Quick Installation Guide

C225E0-A1

Wireless PCI Express with Integrated Bluetooth 2.1/3.0/4.0 MiniPCIE Module

802.11a/b/g/n

Version 1.0

Aug 18, 2015

Hardware installation

This Hardware Installation provides you with basic instructions only.

The following instructions will guide you through overall installation procedure.

System Requirements

Laptop/ PC containing:
32-bit PCI Express Bus
32 MB memory or greater
300 MHz processor or higher
Microsoft Windows 10,Windows8.1, Windwos7

Step 1: Remove the system case and put Wireless module in your system.
Note: Make sure your system interface has Half Mini Card slot.

Installing wireless driver

Profile Management

Configure the wireless network adapter (wireless card) from the Profile Management tab of the Atheros Client Utility.
Add a profile
Edit a profile
Import a Profile
Export a Profile
Order profiles
Switch to a different profile
Remove a profile
Connect to a Different
Network
The wireless network adapter works in either infrastructure mode (which uses an access point) or ad hoc mode (a group of stations participating in the wireless LAN).

Create or Modify a Configuration Profile

To add a new configuration profile, click New on the Profile Management tab. To modify a configuration profile, select the configuration from the Profile list and click the Modify button.
The Profile Management dialog box displays the General tab. In profile management:
Edit the General tab.
Edit the Security tab.
Edit the Advanced tab.
To configure a profile for ad hoc or access point (infrastructure) mode, edit the Network Type field on the Advanced tab.
Note that the ACU only allows the creation of 16 configuration profiles. After the creation of 16 profiles, clicking the New button displays an error message. Remove an old profile or modify an existing profile for a new use.

Remove a Configuration Profile

1. Go to the Profile Management tab.
2. Select the profile to remove from the list of configuration profiles.

3. Click the Remove button.

Auto Profile Selection Management
Including a profile in the auto selection feature allows the wireless adapter to automatically select that profile from the list of profiles and use it to connect to the network.

Including a profile in auto profile selection:
1. On the Profile Management tab, click the Order Profiles button.
2. The Auto Profile Selection Management window appears, with a list of all created profiles in the Available Profiles box.
3. Highlight the profiles to add to auto profile selection, then click Add. The profiles appear in the Auto Selected Profiles box.

Ordering the auto selected profiles:
1. Highlight a profile in the Auto Selected Profiles box.
2. Click Move Up, Move Down, or Remove as appropriate. The first profile in the Auto Selected Profiles box has highest priority, and the last profile has lowest priority.
3. Click OK.
4. Check the Auto Select Profiles box.
5. Save the modified configuration file.

When auto profile selection is enabled by checking Auto Select Profiles on the Profile Management tab, the adapter scans for an available network. The profile with the highest priority and the same SSID as one of the found networks is the one that is used to connect to the network. If the connection fails, the adapter tries the next highest priority profile that matches the SSID, and so on.

With auto profile selection enabled, the wireless adapter scans for available networks. The highest priority profile with the same SSID as a found network is used to connect to the network. On a failed connection, the adapter tries with the next highest priority profile.

Remove a Configuration Profile
1. Go to the Profile Management tab.
2. Select the profile to remove from the list of configuration profiles.
3. Click the Remove button.

Auto Profile Selection Management
Including a profile in the auto selection feature allows the wireless adapter to automatically select that profile from the list of profiles and use it to connect to the network.

Including a profile in auto profile selection:
1. On the Profile Management tab, click the Order Profiles button.
2. The Auto Profile Selection Management window appears, with a list of all created profiles in the Available Profiles box.
3. Highlight the profiles to add to auto profile selection, then click Add. The profiles appear in the Auto Selected Profiles box.

Ordering the auto selected profiles:

1. Highlight a profile in the Auto Selected Profiles box.
2. Click Move Up, Move Down, or Remove as appropriate. The first profile in the Auto Selected Profiles box has highest priority, and the last profile has lowest priority.
3. Click OK.
4. Check the Auto Select Profiles box.
5. Save the modified configuration file.

When auto profile selection is enabled by checking Auto Select Profiles on the Profile Management tab, the adapter scans for an available network. The profile with the highest priority and the same SSID as one of the found networks is the one that is used to connect to the network. If the connection fails, the adapter tries the next highest priority profile that matches the SSID, and so on.

With auto profile selection enabled, the wireless adapter scans for available networks. The highest priority profile with the same SSID as a found network is used to connect to the network. On a failed connection, the adapter tries with the next highest priority profile.

General Tab

In the Atheros Client Utility, access the General tab by clicking New or Modify on the Profile Management tab. Edit the fields in the General tab to configure the configuration profile. Make sure to also edit the Security and Advanced tabs.

Profile Name Identifies the configuration profile. This name must be unique. Profile names are not case sensitive.

Client Name Identifies the client machine.

Network Names (SSIDs) The IEEE 802.11 wireless network name. This field has a maximum limit of 32 characters.
Configure up to three SSIDs (SSID1, SSID2, and SSID3).

Advanced Tab

In the Atheros Client Utility, access the Advanced tab by clicking New or Modify on the Profile Management tab, then clicking the Advanced tab in Profile Management. Edit the fields in the Advanced tab of Profile Management to configure the profile.

Transmit Power Level

Selects the transmit power level in mW. Actual transmit power may be limited by hardware.

Power Save Mode

Specify:

Maximum mode causes the access point to buffer incoming messages for the wireless adapter. The adapter periodically polls the access point to see if any messages are waiting.

Normal uses maximum when retrieving a large number of packets, then switches back to power save mode after retrieving the packets.

Off turns power saving off, thus powering up the wireless adapter continuously for a short message response time.

Network Type Specifies the network as either infrastructure or ad hoc.

802.11b
Preamble

Specifies the preamble setting in 802.11b. The default setting is Short & Long (access point mode), which allows both short and long headers in the 802.11b frames. The adapter can only use short radio headers if the access point supports and uses them. Set to Long Only to override allowing short frames.

Authentication
Mode

Select the mode the wireless adapter uses to authenticate to an AP:
Auto causes the adapter to attempt authentication using shared, but switches it to open authentication if shared fails.
Open enables an adapter to attempt authentication regardless of its WEP settings. It will only associate with the access point if the WEP keys on both the adapter and the access point match.
Shared only allows the adapter to associate with access points that have the same WEP key.
For infrastructure (access point) networks, click the Preferred APs button to specify up to four access points to which the adapter should attempt to associate.

Security Tab

In the Atheros Client Utility, access the Security tab by clicking New or Modify on the Profile Management tab. Click the Security tab in the Profile Management window.
Edit the fields in the Security tab of Profile Management to configure the profile. To define the security mode, select the radio button of the desired security mode. Make sure to also edit the General and Advanced tabs.

WPA/WPA2 Enables the use of Wi-Fi Protected Access (WPA).
Choosing WPA/WPA2 opens the WPA/WPA2 EAP drop-down menu. The options include:
EAP-FAST
EAP-TLS
EAP-TTLS
PEAP (EAP-GTC)
PEAP (EAP-MSCHAP V2)
LEAP

WPA/WPA2
Passphrase

Enables WPA/WPA2 Passphrase security. Click on the Configure button and fill in the WPA/WPA2 Passphrase.

802.1x Enables 802.1x security. This option requires IT administration.
Choosing 802.1x opens the 802.1x EAP type drop-down menu. The options include:
EAP-FAST
EAP-TLS
EAP-TTLS

PEAP (EAP-GTC)
PEAP (EAP-MSCHAP V2)
LEAP
If the access point that the wireless adapter is associating to has WEP set to Optional and the client has WEP enabled, make sure that Allow Association to Mixed Cells is checked on the Security Tab to allow association. **Note:** If the Lock checkbox is checked, you cannot change any values in this profile. See your system administrator.

Pre-Shared Key
(Static WEP)
Enables the use of pre-shared keys that are defined on both the access point and the station.
To define pre-shared encryption keys, choose the Pre-Shared Key radio button and click the Configure button to fill in the Define Pre Shared Keys window.
If the access point that the wireless adapter is associating to has WEP set to Optional and the client has WEP enabled, make sure that Allow Association to Mixed Cells is checked on the Security Tab to allow association.

None No security (not recommended).

Using EAP-TLS Security

To use EAP-TLS security In the Atheros Client Utility, access the Security tab in the Profile Management window.
1. On the Security tab, choose the WPA radio button.
OR: On the Security tab, choose the 802.1x radio button.
2. Choose EAP-TLS from the drop-down menu.

Enabling EAP-TLS security:

To use EAP-TLS security, the machine must already have the EAP-TLS certificates downloaded onto it. Check with the IT manager.
1. If EAP-TLS is supported, choose EAP-TLS from the drop-down menu on the right, then click the Configure button.
2. Select the appropriate certificate authority from the list. The server/domain name and the login name are filled in automatically from the certificate information. Click OK.
3. Click OK.
4. Activate the profile.

Using EAP-TTLS Security

To use EAP security In the Atheros Client Utility, access the Security tab in the Profile Management window.
1. On the Security tab, choose the WPA/WPA2 radio button.
OR: On the Security tab, choose the 802.1x radio button.
2. Choose EAP-TTLS from the drop-down menu.

Enabling EAP-TTLS security:

To use EAP-TTLS security, the machine must already have the EAP-TTLS certificates

downloaded onto it. Check with the IT manager.
1. If EAP-TTLS is supported, choose EAP-TTLS from the drop-down menu on the right then click the Configure button.
2. Select the appropriate certificate from the drop-down list and click OK.
3. Specify a user name for EAP authentication:
Check Use Windows User Name to use the Windows user name as the EAP user name.
OR: Enter an EAP user name in the User Name field to use a separate user name and password and start the EAP authentication process.
4. Click Advanced and:
Leave the server name field blank for the client to accept a certificate from any server with a certificate signed by the authority listed in the Network Certificate Authority drop-down list. (recommended)
Enter the domain name of the server from which the client will accept a certificate.
Change the login name if needed.
5. Click OK.
6. Enable the profile.

Using PEAP (EAP-GTC) Security

To use PEAP (EAP-GTC) security In the Atheros Client Utility, access the Security tab in the Profile Management window.
1. On the Security tab, choose the WPA radio button.
OR: On the Security tab, choose the 802.1x radio button.
2. Choose PEAP (EAP-GTC) from the drop-down menu.
To use PEAP (EAP-GTC) security, the server must have WPA-PEAP certificates, and the server properties must already be set. Check with the IT manager.
1. Click the Configure button.
2. To avoid the need to log on again after resuming operation (for example, after your computer goes into standby or hibernate mode), check Always Resume the Secure Session.
3. Select the appropriate network certificate authority from the drop-down list.
4. Specify a user name for inner PEAP tunnel authentication:
Check Use Windows User Name to use the Windows user name as the PEAP user name.
OR: Enter a PEAP user name in the User Name field to use a separate user name and start the PEAP authentication process.
5. Choose Token or Static Password, depending on the user database.
Note that Token uses a hardware token device or the Secure Computing SofToken program (version 1.3 or later) to obtain and enter a one-time password during authentication.
6. Click Settings... and:
Leave the server name field blank for the client to accept a certificate from any server with a certificate signed by the authority listed in the Network Certificate Authority drop-down list. (recommended)
Enter the domain name of the server from which the client will accept a certificate.
The login name used for PEAP tunnel authentication fills in automatically as PEAP-xxxxxxxxxxxx, where xxxxxxxxxxxx is the computer's MAC address. Change the login name if needed.

