PRE-REQUIREMENT

Make sure serial to Wi-Fi application is loaded on this Evaluation board.

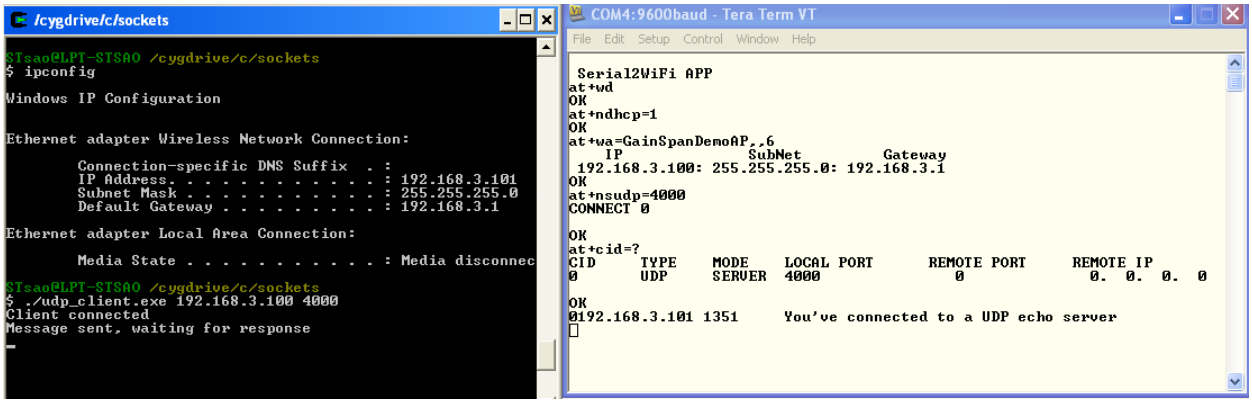
UDP

UDP Server

This section describes the steps to setup UDP Server on the Evaluation board using either command mode or auto-connect mode.

Command Mode

1. Disassociate from the current network
   - at+wd
2. Enable DHCP: *AT+NDHCP=<disable=0/enable=1>*
   - at+ndhcp=1
3. Associate to an access point: *AT+WA=<SSID>[,[<BSSID>][,<Ch>]]*
   - at+wa=GainSpanDemoAP,,6
4. Start a TCP server on a specific port number: *AT+NSUDP=<port>*
   - at+nsudp=4000
5. Upon successful creation of the UDP 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 command: *AT+CID=?*
   - at+cid=?
6. User can now connect to this UDP server by:
   a. Have a PC connected to the GainSpanDemo AP
   b. In PC's command prompt, run UDP client with GS node's IP address (obtained from step 3), and the port number specified in step 4. For example: telnet 192.168.3.101 4000.
   c. Now anything you type in the client's command prompt window will be displayed on the TeraTerm. Here's an example.

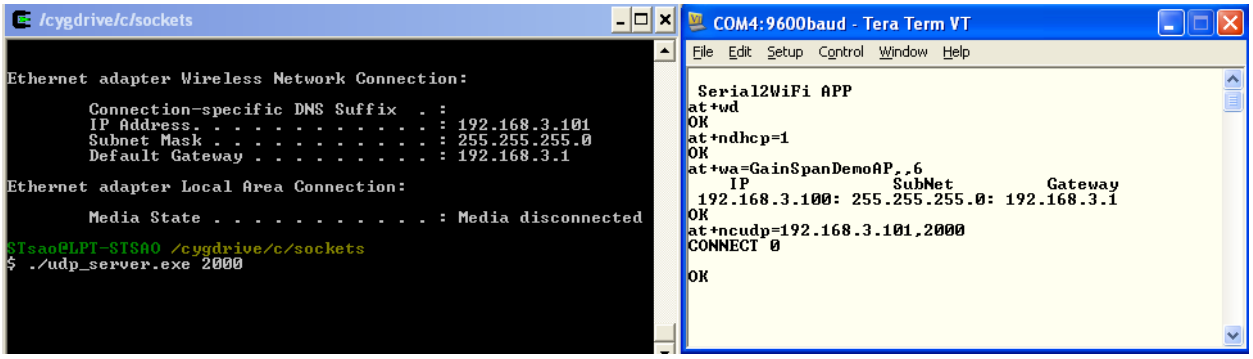


UDP Client

This section describes the steps to setup UDP Client on the Evaluation board using either command mode or auto-connect mode.

