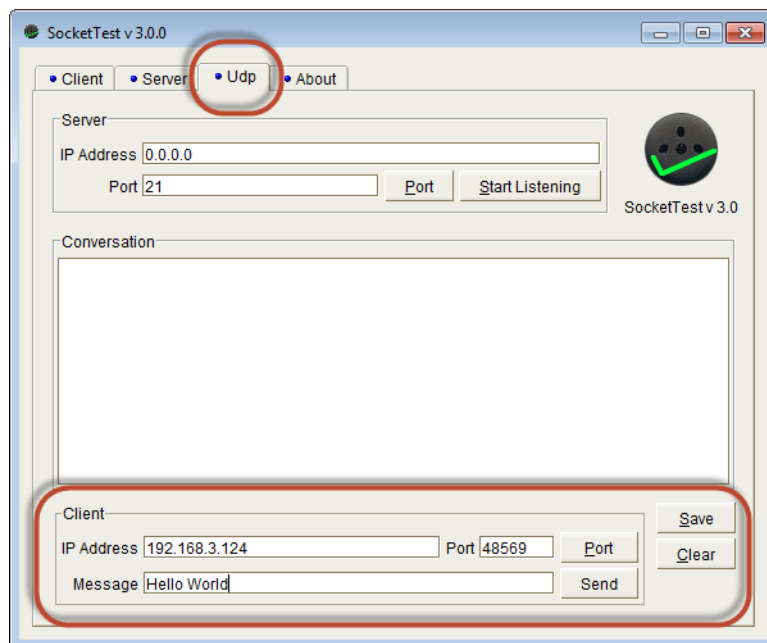
```
AT+CID=?
```

Figure 2 Creating a UDP Server



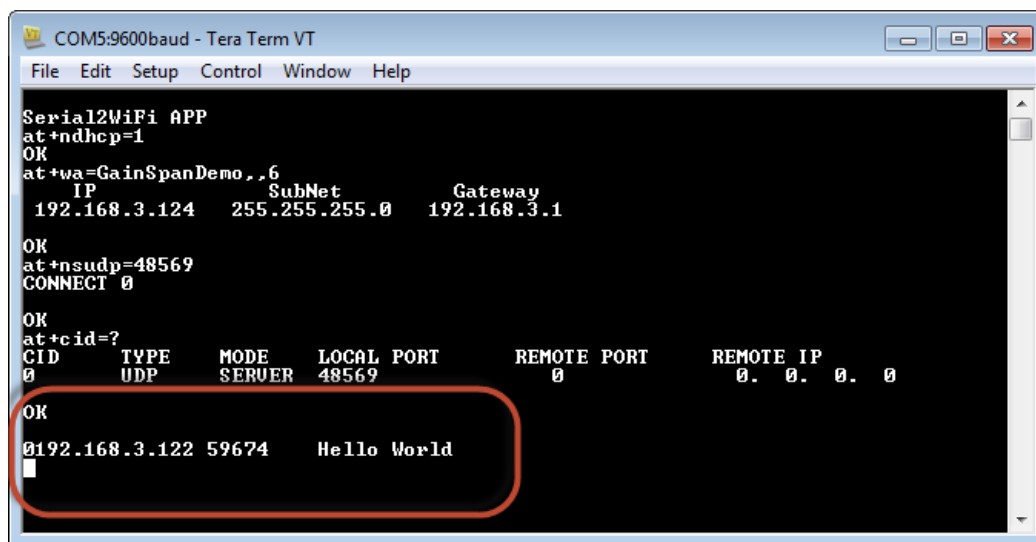
6. Connect to the UDP server by:
 - Have a PC associate to the Access Point (AP).
 - Using the SocketTest tool, have the UDP client send data to the UDP server (see [Figure 3, page 18](#)).
 - Under the UDP tab, enter the Client IP address (192.168.3.124) and Port associated with the AP (48569).

Figure 3 Connect to a UDP Server



- Click the **Send** button. The data will be received on the module side as shown in Figure 4, page 19 below.

Figure 4 Data Received on the Module



The screenshot shows a Tera Term VT window titled "COM5:9600baud - Tera Term VT". The window contains the following text:

```
Serial2WiFi APP
at+ndhcp=1
OK
at+wa=GainSpanDemo,,6
      IP      SubNet      Gateway
192.168.3.124 255.255.255.0 192.168.3.1
OK
at+nsudp=48569
CONNECT 0
OK
at+cidx=?
CID      TYPE      MODE      LOCAL PORT      REMOTE PORT      REMOTE IP
0        UDP        SERVER    48569           0               0. 0. 0. 0
OK
0192.168.3.122 59674    Hello World
```

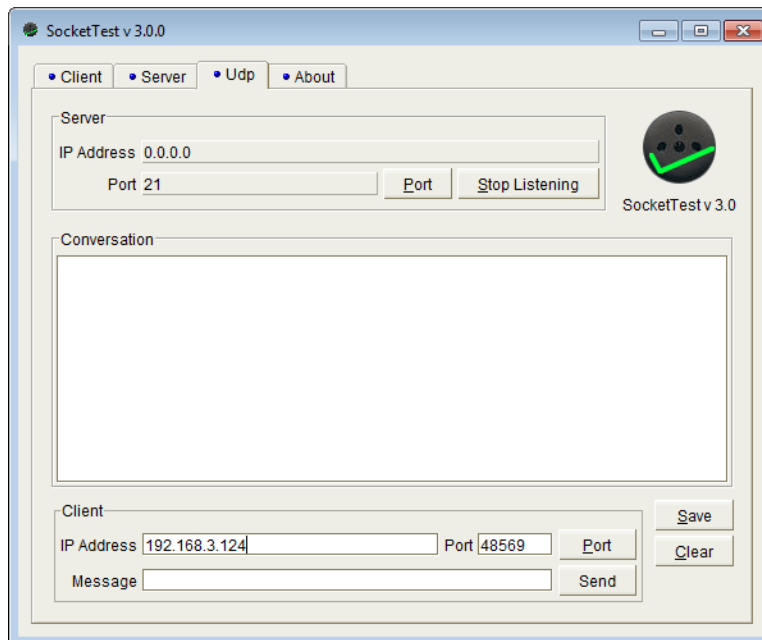
The last line of the output, "0192.168.3.122 59674 Hello World", is highlighted with a red rounded rectangle.

1.3.2 UDP Client

This section describes how to setup the UDP Client on the GainSpan GS2011M or GS2100M evaluation board using AT command mode or auto-connect mode.

1. Connect your PC to an Access Point (AP), and start a UDP Server session. Figure 5, page 20 shows the UDP Client Server is used. This tool can be downloaded from: <http://www.softpedia.com>.

Figure 5 UDP Client Server Session



Run a terminal emulation program (like Tera Term) on the computer that is connected to the evaluation board and enter the following commands.

2. Enable DHCP, if disabled previously.

```
AT+NDHCP=<disable=0/enable=1>
```

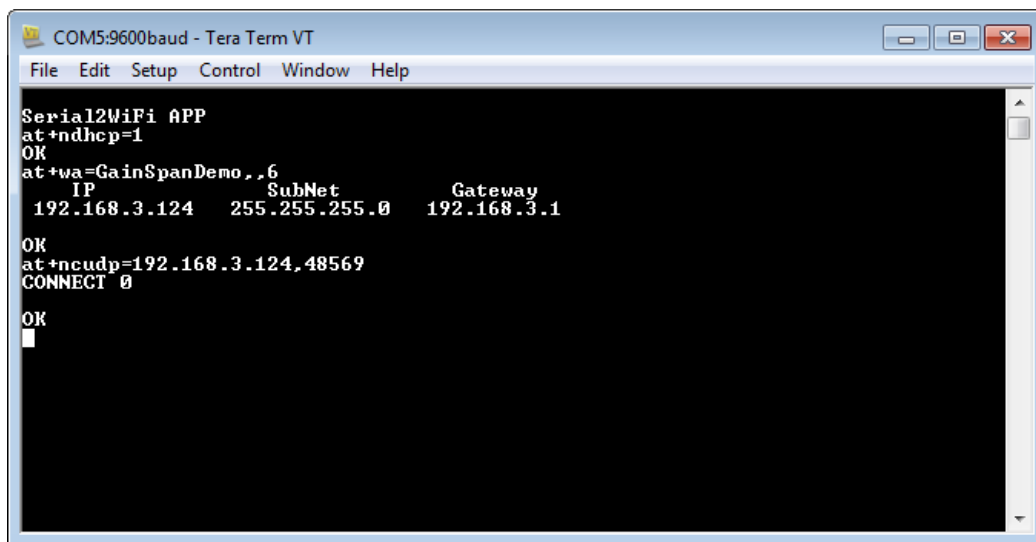
3. Associate to the Access Point (AP). This should be the same AP as the PC is also associated to: AT+WA=<SSID>[,<BSSID>][,<Ch>]

```
AT+WA=GainSpanDemo,,6
```

4. Start the UDP Client and connect to the UDP Server:
AT+NCUDP=<Dest-Address>,<Port>[,<Src.Port>]

```
AT+NCUDP=192.168.3.124,48569
```

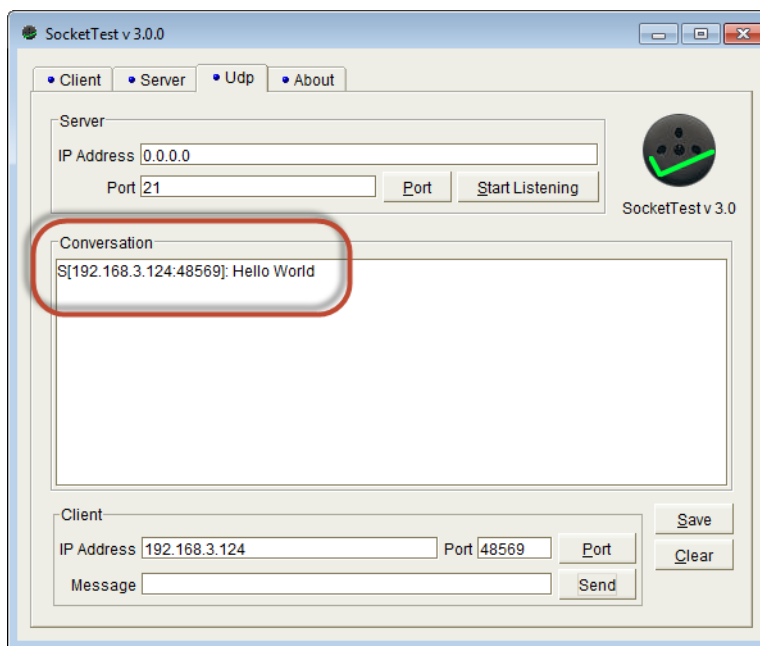
5. Upon successful connection to the UDP Server, you will see a “CONNECT <CID>” message, where CID is the newly allocated connection identifier (see Figure 6, page 21).

Figure 6 UDP Destination Address and Port Identified

6. GainSpan GS2000 module can send data to the UDP Server using the following sequence: <ESC>S<CID><Data><ESC>E

<ESC>S0HELLOWORLD<ESC>E

The text "Hello World" is now received at the UDP Server (see [Figure 7](#), page 21).

Figure 7 UDP Server Hello World

1.4 TCP

1.4.1 TCP Server

This section describes how to setup the TCP Server on the GainSpan GS2011M or GS2100M evaluation board using the AT command mode.