7. Click OK.
8. Enable the profile.

Using PEAP-MSCHAP V2 Security

To use PEAP-MSCHAP V2 security In the Atheros Client Utility, access the Security tab in the Profile Management window.
1. On the Security tab, choose the WPA radio button.
OR: On the Security tab, choose the 802.1x radio button.
2. Choose PEAP (EAP-MSCHAP V2) from the drop-down menu.
To use PEAP (EAP-MSCHAP V2) security, the server must have WPA-PEAP certificates, and the server properties must already be set. Check with the IT manager.
1. Click the Configure button.
2. Select the appropriate certificate from the drop-down list.
3. Specify a user name for inner PEAP tunnel authentication:
Check Use Windows User Name to use the Windows user name as the PEAP user name.
OR: Enter a PEAP user name in the User Name field to use a separate user name and start the PEAP authentication process.
4. Click Advanced and:
Leave the server name field blank for the client to accept a certificate from any server with a certificate signed by the authority listed in the Network Certificate Authority drop-down list. (recommended)
Enter the domain name of the server from which the client will accept a certificate.
The login name used for PEAP tunnel authentication fills in automatically as PEAP-xxxxxxxxxxxx, where xxxxxxxxxxxx is the computer's MAC address. Change the login name if needed.
5. Click OK.
6. Enable the profile.

Using PEAP-MSCHAP V2 Security

To use PEAP-MSCHAP V2 security In the Atheros Client Utility, access the Security tab in the Profile Management window.
1. On the Security tab, choose the WPA radio button.
OR: On the Security tab, choose the 802.1x radio button.
2. Choose PEAP (EAP-MSCHAP V2) from the drop-down menu.
To use PEAP (EAP-MSCHAP V2) security, the server must have WPA-PEAP certificates, and the server properties must already be set. Check with the IT manager.
1. Click the Configure button.
2. Select the appropriate certificate from the drop-down list.
3. Specify a user name for inner PEAP tunnel authentication:
Check Use Windows User Name to use the Windows user name as the PEAP user name.
OR: Enter a PEAP user name in the User Name field to use a separate user name and start the PEAP authentication process.
4. Click Advanced and:
Leave the server name field blank for the client to accept a certificate from any server with a certificate signed by the authority listed in the Network Certificate Authority drop-down list. (recommended)
Enter the domain name of the server from which the client will accept a

certificate.
The login name used for PEAP tunnel authentication fills in automatically as PEAP-xxxxxxxxxxxx, where xxxxxxxxxxxx is the computer's MAC address. Change the login name if needed.
5. Click OK.
6. Enable the profile.

Pre-Shared Encryption Keys
Defining pre-shared encryption keys:
1. Click the Pre-Shared Key (Static WEP) radio button on the Security tab.
2. Click the Configure button.
3. Fill in the fields in the Define Pre-Shared Keys dialog box:

Key Entry Determines the entry method for an encryption key: hexadecimal (0-9, A-F), or ASCII text (all keyboard characters except spaces).

Encryption
Keys
Selects the default encryption keys used. Only allows the selection for a shared First, Second, Third, or Fourth key whose corresponding field has been completed.

WEP Keys
(1-4)
Defines a set of shared encryption keys for network configuration security. At least one Shared Key field must be populated to enable security using a shared key.
Click on the radio button to set the key as the default encryption key.

WEP Key
Size
Defines the size for each encryption key. The options include:
64-bit (enter 10 digits for hexadecimal, 5 ASCII characters)
128-bit (enter 26 digits for hexadecimal, 13 digits for ASCII)
152-bit (enter 32 digits hexadecimal, 16 digits for ASCII)
4. Click OK for the changes to take effect.

Overwriting an Existing Static WEP Key
1. Click the Pre-Shared Key radio button on the Security tab.
2. Click on Configure.
3. In the window, all existing static WEP keys are displayed as asterisks for security reasons. Click in the field of the existing static WEP key to overwrite.
4. Delete the asterisks in that field.
5. Enter a new key.
6. Make sure to select the Transmit Key button to the left of this key is selected for the key to transmit packets.
7. Click OK.

Disabling Static WEP

To disable static WEP for a particular profile, Select any other security option on the Profile Management tab to automatically disable static WEP
OR: choose None on the Security tab to disable security, and click OK (not recommended).

Using WPA Passphrase Security

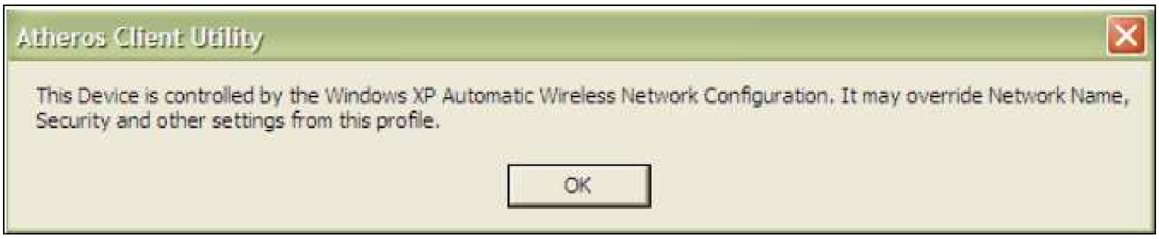
To use WPA Passphrase security In the Atheros Client Utility, access the Security tab in the Profile Management window.
1. On the Security tab, choose the WPA Passphrase radio button.
2. Click on the Configure button.
3. Fill in the WPA Passphrase.
4. Click OK.

Zero Configuration

This section describes the operation of the Atheros Client Utility (ACU) and Windows XP Wireless Configuration Service (WZCS).

Wireless Network Configuration

The Windows WZCS is a service that manages the wireless connection in a largely dynamic way. Only minimal connection information must be identified and configured.
To set Zero Configuration on Windows XP, take the following steps:
1. In Windows XP, open the Wireless Network Configuration Properties dialog box.
2. Select the check box “Use Windows to configure my wireless network settings” to set Zero Configuration.
When this check box is selected, Windows XP takes control of these settings for all configuration profiles:
SSID
Security keys
Ad hoc settings
Note that Windows XP takes control of these settings for all configuration profiles, thus users can
not (create new profiles with different settings while using Windows Zero Configuration.
The Zero Configuration settings override all configuration profiles, even when you select other options. However, the ACU does still control the following settings when Zero Configuration is set:
Power settings
Active/Passive scanning (where applicable)
Transmit power
Wireless band
Short/Long preamble (802.11b)
When Zero Configuration is in use, a pop-up message is displayed on the ACU when you attempt to create or edit a configuration profile from the Profile Management tab of the ACU.



Atheros Client Utility

This Device is controlled by the Windows XP Automatic Wireless Network Configuration. It may override Network Name, Security and other settings from this profile.

To turn Zero Configuration off on Windows XP, take the following steps:
1. In Windows XP, open the Wireless Network Configuration Properties dialog box.
2. Clear the check box "Use Windows to configure my wireless network settings" to set Zero Configuration. When this check box is cleared, all profile settings are controlled by the configuration profile, which is set up from the ACU Profile Management tab.

Check the Status Information or Diagnostics
The Atheros client utility includes a number of tools to display current diagnostics and status information.
Check current status
Check driver information
Check receive and transmit diagnostics

Current Status
The Current Status tab contains general information about the program and its operations. The Current Status tab does not require any configuration. The following table describes the items found on the Current Status screen.

Profile Name The name of the current selected configuration profile. Set up the configuration name on the General tab.

Link Status Shows whether the station is associated to the wireless network.

Wireless Mode Displays the wireless mode. Configure the wireless mode on the Advanced tab.

IP Address Displays the computer's IP address.

Network Type The type of network the station is connected to. Options include:
Infrastructure (access point)
Ad Hoc
Configure the network type on the Advanced tab.
Current Channel Shows the currently connected channel.

Server Based

Authentication
Shows whether server based authentication is used.

Data Encryption Displays the encryption type the driver is using. Configure the encryption type on the Security tab.

Signal Strength Shows the strength of the signal.
Click the Advanced button to see the advanced status diagnostics.

Adapter Information Button
The Adapter Information button contains general information about the network interface card (the wireless network adapter) and the network driver interface specification (NDIS) driver. Access the adapter information from the Diagnostics tab.

Card Name Name of the wireless network adapter.

MAC Address MAC address of the wireless network adapter.

Driver Driver name and path of the wireless network adapter driver.

Driver Version Version of the wireless network adapter driver.

Driver Date Creation date of the wireless network adapter driver.

Client Name Name of the client computer.

Diagnostics Tab

The ACU Diagnostics tab provides allows retrieval of receive and transmit statistics. The Diagnostics tab does not require any configuration. It lists these receive and transmit diagnostics for frames received by or transmitted by the wireless network adapter:

Multicast packets transmitted and received

Broadcast packets transmitted and received

Unicast packets transmitted and received

Total bytes transmitted and received

The Adapter Information button has general information about the wireless network adapter and NDIS driver. The Advanced Statistics button to shows statistics for diagnostics for frames received by or transmitted to the wireless network adapter:

Transmitted Frames

Frames transmitted OK

Frames retried

Frames dropped

No ACK frames

ACK frames

RTS frames

Clear-to-send (CTS) frames

No CTS frames

Retried RTS frames

Retried data frames

Received Frames

Frames received OK

Beacons

Frames with errors

CRC errors

Encryption errors

Duplicate frames

AP mismatches

Data rate mismatches

Authentication time-out

Authentication rejects: the number of AP authentication failures received by the wireless network adapter

Association time-out

Association rejects: the number of AP authentication rejects received by the wireless network adapter

Standard MIC OK

Standard MIC errors

CKIP MIC OK
CKIP MIC errors
Scan Available Networks
Click the Scan button on the Profile Management tab to scan for available infrastructure and ad hoc networks. On this list, click Refresh to refresh the list at any time.

Connecting to a different network

Highlight a network name and click the Activate button to connect an available network. If no configuration profile exists for that network, the Profile Management window opens to the General tab. Fill in the profile name and click OK to create the configuration profile for that network.
Infrastructure
(AP) Network
Connected
Infrastructure
(AP) Network

Display Settings

To change the display settings, choose Options > Display Settings from the menu. The display settings dialog box contains tools to set the:

Signal Strength Display
Units
Sets the units used when displaying signal strength: percentage (%) or dBm.