Command Mode

1. Disassociate from the current network
   - at+wd
2. Enable DHCP: *AT+NDHCP=<disable=0/enable=1>*
   - at+ndhcp=1
3. Associate to an access point: *AT+WA=<SSID>[,[<BSSID>][,<Ch>]]*
   - at+wa=GainSpanDemoAP,,6
4. Start a TCP server: *AT+NCUDP=<Dest-Address>,<Port>>[<,Src.Port>]*
   - at+ncudp=192.168.3.101,2000
5. Upon successful connection to the UDP server, you will see a "CONNECT <CID> " message, where CID is the newly allocated connection identifier



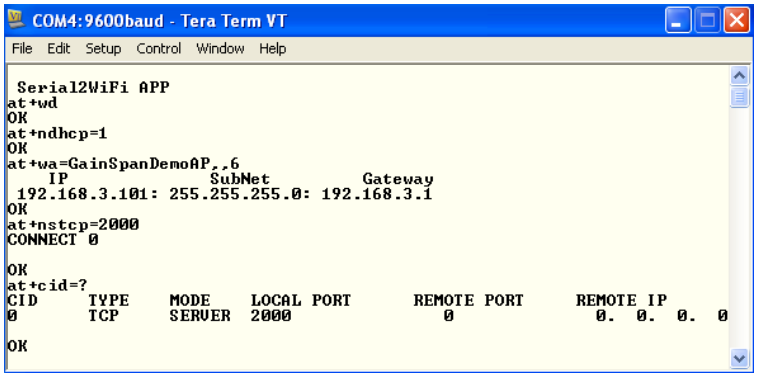
TCP

TCP Server

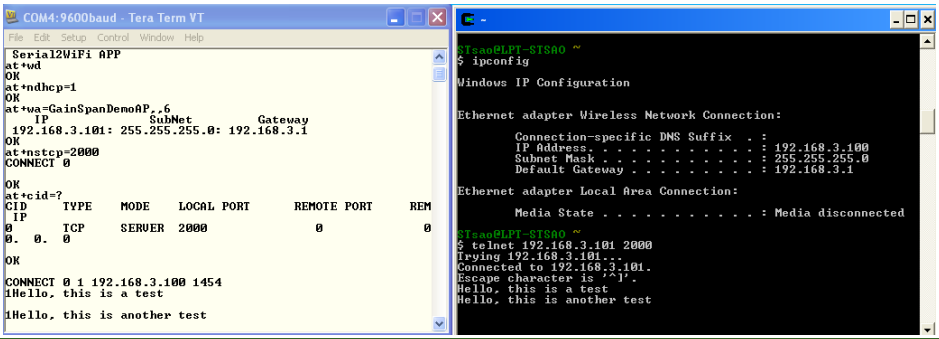
This section describes the steps to setup TCP Server on the Evaluation board using either command mode or auto-connect mode.

Command Mode

1. Disassociate from the current network
   - at+wd
2. Enable DHCP: *AT+NDHCP=<disable=0/enable=1>*
   - at+ndhcp=1
3. Associate to an access point: *AT+WA=<SSID>[,[<BSSID>][,<Ch>]]*
   - at+wa=GainSpanDemoAP,,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 command: *AT+CID=?*
   - at+cid=?



6. User can now telnet into this server by:
   a. Have a PC connected to the GainSpanDemo AP
   b. In PC's command prompt, issue the command:
      telnet <IP address from step 3> <port number set in step 6>
      For example: telnet 192.168.3.101at 2000
   c. Now anything you type in the command prompt window will be displayed on the TeraTerm.



TCP Client

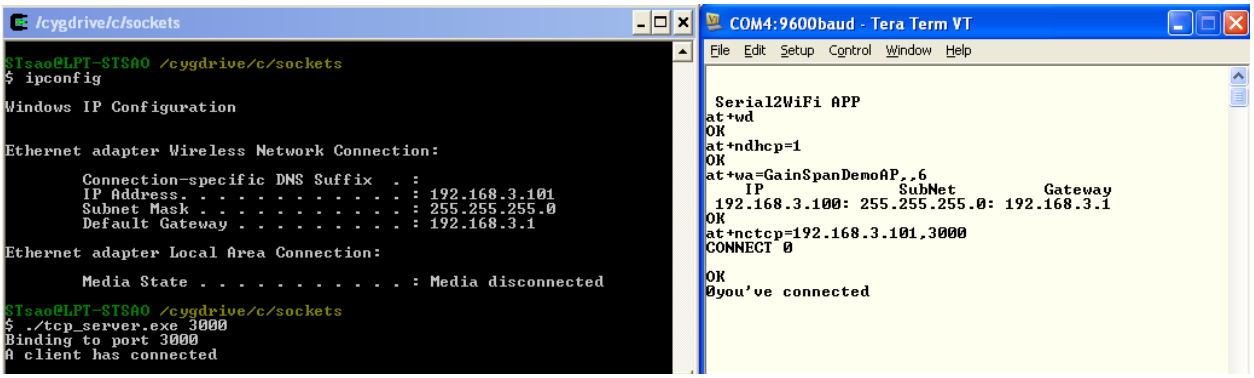
This section describes the steps to setup TCP Client on the Evaluation board using either command mode or auto-connect mode.

Command Mode

Before you start, have a PC connect to the GainSpanDemoAP and start a TCP server on a specific port number. This example uses port 3000.

