Summit Data Communications, Inc.
User's Guide for CF10G, PC10G, and MCF10G

Version 0.8

Table of Contents

1.0 Introduction

Thank you for choosing a compact flash (SDC-CF10G), PCMCIA (SDC-PC10G), or miniature compact flash (SDC-MCF10G) wireless LAN radio module from Summit Data Communications, Inc. This radio module, or WLAN client adapter, enables a computing device to communicate to a computing network using the IEEE 802.11g and IEEE 802.11b protocols.

The hardware components and software for all three radio modules are the same. The PC10G is a CF10G in a specially designed PCMCIA carrier, and the MCF10G is essentially a CF10G with a different layout and a different (Molex) connector.

1.1 Product Overview

For an overview of Summit WLAN radio modules, go to http://www.summitdatacom.com/products.htm.

1.2 This Manual

This manual is a user's guide for a Summit radio module that is installed or will be installed on a computing device that is running one of the following operating systems:

- Windows CE 4.2
- Windows Mobile 2003
- Windows CE 5.0
- Windows Mobile 5.0

The software for all three radio modules is the same. This manual may refer to any of the modules as the CF10G.

1.3 Security Capabilities

Summit radio modules typically are used in business-critical mobile devices that transmit sensitive information, such as inventory data and patient information, over the air that separates the mobile devices from the network. To protect transmitted data as well as the mobile devices and network infrastructure that transmit and receive the data, an organization's IT department often imposes on mobile devices the same strict security standards imposed on other client devices. Summit's integrated approach to security simplifies the task of enforcing a consistent security policy on all devices.

A foundational element of the IEEE 802.11i WLAN security standard is IEEE 802.1X, and a critical application on a mobile device is an 802.1X supplicant. Such a supplicant provides an interface between the radio and the operating system and supports the authentication and encryption elements required for 802.11i, also known as Wi-Fi Protected Access 2 or WPA2, as well as predecessors such as WPA and WEP. Summit software includes an integrated supplicant that supports a broad range of security capabilities, including:

- 802.1X authentication using pre-shared keys or an EAP type, required for WPA2 and WPA
- Data encryption and decryption using WPA2 AES, WPA TKIP, or WEP

The Summit supplicant supports the following EAP types:

- **EAP-TLS:** Uses the same technology as is a follow-on to Secure Socket Layer (SSL). It provides strong security, but relies on client certificates for user authentication.
- **PEAP:** Provides secure user authentication by using a TLS tunnel to encrypt EAP traffic. Two different inner methods are supported with PEAP:
  - EAP-MSCHAPV2, or PEAP-MSCHAP: This is appropriate for use against Windows Active Directory and domains

  - EAP-GTC, or PEAP-GTC: This is for authentication with one-time passwords (OTPs) against OTP databases such as SecureID
- **LEAP:** Is an authentication method for use with Cisco WLAN access points. LEAP does not require the use of server or client certificates. LEAP supports Windows Active Directory and domains but requires the use of strong passwords to avoid a vulnerability to offline dictionary attacks.
- **EAP-FAST:** Is a successor to LEAP and does not require strong passwords to protect against offline dictionary attacks. Like LEAP, EAP-FAST does not require the use of server or client certificates and supports Windows Active Directory and domains.

PEAP and EAP-TLS require the use of Windows facilities for the configuration of digital certificates.

1.4 Interacting with the Radio Module

The software that Summit provides for its radio modules includes:

- A device driver for the operating system running on the computing device that houses the radio module
- An integrated 802.1X supplicant, which is described in the previous section
- The Summit Client Utility (SCU), a configuration, monitoring, and management application designed for Summit radio modules

You can configure radio and security settings, monitor performance and activity, and troubleshoot issues with the radio module using any of the following:

- SCU
- Another application, such as Wavelink Avalanche, that uses the application programming interface (API) for SCU
- Native facilities in the operating system, such as Windows Zero Config (WZC)

This guide assumes that you are using SCU for all interactions with the radio module.