Refresh Interval Use the up/down arrows to set the display refresh interval in seconds.

Data Display Sets the display to cumulative or relative:
Relative displays the change in statistical data since the last update.
Cumulative displays statistical data collected since opening the profile.

ACU Tools

Use the Action menu to access the Atheros Client Utility tools:

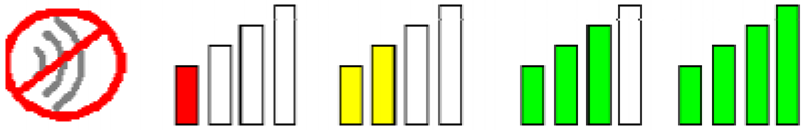
Enable/Disable Radio Enable or disable the RF Signal on all Atheros station reference designs.

Enable/Disable TrayIcon
Enable or disable the tray icon.

Troubleshooting Run the optional Troubleshooting Utility.
Manual LEAP Login Log in to LEAP manually, if LEAP is set to manually prompt for user name and password on each login.

Reauthenticate Reauthenticate to a LEAP-configured access
point.
Exit Exit the Atheros Client Utility application.

Tray Icon
The tray icon appears at the bottom of the screen, and shows the signal strength using colors and the received signal strength indication (RSSI).



Hold the mouse cursor over the tray icon to display the current configuration profile name and association, as well as transmit and receive speed and the wireless adapter name and IP address. Right-click on the tray icon to:
Help Open the online help.

Open Atheros Client
Utility
Launch the Atheros Client Utility (ACU). Use the ACU to
configure a profile or view status and statistics information.

Troubleshooting Run the Troubleshooting Utility.

Preferences Set the ACU startup and menu options. Check to start the
program automatically when Windows starts, and check
menu items that should appear on the popup menu.

Enable/Disable Radio Enable or disable the RF signal.

Manual LEAP Login Log in to LEAP manually, if LEAP is set to manually prompt for user name and password on each login.

Reauthenticate Reauthenticate to the access point.

Select Profile Click a configuration profile name to switch to. If no
configuration profile exists for a connection, add a profile.

Show Connection
Status
This window displays connection information:

Active Profile Displays the active configuration profile name.

Auto Profile
Selection Shows whether auto profile selection is enabled.

Connection
Status
Displays whether the adapter is connected to a

wireless network.

Link Quality Lists the quality of the link connection.

SSID Displays the SSID of the associated network.

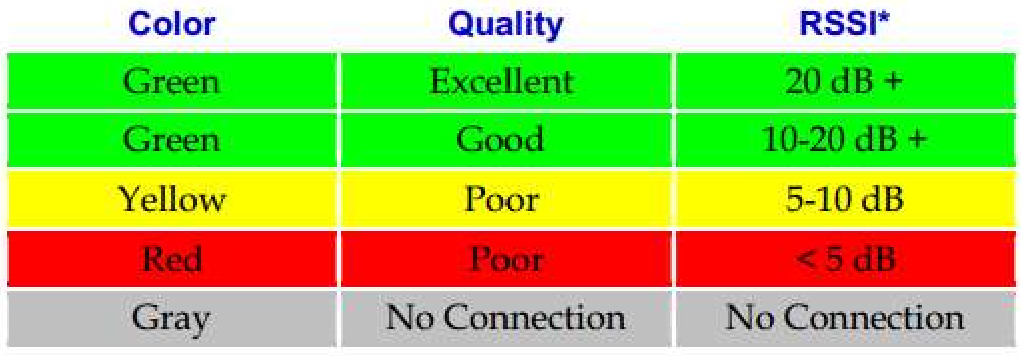
Access Point
Name
Shows the name of the AP the wireless adapter is
connected to.
Access Point
IP Address

Shows the IP address of the access point the
wireless adapter is connected to.
Link Speed Lists the speed of the link connection.

Adapter IP

Address Displays the IP address of the wireless adapter.

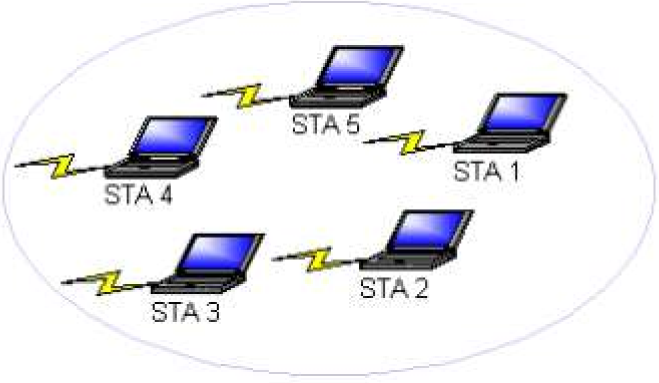
Exit Exit the Atheros Client Utility application.
The colors are defined as follows:



Color	Quality	RSSI*
Green	Excellent	20 dB +
Green	Good	10-20 dB +
Yellow	Poor	5-10 dB
Red	Poor	< 5 dB
Gray	No Connection	No Connection

Color Quality RSSI*
Green Excellent 20 dB +
Green Good 10-20 dB +
Yellow Poor 5-10 dB
Red Poor < 5 dB
Gray No Connection No Connection
*Received signal strength indication RSSI. Displayed in dB or percentage. Enable or disable the tray icon in the Action menu.

Ad Hoc Mode



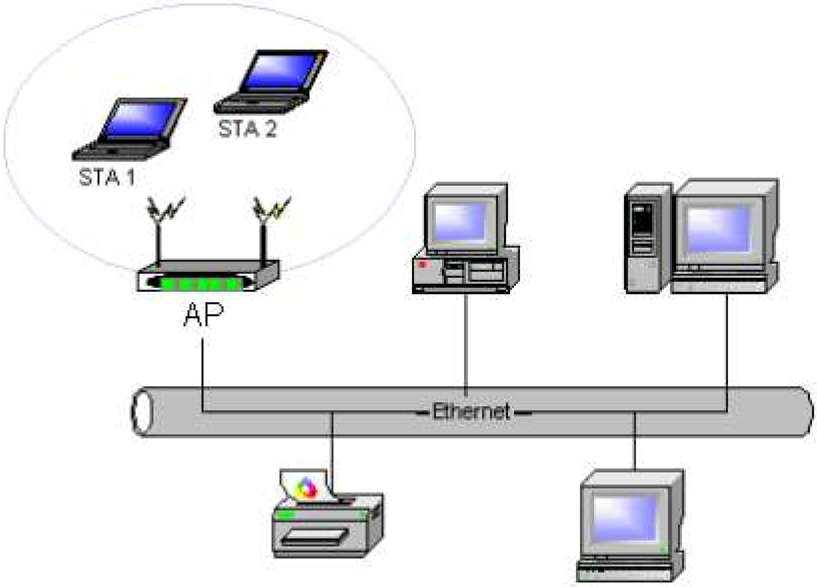
In ad hoc mode, a wireless network adapter works within an independent basic service set (IBSS), as illustrated here. All stations communicate directly with other stations without using an access point (AP).
To connect to an ad hoc network, configure the profile for ad hoc mode. Ad Hoc operation may be limited by Hardware to meet regulatory requirements.

Ad Hoc Mode Profile Configuration

To configure a profile in ad hoc mode, change the Network Type in the Profile Management's Advanced tab. For ad hoc mode, modify the settings:
Network Name (on General Tab)
Transmit Power Level
802.11b Preamble (if using 802.11b)
Wireless Mode When Starting an Ad Hoc Network
Make sure to also edit the General and Security tabs.

Infrastructure (Access Point) Mode

In infrastructure (access point (AP)) mode, the wireless network adapter participates in a basic service set (BSS) as a station, and communicates with the other stations through an AP, as illustrated here.



To connect to an access point network, configure the profile for access point mode.

Infrastructure (Access Point) Mode Profile Configuration

To configure a profile in infrastructure (access point) mode, change the Network Type in the Advanced tab. For access point mode, modify the settings:
Power Save Mode
802.11b Preamble (if using 802.11b)
Wireless Mode
802.11 Authentication Mode
Make sure to also edit the General and Security tabs.

Uninstall an Old Driver

Uninstall an old driver before upgrading to a new NDIS driver release.
To remove the newly installed driver from the system if the system does not have previously installed versions of the NDIS driver, proceed to Step 4.
1. To remove the NDIS driver from the OS, go to Device Manager, right-click Atheros AR500x Wireless Network Adapter, and choose Uninstall.
2. Click OK to uninstall the device.
3. When the device is uninstalled from Device Manager, search for and delete the driver files that reside in the system.
a. Go to the Start menu and choose Search > For Files or Folders.
b. Enter oem*.inf in the Search for files or folders named: field, and enter Atheros in the Containing text: field.
c. Click Search Now. A few files matching these criteria are possible, if previous drivers have not been removed properly.
d. Choose the files that have been found and delete them from the system.
4. To complete the uninstallation, remove the file ar5211.sys from the folder \WINNT\system32\drivers.

Additional Security Features

These security features prevent attacks on a wireless network's WEP keys. The wireless adapter automatically supports each of these features, but these features must be enabled on the access point.

Message Integrity Check (MIC)

MIC prevents bit-flip attacks on encrypted packets. In a bit-flip attack, someone intercepts an encrypted message retransmits it after some alterations. Thus the receiver accepts the message as legitimate. The MIC adds some bytes to each packet to protect it against tampering.

Temporal Key Integrity Protocol (TKIP)

This feature prevents attacks on WEP in which someone catches encrypted packets and uses their initialization vector (IV) to decipher the WEP key. TKIP removes the predictability to protect both unicast and broadcast WEP keys.

Broadcast Key Rotation

EAP authentication provides dynamic unicast WEP keys for wireless adapters, but uses static broadcast keys. In broadcast WEP key rotation, the access point supplies a dynamic broadcast WEP key and changes it at intervals.

Bluetooth Adapter Installation and Operation

Getting Started

This chapter describes how to install, uninstall, launch, and use the Bluetooth Suite. The following major topics are covered in this chapter:

”Installing the Bluetooth Suite”
”Launching the Bluetooth Suite”
”Introduction to the Bluetooth Suite”
“Uninstalling the Bluetooth Suite”

Installing the Bluetooth Suite

You either received a password from Atheros to download the Bluetooth Suite software from the
Atheros web site or received the Bluetooth Suite on a CD.

NOTE: If you are installing Bluetooth Suite on a machine that already has an existing Bluetooth
Suite, you need not uninstall it because Bluetooth Suite supports the upgrade feature. If you need to uninstall Bluetooth Suite, refer to “Uninstalling the Bluetooth Suite” on page 2-10 on how
to uninstall Bluetooth Suite.

Software installation is a three-step process and it is important to perform these steps before you
can use the Bluetooth Suite:

1. Installing the Bluetooth Suite
2. Installing the radio (profile) drivers
3. Updating the drivers

All these steps are explained in the installation process.