1. Disassociate from the current network
   - at+wd
2. Enable DHCP: *AT+NDHCP=<disable=0/enable=1>*
   - at+ndhcp=1
3. Associate to an access point: *AT+WA=<SSID>[,[<BSSID>][,<Ch>]]*
   - at+wa=GainSpanDemoAP,,6
4. Start a TCP client: *AT+ NCTCP=<Dest-Address>,<Port>*
   - at+nctcp=192.168.3.101,3000

Upon successful connection to the TCP server, you will see a “CONNECT <CID> “ message, where CID is the newly allocated connection identifier. Here’s an example:



HTTP GET

This section describes the steps to perform a HTTP GET command using the Serial2WiFi stack.

Command Mode

1. Disassociate from the current network
   - at+wd
2. Enable DHCP
   - at+ndhcp=1
3. Perform network scan
   - at+ws
4. If AP security is open, then skip this step. If AP is using WPA-PSK/TKIP, then set the WPA passphrase with the following command:
   - at+wwpa=<*WPA-PASSWORD*>
5. Associate to a specified SSID, BSSID, and channel. at+wa=<SSID>,<BSSID>,<CHANNEL>
   - at+wa=GainSpanDemoAP,,6
6. Query DNS server for the IP address of hostname URL
   - at+dnslookup=www.gainspan.com
7. Configure the HTTP header parameter "GSN_HTTP_HEADER_USER_AGENT"
   - at+httpconf=20,User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.1.9) Gecko/20100315 Firefox/3.5.9
8. Configure the HTTP header connection parameter "GSN_HTTP_HEADER_CONNECTION". If it is a one-time HTTP GET, set the parameter to "close"
   - at+httpconf=3, close

   If user wants to do consecutive HTTP GET on the same CID, and given that a server do keep the connection open after HTTP GET is complete, set the parameter to "keep alive"
   - at+httpconf=3, keep-alive
9. Configure the HTTP header host parameter "GSN_HTTP_HEADER_HOST"
   - at+httpconf=11,76.12.140.77
10. Open HTTP client connection. This will return a unique CID.
    - at+httpopen=76.12.140.77
11. Send HTTP request to the server using the CID from the previous step

    at+httpsend=<CID>, <type: get=1, post=3>, <timeout>, <page>[,size of the content]
    - at+httpsend=0,1,10,/

Using consecutive CID

If the HTTP server closes the connection after the HTTP GET is complete, then user must issue a HTTP OPEN prior to every HTTP GET. Gainspan.com is an example of such server.

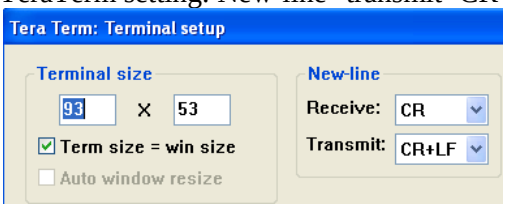
Example 1: Gainspan.com

```
at+wd
at+ndhcp=1
at+wa= GainSpanDemoAP,,6
```

at+dnslookup=www.gainspan.com
at+httpconf=20,User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.1.9) Gecko/20100315 Firefox/3.5.9
at+httpconf=3, keep-alive
at+httpconf=11,76.12.140.77
at+httpopen=76.12.140.77 ← *This returned CID=0*
at+httpsend=0,1,10,/
at+httpopen=76.12.140.77 ← *This returned CID=1*
at+httpsend=1,1,10,/
at+httpopen=76.12.140.77 ← *This returned CID=2*
at+httpsend=2,1,10,/

Example 2: Gainspan.com

1. Change the TeraTerm setting: New-line "transmit=CR+LF"



2. Associate with AP
   AT+NDHCP=1
   AT+WWPA=password
   AT+WA=GS-Guest,,01
3. Start TCP Client to the GainSpan IP and port 80
   AT+NCTCP=76.12.140.77,80
4. Send data to remote server by using the <ESC>S sequence and the CID number:
   Enter the [ESC] key
   Enter the [S] key
   Enter the [CID number from step 3]
5. Copy the highlighted text (the new line should also be copied), and paste it on TeraTerm (via the "Edit" menu, choose "Paste" Option)
   GET / HTTP/1.1
   User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.1.9) Gecko/20100315 Firefox/3.5.9
   Host: 76.12.140.77:80
   Accept: */*
   Connection: keep-alive
   [new line]
   [new line]
6. Indicate end of transmission by using the <ESC>E sequence:
   Enter the [ESC] key
   Enter the [E] key
7. The output of HTTP GET will now be displayed as output on TeraTerm. Since the GainSpan HTTP server closes the connection after HTTP GET is complete, you will see the following output message:
   DISCONNECT <cid>

8. To issue another HTTP GET, repeat step 2-6.

Using same CID

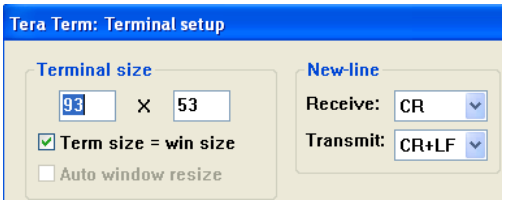
If the HTTP server keeps the connection open after HTTP GET is complete, then user can issue consecutive HTTP GET using the same CID. Google.com is an example of such server.