2.0 Getting Started

Before you can use the CF10G, PC10G, or MCF10G, you must install it in a computing device. Before you install the module, you will require the following items and information:

- A mobile computing device with:
  - An internal compact flash (CF) Type I or Type II slot, internal PCMCIA slot, or internal miniature CF slot
  - One or two internal antennas fitted with Hirose U.FL connectors
  - Microsoft Windows CE Version 4.2 or 5.0, Microsoft Windows Pocket PC 2003, or Windows Mobile Version 5.0
- Summit CF10G software, which is available from the Summit web site, www.summitdatacom.com
- The network name (SSID) of your wireless network

To make the radio module operational, you must perform the following four steps:

1. Install the Summit software
2. Install the radio module in your mobile computing (or host) device
3. Configure the manner of obtaining an IP address
4. Connect to your wireless network

It is recommended that you complete the steps in order. If you insert the card in your device before you install the software, then the "Found New Hardware Wizard" screen will appear, and you must select "**Cancel**" to cancel the Hardware Wizard.

2.1 Step 1: Install the Summit Software

a) Download the appropriate **SDC-CF10G "cab"** file for the type of device you are using. The "cab" file is the software equivalent of a "file cabinet" which contains the driver for the radio as well as the SCU (Summit Client Utility).
b) Copy the file to your device using a supported file transfer mechanism. Common methods of moving the file include:
   - Place the file on a supported Compact Flash or SD memory card and use that card for copying the file to the device
   - Use a program such as FTP or Microsoft ActiveSync
c) On the device, use the resident File Explorer program to locate the "cab" file
d) Run the "cab" file by single-clicking the file or by right-clicking and selecting "run"
e) If asked to replace any existing files on the device, answer "yes to all"

2.2 Step 2: Install the Radio Module in the Host Device

a) Insert the card into a CF or PCMCIA slot or, in the case of the MCF10G, attach the card's Molex connector to the corresponding Molex connector on the device's board
b) Connect the device's internal antenna or antennas to the card via the U.FL connector or connectors – If there is one antenna, connect it to the radio module's main connector, which is nearer to the right edge of the card

2.3 Step 3: Configure the Manner of Obtaining an IP Address

a) Select Programs, then Settings, then the Connections tab at the bottom of the Settings screen
b) Select Connections and then Advanced
c) On the Advanced Connections screen, select the Network Card button and then select the Summit WLAN Adapter from the list of available network devices

d) On the screen that appears, choose that a server will assign an IP address (using DHCP) or enter a specific IP address
e) If you select the Name Servers tab, you can statically configure DNS servers, but if you use DHCP for IP address assignment then DNS usually is supplied by the same server that hands out IP addresses

2.4 Step 4: Connect to Your WLAN

Two methods exist for configuring the radio module for operation on a wireless network. The first and preferred method is to use the Summit Client Utility (SCU). The other method is to use WZC, which is the Microsoft program for configuring any WLAN card.

2.4.1 Preferred Method: Use SCU

To use the SCU to connect to your wireless network, do the following:
a) From the Start menu, select Programs, then select the directory called Summit
b) Inside the Summit directory are two items: a directory for the storage of security certificates and the SCU. To run the SCU, double-click the SCU icon
c) Select the Admin Login button to have privileges to make changes to the configuration. The default password is "SUMMIT"
d) At the bottom of the screen are tabs for Main, Config, Status, Diags, and Global Settings. To create a new profile, select the Config tab
e) When the default configuration appears in the Config drop-down box, select the New button below the Config dialog box
f) When a pop-up screen prompts for a name, enter any alpha-numeric name to identify this configuration (as unique from other configurations or SSIDs on the device)
g) Tap the OK button to return to the Config tab
h) Tap the Commit button to save the configuration name
i) When a message pops up to indicate that this command has been saved, select OK on that pop-up to return to the Config tab
j) To configure the SSID for the network to which you wish to associate, enter an SSID in the text box to the right of "SSID", and select the Commit button and OK at the pop-up
k) To configure authentication and encryption, use the appropriate drop-down boxes on the lower half of the screen, and enter credentials for IEEE 802.1X EAP types or WEP keys just below the drop-down boxes (to view the security drop-down boxes, you may have to minimize the alpha-numeric keyboard provided by the operating system)
l) Configure any other settings that are dictated by the network administrator for the SSID to which you must associate, being sure to select Commit after each change
m) Select the Main tab
n) In the Active Config drop-down box will appear the newly created Config. Select this Config, and the Summit radio module will attempt to connect to the network using the following steps:
   - Associate to the SSID
   - Authenticate to the network
   - If EAP authentication is being used, derive dynamic encryption keys
   - If DHCP is being used by the network, obtain an IP address

To assist with troubleshooting of any connectivity issues, the Status tab reflects the current state of the device and the Diag tab allows for DHCP renewal and ICMP Echo Requests, also known as Pings, to be sent by the device.