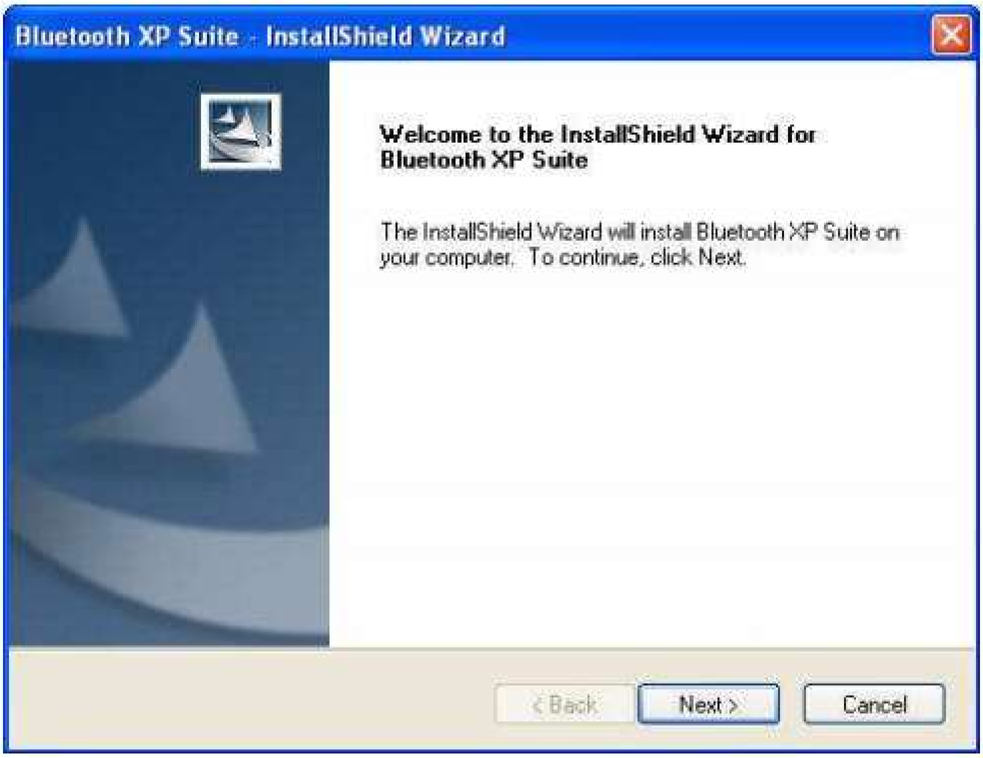
Downloading the Bluetooth Suite

1. Go to the Atheros Support web site: https://support.atheros.com/
2. Login to the web site using your user name and password provided by Atheros Support.
3. Go to the **AR3011 Software Package & Documentation** tab of the Atheros web site.
4. Download the appropriate Bluetooth Suite release, extract the files, and save them on your system.
6. Install the Bluetooth Suite by double-clicking on the Bluetooth Suite **setup.exe** file.
7.

Follow the rest of the installation procedure described in “Copying Bluetooth Suite from the CD” on page 2-2.

Copying Bluetooth Suite from the CD

1. Insert the CD containing the Bluetooth Suite into the CD drive.
2. Double Click on the Bluetooth Suite **setup.exe** file.
The InstallShield Wizard starts to prepare the package for installation. The **Welcome to InstallShield Wizard for** Bluetooth Suite screen (see Figure 2-1) is displayed.

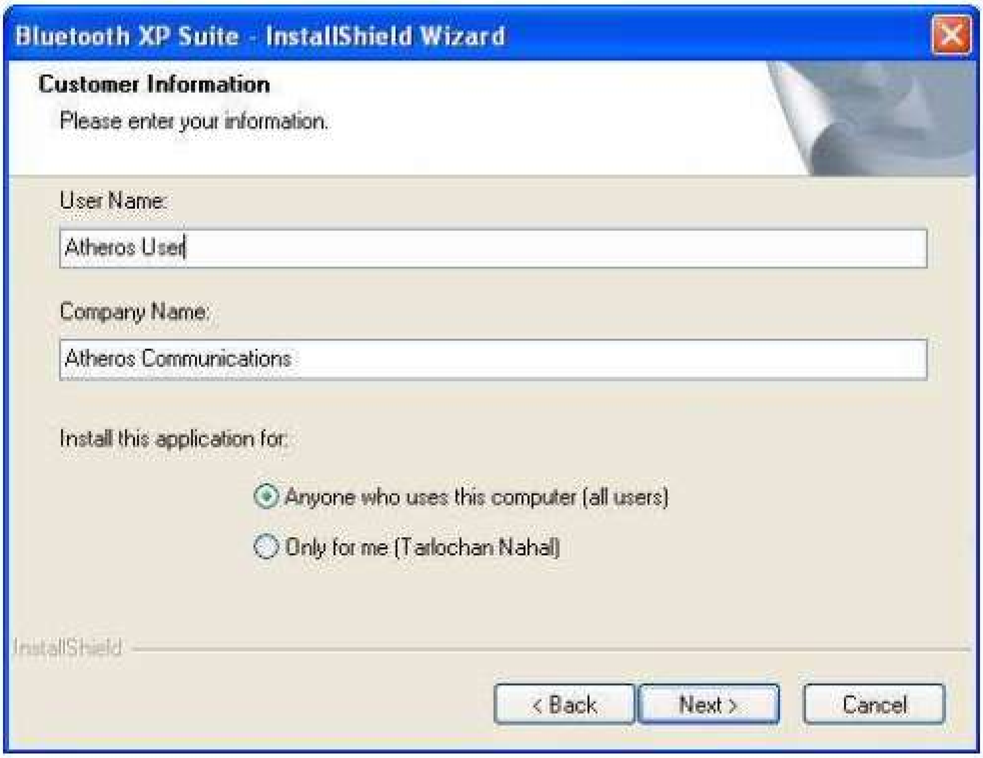


Bluetooth XP Suite - InstallShield Wizard

Welcome to the InstallShield Wizard for Bluetooth XP Suite

The InstallShield Wizard will install Bluetooth XP Suite on your computer. To continue, click Next.

Figure 2-1. **Bluetooth Suite - Welcome Screen**
3. Click Next.
You will see the **Customer Information** screen. See Figure 2-2.



Bluetooth XP Suite - InstallShield Wizard

Customer Information

Please enter your information.

User Name: Atheros User

Company Name: Atheros Communications

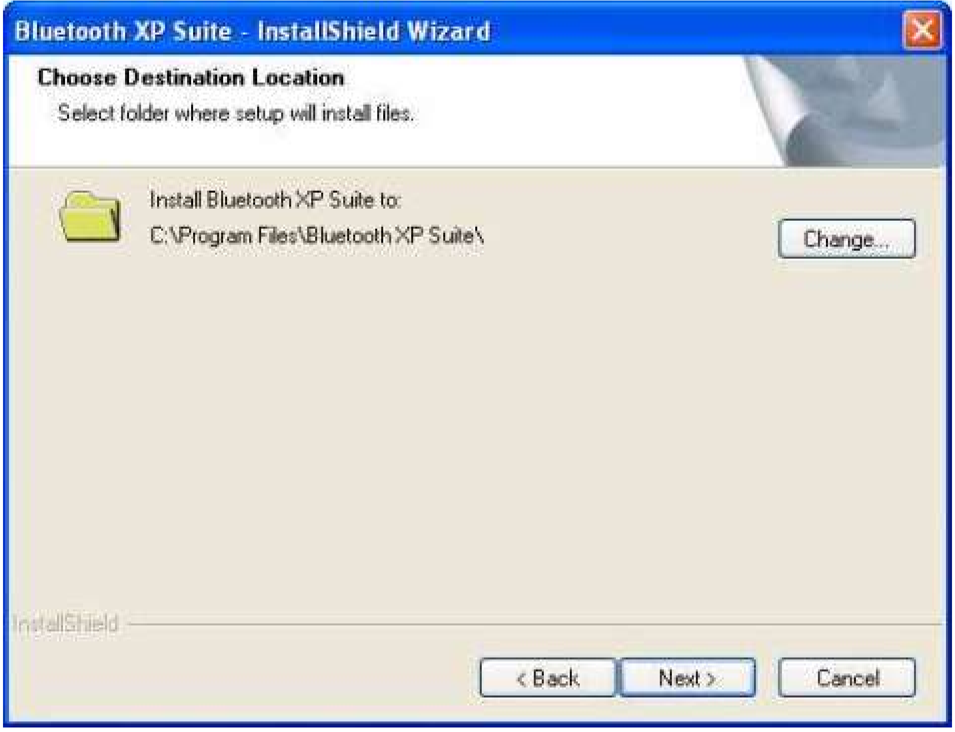
Install this application for:

● Anyone who uses this computer (all users)

○ Only for me (Tarlochan Nahal)

Figure 2-2. **Bluetooth Suite Customer Information Screen**

4. Enter the user name and company name and choose the intended user of this application - “**Anyone who uses this computer (all users)**” or “**Only for me**” and click **Next**.
You will see Choose Destination Location screen. See Figure 2-3.



Bluetooth XP Suite - InstallShield Wizard

Choose Destination Location

Select folder where setup will install files.

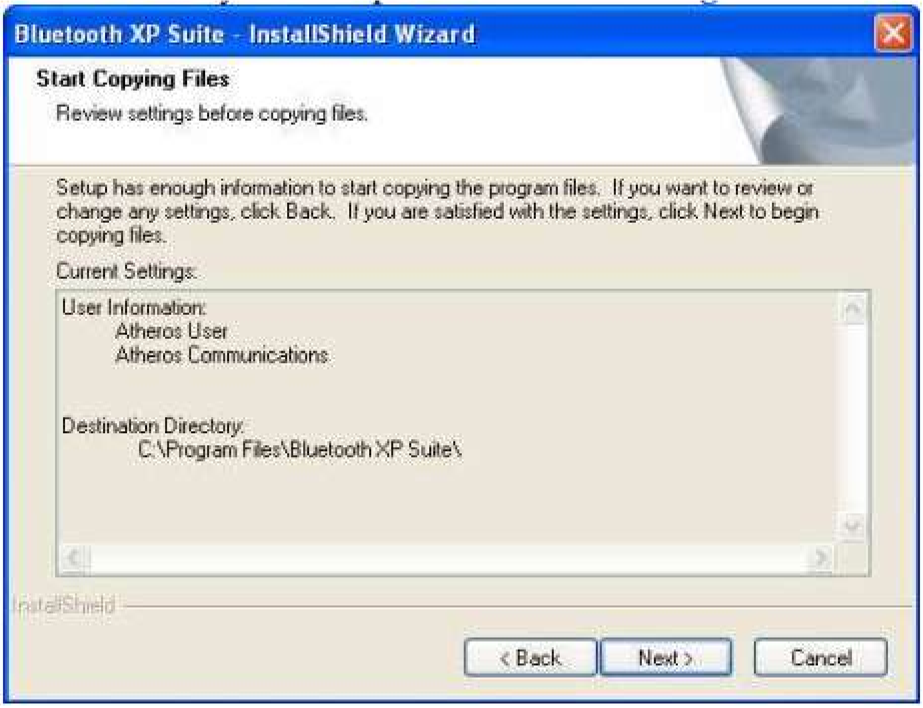
Install Bluetooth XP Suite to:
C:\Program Files\Bluetooth XP Suite\

Figure 2-3. **Bluetooth Suite Choose Destination Location**

5. The default destination location is already selected. Click
Change to browse to a different destination.

6. Click **Next**.

You will see **Start Copying Files** screen that displays the current settings including user information, setup type, and destination directory. This allows you to review and modify the setup information. See Figure 2-4.



