

GT202 MQX PDK Demo Applications

User Guide

September 2014

Longsys



Shenzhen Longsys Electronics Co.,Ltd www.Longsys.com

8/F, 1 Building. Finance Base, NO.8, KeFa Road, Shenzhen, China Tel: 86-755-86168848

10/F, CHINA AEROSPACE CENTRE,143 HOI BUN ROAD,HKTel: 852-23850111

GT202 Demo Applications User Guide 1.3

Revision history

Revision	Date	Description
1.3	September 2014	Initial release



Shenzhen Longsys Electronics Co.,Ltd www.Longsys.com

8/F, 1 Building. Finance Base, NO.8, KeFa Road, Shenzhen, China Tel: 86-755-86168848

10/F, CHINA AEROSPACE CENTRE,143 HOI BUN ROAD,HKTel: 852-23850111

Contents

1 Introduction.....	9
2 Throughput Demo.....	10
2.1 Throughput demo setup.....	10
2.1.1 Windows PC1 setup.....	11
2.1.2 Windows PC2 setup.....	11
2.2 Throughput demo test procedures.....	11
2.3 Console commands.....	12
2.3.1 help.....	14
2.3.2 version.....	14
2.3.3 connect <ssid>.....	14
2.3.4 wepkey.....	14
2.3.5 p <passphrase>.....	15
2.3.6 adhoc.....	15
2.3.7 wepkey.....	15
2.3.8 wps.....	16
2.3.9 disc.....	16
2.3.10 settxpower <val>.....	16
2.3.11 pwrmode.....	16
2.3.12 setchannel.....	16



Shenzhen Longsys Electronics Co.,Ltd www.Longsys.com

8/F, 1 Building. Finance Base, NO.8, KeFa Road, Shenzhen, China Tel: 86-755-86168848

10/F, CHINA AEROSPACE CENTRE,143 HOI BUN ROAD,HKTel: 852-23850111

GT202 Demo Applications User Guide 1.3

2.3.13 wmode.....	17
2.3.14 listen <interval>.....	17
2.3.15 rssi.....	17
2.3.16 suspend.....	17
2.3.17 suspstart.....	17
2.3.18 pmparams.....	18
2.3.19 scanctrl.....	18
2.3.20 assdump.....	18
2.3.21 driver.....	19
2.3.22 allow_aggr.....	19
2.3.23 iwconfig scan.....	19
2.3.24 reset.....	19
2.3.25 macStore.....	19
2.3.26 regdomain.....	19
2.3.27 getrate.....	20
2.3.28 getlasterr.....	20
2.3.29 raw.....	20
2.3.30 ipconfig.....	20
2.3.31 ipstatic.....	20
2.3.32 ipdhcp.....	21
2.3.33 ipdhcp release.....	21
2.3.34 ipv6.....	21
2.3.35 ipv6rtptfx.....	21
2.3.36 mode [ap].....	22



Shenzhen Longsys Electronics Co.,Ltd www.Longsys.com

8/F, 1 Building. Finance Base, NO.8, KeFa Road, Shenzhen, China Tel: 86-755-86168848

10/F, CHINA AEROSPACE CENTRE,143 HOI BUN ROAD,HKTel: 852-23850111

GT202 Demo Applications User Guide 1.3

2.3.37 ap [country].....	22
2.3.38 ap [bconint].....	23
2.3.39 ap [dtim].....	23
2.3.40 ap [inact].....	23
2.3.41 ipdhcppool.....	23
2.3.42 ip_dns_client.....	24
2.3.43 ip_dns_server_addr.....	24
2.3.44 ip_dns_delete_server_addr.....	24
2.3.45 ip_resolve_hostname.....	24
2.3.46 ip_gethostbyname.....	25
2.3.47 ip_gethostbyname2.....	25
2.3.48 ip_http_server.....	25
2.3.49 ip_http_post.....	26
2.3.50 ip_http_get.....	26
2.3.51 ip_http_client.....	27
2.3.52 ip_dns_local_domain.....	27
2.3.53 ip_hostname.....	27
2.3.54 ip_dns.....	28
2.3.55 ssl_start.....	28
2.3.56 ssl_stop.....	28
2.3.57 ssl_config.....	29
2.3.58 ssl_add_cert.....	29
2.3.59 ssl_store_cert.....	29
2.3.60 ssl_delete_cert.....	29



Shenzhen Longsys Electronics Co.,Ltd www.Longsys.com

8/F, 1 Building. Finance Base, NO.8, KeFa Road, Shenzhen, China Tel: 86-755-86168848

10/F, CHINA AEROSPACE CENTRE,143 HOI BUN ROAD,HKTel: 852-23850111

GT202 Demo Applications User Guide 1.3

2.3.61 ssl_list_cert.....	30
2.4 Benchmark component.....	30
2.4.1 Benchmark commands.....	30
2.4.2 Running multi-stream tests with the throughput tool.....	32
2.5 SSL.....	36
2.5.1 Certificate management demo.....	37
3 P2P Demo.....	40
3.1 P2P demo setup.....	40
3.1.1 Windows PC1 setup.....	41
3.1.2 Windows PC2 setup.....	41
3.2 Testing P2P connection using PUSH method.....	43
3.2.1 GT202 development kit as P2P client.....	43
3.2.2 GT202 development kit as P2P autonomous GO.....	46
3.2.3 GT202 development kit as P2P GO.....	49
3.3 Testing P2P connection using PIN method.....	52
3.3.1 GT202 development kit as P2P client.....	52
3.3.2 GT202 development kit as P2P autonomous GO.....	62



Shenzhen Longsys Electronics Co.,Ltd www.Longsys.com

8/F, 1 Building. Finance Base, NO.8, KeFa Road, Shenzhen, China Tel: 86-755-86168848

10/F, CHINA AEROSPACE CENTRE,143 HOI BUN ROAD,HKTel: 852-23850111

Figures

Figure 1-1 GT202 development kit.....9

Figure 2-1 Throughput demo configuration example..... 11

Figure 3-1 Sample system configuration for P2P demonstration..... 40

Longsys



Tables

Table 2-1 Configuration commands..... 12

Longsys



1 Introduction

This document provides instructions for using the demo applications included with the GT202 PDK (Platform Development Kit). The PDK supports the GT202 development kit, which includes GT202 WiFi module, Freedom adaptor board and Freescale Freedom board, as shown in Figure 1-1. The following demo applications are provided with the software release:

- Throughput Demo
- P2P Demo
- AllJoyn Demo

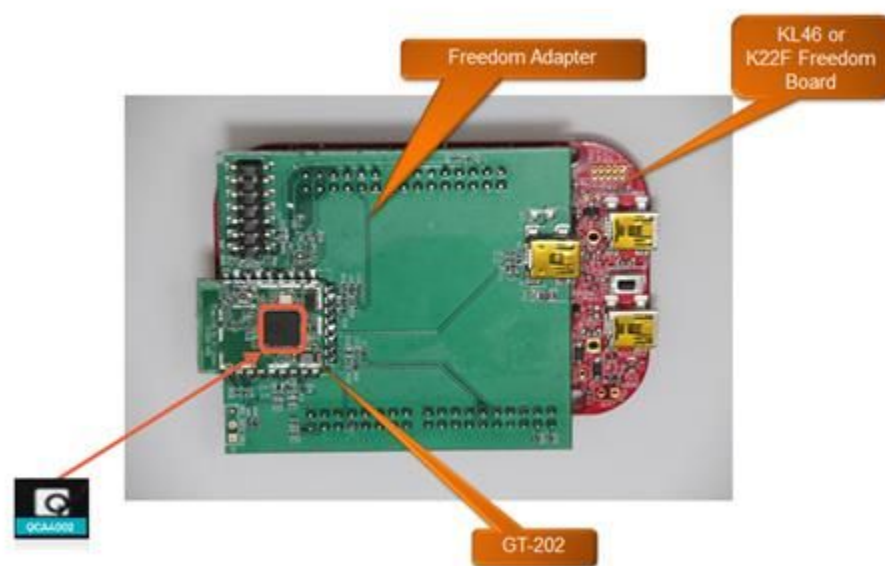


Figure 1-1 GT202 development kit

2 Throughput Demo

The throughput demo target application and PC tool enables software developers to configure and evaluate the performance of the GT-202 WiFi module. The throughput tool performs basic system level throughput testing and is not a full-featured performance tool. The equipment required includes:

- GT-202 development kit
- Microsoft Windows-based PC with throughput demo endpoint application ath_console.exe
- Wi-Fi Access Point

The commands set supported by the throughput tool implements two components (command sets) that can be accessed from the serial port console:

- The configuration component provides an interface to configure and control the behavior of the GT-202 WiFi module. It exposes a set of configuration commands that can be used to configure and connect to an existing network.
- The benchmark component provides a set of commands to run bidirectional throughput streams to analyze network throughput performance. Both TCP and UDP traffic is supported. The ath_console.exe application running on PC supports the benchmark component on its console.

2.1 Throughput demo setup

The Freedom board in GT202 development kit is connected to a PC via OpenSDA USB port on Freedom board using a USB cable. A console application is opened on the PC to input commands for configuration and benchmarking. TCP/UDP streams can be setup between the end point application ath_console.exe running on a PC and the demo application running on the GT-202 development kit over a Wi-Fi link. Figure 2-1 shows a configuration example where the AP subnet is 192.168.0.x. If a different subnet is used, make sure the corresponding IP addresses are set for the endpoints.

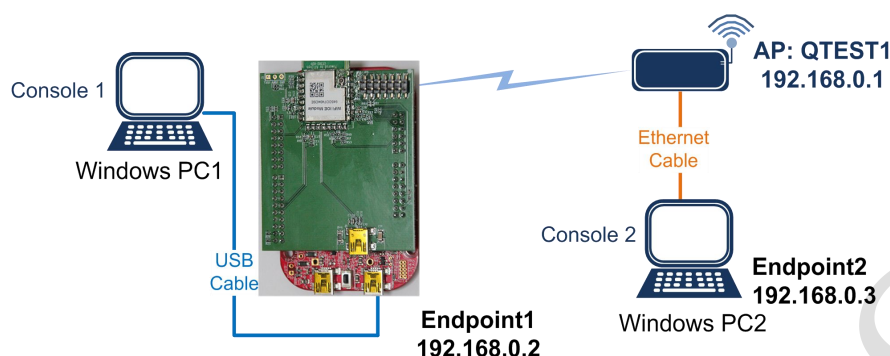


Figure 2-1 Throughput demo configuration example

2.1.1 Windows PC1 setup

1. Use a USB cable to connect PC1 to OpenSDA USB port of the Freedom board in GT-202 development kit
2. Start terminal applications from PC1 to communicate with the Freedom board console port as Console 1. The port setting is: 115200, 8, n, 1, no flow control.
 - a. Freedom board console port: The virtual COM port created by OpenSDA USB connection.

2.1.2 Windows PC2 setup

1. Use the Ethernet cable to connect to the AP and configure the IP address to 192.168.0.3.
2. Run `<PDK Installation Directory>\Demo\throughput_demo\bin\ath_console.exe` as Console 2 at the windows DOS prompt.

2.2 Throughput demo test procedures

Use the following commands in order to measure throughput with the TCP uplink and downlink tests.

TCP uplink test	
Console2	<code>ath_console.exe rx 192.168.0.3 2390 tcp v4</code>
Console1	<code>wmiconfig --connect Qtest-1</code> <code>wmiconfig --ipstatic 192.168.0.2 255.255.255.0 192.168.0.1</code> <code>benchtx 192.168.0.3 2390 tcp 1400 0 20 0</code>

TCP downlink test	
Console1	<code>wmiconfig --connect Qtest-1</code> <code>wmiconfig --ipstatic 192.168.0.2 255.255.255.0 192.168.0.1</code> <code>benchrx tcp 2390</code>
Console2	<code>ath_console.exe tx 192.168.0.2 2390 tcp 1400 0 20 0 v4</code>

2.3 Console commands

This section describes the configuration commands supported by the throughput tool.

Table 2-1 Configuration commands

Command	Description
help	Display the help menu and the syntax of available commands.
version	Display firmware and driver versions.
connect <ssid>	Connect to an AP by SSID in open mode.
wepkey	Connect to an AP in WEP mode.
p <passphrase>	Connect to an AP in WPA/WPA2 mode.
adhoc	Connect to a peer by SSID in Ad-Hoc mode (open).
wepkey	Connect to a peer by SSID in Ad-Hoc mode using WEP security.
wps	Setup and start a WPS operation.
disc	Disconnect from the current AP or peer.
settxpower <val>	Set the transmit power level.
pwrmode	Set the device power mode.
setchannel	Set the channel.
wmode	Set the wireless mode.
listen <interval>	Set the listen interval in TUs.
rsi	Print the link quality (SNR in dB) between the AP and the STA.
suspend	Enable the suspend feature.
suspendstart	Start the suspend feature.
pmparms	Set the power management parameters.
scanctrl	Set the scanning behavior.
assdump	Print the assertion data from the Wi-Fi module.
driver	Unload or reload the Wi-Fi driver.
allow_aggr	Enable aggregation by TID bit mask.
iwconfig scan	Scan for APs.
reset	Resets host driver and target.
macStore	Program a MAC address to the Wi-Fi device.
regdomain	Print the current regulatory domain.
getrate	Print the rate of the last transmitted packet.
getlasterr	Prints the error code of the last driver error.