Example 1: Google.com

```
at+wd
at+ndhcp=1
at+wa=GainSpanDemoAP,,6
at+dnslookup=www.google.com
at+httpconf=20,User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.1.9)
Gecko/20100315 Firefox/3.5.9
at+httpconf=3, keep-alive
at+httpconf=11,72.14.234.104
at+httpopen=72.14.234.104                    ← This returned CID=0
at+httpsend=0,1,10,/
at+httpsend=0,1,10,/
at+httpsend=0,1,10,/
```

Example 2 : Google.com

1. Change the TeraTerm setting: New-line "transmit=CR+LF"



2. Associate with AP
   AT+NDHCP=1
   AT+WWPA=password
   AT+WA=GS-Guest,,01
3. Start TCP Client to Google's IP and port 80
   AT+NCTCP=72.14.234.104,80
4. Send data to remote server by using the <ESC>S sequence and the CID number:
   Enter the [ESC] key
   Enter the [S] key
   Enter the [CID number from step 3]
5. Copy the highlighted text (the new line should also be copied), and paste it on TeraTerm (via the "Edit" menu, choose "Paste" Option)
   GET / HTTP/1.1
   User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.1.9) Gecko/20100315 Firefox/3.5.9
   Host: 72.14.234.104:80
   Accept: */*
   Connection: keep-alive
   [new line]
   [new line]

6. Indicate end of transmission by using the <ESC>E sequence:
   Enter the [ESC] key
   Enter the [E] key
7. The output of HTTP GET will now be displayed as output on TeraTerm. Since Google's HTTP server keeps the connection open, to issue another HTTP GET, just repeat step 4-6.

Example 3: Pachube.com

1. Change the TeraTerm setting: New-line "transmit=CR+LF"
2. Associate with AP
   AT+NDHCP=1
   AT+WWPA=password
   AT+WA=GS-Guest,,01
3. Start TCP Client to the Pachube.com IP and port 80
   AT+NCTCP= 173.203.98.29,80
4. Send data to remote server by using the <ESC>S sequence and the CID number:
   Enter the [ESC] key
   Enter the [S] key
   Enter the [CID number from step 3]

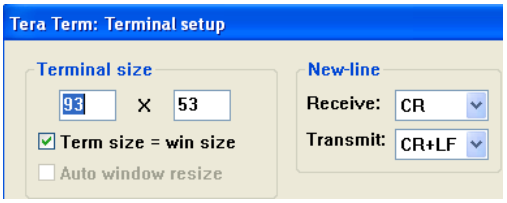
5. Copy the highlighted text (the new line should also be copied), and paste it on TeraTerm (via the "Edit" menu, choose "Paste" Option)
   GET /v2/feeds/11366.csv HTTP/1.1
   User-Agent: curl/7.19.5 (i486-pc-linux-gnu) libcurl/7.19.5 OpenSSL/0.9.8g zlib/1.2.3.3 libidn/1.15
   Host: api.pachube.com
   Accept: */*
   X-PachubeApiKey: 103338a658c84debc9d4d0609362056882b6ccaa312d3de7fbde57e592630007
   Connection: keep-alive
   [new line]
   [new line]
6. Indicate end of transmission by using the <ESC>E sequence:
   Enter the [ESC] key
   Enter the [E] key
7. The output of HTTP GET will now be displayed as output on TeraTerm. To issue another HTTP GET, just repeat step 4-6.

HTTP PUT

This section describes the steps to perform a HTTP PUT command using the Serial2WiFi stack.

Example: Posting to Pachube.com

1. Change the TeraTerm setting: New-line "transmit=CR+LF"



2. Associate with AP
   AT+NDHCP=1
   AT+WWPA=password
   AT+WA=GS-Guest,,01
3. Start TCP Client to Google's IP and port 80
   AT+NCTCP=173.203.98.29,80
4. Send data to remote server by using the <ESC>S sequence and the CID number:
   Enter the [ESC] key
   Enter the [S] key
   Enter the [CID number from step 3]
5. Copy the highlighted text, and paste it on TeraTerm (via the "Edit" menu, choose "Paste" Option)
   PUT /v2/feeds/11366.csv HTTP/1.1
   User-Agent: curl/7.19.5 (i486-pc-linux-gnu) libcurl/7.19.5 OpenSSL/0.9.8g zlib/1.2.3.3 libidn/1.15
   Host: api.pachube.com
   Accept: */*

X-PachubeApiKey:
103338a658c84debc9d4d0609362056882b6ccaa312d3de7fbde57e592630007
Content-Length: 4
Content-Type: application/x-www-form-urlencoded