2.4.2 Alternative: Use Windows Zero Config

Another method of configuring the radio module is through the operating system's WZC feature. If the radio module is inserted and the SCU is not configured, then WZC will attempt to use the card to attach to an available WLAN. A pop-up box will appear that indicates which networks (SSIDs) have been located and asks the user which network the device should use. Selecting an SSID that requires security will prompt the user for security keys or credentials. If the correct credentials are entered, then the WZC process will attempt to associate, authenticate, and run the appropriate encryption required to connect the user to the network.

3.0 Using the Summit Client Utility

The Summit Client Utility (SCU) is an application designed for end users and administrators of mobile devices that use a Summit radio module. Using SCU, an end user can view:

- The contents of profiles, each of which houses the RF, security, and other settings for the radio
- Global settings, which apply to every profile
- A snapshot status of the current wireless network connection
- More detailed status information on the radio, the AP to which it is connected, and the RF connection or link between the two
- In-depth diagnostic information on the connection and the radio, most likely to report it to an administrator when there is a connection or performance issue
- Other information on the radio, such as software versions and regulatory domain

After completing an administrator login to the utility, a user can perform these additional tasks:

- Turn the radio on and off
- Select the profile to be used
- Create, rename, edit, and delete profiles
- Alter global settings, which apply to every profile
- Perform various troubleshooting and diagnostic tests

The SCU provides a graphical user interface (GUI) for access to all of its functions. Access to these functions also is available through an application programming interface (API) that is provided to every Summit customer. A Summit customer can use the API to manage the radio from another utility, such as one that the customer provides with its mobile devices. Wavelink Avalanche also uses this API.

The SCU has five windows: Main, Config, Global Settings, Status, and Diags (or Troubleshooting). Tabs, which are shown as item 8 in Figure 1 below, enable easy navigation between windows. Each window is described in more detail in this section.

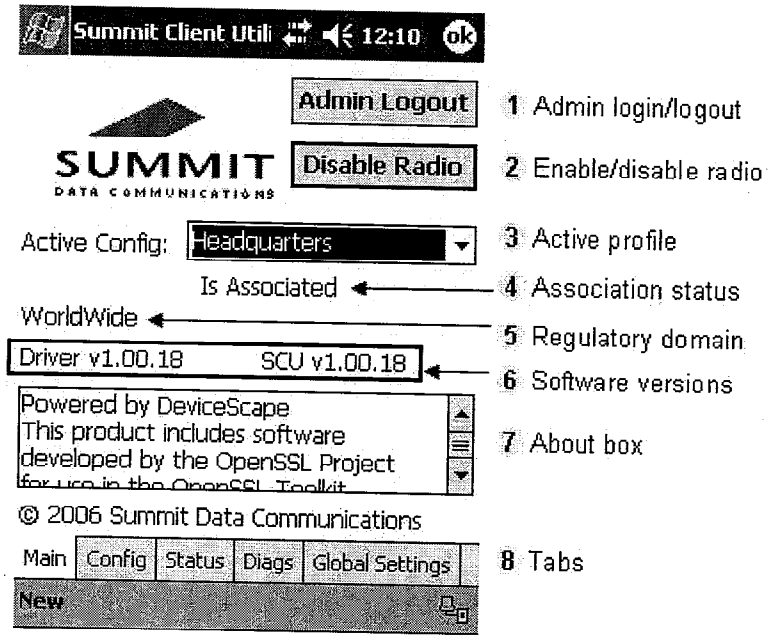

Figure1: Main window

3.1 Main Window

Figure 1 on the previous page is an example of a Main window. Here are the highlights:

1. **Admin login/logout:** To login to SCU as an administrator, you select this button when "Admin Login" is displayed and supply the correct admin password on the dialog box. The default password is "SUMMIT" in all capital letters. (The password can be changed through the Admin Password function on the Global Settings window.) Once you are logged in as an administrator, clicking the button again logs you out as an administrator, leaving you with access only to end-user functions.
2. **Enable/disable radio:** When the radio is enabled, selecting this button disables it; when the radio is disabled, selecting this button enables it.
3. **Active profile:** A user can view the name of the active profile. An administrator can use the selection list to select a different profile.
4. **Association status:** Indicates if the radio is associated to an access point and, if not, what the radio's status is.
5. **Regulatory domain:** Indicates the regulatory domain or domains for which the radio is configured. "Worldwide" means that the radio can be used in any domain. Domain cannot be configured by an administrator or user.
6. **Software versions:** Indicates the version of the device driver and the version of SCU that are running on the ASD.
7. **About box:** Supplies information on SCU that on a Windows application normally would appear under Help | About.