Shenzhen Longsys Electronics Co.,Ltd www.Longsys.com

8/F, 1 Building, Finance Base, NO.8, KeFa Road, Shenzhen, China Tel: 86-755-86168848

10/F, CHINA AEROSPACE CENTRE,143 HOI BUN ROAD,HKTel: 852-23850111

GT202 Demo Applications User Guide 1.3

Command	Description
raw	Send packets with the given parameters.
ipconfig	Print the IP layer parameters (for offloaded IP stack only).
ipstatic	Assign static IP information to the IP stack (for offloaded IP stack only).
ipdhcp	Invoke IPv4 DHCP Client in IP stack.
ipdhcp release	Releases the IP address assigned by the DHCP Server.
ipv6	Enable or disable the IPv6 module.
ipv6rtpfx	Set IPv6 router prefix.
mode [ap]	Set the device to Soft AP mode.
ap [country]	Set the country code for the Soft AP mode.
ap [bconint]	Set the beacon interval for the Soft AP mode.
ap [dtim]	Set the DTIM interval for the Soft AP mode.
ap [inact]	Set the inactive timeout period for the Soft AP mode.
ipdhcp pool	Set the address pool for DHCP Server.
ip_dns_client	Start or stop the DNS Client at run time.
ip_dns_server_addr	Set the DNS Server address for the DNS Client.
ip_dns_delete_server_addr	Delete the DNS Server address used by the DNS Client.
ip_resolve_hostname	Resolve the host name by domain type.
ip_gethostbyname	Resolve the host name (for IPv4 only).
ip_gethostbyname2	Resolve the host name by domain type.
ip_http_server	Start or stop the HTTP Server.
ip_http_post	Post or update the object to HTML page.
ip_http_get	Get the updated database object of a given HTML page.
ip_http_client	Configure the HTTP Client at run time.
ip_dns_local_domain	Configure the domain name of the Soft AP.
ip_hostname	Configure the host name on the device (station mode).
ip_dns	Configure the DNS database on the host.
ssl_start	Start SSL as either server or client.
ssl_stop	Stop SSL server or client.
ssl_config	Configure SSL server or client.
ssl_add_cert	Add a certificate or CA list to either SSL server or client.
ssl_store_cert	Store a certificate or CA list to the flash.
ssl_delete_cert	Delete a certificate or CA list from flash.
ssl_list_cert	List the certificates and CA lists stored in flash.



Shenzhen Longsys Electronics Co.,Ltd www.Longsys.com

8/F, 1 Building. Finance Base, NO.8, KeFa Road, Shenzhen, China Tel: 86-755-86168848

10/F, CHINA AEROSPACE CENTRE,143 HOI BUN ROAD,HKTel: 852-23850111

2.3.1 help

Syntax	wmiconfig --help
Description	Display the help menu and the syntax of available commands.
Parameters	None

2.3.2 version

Syntax	wmiconfig --version
Description	Display the firmware and driver versions.
Parameters	None

2.3.3 connect <ssid>

Syntax	wmiconfig --connect <ssid>
Description	Connect to an AP by SSID in open mode. The connected message is printed upon connection success. The not connected message is printed upon connection failure.
Parameters	<ssid> twork SSID

2.3.4 wepkey

Syntax	wmiconfig --wepkey <key_index> <key> wmiconfig --wep <def_keyix> wmiconfig --connect <ssid>
Description	Connect to an AP in WEP mode. WEP connection is established in three steps: 1. Set the WEP key at the specified key index. The WEP key is either 10 or 26 characters long and contains hexadecimal characters. 2. Use the WEP configuration command to configure WEP mode. 3. Send a connect command to trigger a connection attempt with the WEP parameters. All parameters are mandatory.
Parameters	<key_index> Entered WEP key index [1-4]
	<key> WEP key
	<ssid> Network SSID
	<def_keyix> Default WEP key index [1-4]
Example	wmiconfig --wepkey 1 001122aabb wmiconfig --wep 1 wmiconfig --connect iot



Shenzhen Longsys Electronics Co.,Ltd www.Longsys.com

8/F, 1 Building. Finance Base, NO.8, KeFa Road, Shenzhen, China Tel: 86-755-86168848

10/F, CHINA AEROSPACE CENTRE,143 HOI BUN ROAD,HKTel: 852-23850111

2.3.5 p <passphrase>

Syntax	wmiconfig --p <passphrase> wmiconfig --wpa <ver> <ucipher> <mcipher> wmiconfig --connect <ssid>		
Description	Connect to an AP in WPA/WPA2 mode. WPA/WPA2 connection is established in three steps: Set the passphrase. Use the WPA configuration command to configure the WPA type and ciphers. Send a connect command to trigger a connection attempt with the WPA parameters. All parameters are mandatory.		
Parameters	<ssid>	Network SSID	
	<ver>	1	WPA
		2	WPA2
	<uciper>	TKIP or CCMP	
	<mciper>	TKIP or CCMP	
Example	wmiconfig --p passphrase123 wmiconfig --wpa 1 TKIP TKIP wmiconfig --connect iot		

2.3.6 adhoc

Syntax	wmiconfig --adhoc <ssid>		
Description	Connect to a peer by SSID in Ad Hoc mode (open).		
Parameters	<ssid>	Network SSID	

2.3.7 wepkey

Syntax	wmiconfig --wepkey <key_index> <key> wmiconfig --wep <mode> <def_keyix> wmiconfig --adhoc <ssid>		
Description	Connect to a peer by SSID in Ad Hoc mode using WEP security. The WEP key is either 10 or 26 characters long and contains hexadecimal characters.		
Parameters	<key_index>	WEP key index [1-4]	
	<key>	WEP key	
	<ssid>	Network SSID	
	<mode>	Open or Shared	
	<def_keyidx>	Default WEP key index [1-4]	

2.3.8 wps

Syntax	wmiconfig --wps <connect> <mode> [*pin] [*ssid] [*mac] [*channel]		
Description	Setup and start a WPS operation. Both PUSH and PIN modes are supported. The last three parameters are optional. However if one is specified, the other two must also be provided. All parameters obtained via WPS are printed on the screen.		
Parameters	<connect>	0	Does not attempt to connect after WPS
		1	Attempts to connect after WPS
	<mode>	Push or Pin	
	[pin]	WPS PIN (for pin mode only)	
	[ssid]	Network SSID (optional)	
	[mac]	MAC address of AP (optional)	
	[channel]	Channel of operation [1-14] (optional)	
Example	wmiconfig --wps 1 pin 2235341 iot 000a7f123456 6		

2.3.9 disc

Syntax	wmiconfig --disc
Description	Disconnect from the current AP or peer.
Parameters	None

2.3.10 settxpower <val>

Syntax	wmiconfig --settxpower <val>		
Description	Set the transmit power level. The transmit power must not exceed the limit set by the regulatory domain. This command is used for testing and evaluation. It is recommended to allow the device to determine the Tx output power based on rate.		
Parameters	<val>	Power value (range = 0 to 63). Default = 63 (max).	

2.3.11 pwrmode

Syntax	wmiconfig --pwrmode <val>		
Description	Set the device power mode.		
Parameters	<val>	0	Maximum performance (default value)
		1	Power save (default sleep = 100 ms)

2.3.12 setchannel

Syntax	wmiconfig --setchannel <channel>		
Description	Set the channel. After the channel is set, the device tries to connect on the specified channel. This command must be issued before the connect command. If WPS is used, the device attempts connecting to the channel detected during the exchange. If AP is not found, it tries to connect to another channel.		
Parameters	<channel>	Specified channel [1-14]	

2.3.13 wmode

Syntax	wmiconfig --wmode <mode>		
Description	Set the wireless mode.		
Parameters	<mode>	a	802.11a
		b	802.11b
		g	802.11g
		n	802.11n

2.3.14 listen <interval>

Syntax	wmiconfig --listen <interval>	
Description	Set the listen interval in TUs. (1 TU = approx. 1 ms) This command must be issued before the connect command.	
Parameters	<interval>	Listen interval in TUs. Range = 15 – 5000. Default = 100

2.3.15 rssi

Syntax	wmiconfig --rssi
Description	Print the link quality (SNR in dB) between the AP and the STA. This command is used only when the STA is associated to an AP and downlink data has been received. To obtain Beacon RSSI, the scan command iwconfig scan can be used.
Parameters	None

2.3.16 suspend

Syntax	wmiconfig --suspend
Description	Enable the suspend feature. This command must be issued before connecting the device to a network.
Parameters	None

2.3.17 suspstart

Syntax	wmiconfig --suspstart <time>	
Description	Start the device suspend feature. This command suspends the Wi-Fi module for a specified time period in milliseconds. The suspend feature must be enabled before connecting the device to a network.	
Parameters	<time>	Suspend time (in milliseconds)

2.3.18 pmparams

Syntax	wmiconfig --pmparams --idle <msec> --np <n> --dp <1-4> --txwp <1-2> --ntxw <> --psfp <1-2>		
Description	Set the power management parameters.		
Parameters	--idle < >	Idle period in ms (Default = 200)	
	--np < >	PS poll number. This is the number of power save poll messages the device sends before notifying the AP it is awake. (Default =1)	
	--dp < >	DTIM Policy (Default = Normal)	
		1	Ignore (Device does not listen to any traffic after beacon)
		2	Normal (Wakeup only at TIM interval)
		3	Stick (Wakeup only at DTIM interval)
		4	Auto (Wakeup at both TIM and DTIM intervals)
	--txwp < >	Tx wakeup policy. Policy to determine whether Tx is to wake up WLAN from sleep. (Default = 1)	
		1	Wake upon sleep (Indicate awake to AP upon uplink traffic)
		2	Do not wake (Never transit to awake based on uplink traffic)
	--ntxw < >	Number of uplink frames in a beacon interval to transit to wake up. (Default = 1)	
	--psfp < >	Power save fail event policy. The policy determines whether to send Power Save failure event to host during scanning. (Default = 1)	
		1	Send fail event
		2	Ignore event
Example	wmiconfig --pmparams --idle 100 --np 1 --dp 3 --txwp 1 --ntxw 1 --psfp 1		

2.3.19 scanctrl

Syntax	wmiconfig --scanctrl <foreground> <background>		
Description	Set the scanning behavior.		
Parameters	<foreground>	0	Disable foreground scan
		1	Enable foreground scan
	<background>	0	Disable background scan
		1	Enable background scan

2.3.20 assdump

Syntax	wmiconfig --assdump
Description	Print the assertion data from the Wi-Fi module. This command is used when a Target Assert message is displayed on the console.
Parameters	None

2.3.21 driver

Syntax	wmiconfig --driver <val>		
Description	Unload or reload the Wi-Fi driver.		
Parameters	<val>	down	Unload the driver.
		up	Reload the driver.
		raw	Reload driver in raw mode.
		normal	Reload driver in normal mode.
		quad	Reload driver in quad mode (not supported on MQX).
		rawq	Reload the driver in raw + quad mode.
		flushdown	Wait for Tx clear before unlocking the driver.
		pmu	Reload the driver in PMU enabled mode (MQX only).

2.3.22 allow_aggr

Syntax	wmiconfig --allow_aggr <tx_tid_mask> <rx_tid_mask>	
Description	Enable aggregation by TID bit mask.	
Parameters	<tx_tid_mask>	Transmission TID mask (0x0 – 0x7)
	<rx_tid_mask>	Reception TID mask (0x0 – 0x7)

2.3.23 iwconfig scan

Syntax	iwconfig scan [ssid*]	
Description	Scan for APs. If SSID is specified, only the specified SSID is scanned.	
Parameters	[ssid]	Forces a scan on a given SSID (optional).

2.3.24 reset

Syntax	wmiconfig --reset	
Description	Reset host driver and target.	
Parameters	None	

2.3.25 macStore

Syntax	wmiconfig --macstore <addr>	
Description	Program a MAC address to the Wi-Fi device.	
Parameters	<addr >	MAC address to be programmed

2.3.26 regdomain

Syntax	wmiconfig --regdomain	
Description	Print the current regulatory domain.	
Parameters	None	

2.3.27 getrate

Syntax	wmiconfig --getrate
Description	Print the rate of the last transmitted packet.
Parameters	None

2.3.28 getlasterr

Syntax	wmiconfig --getlasterr
Description	Prints the error code of the last driver error.
Parameters	None

2.3.29 raw

Syntax	wmiconfig --raw <rate> <num_tries> <num_bytes> <channel> <header_type>	
Description	Send packets with the given parameters.	
Parameters	<rate>	Rate index. 0 = 1 Mbps; 1 = 2 Mbps; 2 = 5.5 Mbps, and so on
	<num_tries>	Number of transmits. Range = 1 - 14
	<num_bytes>	Payload size. Range = 0 - 1400
	<channel>	Channel number. Range = 1- 11
	<header_type>	0 Beacon frame
		1 QoS data frame
		2 4-address data frame

2.3.30 ipconfig

Syntax	wmiconfig --ipconfig
Description	Print the IP layer parameters (for offloaded IP stack only). Both IPv4 and IPv6 parameters are displayed.
Parameters	None

2.3.31 ipstatic

Syntax	wmiconfig --ipstatic <IP Address> <Subnet Mask> <Default Gateway>	
Description	Assign static IP information to the IP stack (for Offloaded IP Stack only). Only IPv4 parameters can be assigned.	
Parameters	<IP Address>	IPv4 address for the interface using dot notation
	<Subnet Mask>	IPv4 subnet mask
	<Default Gateway>	IPv4 address of default gateway
Example	wmiconfig --ipstatic 192.168.1.90 255.255.255.0 192.168.1.1	

2.3.32 ipdhcp

Syntax	wmiconfig --ipdhcp
Description	Invoke IPv4 DHCP Client in IP stack. Use the ipconfig command to obtain IP information.
Parameters	none

2.3.33 ipdhcp release

Syntax	wmiconfig --ipdhcp_release
Description	Release the IP address assigned by the DHCP server.
Parameters	none

2.3.34 ipv6

Syntax	wmiconfig --ipv6 <status>		
Description	Enable or disable the IPv6 module.		
Parameters	<status	on	Enable the IPv6 module
	>	off	Disable the IPv6 module

2.3.35 ipv6rtprfx

Syntax	wmiconfig --ip6rtprfx <prefix> <prefixlen> <prefix_lifetime> <valid_lifetime>	
Description	Set IPv6 router prefix.	
Parameters	<prefix>	Set the IPv6 prefix.
	<prefixlen>	Set the IPv6 prefix length.
	<prefix_lifetime>	Set the IPv6 prefix lifetime.
	<valid_lifetime>	Set the IPv6 valid lifetime.