To setup the TCP Server, perform the following (see [Figure 8, page 22](#)):

1. Disassociate from the current network.

```
AT+WD
```

2. Enable DHCP, if disabled previously.

```
AT+NDHCP=<disable=0/enable=1>
```

3. Associate to an Access Point (AP): AT+WA=<SSID>[, [<BSSID>] [, <Ch>]]

```
AT+WA=GainSpanDemo,,6
```

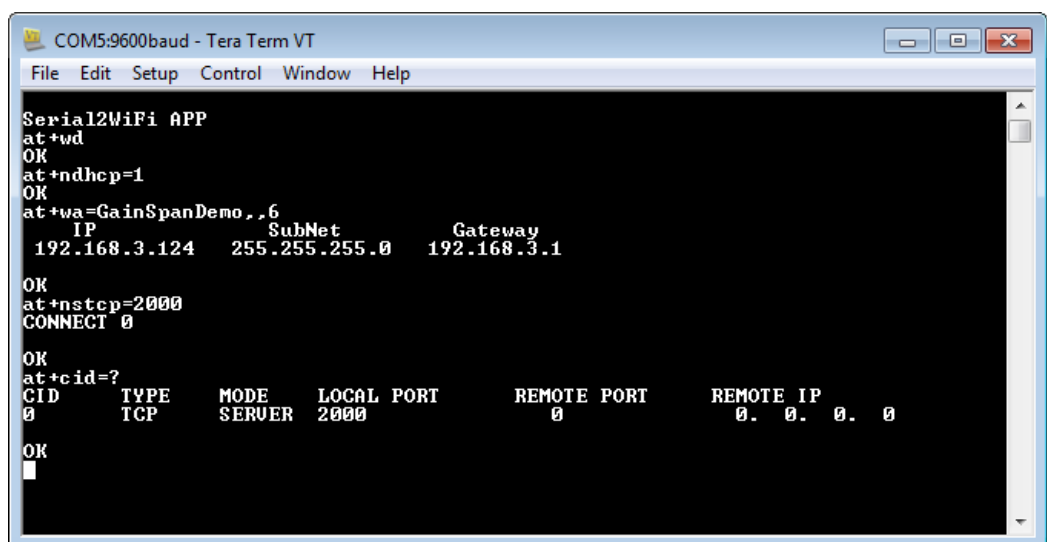
4. Start a TCP Server: AT+NSTCP=<port>

```
AT+NSTCP=2000
```

5. Upon successful creation of the TCP Server, you will see a “CONNECT <CID>” message where CID is the newly allocated connection identifier. You can check for this new CID by issuing the following command: AT+CID=?

```
AT+CID=?
```

Figure 8 Creating a TCP Server



6. The user can Telnet into this server:

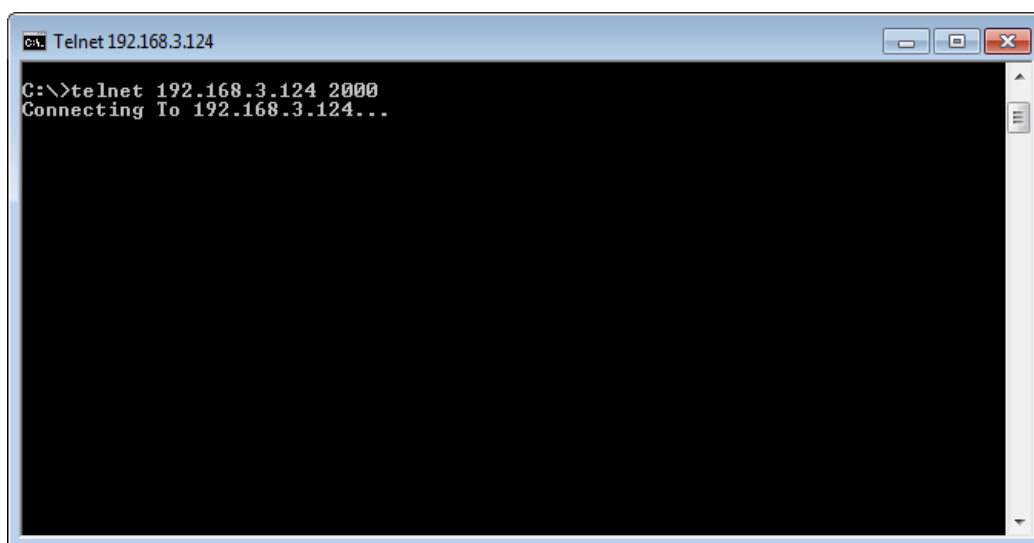
- Have a PC connected to the *GainSpanDemo* Access Point (AP)
- In the PC's command prompt, issue the following command:

```
Telnet <IP address > <port number>
```

For example: Telnet 192.168.3.124 2000 (see [Figure 9, page 23](#))

- Anything that is typed in the command prompt window will display on the Tera Term VT.

Figure 9 Connecting Telnet to Access Point



1.4.2 TCP Client

This section describes how to setup the TCP Client on the GainSpan GS2011M and GS2100M evaluation board using the AT command mode.

To setup the TCP Client, perform the following (see [Figure 10, page 25](#)):

Before you begin, have a PC connected to the GainSpanDemo and start a TCP Server on a specific port number. This example uses port number 3000.

1. Disassociate from the current network.

```
AT+WD
```

2. Enable DHCP, if disabled previously.

```
AT+NDHCP=<disable=0/enable=1>
```

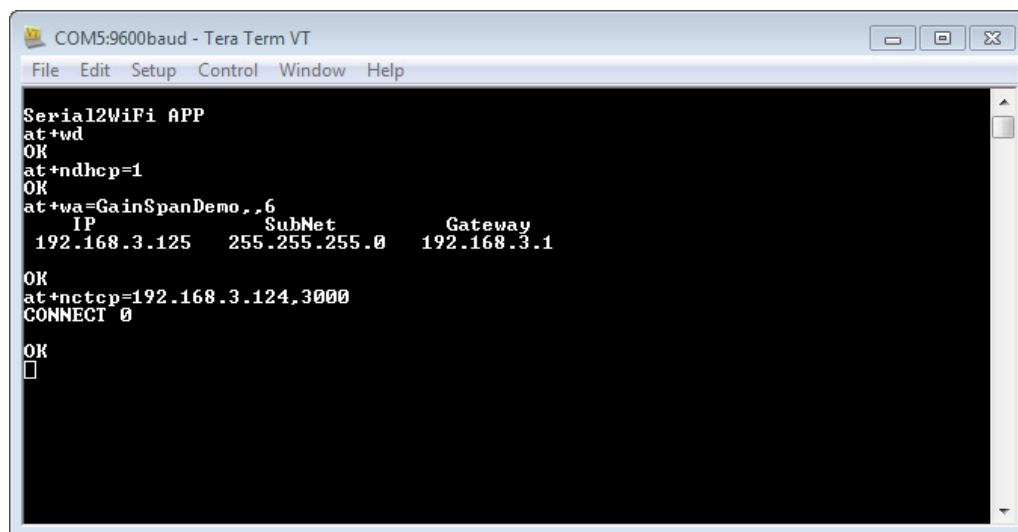
3. Associate to an Access Point (AP): AT+WA=<SSID>[, [<BSSID>] [, <Ch>]]

```
AT+WA=GainSpanDemo, , 6
```

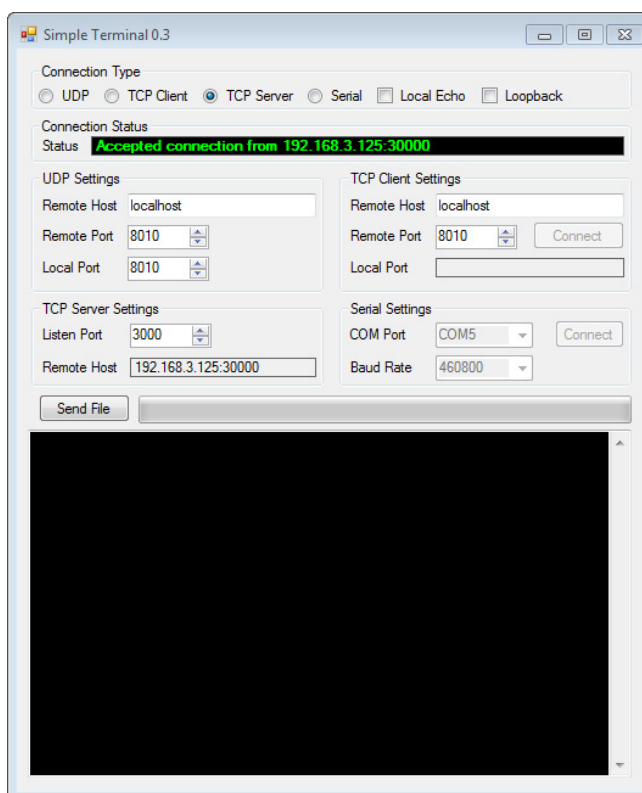
4. Start a TCP Client: AT+NCTCP=<Dest-Address>,<Port>

```
AT+NCTCP=192.168.3.124, 3000
```

Upon successful connection to the TCP Server, you will see a “CONNECT <CID>” message, where CID is the newly allocated connection identifier (see [Figure 11, page 25](#)).

Figure 10 TCP Client Session

```
Serial2WiFi APP
at+wd
OK
at+ndhcp=1
OK
at+wa=GainSpanDemo,,6
IP      SubNet      Gateway
192.168.3.125  255.255.255.0  192.168.3.1
OK
at+nctcp=192.168.3.124.3000
CONNECT 0
OK
█
```

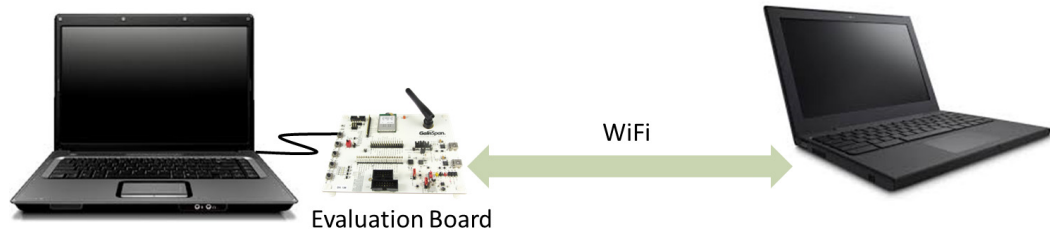
Figure 11 TCP Server Connection

1.5 Limited AP Mode

1.5.1 Creating Limited AP Mode With No Security

Figure 12, page 26 illustrates Limited AP mode setup.

Figure 12 Limited AP Mode (Open)



Use the following steps to create limited AP mode.

1. Configure network stack parameter.

```
AT+NSET=<SrcAddr>,<Net-Mask>,<Gateway>
```

2. Configure wireless mode to Limited AP.

```
AT+WM=<infrastructure=0,adhoc=1,limited AP=2>
```

3. Create the limited AP network.

```
AT+WA=<SSID>[, [<BSSID>] [, <Ch>]]
```

4. Enable DHCP server.

```
AT+DHCSRVR=<disable=0/enable=1>
```

5. (*Optional*) Start the DNS server and specify a DNS name.

```
AT+DNS=<disable=0/enable=1,<url>
```

Example

```
AT+NSET=192.168.1.1,255.255.255.0,192.168.1.1
AT+WM=2
AT+WA=GS_Limited_AP,,11
AT+DHCSRVR=1
```

Figure 13, page 27 illustrates Limited AP mode created.

Figure 13 Creating Limited AP Mode (Open)

```

COM19:9600baud - Tera Term VT
File Edit Setup Control Window Help

Serial2WiFi APP
AT+NSET=192.168.1.1,255.255.255.0,192.168.1.1
OK
AT+WM=2
OK
AT+WA=GS_Limited_AP,,11
      IP          SubNet          Gateway
192.168.1.1: 255.255.255.0: 192.168.1.1
OK
AT+DHCSRVR=1
OK

```

1.5.2 Creating Limited AP WPA2-PSK Mode (Secure Network)

The instructions below outline how to create limited AP in WPA2-PSK mode with DHCP and DNS sever enabled. Figure 14, page 28 illustrates Limited AP mode (secure network) setup.

1. Configure network stack parameter.

```
AT+NSET=<Src Addr>,<Net-Mask>,<Gateway>
```

2. Compute WPA2-PSK from a given SSID and Passphrase.

```
AT+WPAPSK=<SSID>,<PASSPHRASE>
```

3. Configure security to WPA2-PSK.

```
AT+WSEC=<n>
```

4. Configure authentication mode to NONE.

```
AT+WAUTH=<none,WPA/WPA2=0, open=1, WEP=2>
```

5. Configure wireless mode to Limited AP.

```
AT+WM=<infrastructure=0, ad hoc=1, limited AP =2>
```

6. Enable DHCP server.

```
AT+DHCSRVR=<disable=0/enable=1>
```

7. Create the infrastructure network.

```
AT+WA=<SSID>[ , [<BSSID>] [ , <Ch>] ]
```

8. Start the DNS server and specify a DNS name.

Example

```
AT+DNS=<disable=0/enable=1, <url>

AT+NSET=192.168.3.124,255.255.255.0,192.168.3.1
AT+WPAPSK=limitedAP,1234567890
AT+WSEC=8
AT+WAUTH=0
AT+WM=2
AT+DHCSRVR=1
AT+WA=limitedAP,,6
AT+DNS=1,www.limitedAP.com
```

Figure 14 Creating Limited AP Mode (Secure Network)



NOTE: The TCP/UDP example is common to whether you associate with an open or secure network.