3.2 Config Window

Config settings are radio and security settings that are stored in the registry as part of a config, or profile. When a config is selected as the active config, the settings for that config become active. An administrator can define, change, and delete a config on the Config window in SCU.

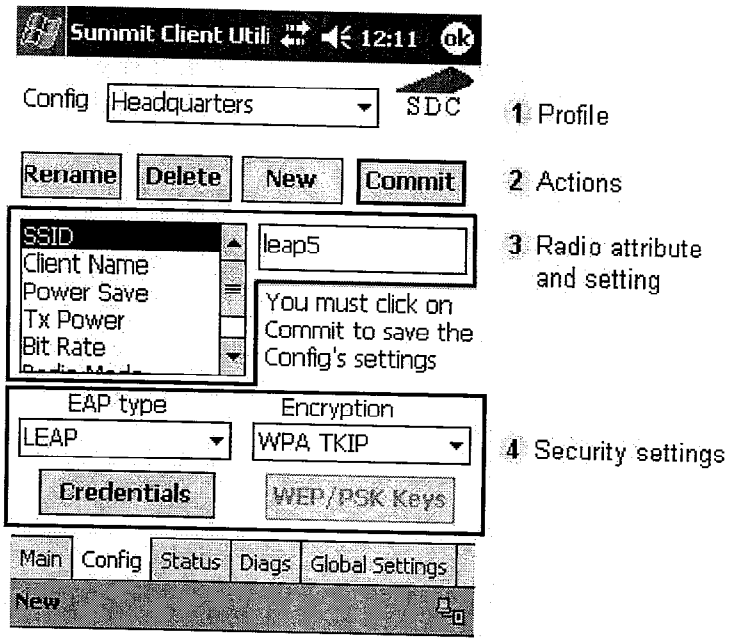

Figure 2: Config window

Figure 2 above is an example of a Config window. Here are the highlights:

- **Profile:** This is used to select the profile to be viewed or, if you are an administrator, edited.
- **Actions:** Four actions are available to an administrator:
  - Rename: Give the profile a new name, one that is not assigned to another profile
  - Delete: Delete the profile, provided that it is not the active profile
  - New: Create a new profile with default settings and give it a name (and then change settings using other selections on the window)
  - Commit: Ensure that changes to profile settings made on the window are saved in the profile
- **Radio attribute and setting:** Attributes in the list box can be selected individually. When an attribute is selected, the current setting or an appropriate selection box with the current setting highlighted appears on the right. For example, selecting SSID causes an edit box to appear; selecting transmit power causes SCU to display a drop-down list box with available settings.
- **Security settings:** The items at the bottom of the window enable the administrator to configure the settings for authentication and encryption.

The following table provides details for the settings that are available on the Config window:

Name on SCU Config Window	Description	Potential Value(s)	Default
Config	Name of config, or profile; can be changed through Rename function	A string of up to 32 characters	None
SSID	Service set identifier (SSID) for WLAN to which radio will connect	A string of up to 32 characters	None
Client Name	Name assigned Summit radio and client device that uses it	A string of up to 16 characters	None
Power Save	Power save mode for radio	• Off: Constantly awake mode, or CAM • Maximum: Maximum power savings • Fast: Fast power save mode	Fast
Tx Power	Maximum transmit power	• Max: Maximum defined for current regulatory domain – Required setting if Cisco AP is to define maximum transmit power for client • One of the following values in milliwatts (mW): 50, 30, 10, 1	Max
Bit Rate	Bit rate used by radio when interacting with WLAN access point (AP)	Auto (rate negotiated automatically with AP) or one of the following rates in megabits per second (Mbps): 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54	Auto
Radio Mode	Use of 802.11g and/or 802.11b when interacting with AP	B rates only, BG rates full, G rates only, BG LRS (B+G 24, 54)	BG rates full
Auth Type	802.11 authentication type, used when associating to AP	Open, shared-key, or Network EAP	Open
EAP	Extensible Authentication Protocol type used for 802.1X authentication to AP	None, LEAP, EAP-FAST, PEAP-MSCHAP, PEAP-GTC, EAP-TLS	None
Credentials	Authentication credentials for an EAP type such as PEAP-MSCHAP	• Username or Domain\Username (up to 64 characters) • Password (up to 64 characters) • CA Certificate Filename (if using an EAP type that requires a server certificate)	None
Encryption	Type of encryption (and decryption) used to protect transmitted data	Off, Manual WEP, Auto WEP (generated during EAP authentication), WPA-PSK, WPA-TKIP, WPA2-PSK, WPA2-TKIP, WPA2-AES, CCKM-TKIP, CCKM-AES	None