2.3.36 mode [ap]

Syntax	<code>wmiconfig --mode [ap <hidden><wps> station]</code>	
Description	Set the device to Soft AP mode. This command only changes the mode to AP. To start Soft AP operation, issue the <i>connect</i> command. If country code, beacon interval, or DTIM interval is different from the default values, it must be set before the connect command. DHCP server is enabled once the Soft AP operation is started.	
Parameters	<code><ap></code>	Set AP mode.
	<code><hidden></code>	Enable hidden mode for Soft AP.
	<code><wps></code>	Enable WPS registrar mode for Soft AP.
	<code><station></code>	Set Station mode.
Example	<code>wmiconfig --mode ap wps</code> <code>wmiconfig --mode ap hidden</code> <code>wmiconfig --mode station</code>	
	<code>wmiconfig --mode ap</code> <code>wmiconfig --ap country US</code> <code>wmiconfig --ap bconint 200</code> <code>wmiconfig --ap dtim 10</code> <code>wmiconfig --connect testap</code>	

2.3.37 ap [country]

Syntax	<code>wmiconfig --ap [country <country code>]</code>	
Description	Set the country code for the Soft AP mode. This command is issued before the <i>connect</i> command.	
Parameters	<code><country code></code>	Country code, for example, US

2.3.38 ap [bconint]

Syntax	wmiconfig --ap [bconint<intvl>]	
Description	Set the beacon interval for the Soft AP mode. This command is issued before the <i>connect</i> command.	
Parameters	<intvl>	Interval in milliseconds. Default = 100 ms

2.3.39 ap [dtim]

Syntax	wmiconfig --ap [dtim<val>]	
Description	Set the DTIM interval for the Soft AP mode. DTIM informs the clients of the buffered multicast/broadcast data on the access point. This command is issued before the <i>connect</i> command.	
Parameters	<val>	Number of beacon intervals. Range = 1 – 255. Default = 5.

2.3.40 ap [inact]

Syntax	wmiconfig --ap [inact <minutes>]>	
Description	Sets the inactive timeout period for the Soft AP mode. This command is issued before the <i>connect</i> command.	
Parameters	<minutes>	Inactive timeout in minutes. Default = 5.

2.3.41 ipdhcppool

Syntax	wmiconfig --ipdhcppool <start ipaddr> <End ipaddr> <Lease time>	
Description	Set the address pool for DHCP Server. This command is issued before the <i>connect</i> command.	
Parameters	<start ipaddr>	Start IP address of the DHCP Pool.
	<End ipaddr>	End IP address of the DHCP pool.
	<Lease time>	DHCP lease time in seconds.

2.3.42 ip_dns_client

Syntax	wmiconfig --ip_dns_client [<start/stop>]	
Description	Start or stop the DNS Client at run time.	
Parameters	<start>	Enable the DNS Client.
	<stop>	Disable the DNS Client.

2.3.43 ip_dns_server_addr

Syntax	wmiconfig --ip_dns_server_addr <ip addr>	
Description	Set the DNS Server address for the DNS Client.	
Parameters	<ip_addr>	IP address of the DNS Server

2.3.44 ip_dns_delete_server_addr

Syntax	wmiconfig --ip_dns_delete_server_addr <ip addr>	
Description	Delete the DNS Server address used by the DNS Client.	
Parameters	<ip_addr>	IP address of the DNS Server

2.3.45 ip_resolve_hostname

Syntax	wmiconfig --ip_resolve_hostname [<host name> <domain_type>]	
Description	Resolves the host name by domain type.	
Parameters	<host name>	Host name
	<domain type>	Domain type 2 = IPv4 3 = IPv6

2.3.46 ip_gethostbyname

Syntax	wmiconfig --ip_gethostbyname [<host name>]	
Description	Resolve the host name (for IPv4 only).	
Parameters	<host name>	Host name to resolve

2.3.47 ip_gethostbyname2

Syntax	wmiconfig --ip_gethostbyname2 [<host name> <domain_type>]	
Description	Resolve the hostname by domain type.	
Parameters	<host name>	Host name
	<domain type>	Domain type 2 = IPv4 3 = IPv6

2.3.48 ip_http_server

Syntax	wmiconfig --ip_http_server [<start/stop>]	
Description	Start or stop the HTTP Server at run time.	
Parameters	<start>	Enable the HTTP Server.
	<stop>	Disable the HTTP Server.

2.3.49 ip_http_post

Syntax	wmiconfig --ip_http_post <page name> <obj_name> <obj_type> <obj_len> <obj_value>	
Description	Post or update the object to HTML page. This updated database is reflected on the browser for the subsequent GET requests.	
Parameters	<page name>	The name of the Page for which the data is to be updated.
	<obj_name>	Object name to update
	<Obj_type>	1= Bool; 2 = Integer; 3 = String
	<Obj_len>	Length of the object
	<Obj_value>	Object value

2.3.50 ip_http_get

Syntax	wmiconfig --ip_http_get <page name> <obj_name> <obj_type>	
Description	Get the updated database object of a given HTML page.	
Parameters	<page name>	The name of the page from which the data is to be fetched.
	<obj_name>	Object name to get.

2.3.51 ip_http_client

Syntax	wmiconfig --ip_http_client <connect get query post disc> <data1> <data2>	
Description	Configure the HTTP client at run time.	
Parameters	connect	Connect to the HTTP server. Return error if any. <data1> is domain name /IP address of the HTTP server. <data2> is port number (optional). Default port is 80.
	get	Request a page from the server. <data1> is the page name to request (mandatory).
	query	Update the content of page to be posted to server. Configure the (name, value) pair before POST/GET. <data1> is the name. <data2> is the value.
	post	Sent a POST request to the HTTP server. <data1> is the page name to request (mandatory).
	disc	Disconnect the HTTP server and close the HTTP client session.

2.3.52 ip_dns_local_domain

Syntax	ip_dns_local_domain [<domain name>]	
Description	Configure the domain name on the Soft AP.	
Parameters	<domain name>	Configures the domain name.

2.3.53 ip_hostname

Syntax	iphostname [<domain name>]	
Description	Configure the host name on the device (station mode).	
Parameters	<domain name>	Configures the domain name on the Station. This name is advertised by DHCP Client on STA to DHCP Server on Soft AP.

GT202 Demo Applications User Guide 1.3

2.3.54 ip_dns

Syntax	ip_dns <add/delete> <domain name> <addr>	
Description	Configure the DNS database on the host.	
Parameters	<add/delete>	Creates or deletes an entry in the DNS.
	<domain name>	Configures the domain name.
	<addr>	Either IPv4 or IPv6 address

2.3.55 ssl_start

Syntax	ssl_start server client	
Description	Start SSL as either server or client.	
Parameters	<server/client>	Start SSL as server or client.

2.3.56 ssl_stop

Syntax	ssl_stop server client	
Description	Stop SSL as either server or client.	
Parameters	<server/client>	Stop SSL server or client.



Shenzhen Longsys Electronics Co.,Ltd www.Longsys.com

8/F, 1 Building. Finance Base, NO.8, KeFa Road, Shenzhen, China Tel: 86-755-86168848

10/F, CHINA AEROSPACE CENTRE,143 HOI BUN ROAD,HKTel: 852-23850111

2.3.57 ssl_config

Syntax	ssl_config server client [protocol <protocol>] [time 0 1] [domain 0 <name>] [cipher <cipher>]	
Description	Configure SSL server or client.	
Parameters	<protocol>	Protocol options: SSL3, TLS1.0, TLS1.1, TLS1.2
	<time>	Disable/Enable certificate time validation. (Optional)
	<domain>	Disable/enable validation of peer domain name against name.
	<alert>	Disable/enable sending SSL alert when certificate validation fails.
	<cipher>	Select cipher (enum name) suite to use. Can be repeated 8 times. (Optional)

2.3.58 ssl_add_cert

Syntax	ssl_add_cert server client certificate calist [<name>]	
Description	Add a certificate or CA list to SSL server or client.	
Parameters	<name>	Name of the file to be loaded from flash

2.3.59 ssl_store_cert

Syntax	ssl_store_cert <name>	
Description	Store a certificate or CA list to the flash.	
Parameters	<name>	Name of the file to be stored to the flash.

2.3.60 ssl_delete_cert

Syntax	ssl_delete_cert <name>	
Description	Delete a certificate or CA list by name from flash.	
Parameters	<name>	Name of the file to be deleted from the flash.



Shenzhen Longsys Electronics Co.,Ltd www.Longsys.com

8/F, 1 Building. Finance Base, NO.8, KeFa Road, Shenzhen, China Tel: 86-755-86168848

10/F, CHINA AEROSPACE CENTRE,143 HOI BUN ROAD,HKTel: 852-23850111

2.3.61 ssl_list_cert

Syntax	ssl_list_cert
Description	List the names of the certificates and CA lists stored in the flash.
Parameters	None

2.4 Benchmark component

The benchmark component allows running uplink and downlink TCP/UDP streams to analyze throughput performance. The remote end of the stream is controlled by the Throughput Demo tool (command line tool ath_console.exe) running on PC. Before running the throughput tests, ensure that the remote PC is connected on the same network. Up to two simultaneous streams are allowed. The demo application works seamlessly across Host MCU-enabled stack versus IP offload-enabled stack. Since the option to enable or disable IP offload is made at compile time, two throughput demo applications are provided. For the Host MCU-enabled stack, use the demo application in the non_offload directory.

The benchmode and multiset commands are used for the IP offload demo application only.

- The benchmode command instructs the throughput demo to use IPv4 or IPv6. The MCU-enabled mode supports IPv4 only and thus does not require this command.
- The multiset command is used during scalability test to check the number of sockets tested in the firmware, which is valid only for the IP offload mode.
- Other demo applications such as P2P, Store-recall, HTTP, and DNS assume IP offload is enabled and running on the QCA4004 chip.

2.4.1 Benchmark commands

This section discusses the benchmark commands supported by the throughput tool.

Command	Description
benchtx	Run the transmit (Tx) traffic test
benchrx	Run the receive (Rx) traffic test
benchmode	Set mode to IPv4 or IPv6 (available for IP offload mode only)
benchrx_multi_socket	Open a multi socket receiver (available for IP offload mode only)



Shenzhen Longsys Electronics Co.,Ltd www.Longsys.com

8/F, 1 Building. Finance Base, NO.8, KeFa Road, Shenzhen, China Tel: 86-755-86168848

10/F, CHINA AEROSPACE CENTRE,143 HOI BUN ROAD,HKTel: 852-23850111

GT202 Demo Applications User Guide 1.3

2.4.1.1 benchtx

Syntax	benchtx <Rx IP> <port> <protocol> <size> <test mode> <packets time> <delay>		
Description	Run the transmit traffic test. Before running this test, make sure the remote end is set to Rx mode. The test can be run for a number of packets or a time period. To terminate the test, enter <i>benchquit</i> .		
Parameters	<Rx IP>	IP address of the remote end (receiver) in format of [A.B.C.D]	
	<port>	Listening port	
	<protocol>	tcp	TCP
		udp	UDP
		ssl	SSL
	<size>	Packet size in bytes	
	<test mode>	0	Time test (test run for a specified time period)
		1	Packet test (test run for specified number of packets)
	<packets time>	Test mode = 0: Enter the test time in seconds. Test mode = 1: Enter the number of packets to transmit.	
	<delay>	Delay in milliseconds between packets (bandwidth control). The delay is used to prevent one stream starving the other in cases where two streams run simultaneously.	

2.4.1.2 benchrx

Syntax	benchrx <protocol> <port> <multicast IP *> <Local IP *>		
Description	Run the receive traffic test. The command puts the client in receive mode, waiting for data. The remote PC tool shall be initiated to transmit data. To terminate the test, enter <i>benchquit</i> .		
Parameters	<protocol>	tcp	TCP receiver
		udp	UDP receiver
		ssl	SSL
	<port>	Receiver port	
	<multicast address>	IP address of multicast group to join (optional)	
	<local address>	IP address of interface (optional)	

2.4.1.3 benchmode

Syntax	benchmode <v4 v6>		
Description	Set the IP mode to IPv4 or IPv6. Default mode is IPv4. This command must be issued before the IPv6 throughput tests.		
Parameters	Mode	v4	Enable IPv4 mode
		v6	Enable IPv6 mode



Shenzhen Longsys Electronics Co.,Ltd www.Longsys.com

8/F, 1 Building. Finance Base, NO.8, KeFa Road, Shenzhen, China Tel: 86-755-86168848

10/F, CHINA AEROSPACE CENTRE,143 HOI BUN ROAD,HKTel: 852-23850111

2.4.1.4 benchrx_multi_socket

Syntax	benchrx_multi_socket [tcp udp] <port1> - <port2>	
Description	Open a multi-socket receiver and received traffic on any of the socket. Valid only when IP offload is enabled. Up to 7 TCP sockets and 8 UDP sockets are supported.	
Parameters	<tcp udp >	Specifies the type of stream
	<port1>	Start port number
	<port2>	End port number
Example	benchrx_multi_socket tcp 7000 – 7002 benchrx_multi_socket udp 7000 – 7003	

2.4.2 Running multi-stream tests with the throughput tool

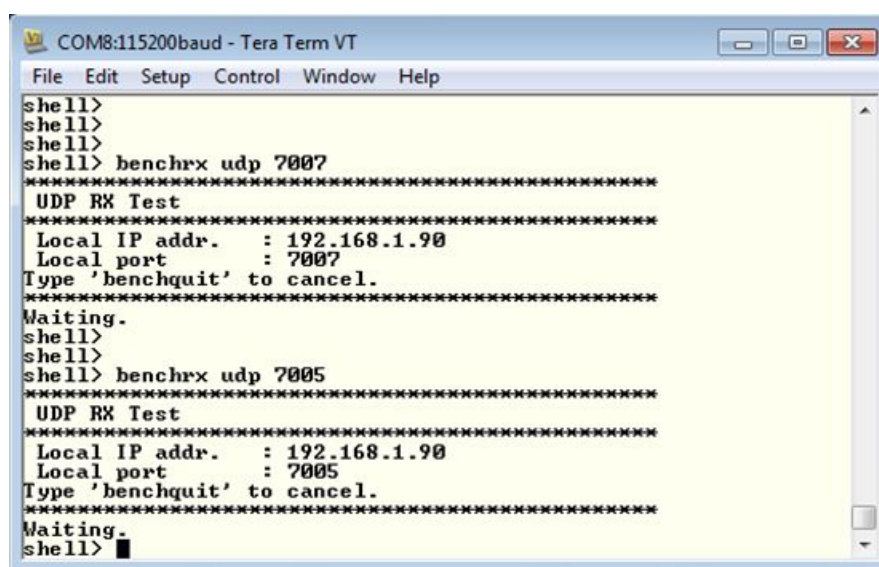
This section describes the best practices for running the bidirectional traffic tests using the throughput tool. Diverging from the steps outlined below may lead to undesired behaviors.

- Always set up the receiver before initiating any traffic stream.
- During a TCP + UDP test, UDP stream will overpower TCP. To allow TCP to run, include a substantial delay between UDP packets.
- During uplink + downlink tests, avoid using the same port numbers for two streams because the UDP transmitter uses the Rx port number for feedback purposes.