1,44

6. Indicate end of transmission by using the <ESC>E sequence:
   Enter the [ESC] key
   Enter the [E] key
7. You should now see the data "1,44" on http://pachube.com/feeds/11366
8. Close current connection:
   AT+NCLOSE=0
9. Start a connection to the Pachube.com IP and port 80
   AT+NCTCP=173.203.98.29,80
10. Send data to remote server by using the <ESC>S sequence and the CID number:
    Enter the [ESC] [S][CID number from step 9]
11. Copy the highlighted text, and paste it on TeraTerm (via the "Edit" menu, choose "Paste" Option)
    PUT /v2/feeds/11366.csv HTTP/1.1
    User-Agent: curl/7.19.5 (i486-pc-linux-gnu) libcurl/7.19.5 OpenSSL/0.9.8g zlib/1.2.3.3 libidn/1.15
    Host: api.pachube.com
    Accept: */*
    X-PachubeApiKey:
    103338a658c84debc9d4d0609362056882b6ccaa312d3de7fbde57e592630007
    Content-Length: 4
    Content-Type: application/x-www-form-urlencoded

    0,19
12. Indicate end of transmission by using the <ESC>E sequence:
    Enter the [ESC] key
    Enter the [E] key
13. You should now see the data "0,19" on http://pachube.com/feeds/11366
14. To post another set of data points to Pachube.com, just repeat step 8-12

LIMITED AP

Use the following steps to create a limited AP.

- Set the security type.
- Create the limited AP.
- Enable DHCP server, if needed.
- Enable DNS server, if needed.

Setting security type

To have WPA/WPA2 PSK security, issue the following AT command.

To have the WPA/WPA2 PSK authentication mechanism, make sure GSN_SECURITY_PSK_AVAILABLE and GSN_SECURITY_WPA_AUTH_AVAILABLE compile time options are enabled in S2W application.

- AT+WWPA, AT+WPAPSK or AT+WPSK command.
- AT+WSEC to 4, 8 or 64 for WPA-PSK TKIP, WPA2-PSK AES or WPA2-PSK AES-TKIP correspondingly.
- AT+WAUTH to 0.

To have WEP security issue the following AT command

- AT+WAUTH to 1 or 2 for open or shared authentication
- AT+WWEPn to configure the WEP key.

Creating limited AP

The following AT command has to be set to create limited AP.

- Issue AT command to select the WLAN mode of operation to limited AP by setting AT+WM to 2.
- Issue AT+WA command to initiate the limited AP.

Enabling DHCP server

To enable the DHCP server, issue the following: AT+DHCPSRVR to 1.

To disable the DHCP server, issue the following: AT+DHCPSRVR to 0.

Make certain to configure the preferred IP address by using AT+NSET command before issuing this command. The DHCP server will automatically start allocating IP address one higher than the assigned IP address to the node.

Make sure that the S2W application has GSN_DHCP_SERVER_ENABLE compile type option enabled.

Enabling DNS server

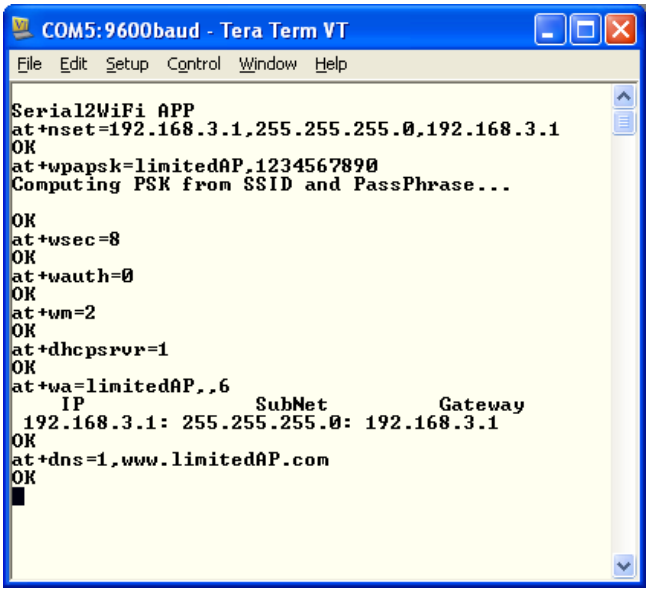
To enable DNS server issue AT+DNS to 1 and give the host name to be used.

To disable DNS server: AT+DNS to 0. S2W application automatically takes the node IP address as the IP address of the host.

Make sure that the S2W application has GSN_DNS_SERVER_ENABLE compile time option enabled.