Name on SCU Config Window	Description	Potential Value(s)	Default
		• For Manual WEP: Up to four static WEP keys • For PSK: ASCII passphrase or hex PSK	

If the profile named "3rdPartyConfig" is selected as the active profile, then SCU passes control to Windows Zero Config for configuration of all radio and security settings for the radio module.

3.3 Global Settings Window

Global settings include:

- Radio and security settings that apply to all profiles
- Settings that apply to SCU itself

An administrator can define and change most global settings on the Global Settings window in SCU. A sample Global Settings window is shown in Figure 3.

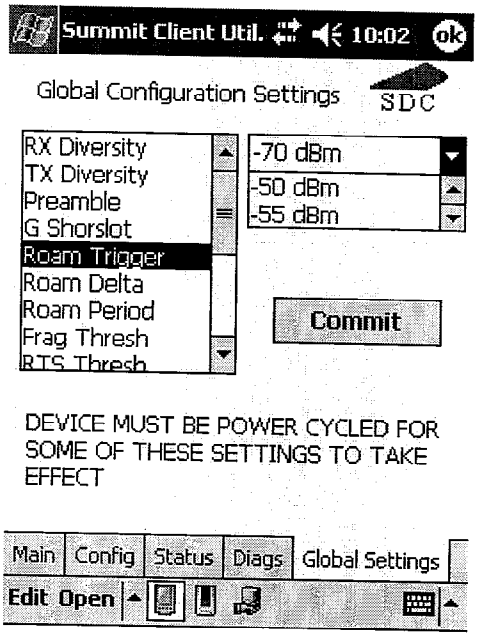

Figure 3: Global Settings window

The Global Settings listed in the table below can be changed in SCU:

Name on SCU Global Settings Window	Description	Potential Value(s)	Default
Rx Diversity	How to handle antenna diversity when receiving data from AP	• Main only: Use main antenna only • Aux only: Use auxiliary antenna only • On-Start on Main: On startup use main antenna • On-Start on Aux: On startup, use auxiliary antenna	On-Start on Main
Tx Diversity	How to handle antenna diversity when transmitting data to AP	• Main only: Use main antenna only • Aux only: Use auxiliary antenna only	On

Name on SCU Global Settings Window	Description	Potential Value(s)	Default
		• On: Use diversity	
Preamble	Type of radio preamble, or header[1]	Auto, short, long	Auto
G short slot	802.11g short slot timing mode[2]	Auto, off, on	Auto
Roam Trigger	If signal strength (RSSI) received from AP is less than trigger value, then radio will look for "better" AP	dBm: -50, -55, -60, -65, -70, -75	-70
Roam Delta	Amount by which second AP's RSSI must exceed current AP's RSSI before radio will attempt to roam to second AP	dBm: 5, 10, 15, 20, 25, 30, 35	15
Roam Period	How long RSSI scan data is collected before radio makes roaming decision	Seconds: 5, 10, 15, 20, 25, 30, 35, 40, 45, 50, 55, 60	10
Frag Threshold	If packet size (in bytes) exceeds threshold, then packet is fragmented	An integer from 256 to 2346	2346
RTS Threshold	Packet size above which RTS/CTS is required on link	An integer from 0 to 2347	2347
Ping Payload	Amount of data to be transmitted on a ping	Bytes: 32, 64, 128, 256, 512, 1024	32
Ping Timeout	Amount of time that transpires without a response before ping request is consider a failure	Milliseconds (ms): Specified value	5000
Ping Delay	Amount of time between successive ping requests	Milliseconds (ms): Specified value	1000
LED	Available only with MCF10G	On, off	Off
Hide Passwords	If on, SCU masks passwords	On, off	Off
Admin Password	Password that must be specified when Admin Login button pressed	A string of up to 64 characters	SUMMIT
Certs Path	Directory where certificate(s) for EAP authentication are housed	A valid directory path of up to 64 characters	Depends on device