2.4.2.1 Host Rx + host Rx (two simultaneous downlink streams)

This procedure is valid for UDP + UDP, TCP + TCP, UDP + TCP tests.

3. On the host, enter the first receive command. The host prints a *waiting...* prompt.
4. Enter the second receive command. Do not start any traffic.



```
COM8:115200baud - Tera Term VT
File Edit Setup Control Window Help
shell>
shell>
shell>
shell> benchrx udp 7007
*****
UDP RX Test
*****
Local IP addr. : 192.168.1.90
Local port    : 7007
Type 'benchquit' to cancel.
*****
Waiting.
shell>
shell>
shell> benchrx udp 7005
*****
UDP RX Test
*****
Local IP addr. : 192.168.1.90
Local port    : 7005
Type 'benchquit' to cancel.
*****
Waiting.
shell>
```

5. Start two Tx streams from the two instances of the PC application.

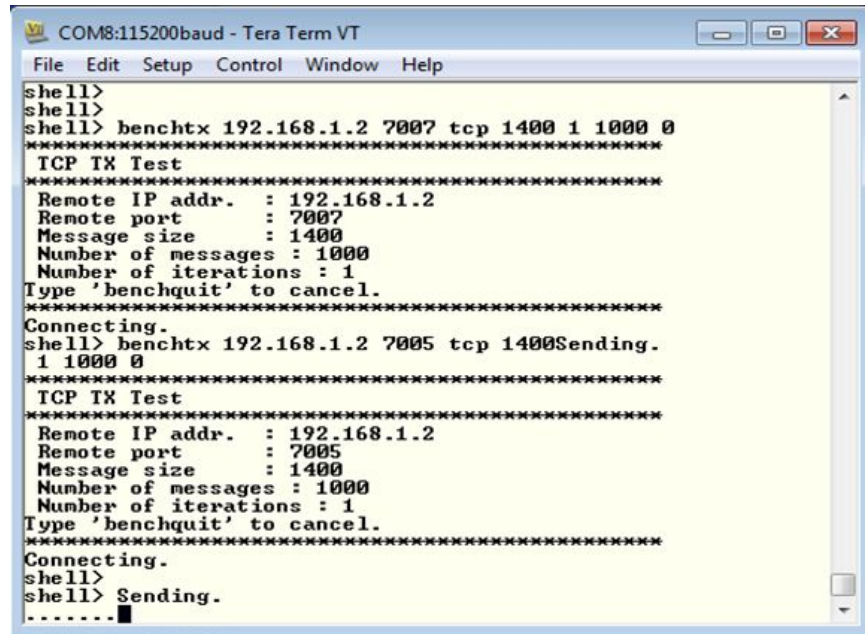
2.4.2.2 Host Tx + host Tx (two simultaneous uplink streams)

This procedure is valid for UDP + UDP, TCP + TCP, UDP + TCP tests.

6. Set the two instances of PC throughput tool in receive mode.
7. Start the first transmit stream from the host.
8. Start the second transmit stream from the host.

On some consoles the two commands can be pasted at once. On some other consoles, the second command may have to be typed manually.

GT202 Demo Applications User Guide 1.3



```
COM8:115200baud - Tera Term VT
File Edit Setup Control Window Help
shell>
shell>
shell> benchtx 192.168.1.2 7007 tcp 1400 1 1000 0
*****
TCP TX Test
*****
Remote IP addr. : 192.168.1.2
Remote port    : 7007
Message size   : 1400
Number of messages : 1000
Number of iterations : 1
Type 'benchquit' to cancel.
*****
Connecting.
shell> benchtx 192.168.1.2 7005 tcp 1400
1 1000 0
*****
TCP TX Test
*****
Remote IP addr. : 192.168.1.2
Remote port    : 7005
Message size   : 1400
Number of messages : 1000
Number of iterations : 1
Type 'benchquit' to cancel.
*****
Connecting.
shell>
shell> Sending.
.....
```

2.4.2.3 Host Tx + host Rx (simultaneous uplink and downlink streams)

This procedure is valid for UDP + UDP, TCP + TCP, UDP + TCP tests.

9. Enter the receive command on host. The host prints a *waiting...* prompt.
10. Start the first instance of the PC application in receive mode. Do not start any traffic.
11. Enter the transmit command at the host and start transmission.

The host must start transmission before the PC because the incoming data processing takes higher priority over shell, which prevents user from entering the transmit command.

12. Start the transmission from the second instance of the PC application.



Shenzhen Longsys Electronics Co.,Ltd www.Longsys.com

8/F, 1 Building. Finance Base, NO.8, KeFa Road, Shenzhen, China Tel: 86-755-86168848

10/F, CHINA AEROSPACE CENTRE,143 HOI BUN ROAD,HKTel: 852-23850111

```
COM8:115200baud - Tera Term VT
File Edit Setup Control Window Help
shell>
shell> benchrx udp 7007
*****
UDP RX Test
*****
Local IP addr.   : 192.168.1.90
Local port      : 7007
Type 'benchquit' to cancel.
*****
Waiting.
shell>
shell> benchtx 192.168.1.2 7005 udp 1400 1 100000 0
*****
UDP TX Test
*****
Remote IP addr. : 192.168.1.2
Remote port     : 7005
Message size    : 1400
Number of messages : 100000
Number of iterations : 1
Type 'benchquit' to cancel.
*****
Connecting.
Sending.
shell> Receiving from 192.168.1.2:54206
```

2.4.2.4 PC throughput command line tool

The throughput command line tool is the command line version of the PC throughput GUI application and aims to provide similar functionality. Multiple versions of the tool can be run concurrently.

The command line versions for transmit and receive are:

Transmit command:

`ath_console.exe tx <Remote IP Address> <Remote Port> <Protocol [tcp|udp]> <size> <mode> <arg> <delay> <v4|v6> <traffic class [Optional]>`

Receive command:

`ath_console.exe rx <Local IP Address> <Local Port> <Protocol [tcp|udp]> <v4|v6> <Multicast IP address [optional]>`

Where:

size	Size of transmit packet in bytes		
mode	Test mode	0	Transmit for the specified time in seconds.
		1	Transmit for the specified number of packets.
arg	If test mode = 0	<transmission time in seconds>	
	If test mode = 1	<number of packets>	
delay	Time between packets, in milliseconds		
v4 v6	The user must specify the version of IP protocol for each test. To run IPv6 tests, make sure the router and PC support the IPv6 protocol.		
traffic class	Optional parameter (CLI version only, not available on MQX)	BE	Best effort
		BG	Background
		VI	Video
		VO	Voice

Shenzhen Longsys Electronics Co.,Ltd www.Longsys.com

8/F, 1 Building. Finance Base, NO.8, KeFa Road, Shenzhen, China Tel: 86-755-86168848

10/F, CHINA AEROSPACE CENTRE,143 HOI BUN ROAD,HKTel: 852-23850111



Caveats

- Do not use same value for the remote and the local ports when Tx and Rx tests are run simultaneously. The UDP transmitter uses the specified port for feedback.
- After the test is completed, press Ctrl + C to exit (by design).
- The traffic class option is not available in the GUI version.
- The traffic class option is not available on the MQX platform because the RTCS stack does not support 802.1p QoS classes.

2.5 SSL

SSL (Secure socket Layer) is a standard security technology for establishing encrypted link between a server and a client – typically a webserver (website) and a browser or a mail server and a mail client. Once the client and server have decided to use TLS, they negotiate a stateful connection by using a handshaking procedure. During this handshake, the client and server agree on various parameters used to establish the connection's security:

13. The client sends the server the client's SSL version number, cipher settings, session-specific data, and other information that the server needs to communicate with the client using SSL.
14. The server sends the client the server's SSL version number, cipher settings, session-specific data, and other information that the client needs to communicate with the server over SSL. The server also sends its own certificate, and if the client is requesting a server resource that requires client authentication, the server requests the client's certificate.
15. The client uses the information sent by the server to authenticate the server—e.g., in the case of a web browser connecting to a web server, the browser checks whether the received certificate's subject name actually matches the name of the server being contacted, whether the issuer of the certificate is a trusted certificate authority, whether the certificate has expired, and, ideally, whether the certificate has been revoked.[7] If the server cannot be authenticated, the user is warned of the problem and informed that an encrypted and authenticated connection cannot be established. If the server can be successfully authenticated, the client proceeds to the next step.
16. Using all data generated in the handshake thus far, the client (with the cooperation of the server, depending on the cipher in use) creates the pre-master secret for the session, encrypts it with the server's public key (obtained from the server's certificate, sent in step 2), and then sends the encrypted pre-master secret to the server.
 - If the server has requested client authentication (an optional step in the handshake), the client also signs another piece of data that is unique to this handshake and known by both the client and server. In this case, the client sends both the signed data and the client's

own certificate to the server along with the encrypted pre-master secret.

- If the server has requested client authentication, the server attempts to authenticate the client. If the client cannot be authenticated, the session ends. If the client can be successfully authenticated, the server uses its private key to decrypt the pre-master secret, and then performs a series of steps (which the client also performs, starting from the same pre-master secret) to generate the master secret.
- 17. Both the client and the server use the master secret to generate the session keys, which are symmetric keys used to encrypt and decrypt information exchanged during the SSL session and to verify its integrity (that is, to detect any changes in the data between the time it was sent and the time it is received over the SSL connection).
- 18. The client sends a message to the server informing it that future messages from the client will be encrypted with the session key. It then sends a separate (encrypted) message indicating that the client portion of the handshake is finished.
- 19. The server sends a message to the client informing it that future messages from the server will be encrypted with the session key. It then sends a separate (encrypted) message indicating that the server portion of the handshake is finished.
- 20. The SSL handshake is now complete and the session begins. The client and the server use the session keys to encrypt and decrypt the data they send to each other and to validate its integrity.

2.5.1 Certificate management demo

The certificate management module is an application on the MCU that enables downloading the certificate to the host over the air. Once the certificate is downloaded to the MCU the certificate can be pushed to the target through WMI commands and written to the flash on the target.

The following test procedure is an example to demonstrate how to download SSL certificate to the device. The reference of “foo” is a name example.

- 21. Generate a device certificate using OpenSSL.
 - a. Generate a private key.
`openssl genrsa -des3 -out foo.key 1024`
 - b. Generate a self-signed certificate.
`openssl req -new -key foo.key -out foo.pem -x509 -days 365`
 - c. Remove the passphrase from the key.
`mv foo.key foo.key.withpass`



Shenzhen Longsys Electronics Co.,Ltd www.Longsys.com

8/F, 1 Building. Finance Base, NO.8, KeFa Road, Shenzhen, China Tel: 86-755-86168848

10/F, CHINA AEROSPACE CENTRE,143 HOI BUN ROAD,HKTel: 852-23850111

GT202 Demo Applications User Guide 1.3

```
openssl rsa -in foo.key.withpass -out foo.key
```

22. Convert certificate to SharkSSL binary format.

- a. Generate binary certificate file.

```
SharkSSLParseCert foo.pem foo.key -b foo.cert.bin
```

- b. Generate binary CA List file.

```
SharkSSLParseCAList -b foo.calist.bin foo.pem
```

23. Start the certificate server on the Linux PC.

- a. Copy the **foo.cert.bin** and **foo.calist.bin** files to the **certcs** directory which also contains the **certcs** executable.

- b. Start the certificate server.

```
./certcs -s
```

- c. Test the certificate server from another PC.

```
./certcs HOSTNAME/foo.calist.bin
```

HOSTNAME is the host name of the PC where the certificate server is started.

24. Download the certificate and CA list from the server and write them to the flash.

- a. Download and flash the certificate.

```
getcert foo.cert.bin IPADDR -s kf.crt
```

- b. Download and flash the CA list.

```
getcert foo.calist.bin IPADDR -s kf.ca
```

IPADDR is the IP address of the certificate server.

25. Use the certificate and the CA list stored in the flash.

The kf.crt and kf.ca will be subsequently used with the other SSL wmiconfig commands.

- Add certificate to the server SSL context

```
wmiconfig --ssl_add_cert server certificate foo.crt
```

- Add CA list to the client SSL context.

```
wmiconfig --ssl_add_cert client calist foo.ca
```

- Delete the files.

```
wmiconfig --ssl_delete_cert foo.ca
```



Shenzhen Longsys Electronics Co.,Ltd www.Longsys.com

8/F, 1 Building. Finance Base, NO.8, KeFa Road, Shenzhen, China Tel: 86-755-86168848

10/F, CHINA AEROSPACE CENTRE,143 HOI BUN ROAD,HKTel: 852-23850111

GT202 Demo Applications User Guide 1.3

Test example, SSL server

```
wmiconfig --ssl_start server
```

```
wmiconfig --ssl_add_cert server certificate name
```

```
wmiconfig --ssl_configure cipher TLS_RSA_WITH_AES_256_CBC_SHA //Optional
```

```
benchrx ssl 1443
```

Test example, SSL client

```
wmiconfig -- ssl_start client
```

```
wmiconfig --ssl_add_cert server calist name
```

```
wmiconfig --ssl_configure protocol SSL3 time 1 cipher TLS_RSA_WITH_AES_256_
CBC_SHA
```

```
benchtx 10.1.33.100 1443 ss
```

Longsys



Shenzhen Longsys Electronics Co.,Ltd www.Longsys.com

8/F, 1 Building. Finance Base, NO.8, KeFa Road, Shenzhen, China Tel: 86-755-86168848

10/F, CHINA AEROSPACE CENTRE,143 HOI BUN ROAD,HKTel: 852-23850111

3 P2P Demo

This chapter describes the setup and test procedures for the P2P demo application. The required equipment includes:

- GT202 Development Kit
 - P2P demo application loaded on Freedom board in GT202 Development Kit
- The P2P demo application implements a P2P command set for access from the serial console. The P2P command set provides an interface to configure and control the QCA4004 Wi-Fi chipset for connecting with a P2P device.
- Microsoft Windows 7 laptop (as a P2P peer device)
 - Qualcomm Atheros XB92 PCI Express Card
 - Qualcomm Atheros Direct Connect software

3.1 P2P demo setup

The Freedom board in GT202 development kit is connected to a PC via OpenSDA USB port on Freedom board using a USB cable. A console application running on the PC1 is used to input command for P2P configuration and connection. Using these commands, a Wi-Fi link can be created between the P2P peer device (PC2) and GT202 development kit in different scenarios. [Figure 3-1](#) shows an example configuration.