1.5.3 UDP Server

1. Configure the GainSpan module to operate in Limited AP Mode and start the UDP server (see [Figure 15, page 29](#)).

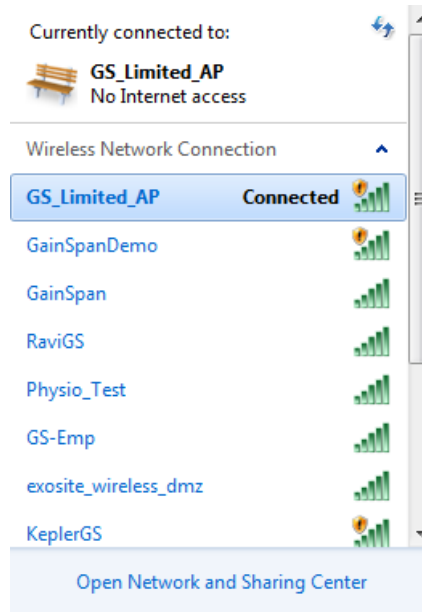
```
AT+WRXACTIVE=1
AT+NSET=192.168.1.1,255.255.255.0,192.168.1.1
AT+WM=2
AT+WA=GS_Limited_AP,,11
AT+DHCPSTVR=1
AT+NSUDP=48569
AT+CID=?
```

Figure 15 Starting UDP Server in Limited AP Mode

```
COM5:9600baud - Tera Term VT
File Edit Setup Control Window Help
Serial2WiFi APP
at+wxactive=1
OK
at+nset=192.168.1.1,255.255.255.0,192.168.1.1
OK
at+wm=2
OK
at+wa=GS_Limited_AP,,11
OK
      IP      SubNet      Gateway
192.168.1.1  255.255.255.0  192.168.1.1
OK
at+dhcprvr=1
OK
at+nsudp=48569
CONNECT 0
OK
at+cids=?
CID      TYPE      MODE      LOCAL PORT      REMOTE PORT      REMOTE IP
0        UDP      SERVER    48569           0                0.0.0.0
OK
```

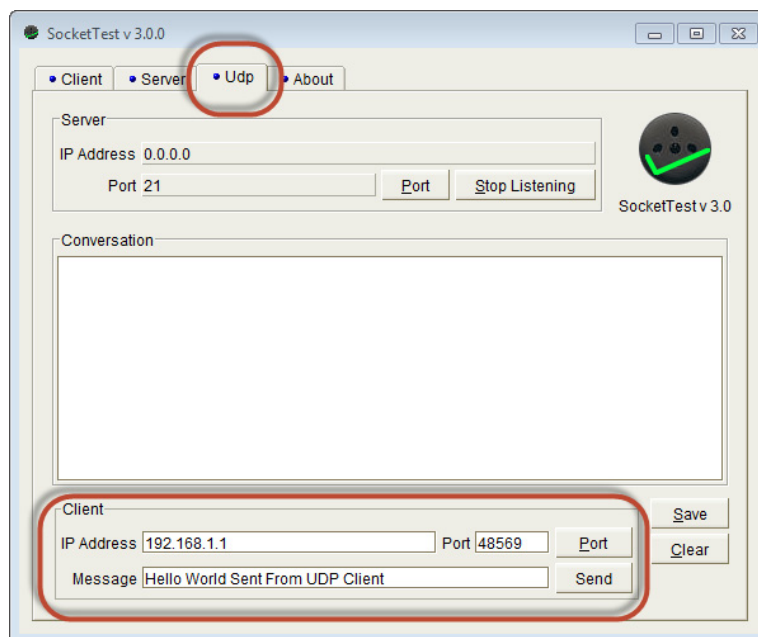
2. Have PC associate to the Limited AP (see Figure 16, page 30).

Figure 16 Associate PC to the Limited AP for UDP Server



3. Using the “SocketTest” tool, have the UDP Client send data to the UDP Server (see Figure 17, page 30).

Figure 17 UDP Client Sends Data to UDP Server



4. Data should be received on the module side (see Figure 18, page 31).

Figure 18 Data Received on the Module

COM5:9600baud - Tera Term VT

```

File Edit Setup Control Window Help

at+wrxactive=1
OK
at+nset=192.168.1.1,255.255.255.0,192.168.1.1
OK
at+wm=2
OK
at+wa=GS_Limited_AP,,11
      IP      SubNet      Gateway
192.168.1.1  255.255.255.0  192.168.1.1
OK
at+dhcprvr=1
OK
at+nsudp=48569
CONNECT 0
OK
at+cidx=?
CID      TYPE      MODE      LOCAL PORT      REMOTE PORT      REMOTE IP
0        UDP        SERVER    48569           0               0.0.0.0
OK
0192.168.1.3 62210      Hello World Sent From UDP Client

```

Figure 19 Creating a UDP Server

COM5:9600baud - Tera Term VT

```

File Edit Setup Control Window Help

Serial2WiFi APP
at+ndhcp=1
OK
at+wa=GainSpanDemo,,6
      IP      SubNet      Gateway
192.168.3.124 255.255.255.0  192.168.3.1
OK
at+nsudp=48569
CONNECT 0
OK
at+cidx=?
CID      TYPE      MODE      LOCAL PORT      REMOTE PORT      REMOTE IP
0        UDP        SERVER    48569           0               0.0.0.0
OK

```

1.5.4 UDP Client

To configure the GainSpan module to operate in Limited AP mode and UDP Client, perform the following:

1. Enter the following AT commands.

```
AT+NSET=192.168.1.1,255.255.255.0,192.168.1.1
```

```
AT+WM=2
```

```
AT+WA=GS_Limited_AP,,11
```

```
AT+DHCPSRVR=1
```

2. Have PC associate to the Limited AP (see [Figure 16, page 30](#)).

Figure 20 Associate PC to the Limited AP for UDP Client

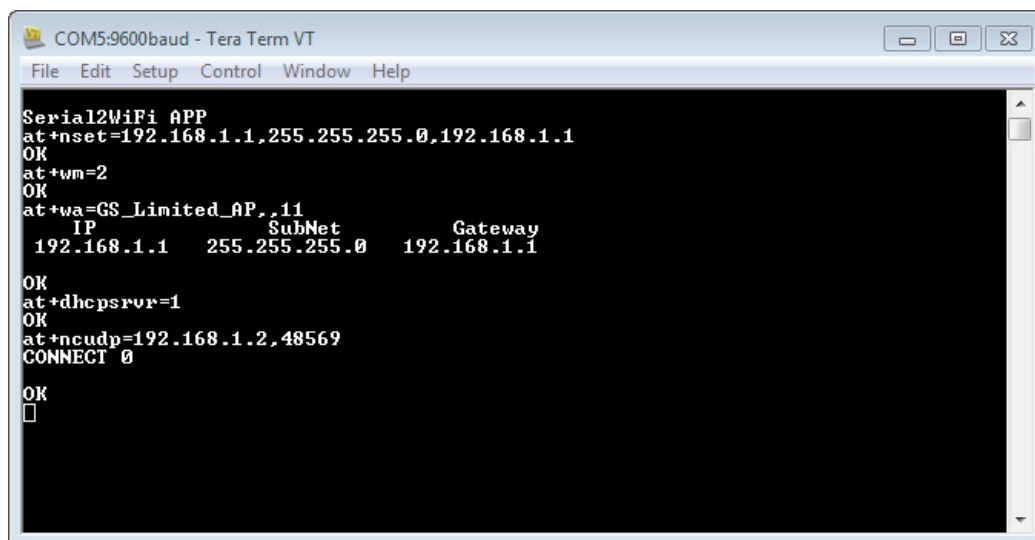


3. Start the UDP Server on the PC. UDP Server automatically picks up the IP address once the PC is connected to Limited AP on the evaluation board.

4. Connect GainSpan module to the UDP Server (see [Figure 21, page 33](#)).

```
AT+NCUDP=192.168.1.2,48569
```

Figure 21 Connect Module UDP Server



```
COM5:9600baud - Tera Term VT
File Edit Setup Control Window Help

Serial2WiFi APP
at+nset=192.168.1.1,255.255.255.0,192.168.1.1
OK
at+wm=2
OK
at+wa=GS_Limited_AP,,11
      IP      SubNet      Gateway
192.168.1.1  255.255.255.0  192.168.1.1
OK
at+dhcprvr=1
OK
at+ncudp=192.168.1.2,48569
CONNECT 0
OK
□
```

Upon successful connection to the UDP server, you will see a “CONNECT <CID>” message, where CID is the newly allocated connection identifier (see [Figure 21, page 33](#)).

1.5.5 TCP Server

1. Issue the following AT command sequence to create a Limited AP and start TCP server on port 8010.

```
AT+NSET=192.168.1.1,255.255.255.0,192.168.1.1
```

```
AT+WM=2
```

```
AT+WA=GS_Limited_AP,,11
```

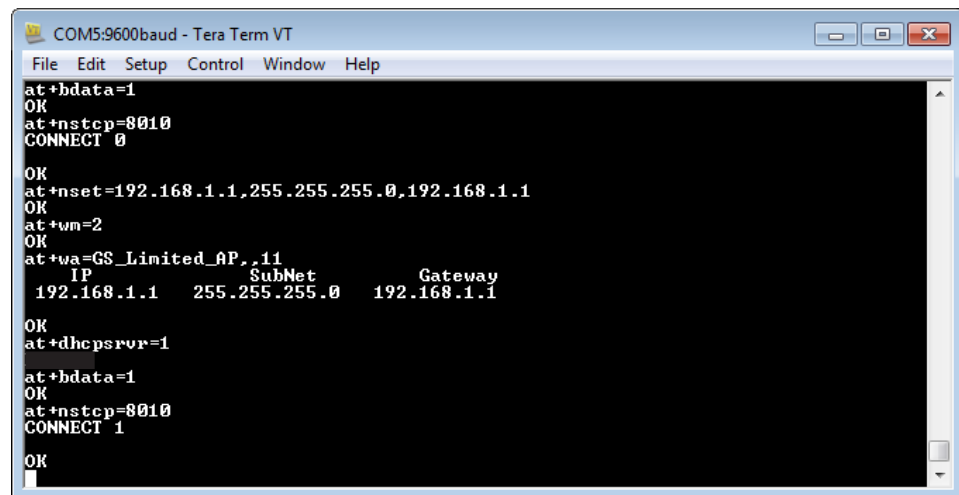
```
AT+DHCPSRVR=1
```

```
AT+BDATA=1
```

```
AT+NSTCP=8010
```

2. A sample output will display in the Tera Term VT window (see [Figure 22, page 34](#)).

Figure 22 Sample Output in Tera Term VT



The screenshot shows a Tera Term VT window titled "COM5:9600baud - Tera Term VT". The window contains the following text:

```
at+bdata=1
OK
at+nstcp=8010
CONNECT 0

OK
at+nset=192.168.1.1,255.255.255.0,192.168.1.1
OK
at+wm=2
OK
at+wa=GS_Limited_AP,,11
  IP      SubNet      Gateway
192.168.1.1 255.255.255.0 192.168.1.1
OK
at+dhcprvr=1
at+bdata=1
OK
at+nstcp=8010
CONNECT 1
OK
```

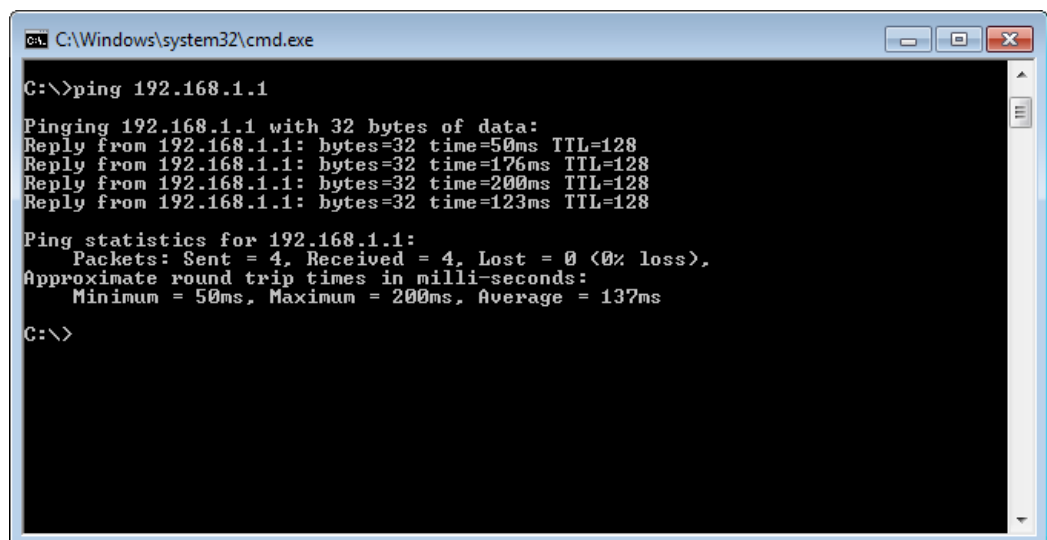
3. In the Wireless Network Connection window, the “GS_Limited_AP” will show being connected (see Figure 23, page 35).