Example: Creating Limited AP in WPA2-PSK mode with DHCP and DNS server enabled

1. Configure network stack parameter: *AT+NSET=<Src Addr>,<Net-Mask>,<Gateway>*
   AT+NSET=192.168.3.1,255.255.255.0,192.168.3.1
2. Compute WPA2-PSK from a given SSID and Passphrase: *AT+WPAPSK=<SSID>,<PASSPHRASE>*
   AT+WPAPSK=limitedAP,1234567890
3. Configure security to WPA2-PSK: *AT+WSEC=<n>*
   AT+WSEC=8
4. Configure authentication mode to NONE: *AT+WAUTH=<none,WPA/WP2=0, open=1, WEP=2>*
   AT+WAUTH=0
5. Configure wireless mode to Limited AP: *AT+WM=<infrastructure=0, ad hoc=1,limited AP = 2>*
   AT+WM=2
6. Start the DHCP server: *AT+DHCPSRVR=<disable=0/enable=1>*
   AT+DHCPSRVR=1
7. Create the infrastructure network: *AT+WA=<SSID>[,[<BSSID>][,<Ch>]]*
   AT+WA=limitedAP,,6
8. Start the DNS server and specify a DNS name: *AT+DNS=<disable=0/enable=1, <url>*
   AT+DNS= 1,www.limitedAP.com

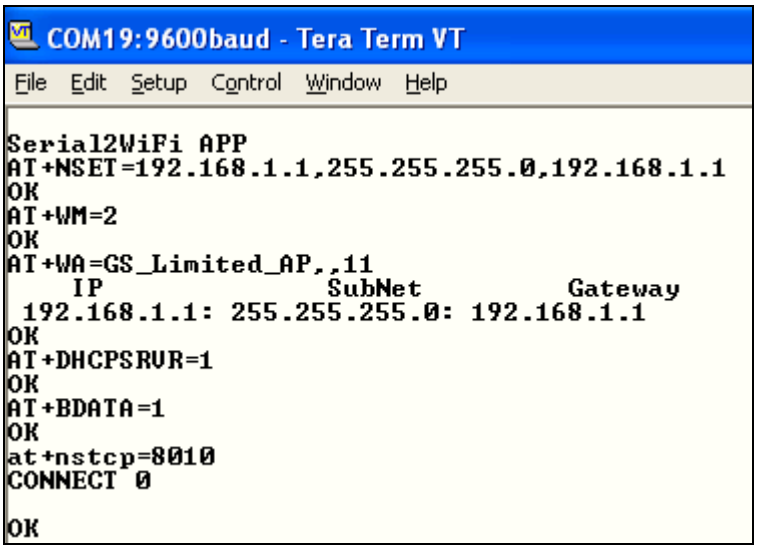


Example: Creating Limited AP in Open Security mode with TCP server enabled

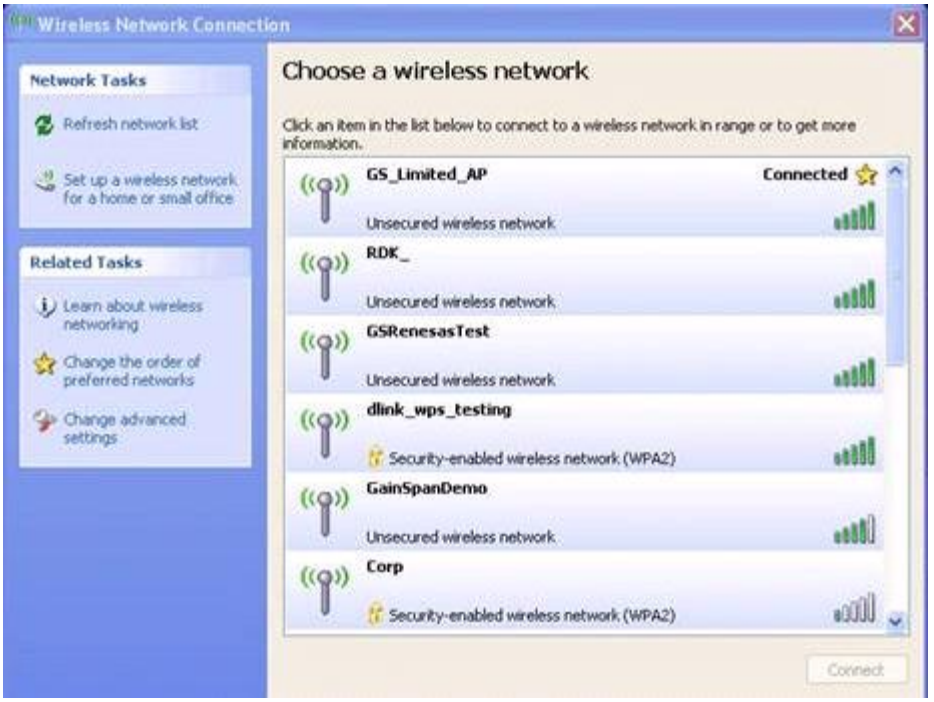
1. Issue the following AT command sequence to create a Limited AP and start TCP server on port 8010.