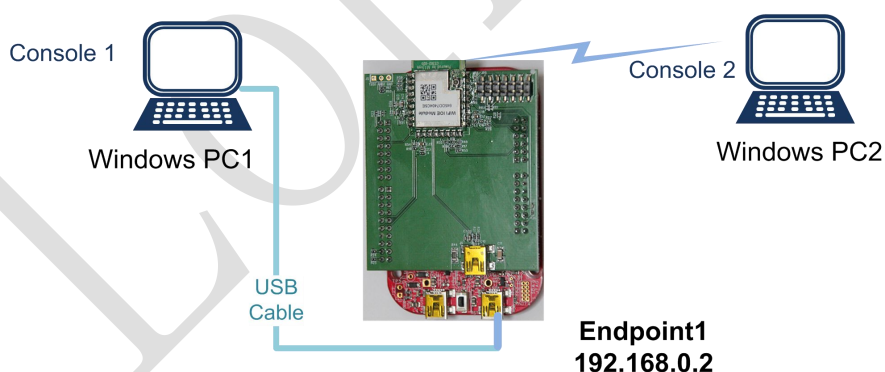


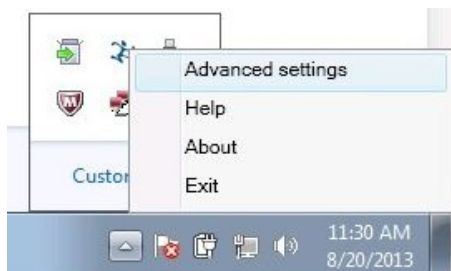
Figure 3-1 Sample system configuration for P2P demonstration

3.1.1 Windows PC1 setup

1. Use a USB cable to connect PC1 to OpenSDA USB port of the Freedom board in GT-202 development kit
2. Start terminal applications from PC1 to communicate with the Freedom board console port as Console 1. The port setting is: 115200, 8, n, 1, no flow control.
 - a. Freedom board console port: The virtual COM port created by OpenSDA USB connection.

3.1.2 Windows PC2 setup

1. Plug the XB92 PCI Express card to PC2 and install the Qualcomm Atheros Direct Connect software.
2. Select **All Programs** → **Qualcomm Atheros Direct Connect** → **Qualcomm Atheros Direct Connect** to start Direct Connect.
3. The program generates an icon in the system tray. Right click the icon in the system tray and select **Advanced Settings**.



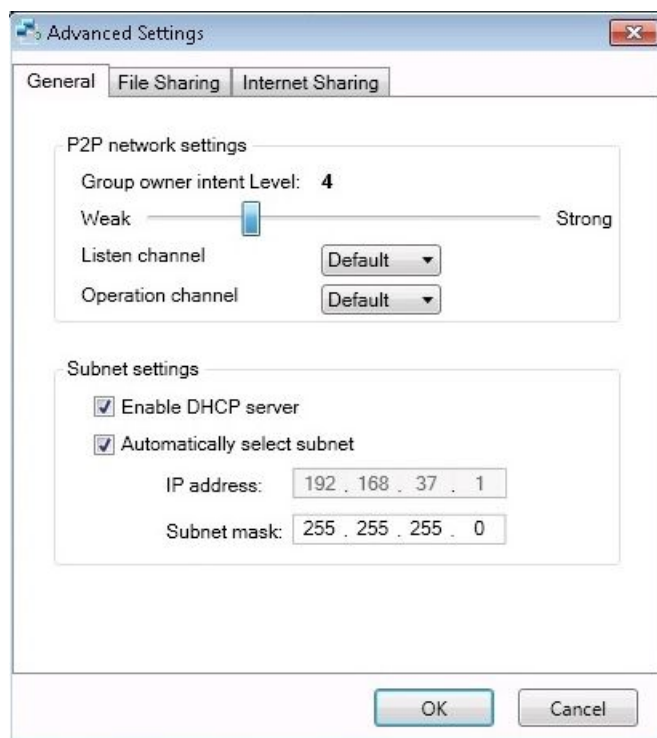
If the **Advanced Settings** item is not visible, update C:\Program Files(x86)\Qualcomm Atheros Direct Connect\P2PUIMain.exe.config and set:

```
key="OperationChannel" value="2412"
```

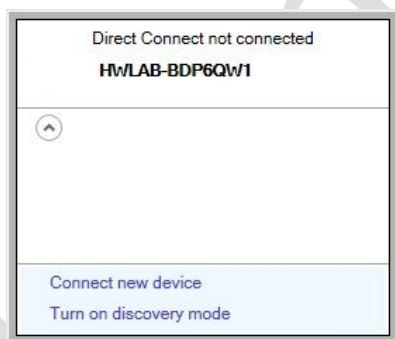
```
key="DCMTrayIconMenuEnableAdvancedSettings" value="True"
```

GT202 Demo Applications User Guide 1.3

4. In the **General** tab, set **P2P Group owner intent level** to **4**. Click **OK**.



5. Click the **Direct Connect** icon in the system tray to open the Direct Connect window.



3.2 Testing P2P connection using PUSH method

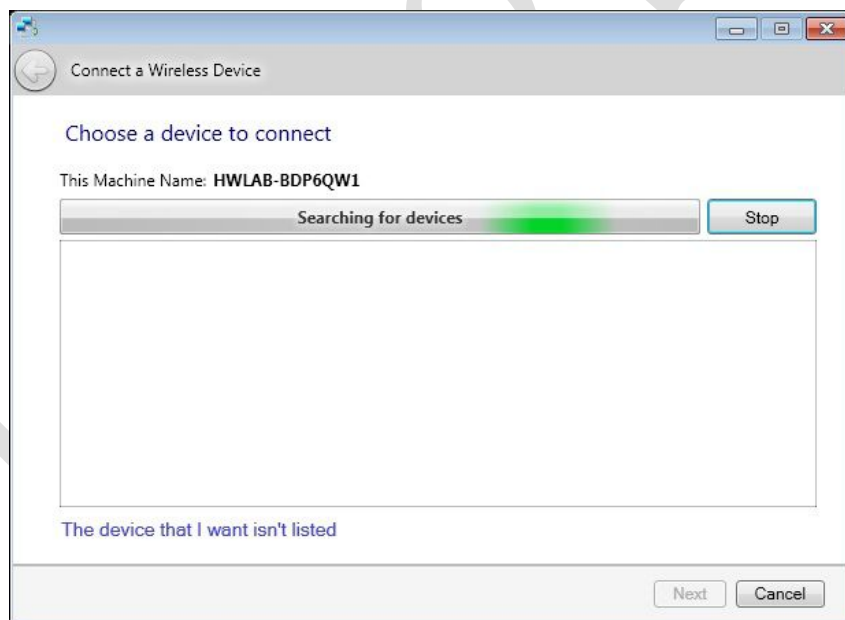
3.2.1 GT202 development kit as P2P client

3.2.1.1 GT202 development kit connecting to peer device

1. On the peer device, click the **Direct Connect** icon on the system tray. Then click **Connect new device**.



The following window appears.



2. On the GT202 development kit, type the commands:
`wmiconfig --p2p on`
`wmiconfig --p2p find`

GT202 Demo Applications User Guide 1.3

```
wmiconfig --p2p nodelist
```

```
wmiconfig --p2p connect <peer_mac> push
```

The **p2p find** command initiates P2P Discovery and makes firmware populate peer P2P devices. The **p2p nodelist** command requests the firmware for the populated P2P device list and prints the results in the shell. The **p2p find** commands must be issued before **p2p nodelist**. See a nodelist printout example in section 3.2.3.1 step 7.

3. On the peer device, accept the connection from the GT202 development kit.
4. A four-way handshake success message indicates a successful connection.

Other useful commands

- Get IP address from DHCP.

```
wmiconfig --ipdhcp
```

- Set a static IP address.

```
wmiconfig --ipstatic <ip address> <subnet mask> <gateway>
```

- Disconnect P2P connection from the GT202 development kit.

```
wmiconfig P2P cancel
```

3.2.1.2 Peer device connecting to GT202 development kit

1. On the GT202 development kit, type the commands:

```
wmiconfig --p2p on
```

```
wmiconfig --p2p find
```

```
wmiconfig --p2p nodelist
```



Shenzhen Longsys Electronics Co.,Ltd www.Longsys.com

8/F, 1 Building. Finance Base, NO.8, KeFa Road, Shenzhen, China Tel: 86-755-86168848

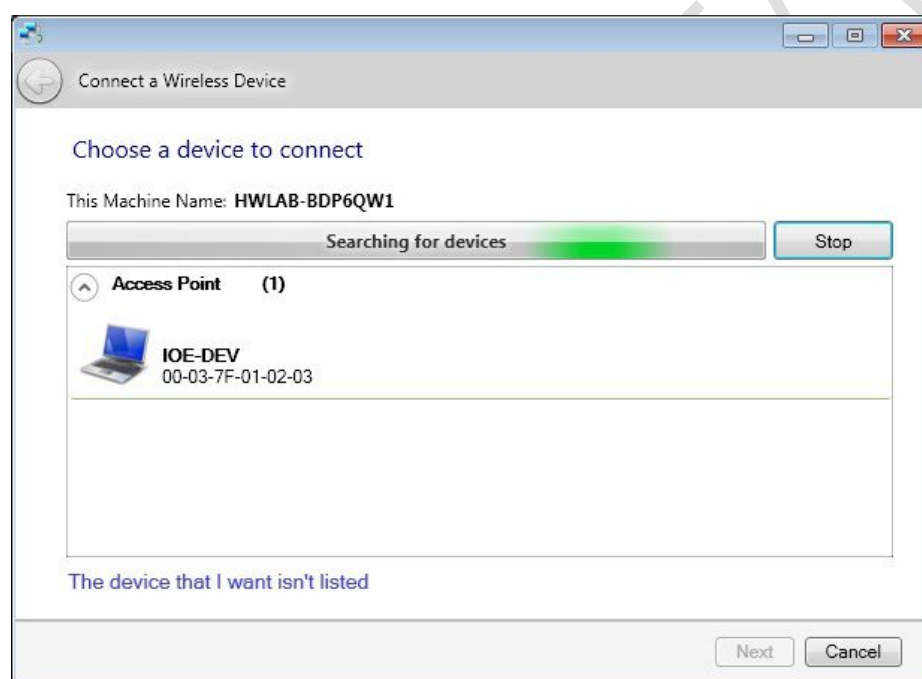
10/F, CHINA AEROSPACE CENTRE,143 HOI BUN ROAD,HKTel: 852-23850111

GT202 Demo Applications User Guide 1.3

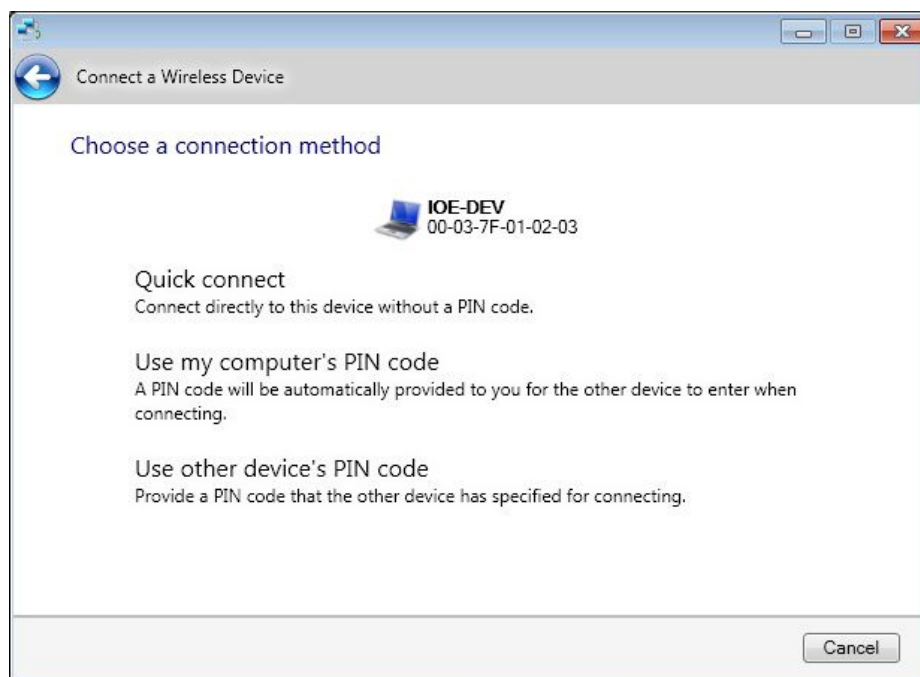
- Click the **Direct Connect** icon on the system tray. Then click **Connect new device**.



- Select **IOE DEV** and click **Next**.



4. Select **Quick Connect**.



5. On the GT202 development kit, type the command:
`wmiconfig --p2p auth <peer mac> push`
6. A four-way handshake success message indicates a successful connection.

3.2.2 GT202 development kit as P2P autonomous GO

The default SSID for the GT202 development kit is **DIRECT-iO**. The default passphrase is 1234567890. User can change the SSID and passphrase using the command:

```
wmiconfig --p2p passphrase <PASSPHRASE> <SSID>
```

<SSID> must be "DIRECT-<random><random>".

3.2.2.1 Peer device connecting to GT202 development kit

1. On the GT202 development kit, type the commands:
`wmiconfig --p2p on`
`wmiconfig --p2p autogo`
`wmiconfig --wps 0 push`
2. Click the **Direct Connect** icon on the system tray. Then click **Connect new device**.