Figure 23 PC Connected to GS_Limited_AP



4. Confirm that the connection is established by sending a ping to **192.168.1.1** from the PC (see Figure 24, page 35).

Figure 24 Confirm Connection Established



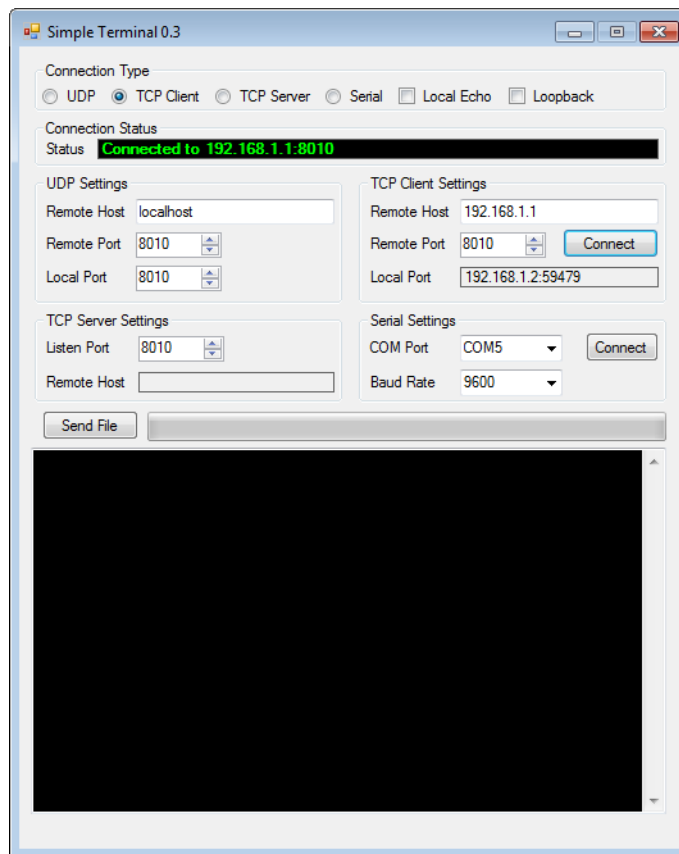
5. Launch the Simple Terminal application and connect to the GainSpan module (e.g., GS2011M or GS2100M) (see [Figure 25](#), page 36).



NOTE: The Simple Terminal application can be open from the SW Utilities directory from the evaluation software folder.

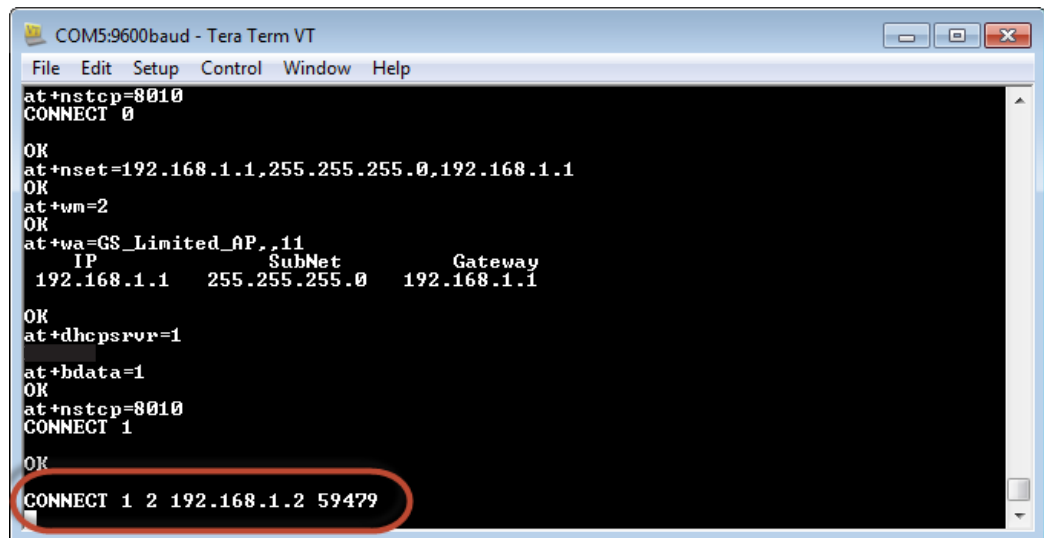
192.168.1.1, 8010

Figure 25 Simple Terminal Connected to TCP Client



6. Upon successful TCP connection, locate the “CONNECT <CID> <CID> <IP Address> <Port number>” message displayed on Tera Terminal VT (see [Figure 26](#), [page 37](#)).

Figure 26 TCP Connection Message Displayed on Tera Term VT Window

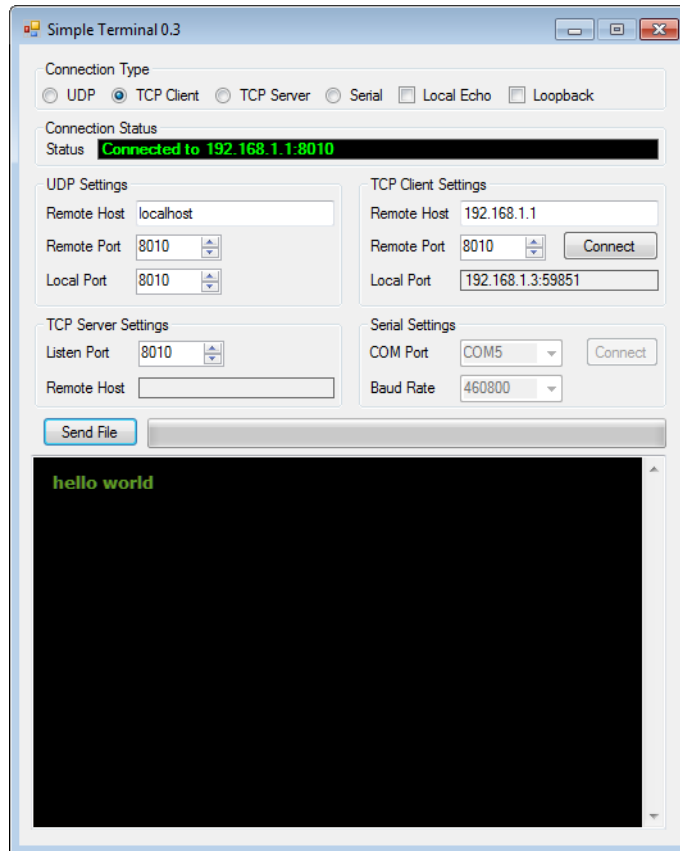


7. To send data (for example: hello) from the TCP Server (for example: GS2011M) to TCP Client (Simple Terminal), go to Tera Term VT and enter:

<ESC>Z10005hello

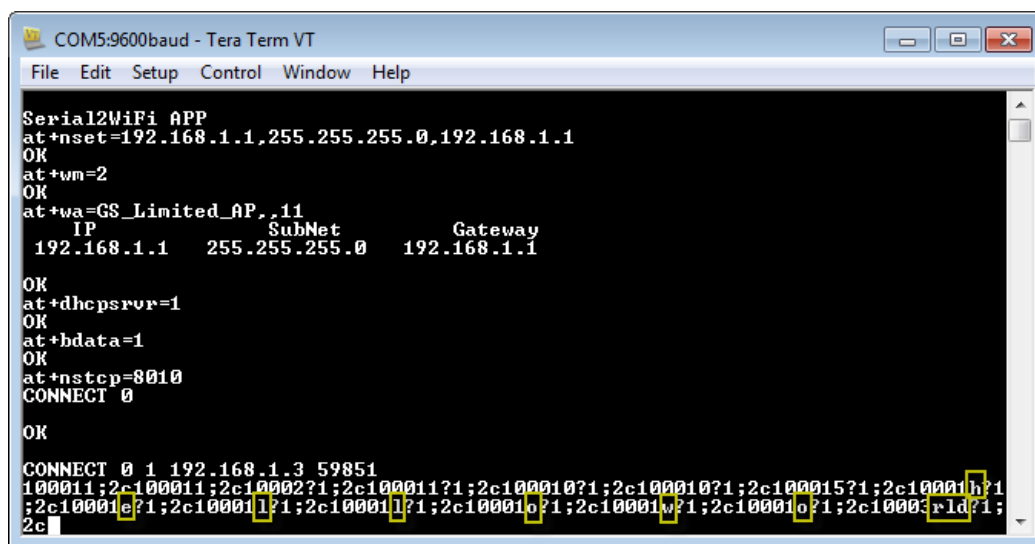
You should now see “hello” received in the Simple Terminal window (see [Figure 27](#), page 38).

Figure 27 Sending Data from TCP Server to TCP Client



8. If you want to send data from TCP Client to TCP Server, simply enter any text in the Simple Terminal window. In the example shown below the user entered the text “world” in the Simple Terminal, and the text is seen received on the Tera Term VT screen (see [Figure 28, page 39](#)).

Figure 28 TCP Server Text Received Within Tera Term Window



For additional security AT commands, refer to the *GainSpan Serial-to-WiFi Adapter Application Programmer Reference Guide*.

- This page intentionally left blank -

Chapter 2 Serial-to-WiFi Provisioning

This chapter provides procedures on how to provision the GainSpan® GS2011M or GS2100M for Serial-to-WiFi Web Provisioning and WiFi Protected Setup (WPS).

- [Introduction, page 41](#)
- [Setting Up Web Provisioning Using Limited AP Provisioning Mode, page 42](#)
- [Setting Up WPS Based Provisioning, page 58](#)

2.1 Introduction

The Serial-to-WiFi application supports multiple methods of provisioning the device to connect different Access Points (AP).

- Web Provisioning using Limited AP Provisioning Mode
- WiFi Protected Setup (WPS) Based Provisioning

The Web Server based provisioning allows the user to scan and choose a WiFi Access Point (AP) to connect to using a web browser either on your PC or Hand Held device. You may then select an AP and input the security pass code to connect to the AP.

WiFi Protected Setup (WPS) enables you to connect your GS2000 based module device to your WPS enabled AP without having to input any pass codes. This method requires the AP to support WPS and have enabled either push button method or pin method for association and authentication.

2.2 Setting Up Web Provisioning Using Limited AP Provisioning Mode

In the Serial-to-WiFi application, you may also access the embedded web pages by putting the device into the Limited AP Provisioning Mode. In this mode, the device acts as an Access Point (AP) for other devices, such as Smart Phones, Tablets, etc., to connect as a client and provision the device.



NOTE: The parameters, such as IP addresses, SubNet addresses, and Gateways used throughout this document are examples only.



NOTE: The GS2011M and GS2100M evaluation boards have to be programmed before running these procedures.