A few global settings can be defined or set only through a separate utility such as the Summit Manufacturing Utility, which is made available only to device manufacturers and not to their customers. These global settings are listed in the table below:

Description	Potential Value(s)	Default
Regulatory domain for radio	FCC, ETSI, TELEC, Worldwide	Worldwide
Bluetooth coexistence	On, off	Off
Administrative override		
Maximum transmit power: For a radio that will be used with high-gain antennas		
WEP key length	Not set, 40 bits, 128 bits	
FCC test	Off, Transmit, Receive, Frequency	
Test channel		
Test rate: Bit rate		
Test power	0-100%	

[1] See http://www.cisco.com/univercd/cc/td/doc/product/wireless/airo1100/accsspts/i12213ja/i12213sc/s13rf.htm#wp1037656

[2] See http://www.cisco.com/univercd/cc/td/doc/product/wireless/airo1100/accsspts/i12213ja/i12213sc/s13rf.htm#wp1044425

Description	Potential Value(s)	Default
Transmit Test Timeout: Number of seconds	An integer of up to 59999; 60000 means no timeout	

3.4 Status Window

The Status window provides status information on the radio. Status items include IP address and MAC address for the client radio, IP address and MAC address for the AP, signal strength, channel, transmit power, and data rate. A sample Status window is shown in Figure 4.

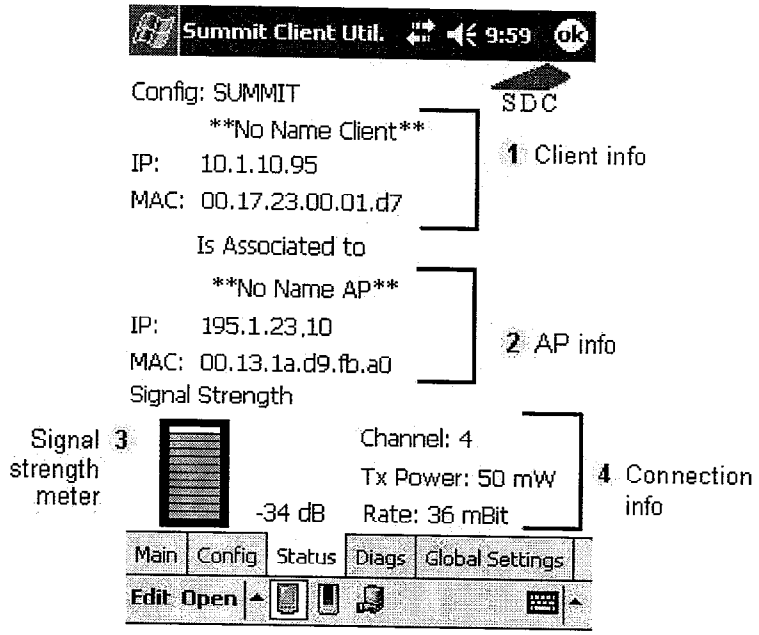

Figure 4: Status window

Here are the highlights:

1. Client info: Name of active config, client name, client IP address, and client MAC address
2. AP info: AP name, AP IP address, and AP MAC address
3. Signal strength, shown both graphically and numerically
4. Other connection info: Channel, transmit power, and bit rate

A few status items are shown on the Main window. Those items are:

- Card state: Down (not recognized), Not Associated, or Associated
- SCU software version
- Driver software version
- Regulatory domain for radio: FCC, ETSI, TELEC, or Worldwide

3.5 Diags Window

A sample Diags, or troubleshooting, window is shown in Figure 5 on the next page. Here are the functions available on the Diags window:

- (Re)connect: Disable and enable the radio, apply or reapply the current profile, and attempt to associate and authenticate to the wireless LAN, logging all activity in the output area at the bottom.