Shenzhen Longsys Electronics Co.,Ltd www.Longsys.com

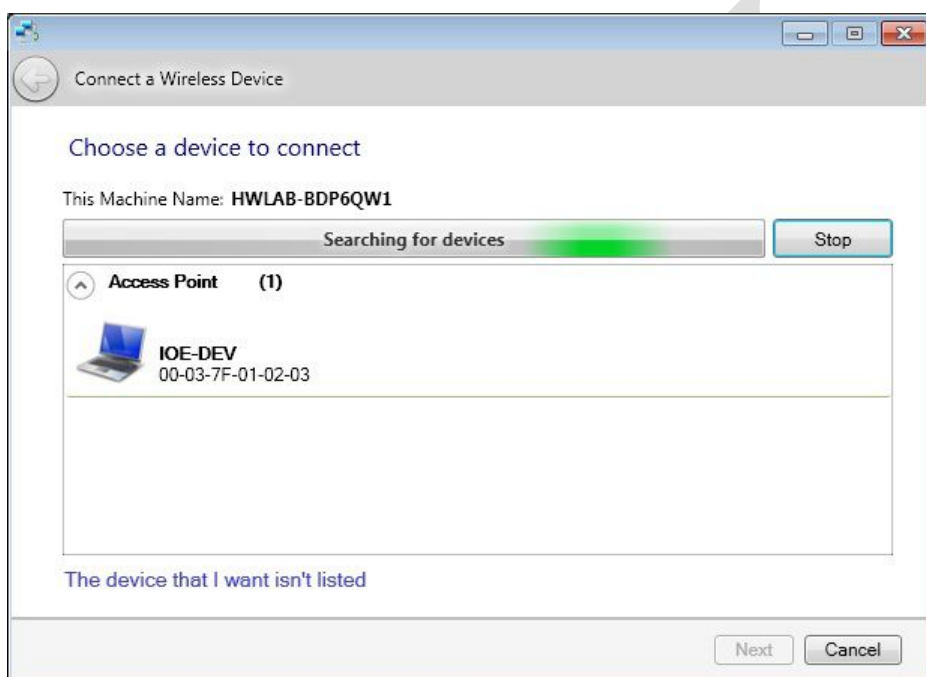
8/F, 1 Building. Finance Base, NO.8, KeFa Road, Shenzhen, China Tel: 86-755-86168848

10/F, CHINA AEROSPACE CENTRE,143 HOI BUN ROAD,HKTel: 852-23850111

GT202 Demo Applications User Guide 1.3



3. Select **IOE DEV** and click **Next**.



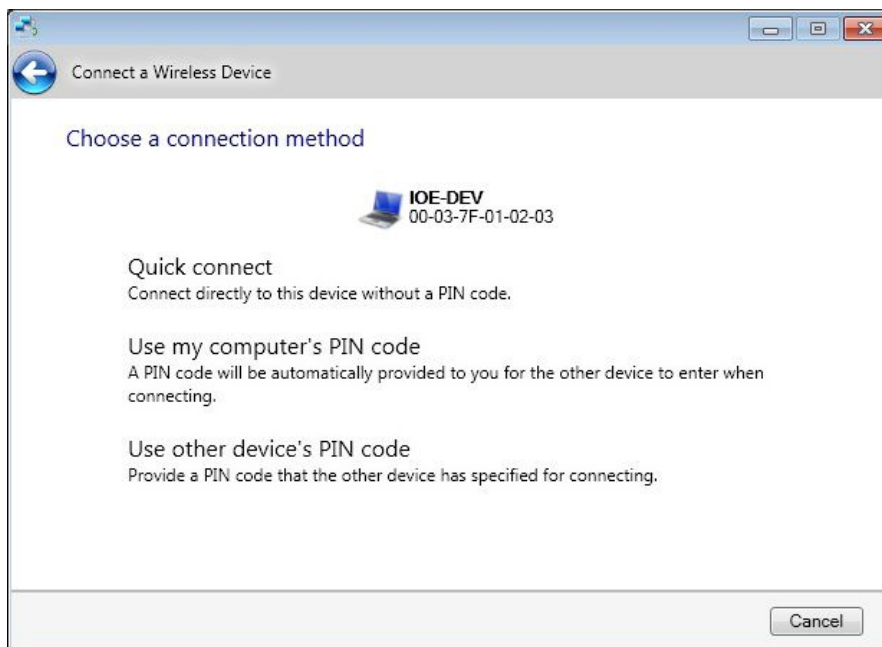
Shenzhen Longsys Electronics Co.,Ltd www.Longsys.com

8/F, 1 Building. Finance Base, NO.8, KeFa Road, Shenzhen, China Tel: 86-755-86168848

10/F, CHINA AEROSPACE CENTRE,143 HOI BUN ROAD,HKTel: 852-23850111

GT202 Demo Applications User Guide 1.3

4. Select Quick Connect.



5. A Connected message indicates a successful connection:

```
*****
IOT Config Tool
*****

shell> wmicongfig --p2p on
shell> wmicongfig --p2p find
shell> wmicofnig --p2p autogo
unknown cmd: wmicofnig

shell> wmicongfig --p2p autogo
Starting Autonomous GO

shell> connected
wmicongfig --wps 0 push

shell>
source addr : 2:3:7f:10:51:2c

wps_config_method : 80
Provisional Disc Request - Push Button
Connected
Not Connected

***** WPS PROFILE *****
DIRECT-io
SSID received DIRECT-io
Security type is WPA2, Encryption Type is AES
Passphrase 1234567890
Connected
```

NOTE: When the final connected message is printed, the peer device is assigned an IP address by DHCP server in the range of 192.168.1.xx. The default IP address for the GT202 development kit Auto GO is 192.168.1.10.



Shenzhen Longsys Electronics Co.,Ltd www.Longsys.com

8/F, 1 Building. Finance Base, NO.8, KeFa Road, Shenzhen, China Tel: 86-755-86168848

10/F, CHINA AEROSPACE CENTRE,143 HOI BUN ROAD,HKTel: 852-23850111

3.2.3 GT202 development kit as P2P GO

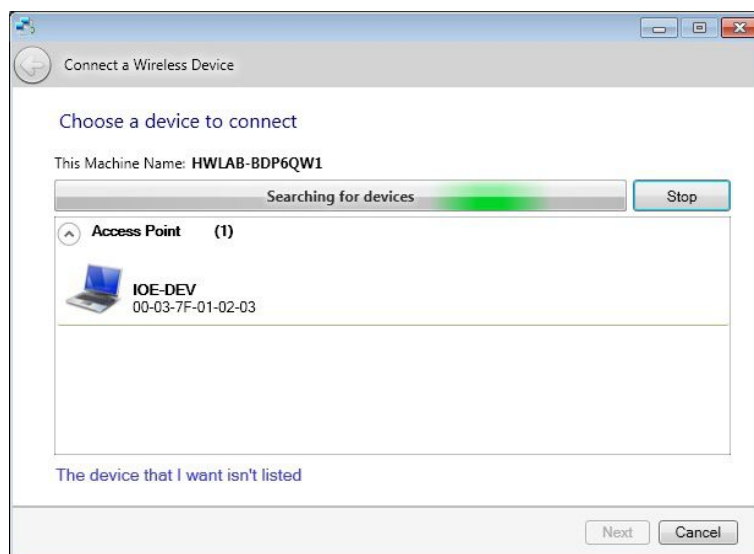
3.2.3.1 Peer device connecting to GT202 development kit

1. On the GT202 development kit, type the commands:
`wmiconfig --p2p on`
`wmiconfig --p2p setconfig 15 6 6 US 300`
`wmiconfig --p2p find`
`wmiconfig --p2p nodelist`
2. Click the **Direct Connect** icon on the system tray. Then click **Connect new device**.

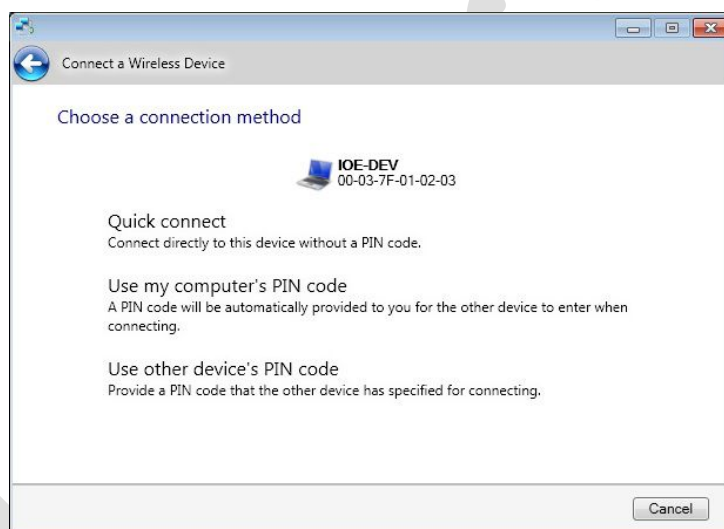


GT202 Demo Applications User Guide 1.3

3. Select **IOE DEV** and click **Next**.



4. Select Quick Connect.



GT202 Demo Applications User Guide 1.3

5. On the GT202 development kit, type the command:

```
wmiconfig --p2p auth <peer mac> push
```

A four-way handshake message indicates a successful connection.

```
*****
IOT Config Tool
*****

shell> wmiconfig --p2p on
shell> wmiconfig --p2p setconfig 15 6 6 US 300
shell> wmiconfig --p2p find
shell> wmiconfig --p2p nodelist
shell>
      p2p_device_name       : HWLAB-BDP6QW1
      p2p_interface_addr    : 0:0:0:0:0:0
      p2p_device_addr       : 2:3:7f:10:51:2c
      p2p_device_capability : 27
      p2p_group_capability  : 0

shell>
source addr : 2:3:7f:10:51:2c
dev_password_id : 4

shell> wmiconfig --p2p auth 02:03:7f:10:51:2c push
shell> P2P GO Negotion Result :
Status      :SUCCESS
P2P Role    :P2P GO
SSID        :DIRECT-aU
Channel     :2437
WPS Method  :PBC
Connected
Connected
```



Shenzhen Longsys Electronics Co.,Ltd www.Longsys.com

8/F, 1 Building. Finance Base, NO.8, KeFa Road, Shenzhen, China Tel: 86-755-86168848

10/F, CHINA AEROSPACE CENTRE,143 HOI BUN ROAD,HKTel: 852-23850111

3.3 Testing P2P connection using PIN method

The default WPS PIN of the GT202 development kit is 12345670. The following command can be used to change the WPS PIN. This demo uses the default WPS PIN.

```
wmicnfig --p2p wpspin <wps pin value>
```

3.3.1 GT202 development kit as P2P client

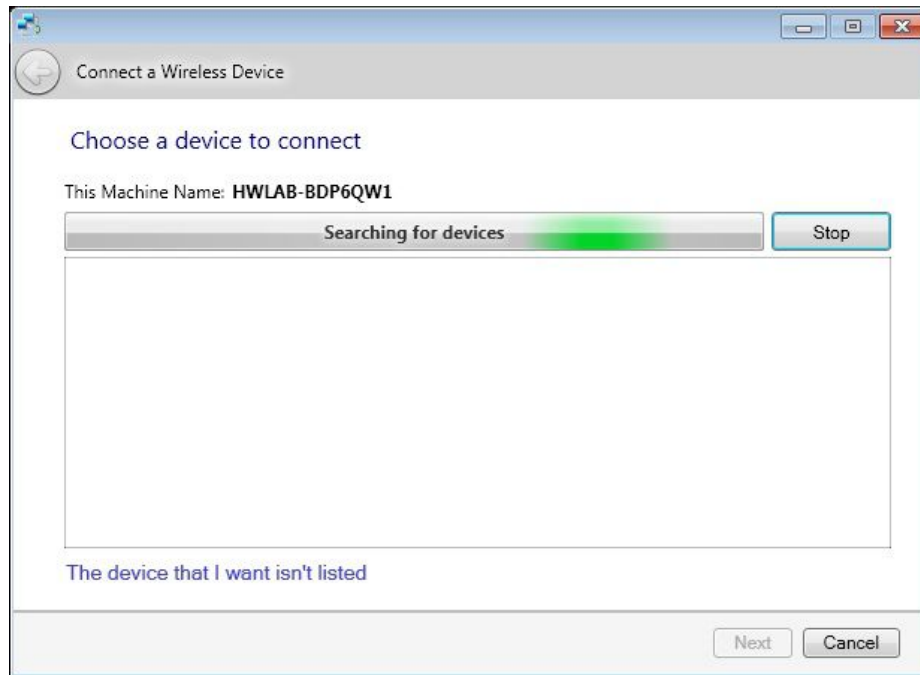
3.3.1.1 GT202 development kit connecting to peer device using Direct Connection PIN

1. Click the **Direct Connect** icon on the system tray. Then click **Connect new device**.



GT202 Demo Applications User Guide 1.3

The following window appears.

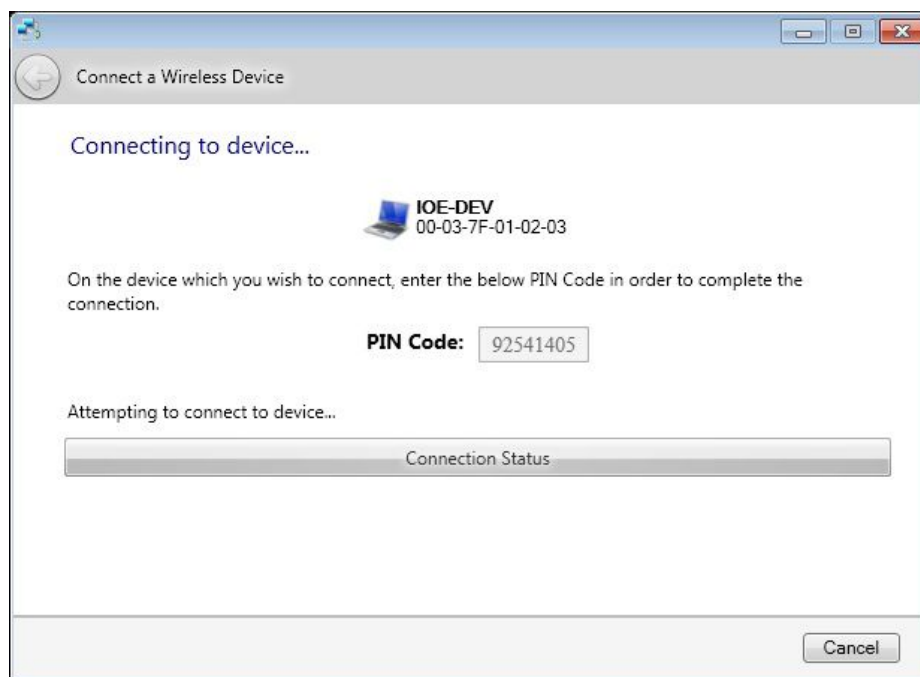


2. On the GT202 development kit, type the commands:

```
wmiconfig --p2p on  
wmiconfig --p2p find  
wmiconfig --p2p nodelist  
wmiconfig --P2P prov <peer mac> display
```

GT202 Demo Applications User Guide 1.3

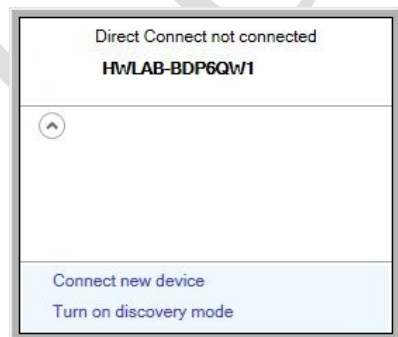
3. On the peer device, accept the connection from the GT202 development kit. The Direct Connect displays the PIN.