In the Tera Term VT terminal emulation window, execute the following AT commands:

1. Set the Static IP Address on the GS2000 based module evaluation board.

```
AT+NSET=192.168.1.1,255.255.255.0,192.168.1.1
```

2. Set the wireless mode to limited AP mode so that the adapter can act as a limited wireless Access Point (AP).

```
AT+WM=2
```

3. Set the AP network (example - created using SSID *GS_Limited_AP* on channel 11).

```
AT+WA=GS_Limited_AP,,11
```

```
IP           SubNet       Gateway
192.168.1.1:255.255.255.0:192.168.1.1
```

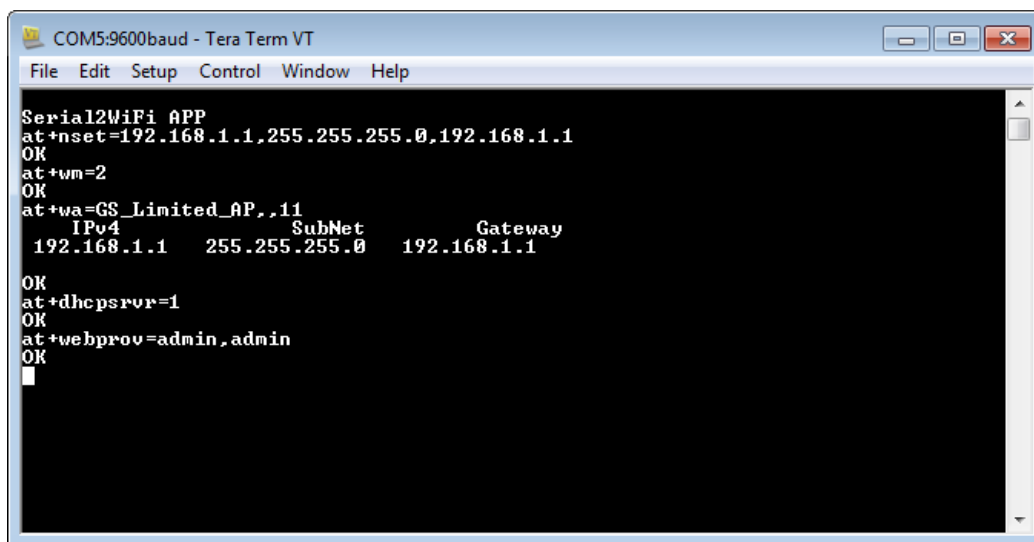
4. Start the DHCP server.

```
AT+DHCPSTVR=1
```

5. Start provisioning through web pages. Enable saving profile and start a new NCM (network connection manager). (see [Figure 29, page 43](#)).

```
AT+WEBPROV=admin,admin
```

Refer to the *GainSpan GS2000 Based Module Programming User Guide* for instructions on how to program the GS2011M and GS2100M evaluation boards.

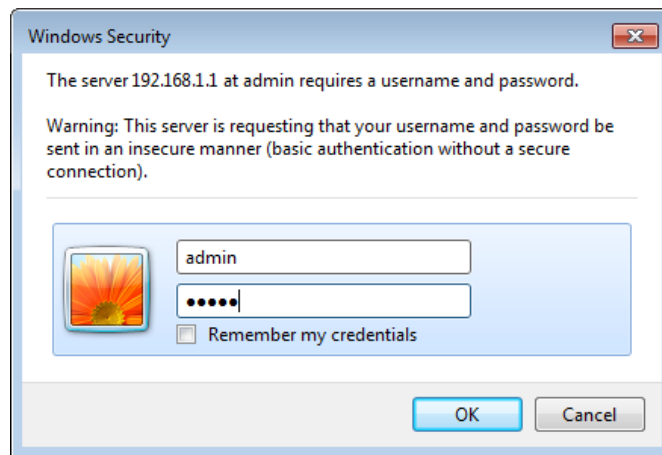
Figure 29 Provisioning GainSpan Web Site

6. Associate the PC acting as the configuring device to provision the GS2000 based module evaluation board.
7. Select the Wireless Network created in **Step 3**. In this example it is **GS_Limited_AP**, and click **Connect** (see [Figure 30, page 43](#)).

Figure 30 Connecting to a Wireless Network Connection

8. Once the connection is established, open a web browser and type the IP address and the URL of the GS2000 based module evaluation board (in this example, it is <http://192.168.1.1/gsprov.html>). The IP address 192.168.1.1 was set in the previous steps. This will prompt for a User name and Password. Enter the **User name** and **Password** and press **Enter** or click **OK** (see Figure 31, page 44).

Figure 31 Enter User Name and Password



9. The GainSpan Device Setup web provisioning page will display (see Figure 32, page 44).

Figure 32 GainSpan Device Setup



You can navigate to different pages:

- Client Settings
- Limited AP Settings
- Operation Mode Selection
- Administrator Settings

2.2.1 Wireless and Network Configuration

You can connect to a Wireless network by one of the following methods:

- Select an Existing Network
- Manually Configure to Join a Network

2.2.1.1 Select an Existing Network

When selecting an existing network, the node will start scanning and displaying a list of available APs.

1. Click the **Select** button to connect to the selected AP by providing required credentials (Passphrase) (see [Figure 33, page 45](#)).

Figure 33 Selecting Existing Network



2. After entering a passphrase, you can select the advanced options, which displays the selection methods for obtaining an IP address (see [Figure 34, page 46](#)). You can get the IP address in two ways.
 - DHCP
 - Static IP

Figure 34 Enter Passphrase and Advanced Options

GainSpan®

Client Settings

Configure Wireless and Network Settings

These settings govern the functioning of the device when it is operating in Client mode.

SSID: GainSpanDemo

Channel: 6

Security: WPA/WPA2 Personal

Passphrase:

Confirm Passphrase:

☒ **Advanced Options**

Select a method to obtain or set the IP address.

☐ Acquire IP Address automatically (DHCP)

☒ Static IP Address Configuration

IP Address: 192 . 168 . 1 . 1

Subnet Mask: 255 . 255 . 255 . 0

Gateway: 192 . 168 . 1 . 1

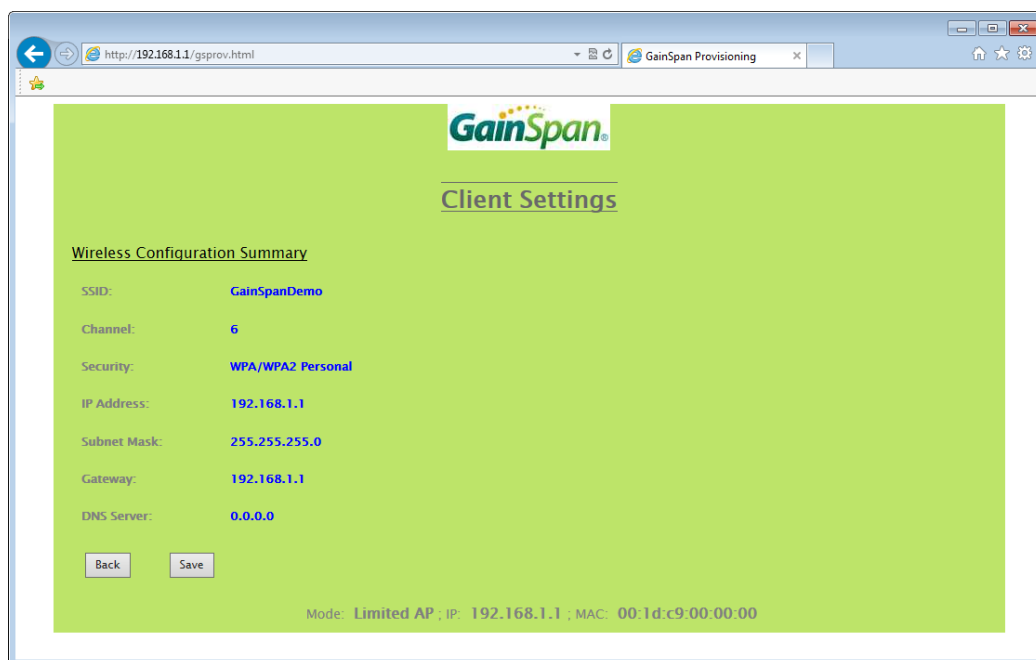
DNS Server: 0 . 0 . 0 . 0

Back Next

Mode: Limited AP ; IP: 192.168.1.1 ; MAC: 00:1d:c9:00:00:00

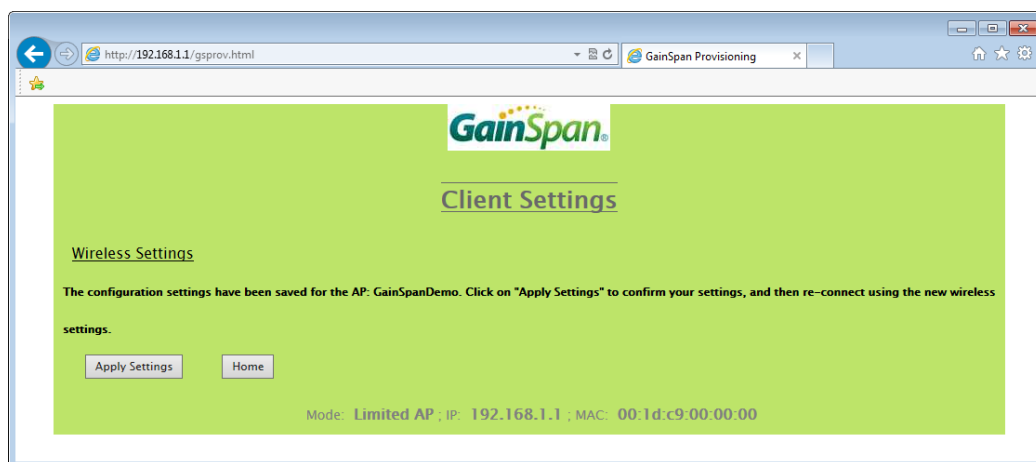
- Click the **Next** button to navigate to the Wireless Configuration Summary page. This page displays the information about the SSID, Channel, Security type and provides an option to save and apply the settings or go back to make changes (see [Figure 35](#), page 47).

Figure 35 View Wireless Configuration Summary



- Click **Save** and the **Apply Settings** buttons to save the wireless settings that will be applied to connect the GainSpan device to the GainSpanDemo network (see [Figure 36](#), page 47).

Figure 36 Save and Apply Wireless Settings to the GainSpan Device





NOTE: The SSID GainSpanDemo is an example.

5. The GainSpan device will now reset and connect to the GainSpanDemo network and start a network connection (see [Figure 37](#), [page 48](#)).

Figure 37 Connecting Device to the Network

A screenshot of a Tera Term VT window titled "COM5:9600baud - Tera Term VT". The window displays a list of network configuration commands for a device. The commands are as follows:

```
SSID=GainSpanDemo
CHNL=6
CONN_TYPE=0
MODE=0
SECURITY=3
PSK_PASS_PHRASE=shadow77
DHCP_ENBL=0
STATIC_IP=192.168.1.1
SUBMT_MASK=255.255.255.0
GATEWAY_IP=192.168.1.1
AUTO_DNS_ENBL=0
AP-SSID=GS_Limited_AP
AP-CHNL=11
AP-BEACON-INTRL=100
AP-SECURITY=1
AP-STATIC_IP=192.168.1.1
AP-SUBMT_MASK=255.255.255.0
AP-GATEWAY_IP=192.168.1.1
AP-DHCP SRVR-ENABLE=1
AP-AP-DHCP SRVR-START IP=192.168.1.2
AP-DHCP SRVR-NO-CONN=8
AP-DNS SRVR-ENABLE=1
AP-DNS-DOMAIN-NAME=
APP Reset-APP SW Reset
```


2.2.1.2 Manual Configuration

The Device Setup can also allow you to manually configure the WiFi related setting SSID, Channel, Security, and Passphrase (see [Figure 38, page 49](#)). There are also Advanced Options to obtain the IP address either by DHCP or by Static IP configuration.

Figure 38 Manually Configure Wireless Settings

The screenshot shows a web browser window with the URL `http://192.168.1.1/gsprov.html`. The page title is "GainSpan Provisioning". The main heading is "Client Settings". Below this is the section "Configure Wireless and Network Settings". A note states: "These settings govern the functioning of the device when it is operating in Client mode."

The configuration fields are as follows:

- SSID:** GSDemoKit
- Channel:** 6
- Security:** WPA/WPA2 Personal
- Passphrase:** [Redacted]
- Confirm Passphrase:** [Redacted]

Below these fields is the "Advanced Options" section, which is checked. It contains the instruction: "Select a method to obtain or set the IP address."