Bluetooth XP Suite - InstallShield Wizard

Start Copying Files

Review settings before copying files.

Setup has enough information to start copying the program files. If you want to review or change any settings, click Back. If you are satisfied with the settings, click Next to begin copying files.

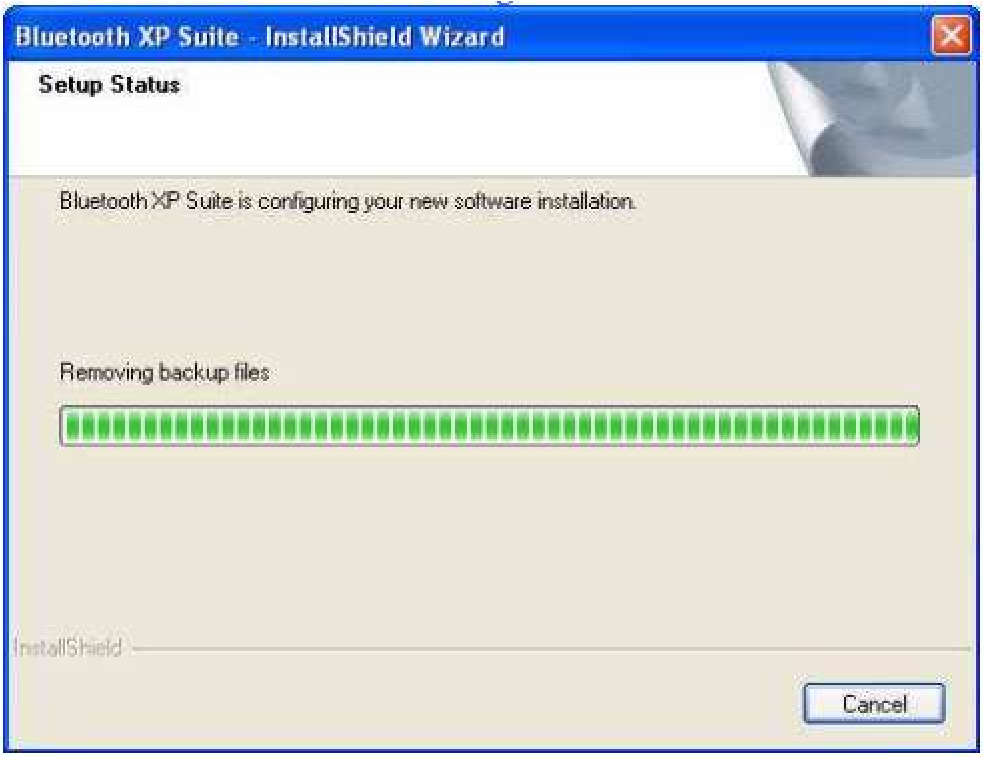
Current Settings:

User Information:
Atheros User
Atheros Communications

Destination Directory:
C:\Program Files\Bluetooth XP Suite\

Figure 2-4. **Bluetooth Suite - Start Copying Screen**

7. Click **Next.** The Bluetooth Suite begins to configure and copy the new software. It also removes any backup files. When the Bluetooth Suite installation is complete, you will see the Finish screen. See Figure 2-5.



Bluetooth XP Suite - InstallShield Wizard

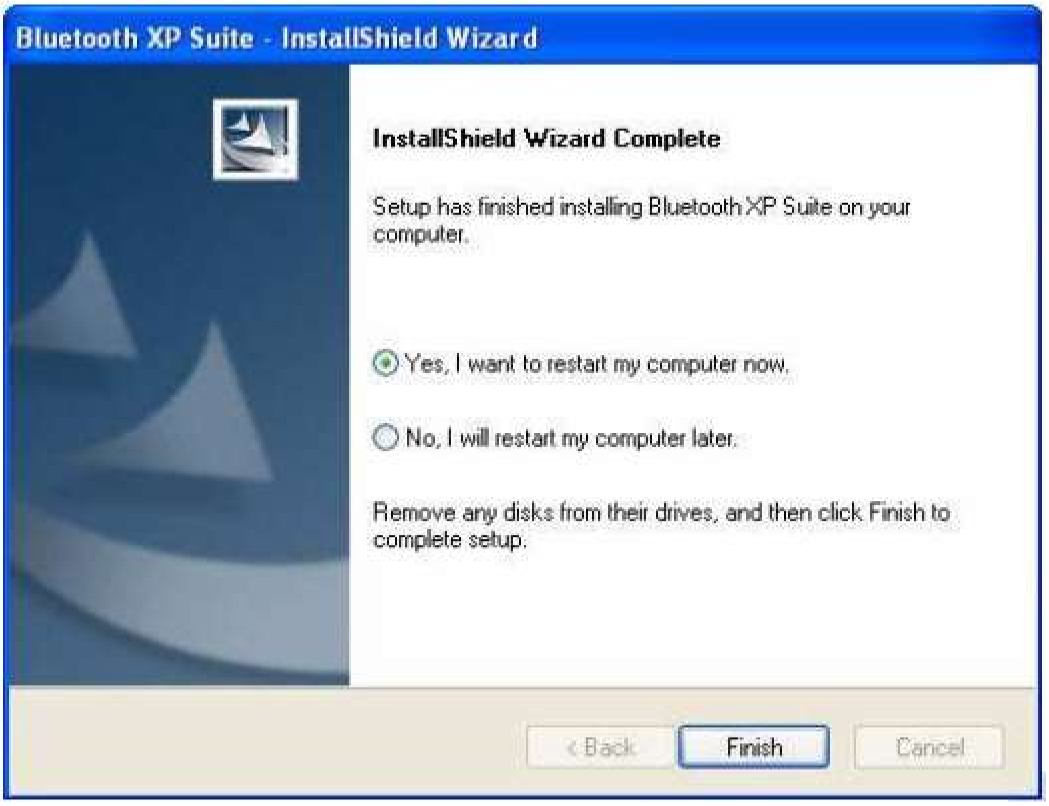
Setup Status

Bluetooth XP Suite is configuring your new software installation.

Removing backup files

Figure 2-5. **Bluetooth Suite - Installation Setup Status**

8. When prompted to restart your computer, select **Yes, I want to restart my computer now** option and click **Finish**.



Bluetooth XP Suite - InstallShield Wizard

InstallShield Wizard Complete

Setup has finished installing Bluetooth XP Suite on your computer.

● Yes, I want to restart my computer now.

○ No, I will restart my computer later.

Remove any disks from their drives, and then click Finish to complete setup.

Figure 2-6. **Bluetooth Suite - Finishing the Installation**

The installation is complete. This process creates a ‘Launch Bluetooth Suite’ shortcut on your desktop. Now you are ready to run Bluetooth Suite.

Launching the Bluetooth Suite

1. Insert the Bluetooth Suite USB device into the USB port of your system.

NOTE: You can insert the Bluetooth Suite USB device in any USB port. You might see **Found New Hardware** message.

2. Double click on the **Bluetooth Suite** icon on your desktop or choose **start > All Programs > Bluetooth Suite > Launch Bluetooth Suite**.

It displays the blank Atheros Bluetooth **Suite** screen.

NOTE: If no Bluetooth devices are found within range, it is normal for new installation. Bluetooth Suite screen does not display such devices when launched for the first time. You need to click on the Discovery button the top left panel of the window to see all the Bluetooth devices in range. See Figure 2-7.

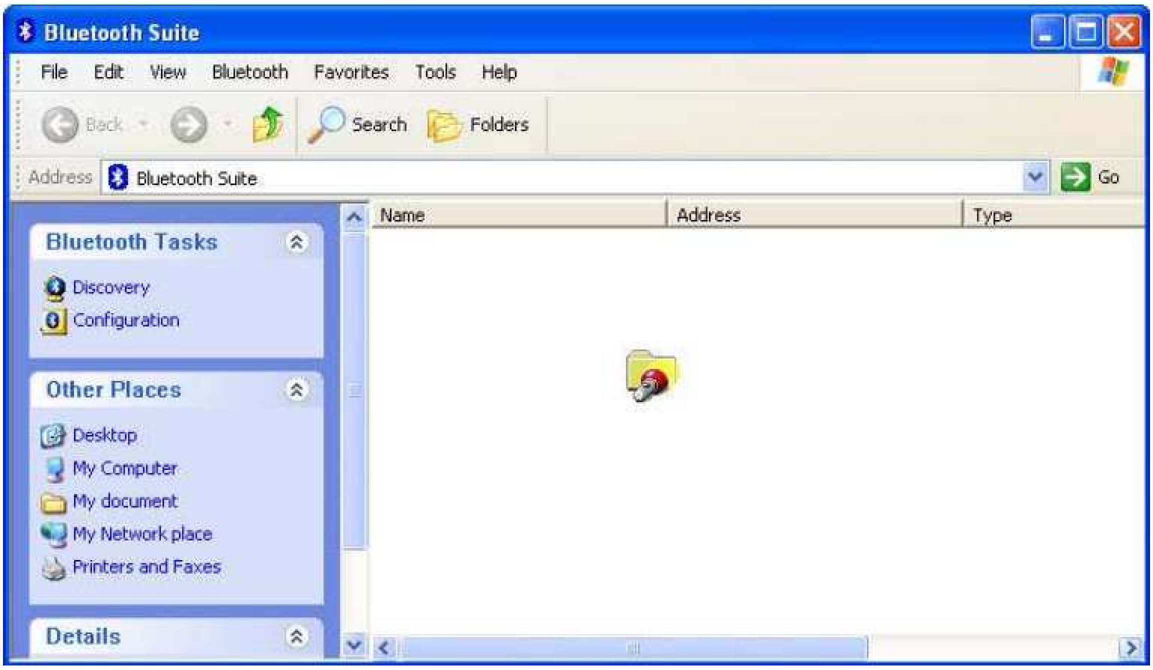
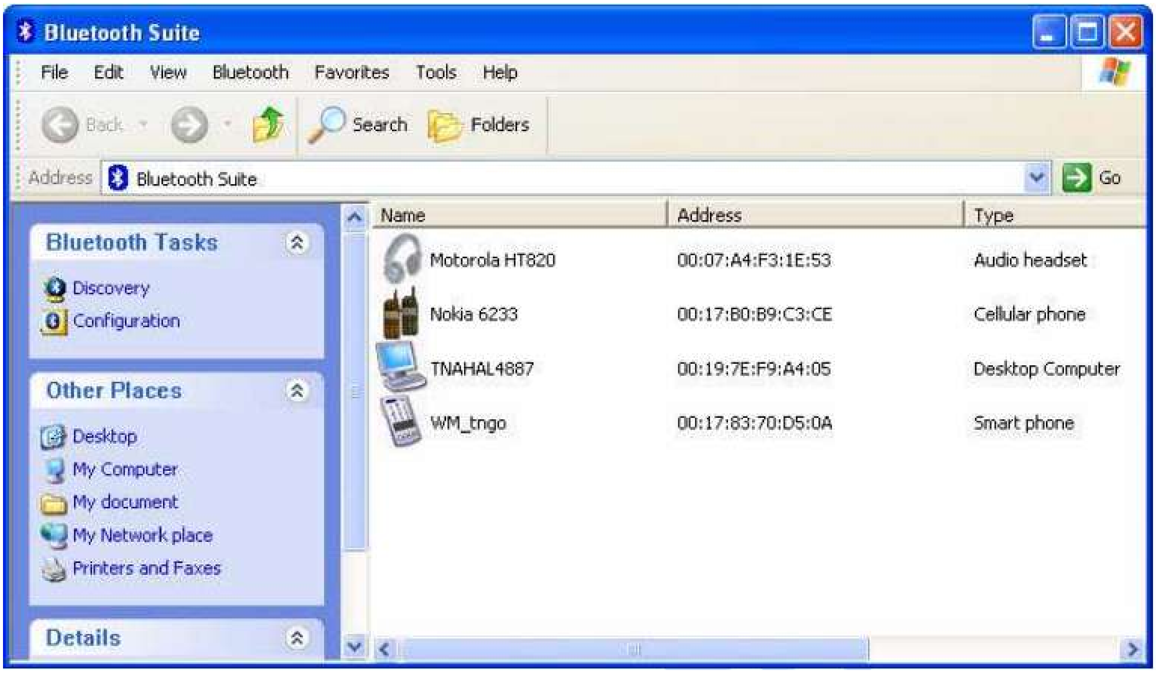