4. On the GT202 development kit, type the command.
`wmiconfig --P2P connect <peer mac> keypad <pin displayed in DC>`
5. A four-way handshake success message indicates a successful connection.

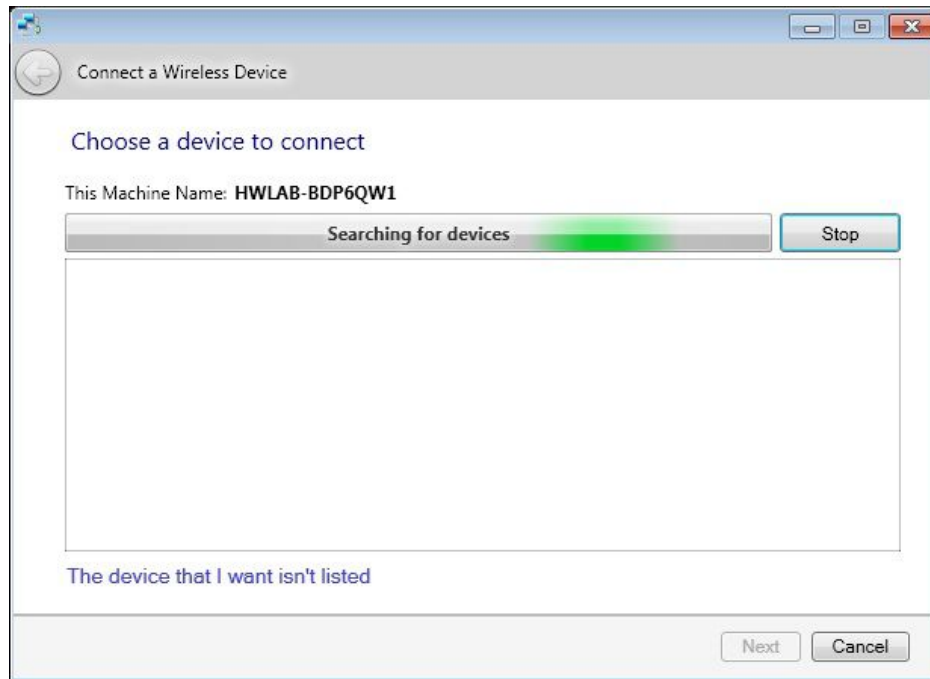
3.3.1.2 GT202 development kit connecting to peer device using GT202 development kit PIN

1. Click the **Direct Connect** icon on the system tray. Then click **Connect new device**.



GT202 Demo Applications User Guide 1.3

The following window appears:



2. On the GT202 development kit, type the commands:

```
wmiconfig --p2p on
```

```
wmiconfig --p2p find
```

```
wmiconfig --p2p nodelist
```

```
wmiconfig --p2p connect <peer mac> display
```

WPS PIN 12345670 is displayed at the GT202 development kit terminal.



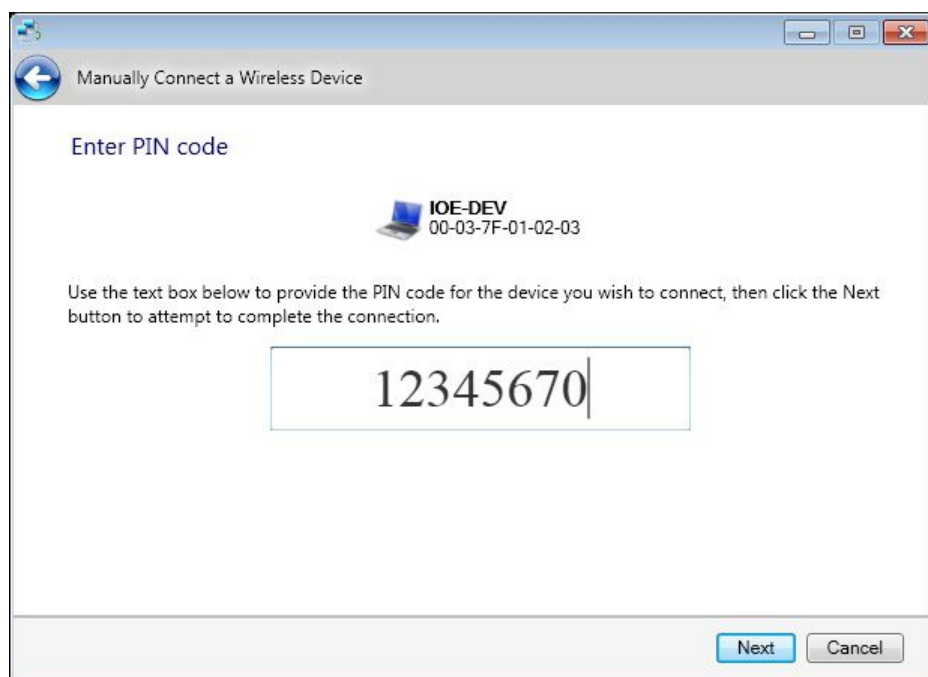
Shenzhen Longsys Electronics Co.,Ltd www.Longsys.com

8/F, 1 Building. Finance Base, NO.8, KeFa Road, Shenzhen, China Tel: 86-755-86168848

10/F, CHINA AEROSPACE CENTRE,143 HOI BUN ROAD,HKTel: 852-23850111

GT202 Demo Applications User Guide 1.3

3. On the peer device, accept and enter the WPS PIN displayed at GT202 development kit terminal and click **Next**.



4. A four-way handshake success message indicates a successful connection:

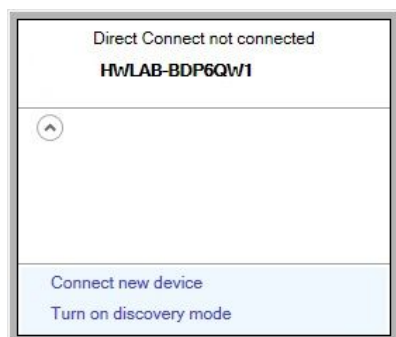
3.3.1.3 Peer device connecting to the GT202 development kit using peer device PIN

1. On the GT202 development kit, type the commands:

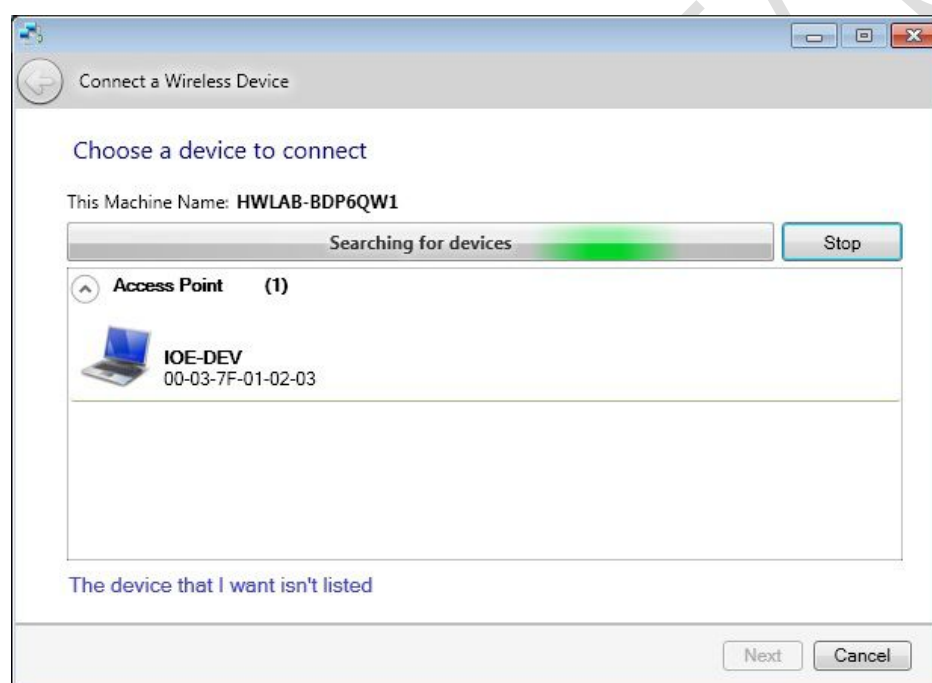
```
wmiconfig --p2p on  
wmiconfig --p2p find  
wmiconfig --p2p nodelist
```

GT202 Demo Applications User Guide 1.3

2. Click the **Direct Connect** icon on the system tray. Then click **Connect new device**.

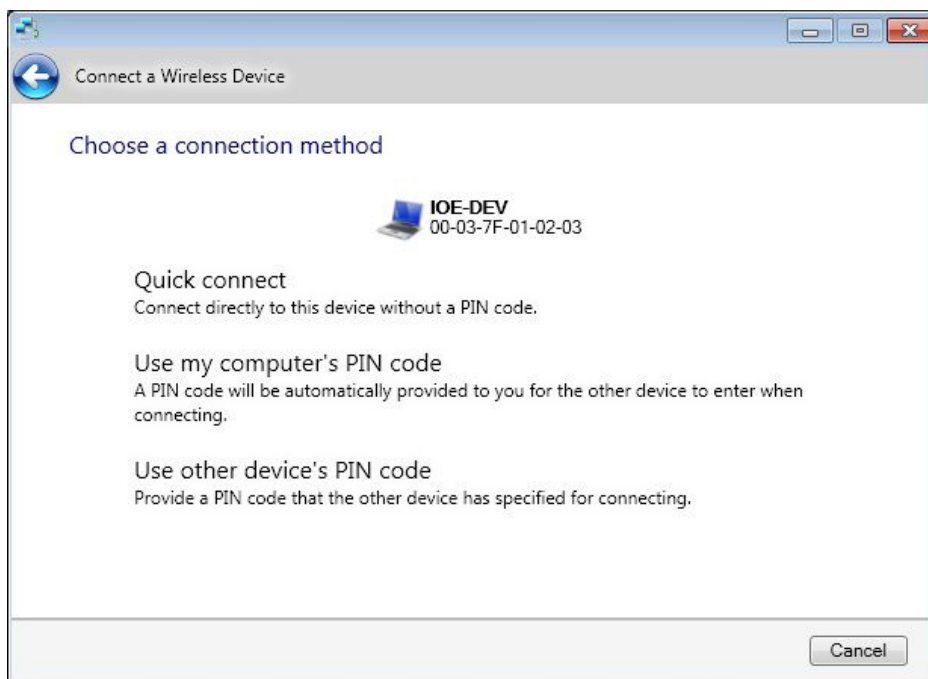


3. Select **IOE DEV** and click **Next**.

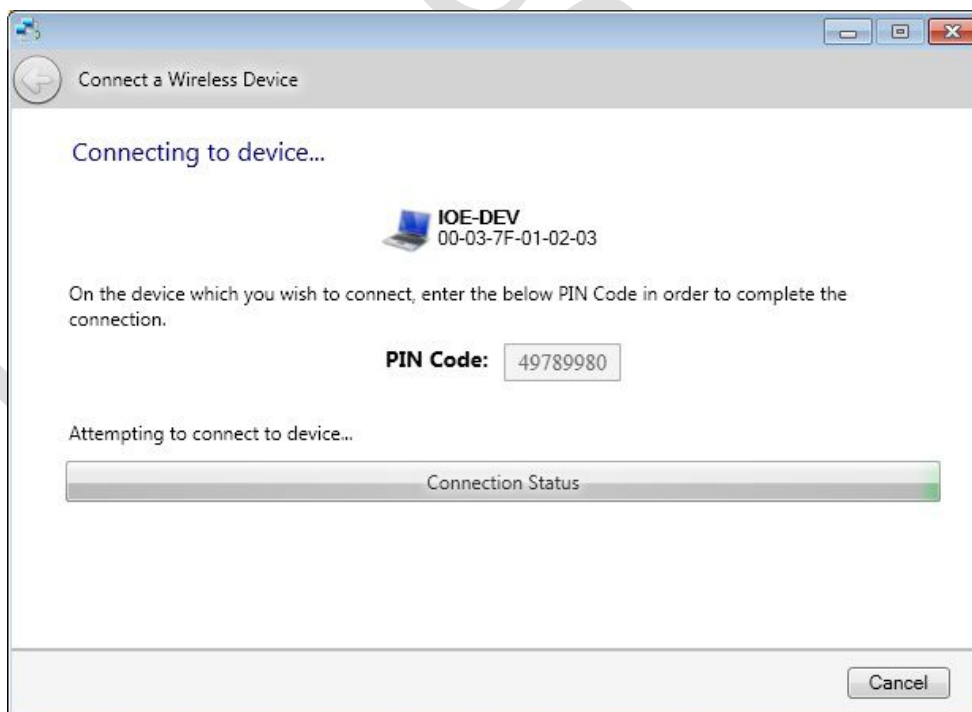


GT202 Demo Applications User Guide 1.3

4. Select **Use my computer's PIN code**.



5. The peer device displays the PIN.



Shenzhen Longsys Electronics Co.,Ltd www.Longsys.com

8/F, 1 Building. Finance Base, NO.8, KeFa Road, Shenzhen, China Tel: 86-755-86168848

10/F, CHINA AEROSPACE CENTRE,143 HOI BUN ROAD,HKTel: 852-23850111

GT202 Demo Applications User Guide 1.3

6. On the GT202 development kit, type the command:

```
wmiconfig --P2P connect <peer mac> keypad <PIN displayed in DC>
```