Two radio buttons are present:

- ☐ Acquire IP Address automatically (DHCP)
- ☒ Static IP Address Configuration

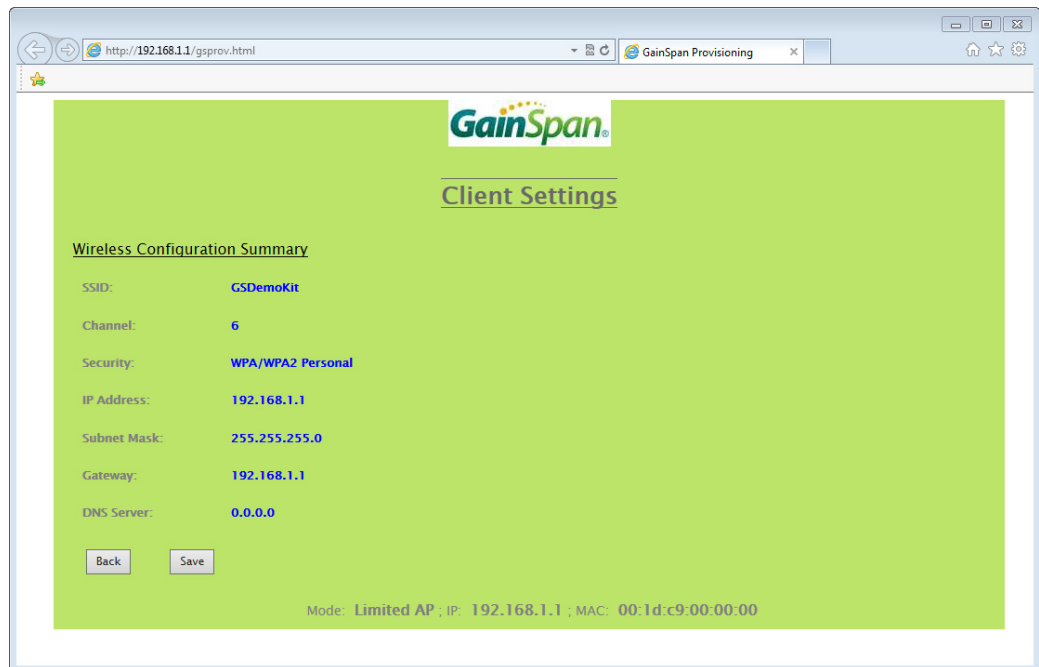
The Static IP configuration fields are:

- IP Address:** 192.168.1.1
- Subnet Mask:** 255.255.255.0
- Gateway:** 192.168.1.1
- DNS Server:** 0.0.0.0

At the bottom of the form are "Back" and "Next" buttons. At the very bottom, the status bar reads: "Mode: Limited AP ; IP: 192.168.1.1 ; MAC: 00:1d:c9:00:00:00".

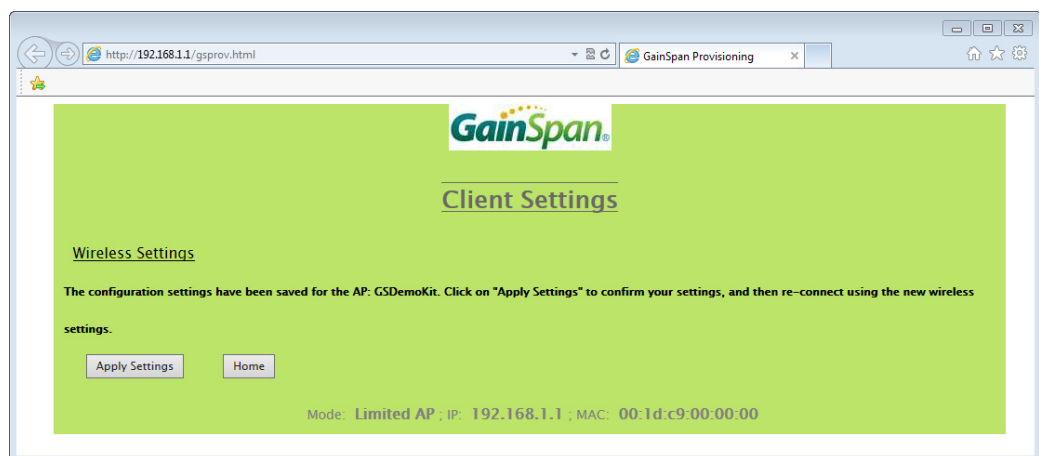
1. Click the **Next** button to navigate to the Wireless Configuration Summary page (see Figure 39, page 50).
2. Click the **Save** button to save the manually configured wireless settings.

Figure 39 Save Manually Configured Wireless Settings



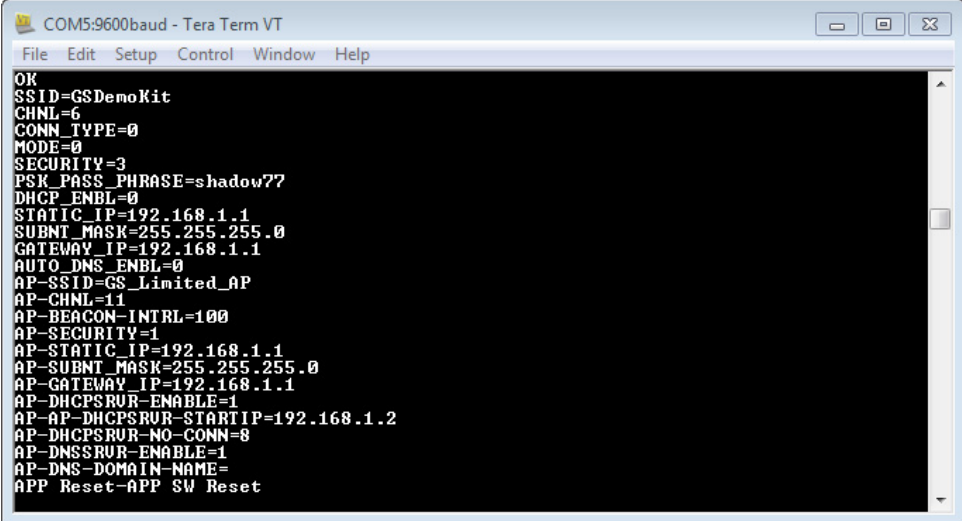
3. Click **Apply Settings** button to apply the selected wireless settings and connect the GainSpan device to the new network (see Figure 40, page 50).

Figure 40 Apply Settings and Connect to a New Network



4. The GainSpan device will now reset and connect to the GSDemoKit network and start a new network connection (see [Figure 37](#), [page 48](#)).

Figure 41 Connecting Device to a New Network



```
COM5:9600baud - Tera Term VT
File Edit Setup Control Window Help
OK
SSID=GSDemoKit
CHNL=6
CONN_TYPE=0
MODE=0
SECURITY=3
PSK_PASS_PHRASE=shadow77
DHCP_ENBL=0
STATIC_IP=192.168.1.1
SUBNT_MASK=255.255.255.0
GATEWAY_IP=192.168.1.1
AUTO_DNS_ENBL=0
AP-SSID=GS_Limited_AP
AP-CHNL=11
AP-BEACON-INTRL=100
AP-SECURITY=1
AP-STATIC_IP=192.168.1.1
AP-SUBNT_MASK=255.255.255.0
AP-GATEWAY_IP=192.168.1.1
AP-DHCPSTRUR-ENABLE=1
AP-AP-DHCPSTRUR-STARTIP=192.168.1.2
AP-DHCPSTRUR-NO-CONN=8
AP-DNSSTRUR-ENABLE=1
AP-DNS-DOMAIN-NAME=
APP Reset-APP SW Reset
```



NOTE: The SSID GSDemoKit is an example.

2.2.2 Limited AP Settings

The Limited AP Settings page displays the information that was entered in the Tera Term VT window using AT commands. You can change anyone of the wireless and network settings (see [Figure 42, page 52](#)).

Figure 42 Limited AP Settings

GainSpan®

Limited AP Settings

Configure Wireless and Network Settings

SSID: Please ensure that this SSID (network name) is unique in your wireless environment.

Channel:

Security:

☒ Advanced Options

Beacon Interval (Range: 100 to 1600 ms):

Network Address Settings:

IP Address:

Subnet Mask:

Gateway:

☒ Enable DHCP Server

Starting Address:

Number of Addresses:

☒ Enable DNS Server

Domain Name:

Mode: Limited AP ; IP: 192.168.1.1 ; MAC: 00:1d:c9:00:00:00

From this page, you can change the following:

- SSID
- Channel
- Security (Open, WEP-40 Open, WPA2 Personal (AES+TKIP))
- Advanced Options (check box):
 - Beacon Interval (Range: 100 to 1600 msec)
 - Network Address Settings (IP Address, Subnet Mask, Gateway)
 - Enable DHCP Server (check box):
 - Starting Address

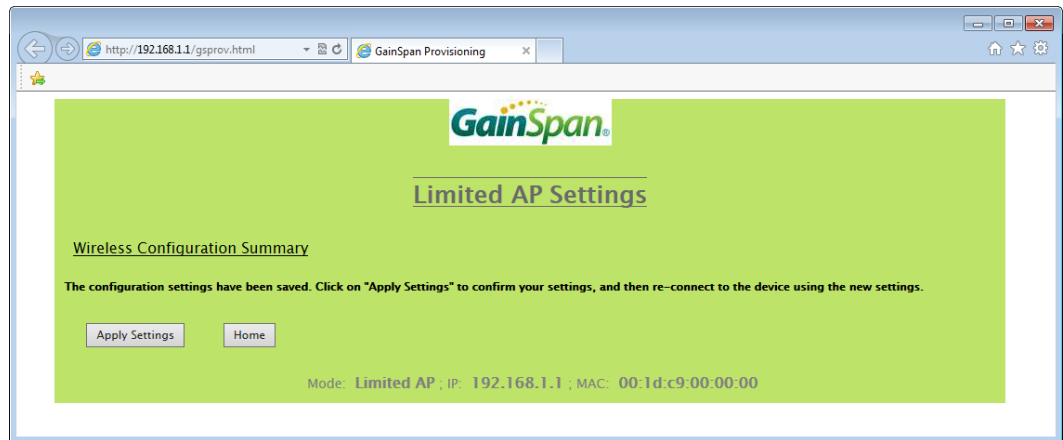
- Number of Addresses
 - Enable DNS Server:
 - Domain Name
1. Click **Next** to view a summary of the wireless configuration (see [Figure 43](#), page 53).

Figure 43 Save the Limited AP Wireless Configuration Settings



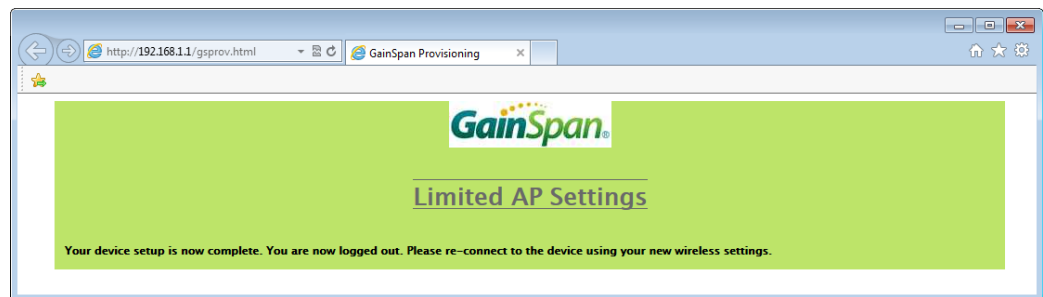
2. Click **Save** and click **Apply Settings** (see Figure 44, page 54). This will confirm that the wireless configuration settings have been saved and the device setup is complete.