   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

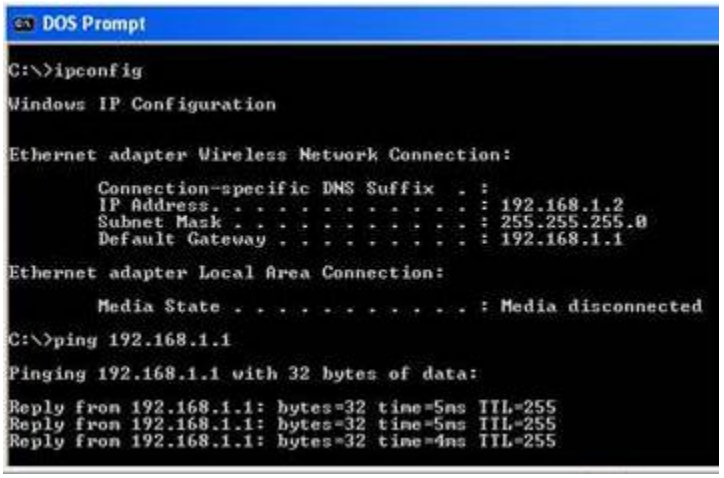
   Example output in TeraTerm:



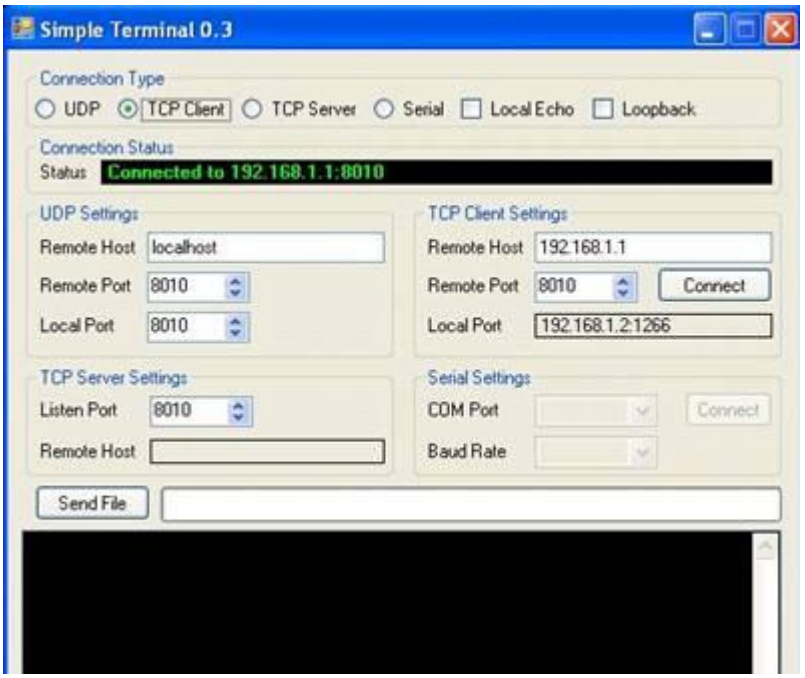
2. PC connected to "GS_Limited_AP".



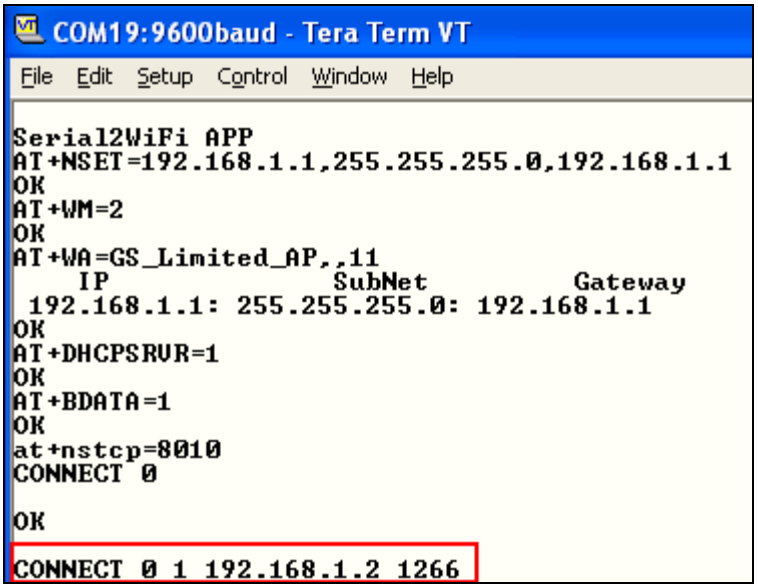
3. Confirm connection is established, ping to 192.168.1.1 from the PC:



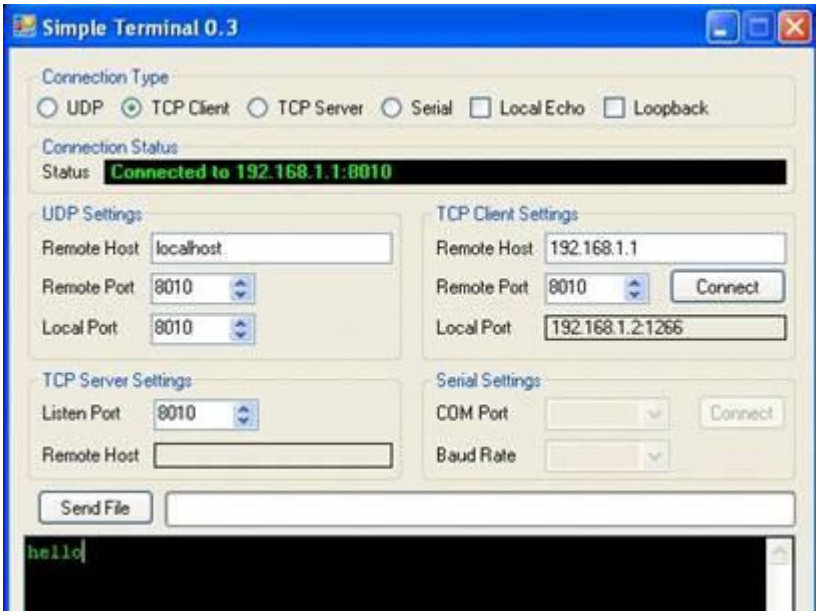
4. On the PC, launch the SimpleTerm and connect to GS1011M (example: 192.168.1.1 8010):



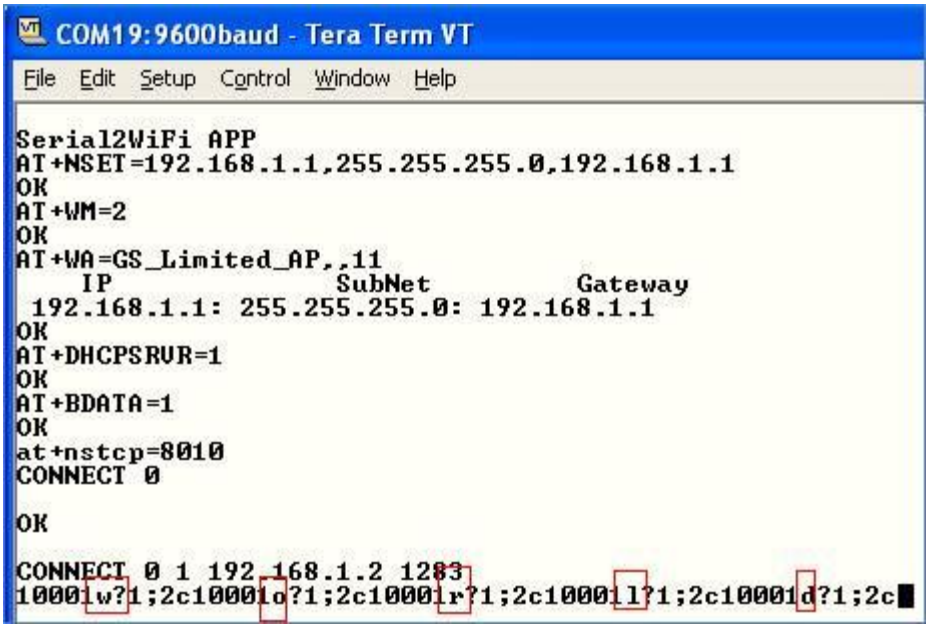
5. Upon successful TCP connection, locate the "CONNECT <CID> <CID> <IP Address> <Port number" message displayed on TeraTerm:



6. To send data (for example: hello) from TCP Server (GS1011M) to TCP client (SimpleTerm), go to TeraTerm and enter: <ESC>Z10005hello. You should now see "hello" received in the Simple Terminal window:



7. 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, user entered the text "world" slowly in the Simple Term, and the text is seen received on the TeraTerm screen:



ADDITIONAL REFERENCES

Serial to Wi-Fi Evaluation Kit Startup Guide.pdf

Serial to WiFi_Adapter_Guide.pdf

Detail description of the AT commands supported

Serial to WiFi_Command_Reference.pdf

List of the various AT commands supported

Serial to Provisioning Methods with S2W App Note AN039.pdf

Example of provisioning method supported as well as the steps necessary to connect to the infrastructure (i.e. Access Point) using either Web Based Provisioning or Wi-Fi Protected Setup (WPS).

Serial to WiFi Bridge App Note AN025.pdf

The GainSpan Ultra-Low-Power Wi-Fi System-On-Chip may be used as a transparent bridge to carry serial (UART) traffic over an 802.11 wireless link. Serial commands are used to manage the wireless network configuration. This application note will give the details necessary to setup this bridge.

Version	Date	Remarks
1.0	10-Oct-2011	Initial Release
1.1	1-Jan-2012	▶ Added Creating Limited AP in WPA2-PSK mode with DHCP and DNS server enabled example.
1.2	27-June-2012	▶ Added example for Posting to Pachube.com
1.3	10-July-2012	▶ Limited AP in Open Security mode with TCP

GainSpan Corporation • +1 (408) 673-2900 • info@GainSpan.com • www.GainSpan.com

SP- 1.3