Figure 2-7. Bluetooth Suite Startup Screen During Discovery

When the Bluetooth Suite finds devices in range, it displays them. See Figure 2-8.



Name	Address	Type
Motorola HT820	00:07:A4:F3:1E:53	Audio headset
Nokia 6233	00:17:B0:B9:C3:CE	Cellular phone
TNAHAL4887	00:19:7E:F9:A4:05	Desktop Computer
WM_tngo	00:17:83:70:D5:0A	Smart phone

Figure 2-8. **Discovered Bluetooth Devices**

NOTE: Trusted remote devices will show Paired status in Device list, and Connected remote devices will show Connected status in Device list. Other devices will display Inrange status.

Introduction to the Bluetooth Suite

Now that you have successfully launched the Bluetooth Suite, spend few minutes in getting to know your Bluetooth Suite. The following few pages explain various features and components associated with the Bluetooth Suite GUI.

The My **Bluetooth Suite** is the main screen that consists of three major parts:

Menu bar

Bluetooth Tasks area
Bluetooth devices along with their IP addresses and types are
displayed on the right panel.
In addition, there is a Bluetooth Suite Tray which allows you to launch
the Bluetooth Suite.

Menu Bar

Bluetooth menu is the primary menu on the **Bluetooth Suite** screen. The options associated with
this menu are:
Search for Device
Bluetooth Configuration
Bluetooth Help Topics
Bluetooth Exchange Folder
About Bluetooth
NOTE: Some of these functions are available from the Bluetooth Suite Tray.
These options are described below in detail.

Search For Device

Clicking this button begins to search for remote Bluetooth devices in range. Found devices will display in right panel.

Bluetooth Configuration

Clicking on the Configuration menu option displays the Bluetooth Suite Configuration screen which allows you to specify Bluetooth Suite tasks and settings associated with Bluetooth device
recovery and device filters. This function is also available through the toolbar. Nine configuration screens are associated with Bluetooth Suite. Those screens are:
Bluetooth Suite Settings
Local Device
Bluetooth Security
Profile Manager
Shared Folders
Object Push
Audio
Basic Imaging
Personal Area Networking
Fax Server Configuration
Sync
These options are described in detail in Chapter 3.

Bluetooth Help Topics

Click this button to display any help topics.

Bluetooth Exchange Folder

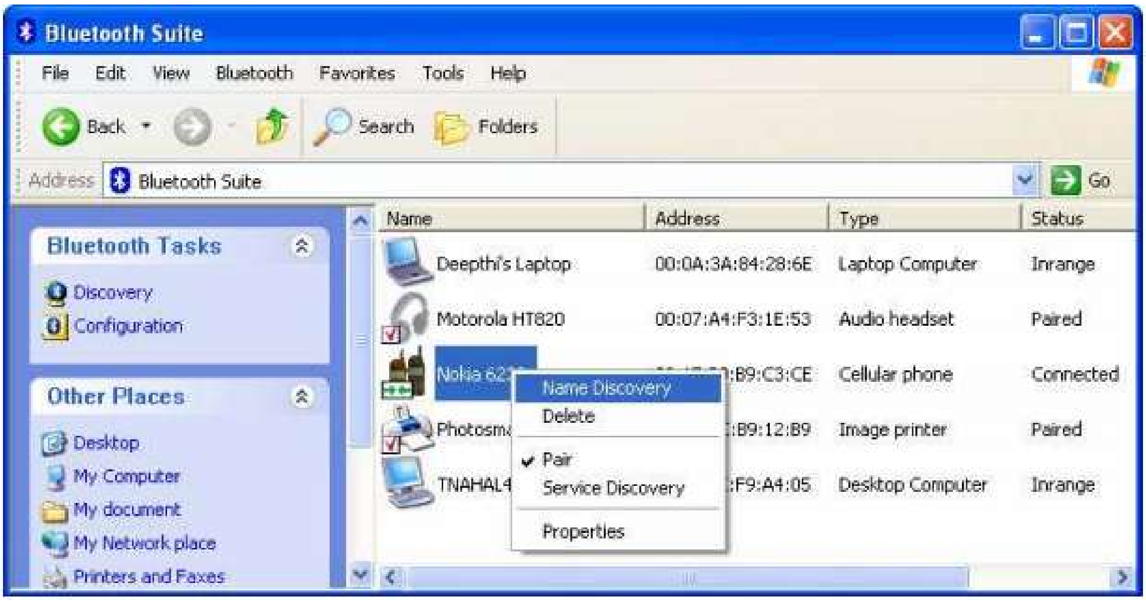
Clicking this button to display the content of Bluetooth exchange folder. From Bluetooth Suite window, choose **Bluetooth->Bluetooth Exchange Folder** to access Exchange share folder for Object Push feature.

Bluetooth Places Panel

When you launch the Bluetooth Suite, various Bluetooth devices in the Bluetooth neighborhood are listed on the right panel. These typically consist of
audio devices, computers (both laptop and desktop), phones, peripheral

devices such as Fax, printer, mouse, headset, and imaging devices. If any of these devices are discovered, they are listed on the right window panel. For example, if a Bluetooth mouse is discovered in the Bluetooth neighborhood, it is shown as peripheral pointing device, its brand name, address, and service status (in range, paired, connected or disconnected). You can select a device and right mouse click button to select the following:

Name discovery
Delete
Pair
Service Discovery
Properties
See Figure 2-9 for details.



Name	Address	Type	Status
Deepthi's Laptop	00:0A:3A:84:28:6E	Laptop Computer	Inrange
Motorola HT820	00:07:A4:F3:1E:53	Audio headset	Paired
Nokia 62	:B9:C3:CE	Cellular phone	Connected
Photosm	:B9:12:B9	Image printer	Paired
TNAHAL4	:F9:A4:05	Desktop Computer	Inrange

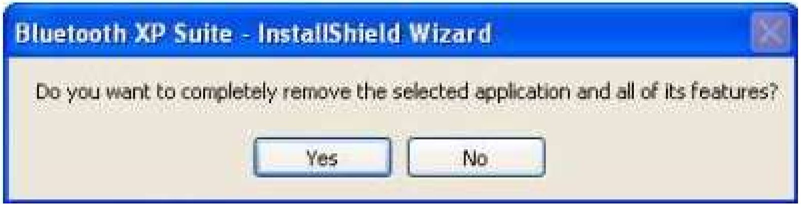
Figure 2-9. **Bluetooth Places Device Opt**

Uninstalling the Bluetooth Suite

Anytime you install a new version of Bluetooth Suite, you need to uninstall any existing version of the Bluetooth Suite. Follow this procedure to uninstall the Bluetooth Suite.

1. Make sure the Bluetooth dongle is removed from any system USB port.
2. Choose **start > All Programs > Bluetooth Suite > Uninstall Bluetooth Suite**.

The system prepares for uninstallation. A screen is briefly displayed that shows that it is ready to uninstall the program. You will see another screen that prompts you to completely remove the application and all of its features. See Figure 2-10.



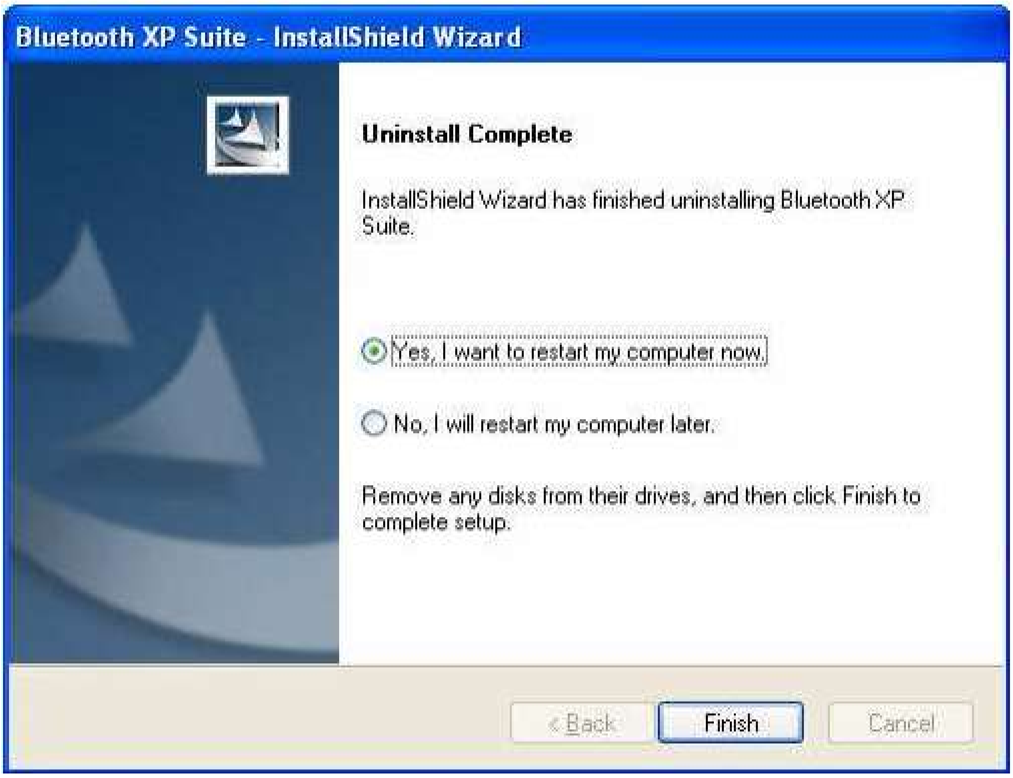
Bluetooth XP Suite - InstallShield Wizard

Do you want to completely remove the selected application and all of its features?