Figure 44 Confirming Wireless Configuration Settings Are Saved



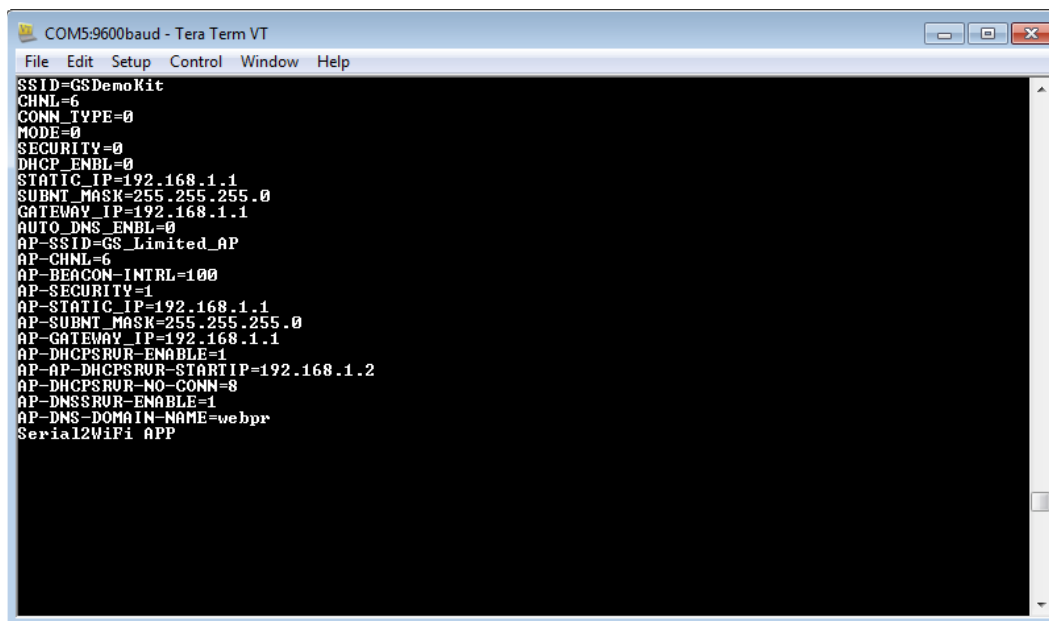
3. Re-connect to the device using any new settings you created and/or updated in the settings screen (see Figure 45, page 54).

Figure 45 Device Setup is Complete



4. When the Limited AP Settings are applied the open Tera Term VT window will display all the AP settings for the Limited AP mode (see [Figure 46, page 55](#)).

Figure 46 Limited AP Settings Displayed in Tera Term Window

A screenshot of a Tera Term VT window titled 'COM5:9600baud - Tera Term VT'. The window has a menu bar with 'File', 'Edit', 'Setup', 'Control', 'Window', and 'Help'. The main display area shows a list of network settings for a Limited AP mode. The settings are as follows:

```
SSID=GSDemoKit
CHNL=6
CONN_TYPE=0
MODE=0
SECURITY=0
DHCP_ENBL=0
STATIC_IP=192.168.1.1
SUBNET_MASK=255.255.255.0
GATEWAY_IP=192.168.1.1
AUTO_DNS_ENBL=0
AP-SSID=GS_Limited_AP
AP-CHNL=6
AP-BEACON-INTVL=100
AP-SECURITY=1
AP-STATIC_IP=192.168.1.1
AP-SUBNET_MASK=255.255.255.0
AP-GATEWAY_IP=192.168.1.1
AP-DHCPSESR-ENABLE=1
AP-AP-DHCPSESR-STARTIP=192.168.1.2
AP-DHCPSESR-NO-CONN=8
AP-DHCPSESR-ENABLE=1
AP-DNS-DOMAIN-NAME=webpr
Serial2WiFi APP
```

2.2.3 Operation Mode Selection

This option allows you to select the mode of operation, **Client** or **Limited AP**.

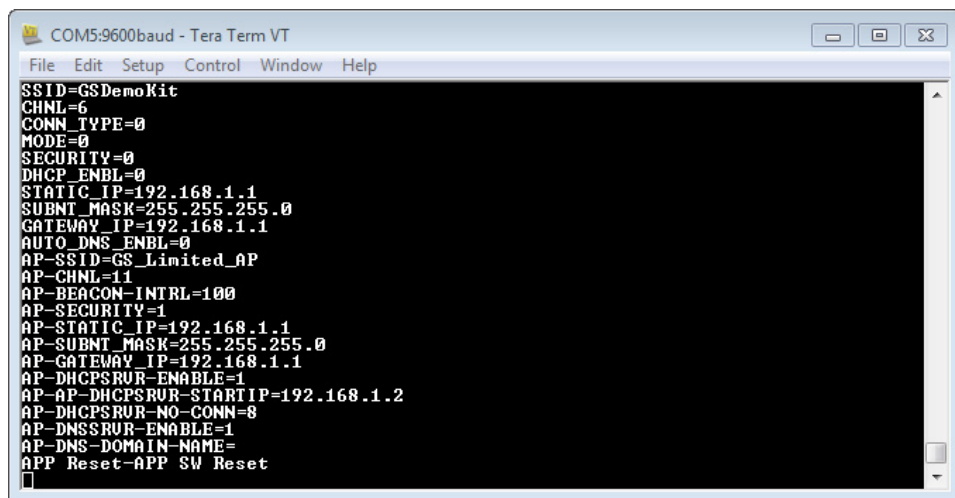
1. Click the **Set Mode** button (see Figure 47, page 56). See , page 66.

Figure 47 Select Mode of Operation



2. When the Client mode is selected, the open Tera Term VT window will display all the AP settings for the Client mode (see Figure 48, page 56).

Figure 48 Client Mode Settings Displayed in Tera Term Window



2.2.4 Administrator Settings

The Administrator Settings allow you to change the User Name and Password of the node. You can also change the System Identification Name. When you completed your selection, click the **Save & Apply** button (see [Figure 49, page 57](#)). The information will be sent to the Host Processor and reset the module. The Host Processor will send the information back to the module for provisioning.

Figure 49 Administrator Settings

The screenshot shows a web browser window with the URL `http://192.168.1.1/gsprov.html`. The page title is "GainSpan Provisioning". The main content area has a green background and the "GainSpan" logo at the top. Below the logo is the heading "Administrator Settings".

The first section is "Web Server Settings". It includes a note: "To disable web server security, please leave the following fields empty." Below this note are three input fields: "Username:" with the value "GS_USER", "Password (at least 4 characters):" with masked characters, and "Confirm Password:" with masked characters. A red rectangle highlights these three fields. Below the input fields are two buttons: "Back" and "Save & Apply".

The second section is "System Identification". It includes a label "System Name (Please ensure this name is unique in your network):" followed by an input field containing "S2W_000000". Below this is a label "UUID:" followed by the value "001dc9000000". Below these are two buttons: "Back" and "Save & Apply".

The third section is "Firmware Information". It lists several versions: "WLAN Version: 5.0.6", "GEPS Version: 5.0.6", "Provisioning Web-app Version: 0.9.13", "Embedded Application Version: 5.0.6", "System HTTP API Version: 1.0.1", and "Module: GS2000".

2.3 Setting Up WPS Based Provisioning

In order to simplify the processing of establishing a secure network, the WiFi Alliance has defined a simplified WiFi Protected Setup protocol allows credentials to be exchanged between a client and Access Point (AP) without the need to manually create an entry for SSID or PSK. There are two modes of operation provided:

- [WPS Push Button Configuration \(PBC\) Mode, page 59](#)
- [WPS Personal Information Number \(PIN\) Mode, page 63](#)

In PIN operation, a unique PIN number can be permanently associated with a client device or entered at the time of use. In PBC mode, the button on the Access Point (AP) must be pressed within a 2-minute period of providing the command to enable WPS on the client (either via button press or AT command). An exchange takes place between the client and AP providing the SSID and randomly-generated passphrase that can thereafter be used for secure communications. In both cases, security is, in part, dependent on the low likelihood of interception during the brief initial setup period.

Refer to the *GainSpan GS2000 Based Module Programming User Guide* to program the Flash on the evaluation board.

2.3.1 WPS Push Button Configuration (PBC) Mode

For the Push Button Configuration (PBC) mode, perform the following:

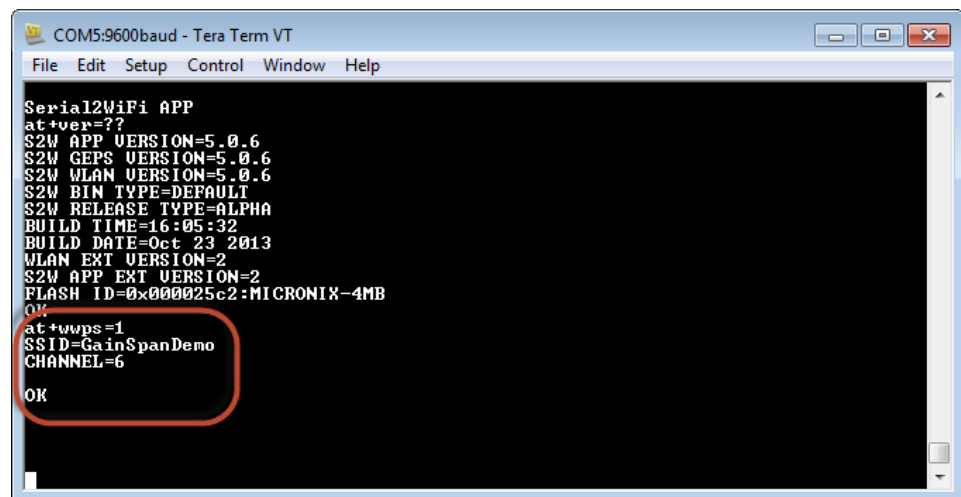
1. Issue the following AT command in the Tera Term VT window to start the WPS process.

```
AT+WWPS=1
```

“1” indicates the Push button mode.

2. Once the connection is complete, a message is sent to the host processor with the SSID, Channel, Passphrase, and Status (see [Figure 50](#), [page 59](#)).

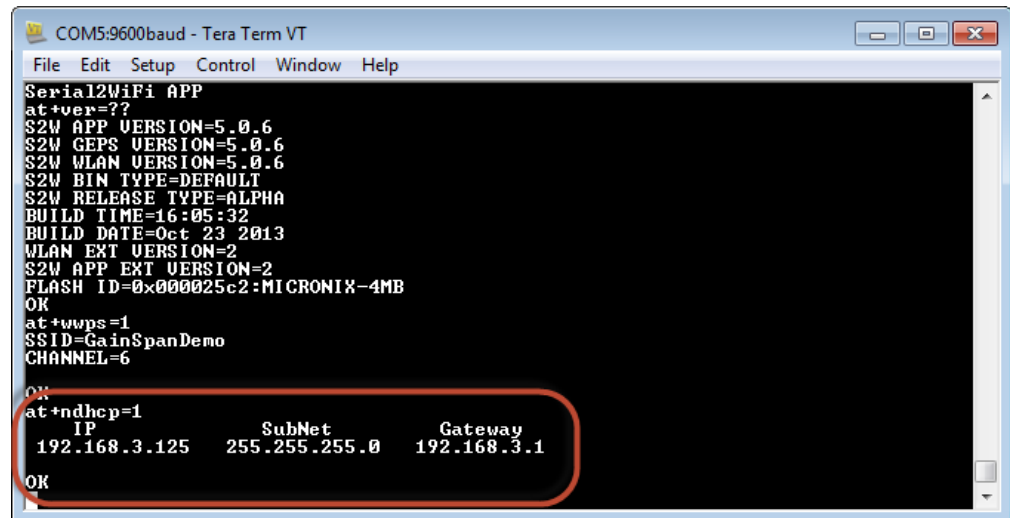
Figure 50 Starting the WPS Process



If the connection is not a success, an ERROR message is sent to the host processor.

3. The evaluation board is now associated with the AP, you can issue the AT command (AT+NDHCP=1) to get the IP address from DHCP server running or set the IP address statically using the AT+NSET command. At this point, you should be able to communicate with the board from the APs network (see [Figure 51](#), page 60).