7. A four-way handshake success message indicates a successful connection:

```
*****
IOT Config Tool
*****

shell> wmiconfig --p2p on
shell> wmiconfig --p2p find
shell> wmiconfig --p2p nodelist
shell>
    p2p_device_name      : CHECBUP213663
    p2p_interface_addr   : 0:0:0:0:0:0
    p2p_device_addr      : 2:3:7f:10:51:e2
    p2p_device_capability : 27
    p2p_group_capability  : 0

shell>
    source addr : 2:3:7f:10:51:e2
    dev_password_id : 5

shell> wmiconfig --p2p connect 02:03:7f:10:51:e2 keypad 49799980
WPS Pin 49799980

    own MAC addr : 0:3:7f:a1:b2:c3
    Peer MAC addr : 2:3:7f:10:51:e2

shell> P2P GO Negotiation Result :
Status      :SUCCESS
P2P Role    :P2P Client
SSID        :DIRECT-18-CHECBUP213663
Channel     :2412
WPS Method  :PIN
Not Connected
Connected
4 way handshake success
```



Shenzhen Longsys Electronics Co.,Ltd www.Longsys.com

8/F, 1 Building. Finance Base, NO.8, KeFa Road, Shenzhen, China Tel: 86-755-86168848

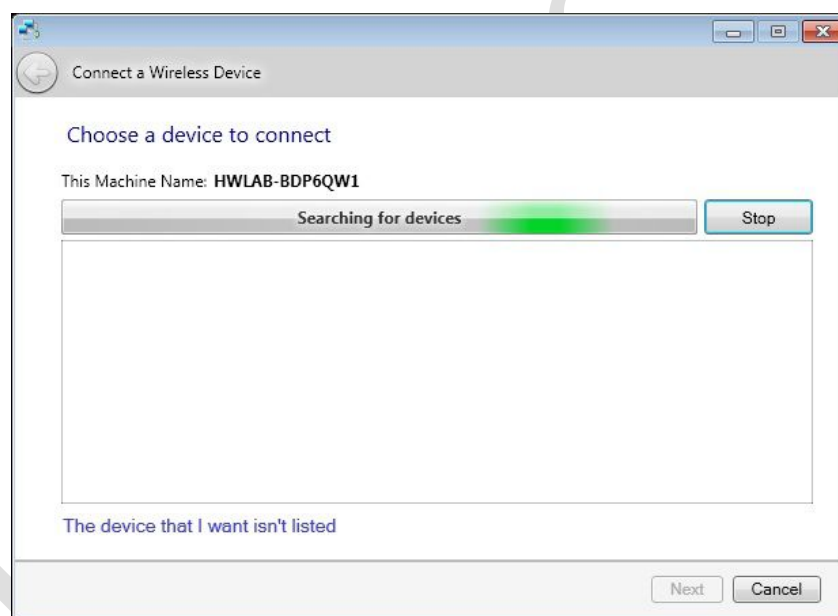
10/F, CHINA AEROSPACE CENTRE,143 HOI BUN ROAD,HKTel: 852-23850111

3.3.1.4 Peer device connecting to the GT202 development kit using GT202 development kit PIN

1. Click the **Direct Connect** icon on the system tray. Then click **Connect new device**.



The following window appears.



2. On the GT202 development kit, type these commands:

```
wmiconfig --p2p on
```

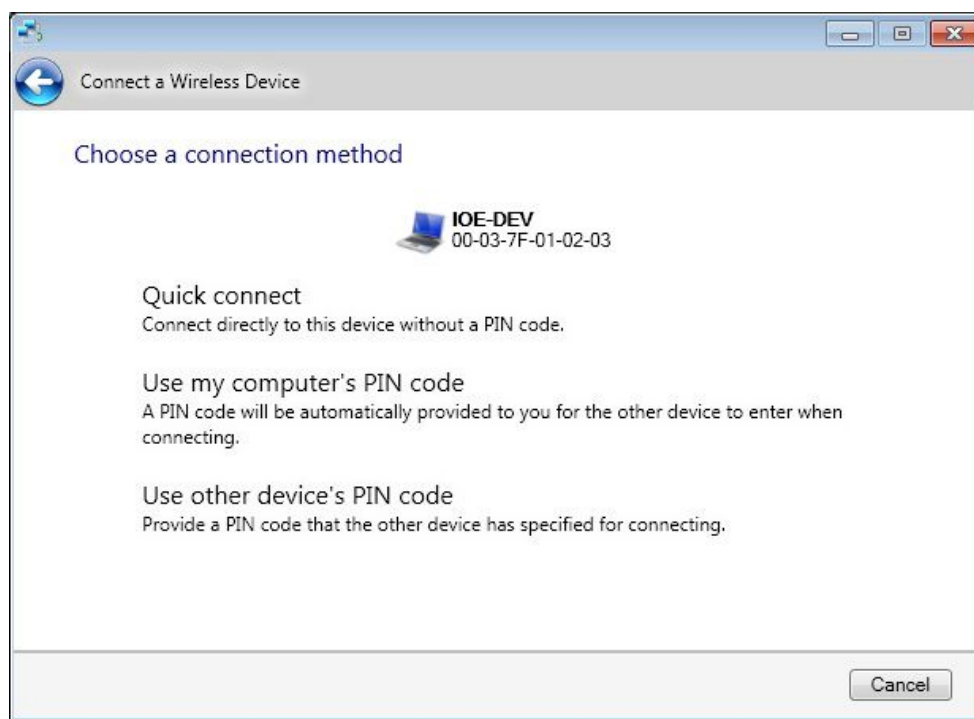
```
wmiconfig --p2p find
```

```
wmiconfig --p2p nodelist
```

```
wmiconfig --p2p auth <peer mac> display
```

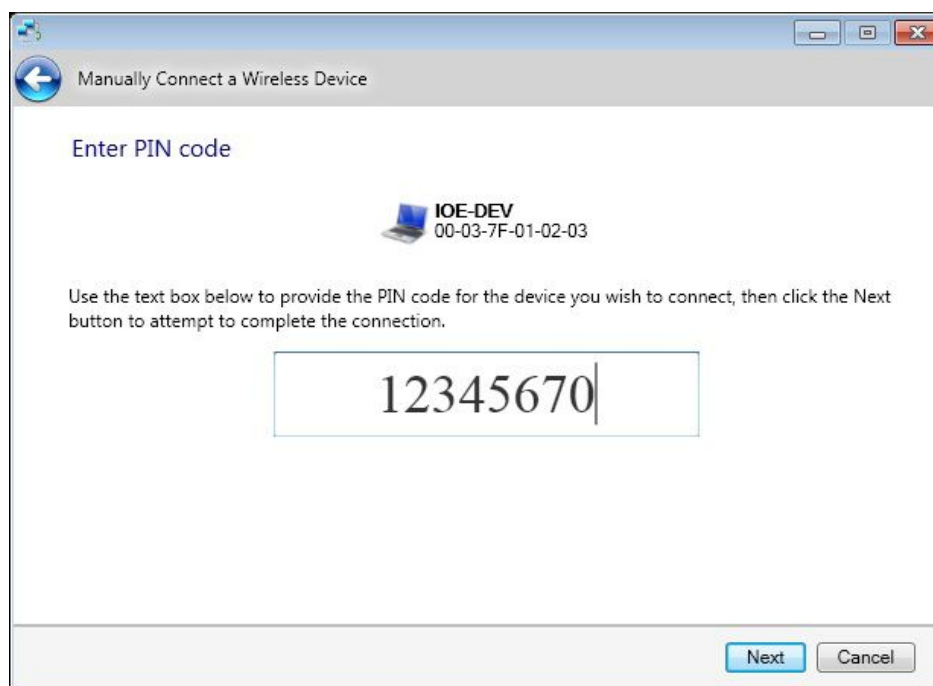
GT202 Demo Applications User Guide 1.3

3. Select **IOE DEV** and select **Use other device's PIN code**.



GT202 Demo Applications User Guide 1.3

4. Enter the PIN displayed at GT202 development kit terminal and click **Next**. A four-way handshake success message indicates a successful connection.



3.3.2 GT202 development kit as P2P autonomous GO

3.3.2.1 Peer device connecting to GT202 development kit

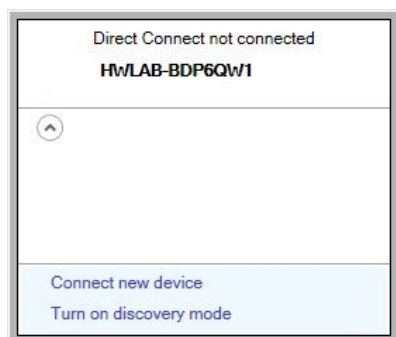
1. On the GT202 development kit, type the commands:

```
wmiconfig --p2p on
```

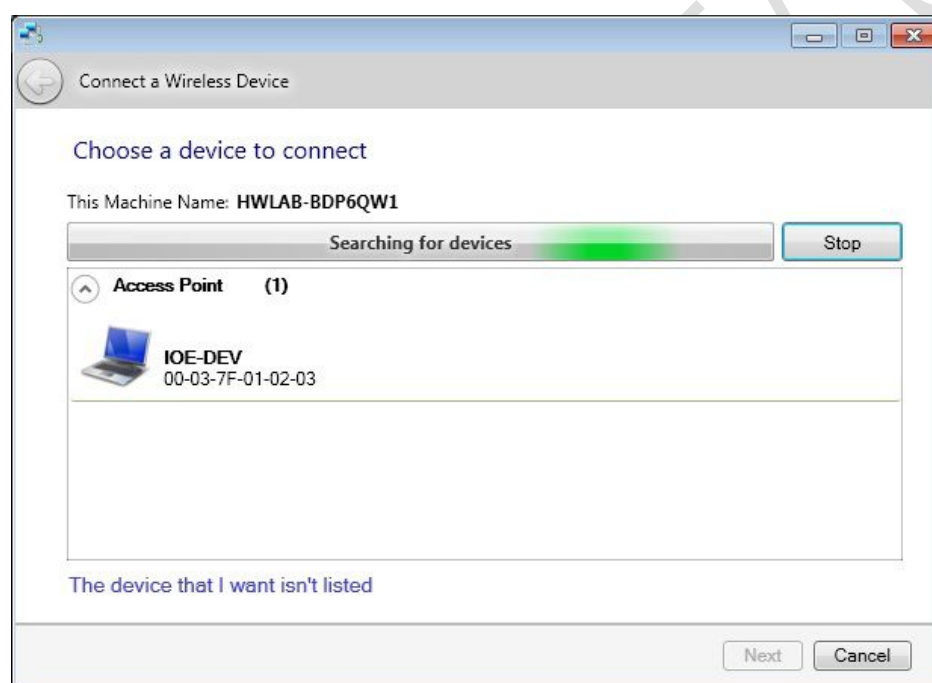
```
wmiconfig --p2p autogo
```

GT202 Demo Applications User Guide 1.3

2. Click the **Direct Connect** icon on the system tray. Then click **Connect new device**.

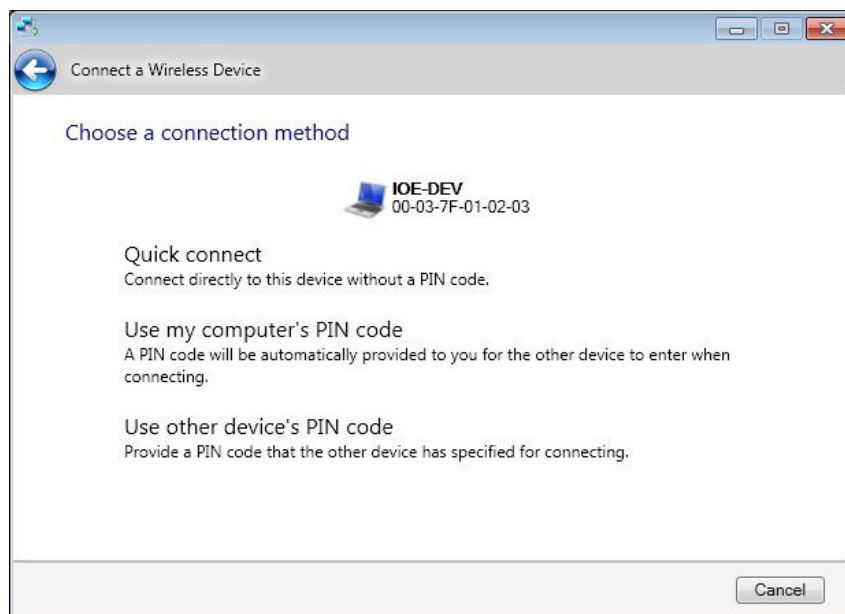


3. Select **IOE DEV** and click **Next**.

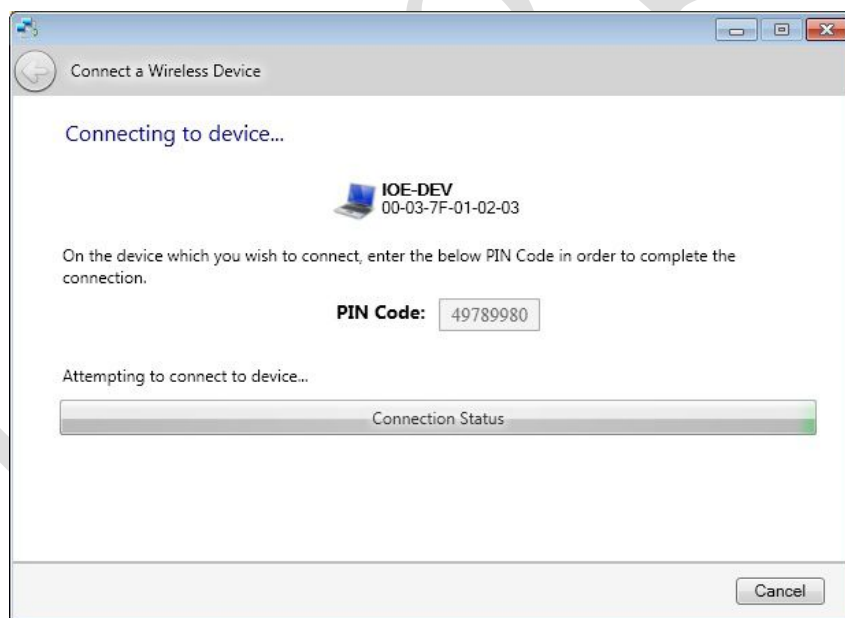


GT202 Demo Applications User Guide 1.3

4. Select **Use my computer's PIN code**.



5. The peer device displays the PIN.



6. On the GT202 development kit, type the command:
`wmiconfig --wps 0 pin <pin displayed in DC>`

A Connected message indicates a successful connection.