Figure 2-10. **Bluetooth Suite Uninstallation Prompt**

3. Click **Yes**.

You will see a Setup Status screen showing that application is being removed followed by another screen showing Uninstall Complete. See Figure 2-11.



Bluetooth XP Suite - InstallShield Wizard

Uninstall Complete

InstallShield Wizard has finished uninstalling Bluetooth XP Suite.

● Yes, I want to restart my computer now.

○ No, I will restart my computer later.

Remove any disks from their drives, and then click Finish to complete setup.

Figure 2-11. **Finishing Bluetooth Suite Uninstallation**

4. Click **Yes, I want to restart my computer now.**

5. Click **Finish**.

The uninstall is complete. You are ready to reinstall the Bluetooth Suite.

Connecting to an HID Device

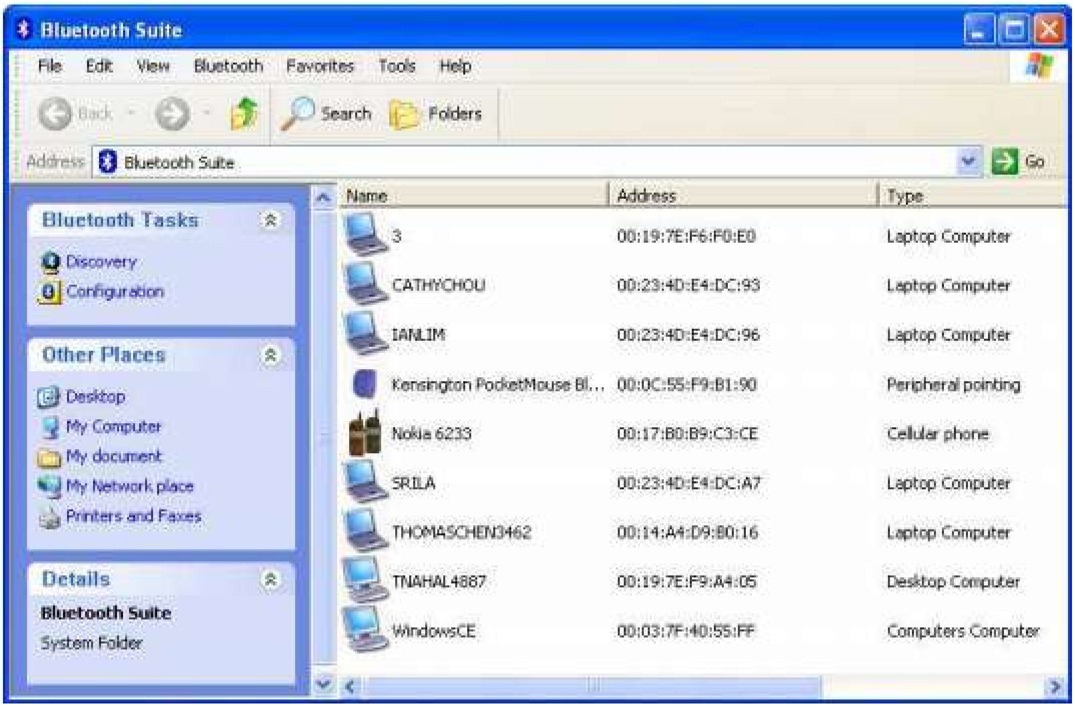
This chapter describes how to connect the Bluetooth laptop to a Bluetooth HID (Human Interface Device) such as a mouse.

Setup Requirements

You need the following devices and equipment in order to accomplish this task:
A PC system running Windows with Bluetooth Suite
Atheros Bluetooth USB Adapter (dongle)
Bluetooth mouse with batteries or keyboard

Launching the Bluetooth Suite

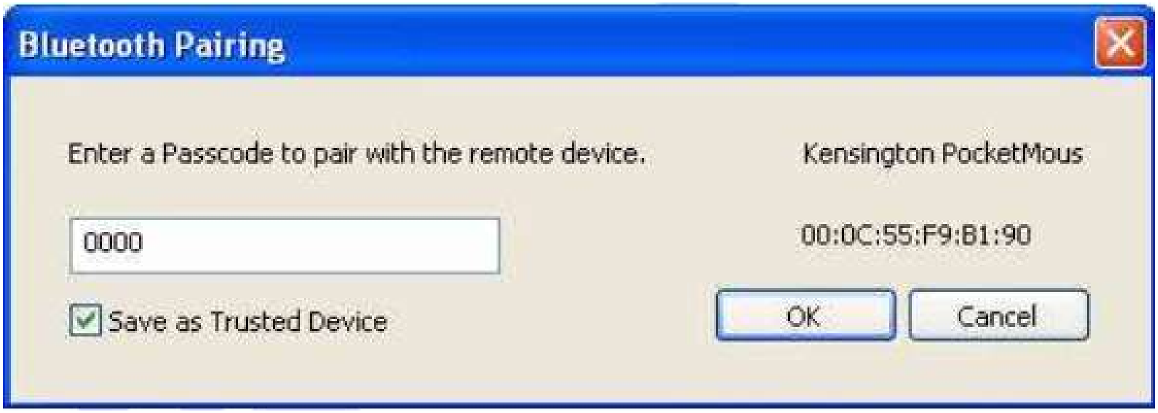
1. Double click on the **Launch Bluetooth Suite** icon on your desktop or launch it from **start > All Programs > Bluetooth Suite > Launch Bluetooth Suite**. It displays theBluetooth Suite start-up screen. See Figure 4-1.
2. Put your mouse in searchable (pairing mode) by doing the following:
a. Turn On the mouse by pressing down its power On/Off button. Refer to the mouse documentation on how to do it.
b. Press the connect button on the mouse to put it in pairing (discoverable) mode. Refer to the mouse documentation for additional information.
3. Right mouse click on the **Bluetooth Suite Tray**, and choose **My Bluetooth Place** option.
It displays all the peripheral devices in the right panel of the screen indicating that these devices
are in range and available to be connected. It also shows the device name, address, type and status (in range, paired, or connected).



Name	Address	Type
3	00:19:7E:F6:F0:E0	Laptop Computer
CATHYCHOU	00:23:4D:E4:DC:93	Laptop Computer
IANLIM	00:23:4D:E4:DC:96	Laptop Computer
Kensington PocketMouse Bl...	00:0C:55:F9:B1:90	Peripheral pointing
Nokia 6233	00:17:B0:B9:C3:CE	Cellular phone
SRILA	00:23:4D:E4:DC:A7	Laptop Computer
THOMASCHEN3462	00:14:A4:D9:B0:16	Laptop Computer
TNAHAL4887	00:19:7E:F9:A4:05	Desktop Computer
WindowsCE	00:03:7F:40:55:FF	Computers Computer

Figure 4-1. **Bluetooth Places Screen**

4. Make sure the device that you wish to pair or connect is powered up and in discoverable mode. If it is in range and has previously been paired, turning on the device will automatically pair it.
5. Right click on the mouse and choose **Pair**. It displays the Bluetooth Pairing Passcode screen. See Figure 4-2.



Enter a Passcode to pair with the remote device.

Kensington PocketMous

0000

00:0C:55:F9:B1:90

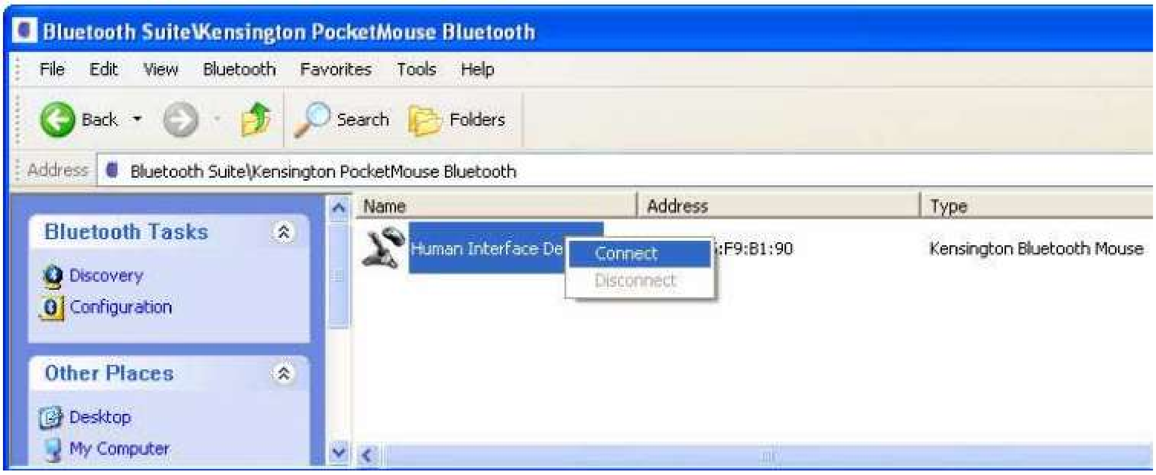
☑ Save as Trusted Device

Figure 4-2. **Entering Bluetooth Pairing Passcode**

6. Enter a passcode to pair with the remote device and click **OK**.

NOTE: The default code shown is 0000. Refer to the documentation of your mouse to find out the passcode of your device and how to change it.

7. Highlight the mouse device under Peripheral Devices in the left panel and choose **Service Discovery**. Highlight the device. Using your laptop pointing device, right click on the Human Interface Device service and choose the **Connect** option to connect to the mouse.