Figure 51 Getting IP Address from DHCP Server

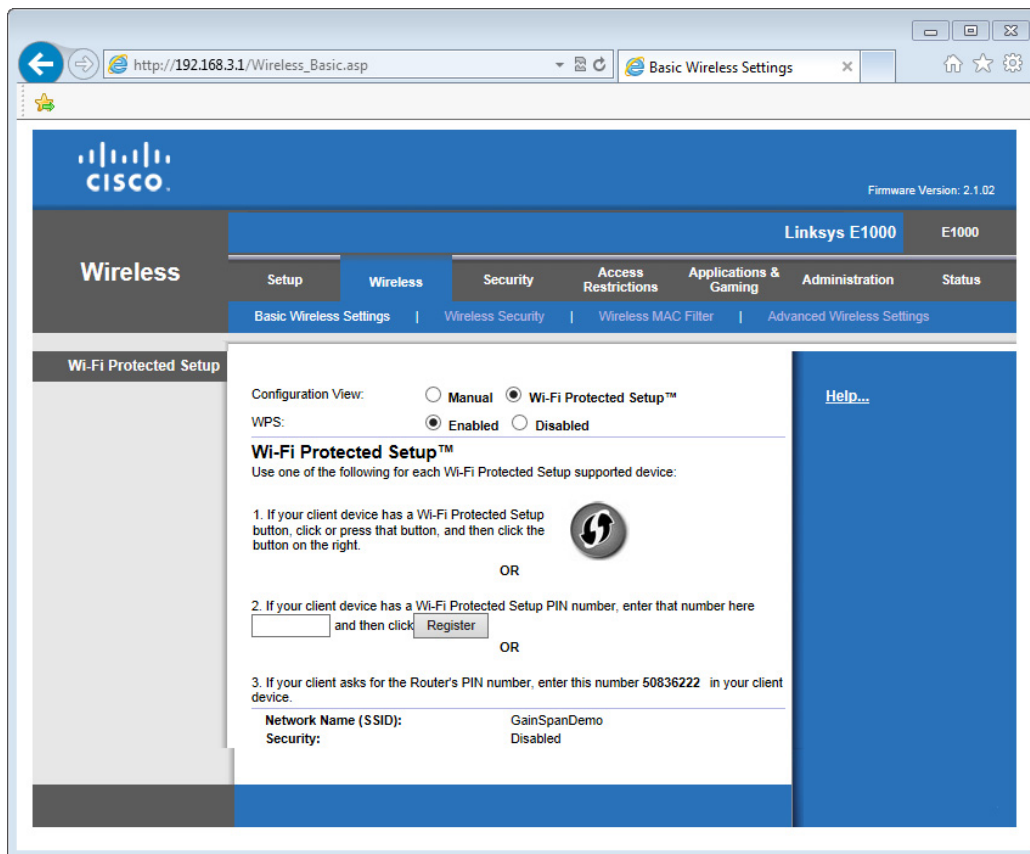


```
COM5:9600baud - Tera Term VT
File Edit Setup Control Window Help
Serial2WiFi APP
at+ver=?
$2W APP VERSION=5.0.6
$2W GEPS VERSION=5.0.6
$2W WLAN VERSION=5.0.6
$2W BIN TYPE=DEFAULT
$2W RELEASE TYPE=ALPHA
BUILD TIME=16:05:32
BUILD DATE=Oct 23 2013
WLAN EXT VERSION=2
$2W APP EXT VERSION=2
FLASH ID=0x000025c2:MICRONIX-4MB
OK
at+wps=1
SSID=GainSpanDemo
CHANNEL=6
OK
at+ndhcp=1
IP          SubNet      Gateway
192.168.3.125 255.255.255.0 192.168.3.1
OK
```

When the Serial-to-WiFi receives the AT command, it scans all the available radio channels looking for beacons whose Selected Register flags are set. The AP corresponding to each such beacon is stored. If the board finds a second Selected Register AP it stops scanning, having detected a session overlap (this is a precaution to prevent connection to the wrong AP). It is presumed that the user has only pressed one button, so a second AP may belong to a different network or even be an attacker. If at the end of scanning all the channels, the Serial-to-WiFi evaluation board has found a single Selected Register AP, it will connect to that AP to perform WPS registration.

4. Open a URL and enter the IP address (*http://192.168.3.1*) and press the **Enter** key.
The virtual Cisco AP will display (see Figure 52, page 61).

Figure 52 Example of Virtual Push Button (Cisco AP)



NOTE: In this example, we are using a Cisco Access Point (AP). You can use your own AP.

5. Select the **DHCP Reservation** option under **Basic Network Setup** to get a list of Client devices. From this screen you can add or remove Clients (see [Figure 53](#), [page 62](#)). At this point you can issue a PING command from the node to the AP and to the node IP address from any host computer in the same subnet.

Figure 53 DHCP Reservation Select Clients

DHCP Reservation - Windows Internet Explorer
http://192.168.3.1/DHCP_Static.asp

CISCO

DHCP Reservation
Select Clients from DHCP Tables

Client Name	Interface	IP Address	MAC Address	Select
LPT-MCASCIOLA	Wireless	192.168.3.124	88:9F:FA:FD:6D:BC	<input type="checkbox"/>

Add Clients

Manually Add Client

Enter Client Name	Assign IP Address	To This MAC Address	
<input type="text"/>	192 . 168 . 3 . <input type="text"/>	<input type="text" value="00:00:00:00:00:00"/>	Add

Clients Already Reserved

Client Name	Assign IP Address	To This MAC Address	MAC Address
-------------	-------------------	---------------------	-------------

Save Settings **Cancel Changes** **Refresh** **Close**

2.3.2 WPS Personal Information Number (PIN) Mode

To setup a valid PIN to the Access Point (AP) which supports the WPS, perform the following:

1. Enter a **WiFi Protected Setup PIN number** for the client device (see [Figure 54](#), page 63).
2. Click the **Register** button.

Figure 54 Enter Client Device WiFi Protected Setup (WPS) PIN Number

The screenshot shows a web browser window with the URL http://192.168.3.1/Wireless_Basic.asp. The page is titled "Basic Wireless Settings" and is for a "Linksys E1000" router with "Firmware Version: 2.1.02". The "Wireless" tab is selected, and the "Wi-Fi Protected Setup" sub-tab is active. The "Configuration View" section has "Wi-Fi Protected Setup™" selected. The "WPS" section has "Enabled" selected. The "Wi-Fi Protected Setup™" section provides instructions for setting up WPS. It lists three methods: 1. Using a client device's WPS button, 2. Entering a PIN number (with a text box containing "12345670" and a "Register" button), and 3. Entering the router's PIN number "50836222" into the client device. Below these instructions, the "Network Name (SSID)" is "GainSpanDemo" and the "Security" is "Disabled". A "Help..." link is visible on the right side of the page.

Configuration View: ☐ Manual ☒ Wi-Fi Protected Setup™

WPS: ☒ Enabled ☐ Disabled

Wi-Fi Protected Setup™

Use one of the following for each Wi-Fi Protected Setup supported device:

1. If your client device has a Wi-Fi Protected Setup button, click or press that button, and then click the button on the right.

OR

2. If your client device has a Wi-Fi Protected Setup PIN number, enter that number here and then click

OR

3. If your client asks for the Router's PIN number, enter this number 50836222 in your client device.

Network Name (SSID): GainSpanDemo

Security: Disabled

[Help...](#)

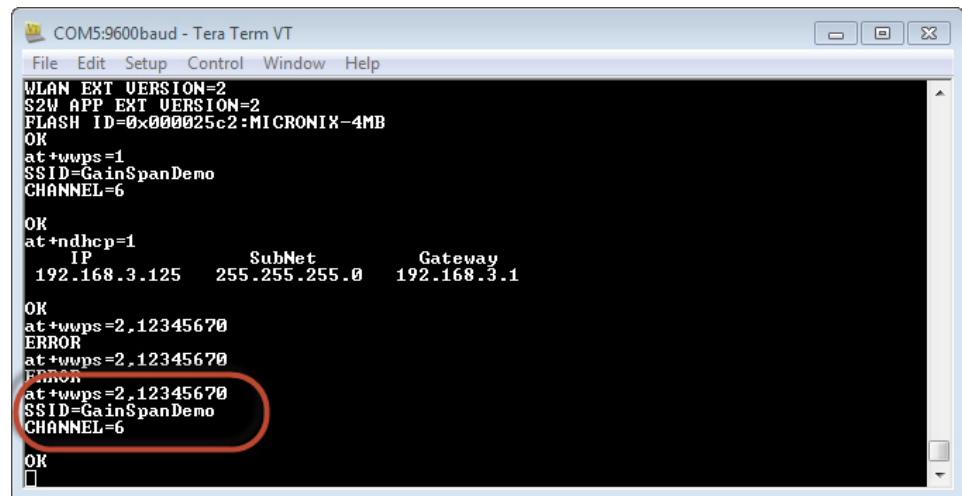
3. Issue the AT command for starting the WPS process.

```
AT+WWPS=2,12345670
```

Here: 2, indicates the PIN mode, and the second parameter is the WPS PIN.

4. Once the connection is complete, a message is sent to the host processor with the SSID, Channel, Passphrase, and Status (see [Figure 55, page 64](#)). If the connection is not successful an ERROR message is sent to the host processor.

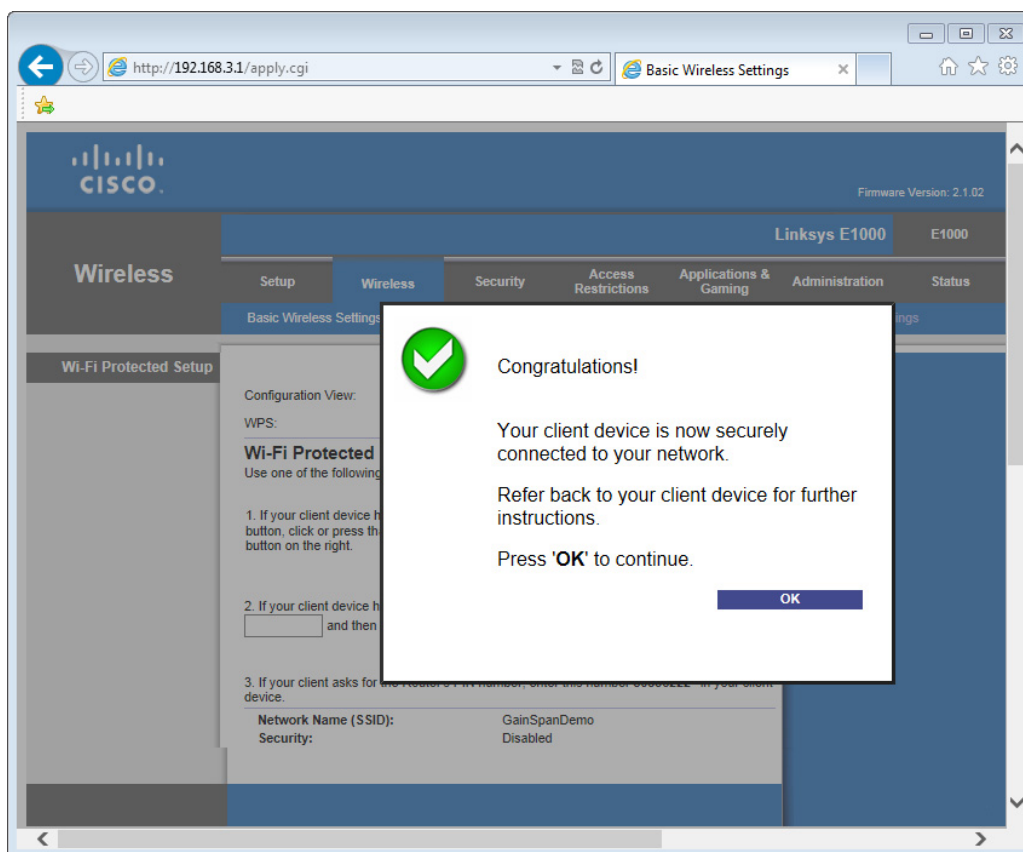
Figure 55 Issuing AT Command Indicating WPS PIN Mode



The AP interface will generally inform the user when a client device has been successfully configured and connected. Other APs may have different GUI, messages, etc.

You can always check the DHCP client table of the AP to ensure that the device is properly connected. Once the evaluation board is associated with the AP, you may issue the AT command (AT+NDHCP=1) to get the IP address from the DHCP server running or set the IP address statically using the AT+NSET command. At this point, you should be communicating with the evaluation board from the APs network. Use the APs Active Client list to discover the IP address the new device has received. You should be able to issue a PING command directed to that IP address from any host computer in the same subnet (see Figure 56, page 65).

Figure 56 Client Device is Securely Connected to the Network



- This page intentionally left blank -