- Release/Renew: Obtain a new IP address through DHCP release/renew, and log all activity in the output area at the bottom.
- Start Ping: Start a continuous ping to the address in the edit box next to it. Once the button is clicked, its name and function will change to Stop Ping. Leaving the Diags window also will stop the ping, as will pressing any other button on the screen.
- Diagnostics: Attempt to (re)connect to an AP, and provide a more thorough dump of data than is obtained with (Re)connect. The dump will include radio state, profile settings, global settings, and a BSSID list of APs in the area.
- Upd. Driver: Update the driver via a dialog and power cycle.
- Site Survey: Launch a separate site survey utility (not yet available).

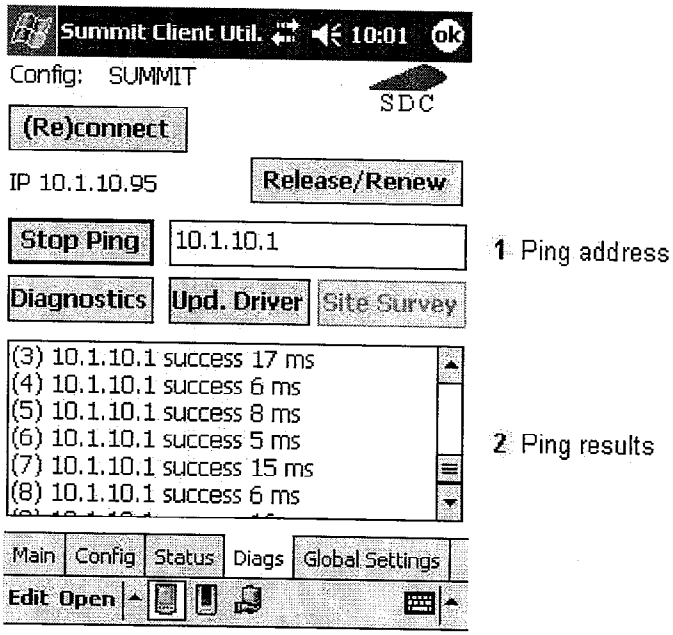

Figure 5: Diags window, with ping active

Appendix: FCC Information

All declarations and instructions for the SDC-CF10G apply to the SDC-PC10G, because the PC10G is a CF10G in a specially designed PCMCIA carrier.

Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

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

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

IMPORTANT NOTE:
FCC Radiation Exposure Statement:
This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.
This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

This device is intended only for OEM integrators under the following conditions:

1) The antenna must be installed such that 20 cm is maintained between the antenna and users;
2) The transmitter module may not be co-located with any other transmitter or antenna; and
3) For all products marketed in the United States, OEM must limit the operating channels to channel 1 through channel 11 for the 2.4 GHz band by using the supplied Summit Manufacturing Utility. OEM shall not supply to its customers (end users) the Summit Manufacturing Utility or any tool or info that will enable an end user to change the regulatory domain or the operating channels for the radio.

As long as the three conditions above are met, further transmitter test will not be required. However, the OEM integrator is still responsible for testing their end-product for any additional compliance requirements required with this module installed (for example, digital device emissions, PC peripheral requirements, etc.).

IMPORTANT NOTE: In the event that these conditions can not be met (for example certain laptop configurations or co-location with another transmitter), then the FCC authorization is no longer considered valid and the FCC ID can not be used on the final product. In these circumstances, the OEM

integrator will be responsible for re-evaluating the end product (including the transmitter) and obtaining a separate FCC authorization.

End Product Labeling

This transmitter module is authorized only for use in device where the antenna may be installed such that 20 cm may be maintained between the antenna and users (for example : Mobile Data Terminals (MDTs), Vehicle Mounted Devices (VMDs)... etc.). The final end product must be labeled in a visible area with the following: "Contains TX FCC ID: TWG-SDMCF10G".

Manual Information That Must be Included

The OEM integrator has to be aware not to provide information to the end user regarding how to install or remove this RF module in the users manual of the end product which integrate this module.

The users manual for OEM integrators must include the following information in a prominent location: IMPORTANT NOTE: To comply with FCC RF exposure compliance requirements, the antenna used for this transmitter must be installed to provide a separation distance of at least 20 cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter.

Summit declares that US model of SDC-MCF10G (FCC ID: TWG-SDMCF10G) is limited in CH1-CH11 for 2.4G band by specific firmware controlled by the manufacturer and is not user changeable.