Address: Bluetooth Suite\Kensington PocketMouse Bluetooth

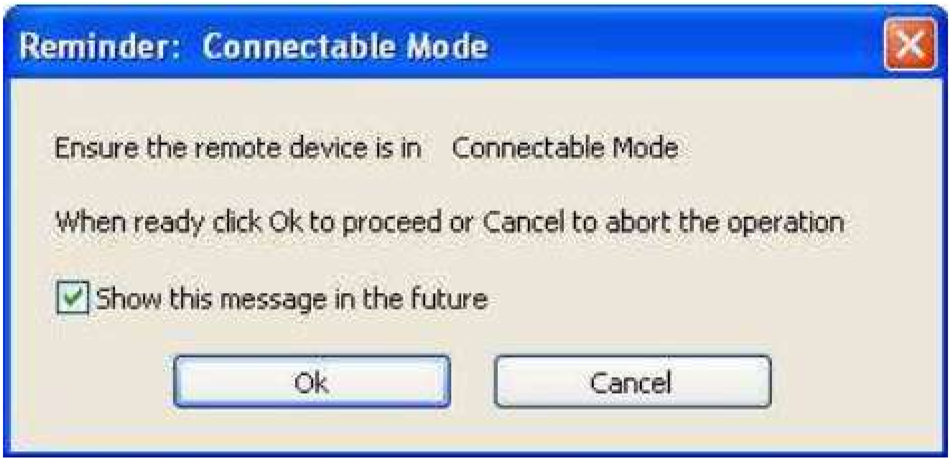
Name	Address	Type
Human Interface De	:F9:B1:90	Kensington Bluetooth Mouse

Figure 4-3. **Connecting the Mouse**

8. Right click the **Connect** button.

9. You will be prompted to make sure the device is in discoverable mode. Make sure the device in ON and in connectable mode. See Figure 4-4.

Figure 4-4. **Putting Device in Connectable Mode**



Reminder: Connectable Mode

Ensure the remote device is in Connectable Mode

When ready click Ok to proceed or Cancel to abort the operation

☑ Show this message in the future

10. Click **OK**.

You will notice that the Wizard begins to install software for the HID device. As soon as the installation is complete, the screen disappears.

Its service status of the HID changes from Disconnected to Connected. Your mouse is now connected and ready to use. You can perform normal mouse functions using this mouse.

Connecting to a Sync Device

This chapter describes how to connect a Bluetooth laptop to a Bluetooth device that supports Synchronization profile. The following topics are covered in this chapter:

"Setup Requirements"

"Launching the Synchronization Process"

Setup Requirements

You need the following devices and equipment in order to accomplish this task:

A laptop system running Windows XP with Bluetooth Suite

Bluetooth USB Adapter

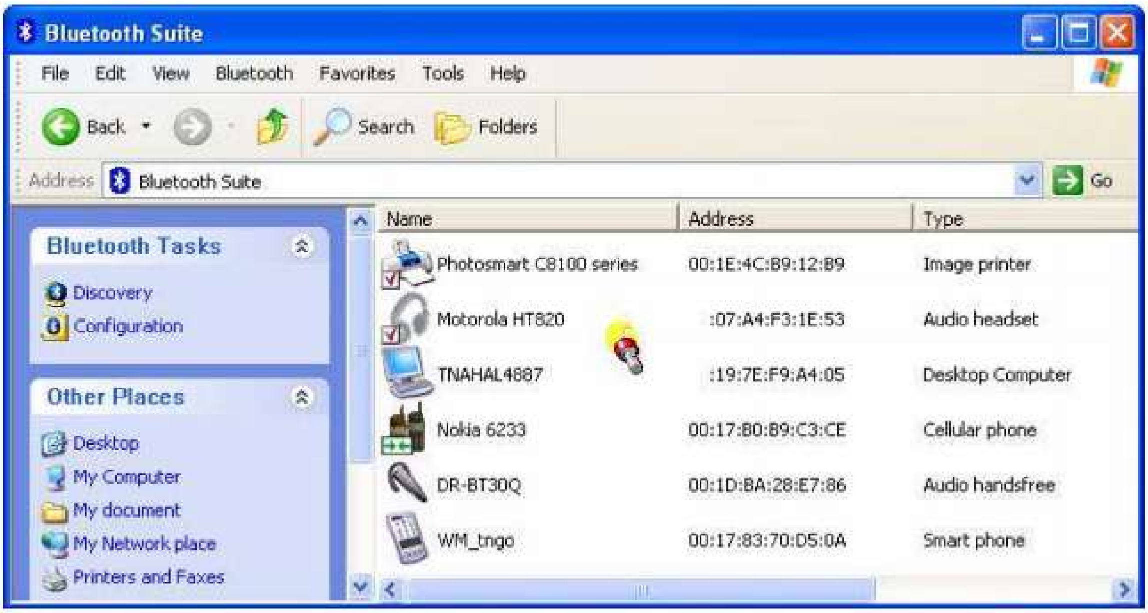
A Bluetooth device such as an e-mail tool and calendar that supports sync profile

Launching the Synchronization Process

1. Launch the Bluetooth Suite.

2. Choose My Bluetooth Place from the Bluetooth tray on your desktop. It displays the My Bluetooth Place start-up screen.

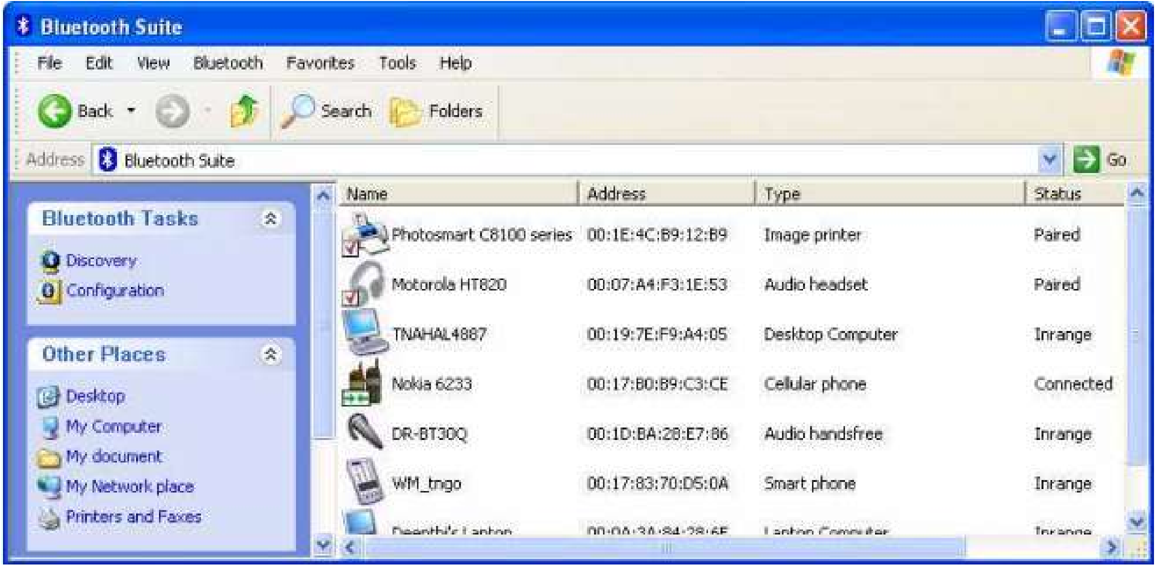
3. Right mouse click the blank panel and choose Device Discovery option. See Figure 10-1.



Name	Address	Type
Photosmart C8100 series	00:1E:4C:B9:12:B9	Image printer
Motorola HT820	:07:A4:F3:1E:53	Audio headset
TNAHAL4887	:19:7E:F9:A4:05	Desktop Computer
Nokia 6233	00:17:B0:B9:C3:CE	Cellular phone
DR-BT30Q	00:1D:BA:28:E7:86	Audio handsfree
WM_tngo	00:17:83:70:D5:0A	Smart phone

Figure 10-1. **Bluetooth Suite Discovery Screen**

4. Highlight the device that you wish to sync with and pair it. See Figure 10-2.

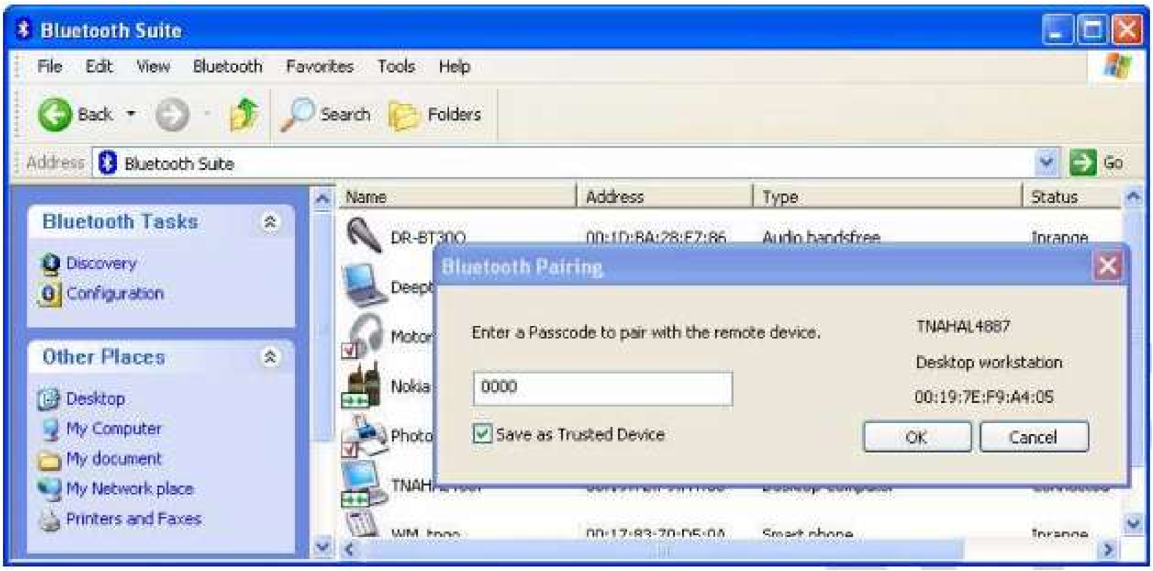


Name	Address	Type	Status
Photosmart C8100 series	00:1E:4C:B9:12:B9	Image printer	Paired
Motorola HT820	00:07:A4:F3:1E:53	Audio headset	Paired
TNAHAL4887	00:19:7E:F9:A4:05	Desktop Computer	Inrange
Nokia 6233	00:17:B0:B9:C3:CE	Cellular phone	Connected
DR-BT30Q	00:1D:BA:28:E7:86	Audio handsfree	Inrange
WM_tngo	00:17:83:70:D5:0A	Smart phone	Inrange
Deepthi's Laptop	00:0A:3A:84:28:6F	Laptop Computer	Inrange

Figure 10-2. **Pairing the Device for Syncing**

5. Right mouse click on the desired bluetooth device and select the **Pair** option.

6. Enter the pairing code (0000) to pair it and click **OK**. See Figure 10-3.



Enter a Passcode to pair with the remote device.

TNAHAL4887
Desktop workstation
00:19:7E:F9:A4:05

0000

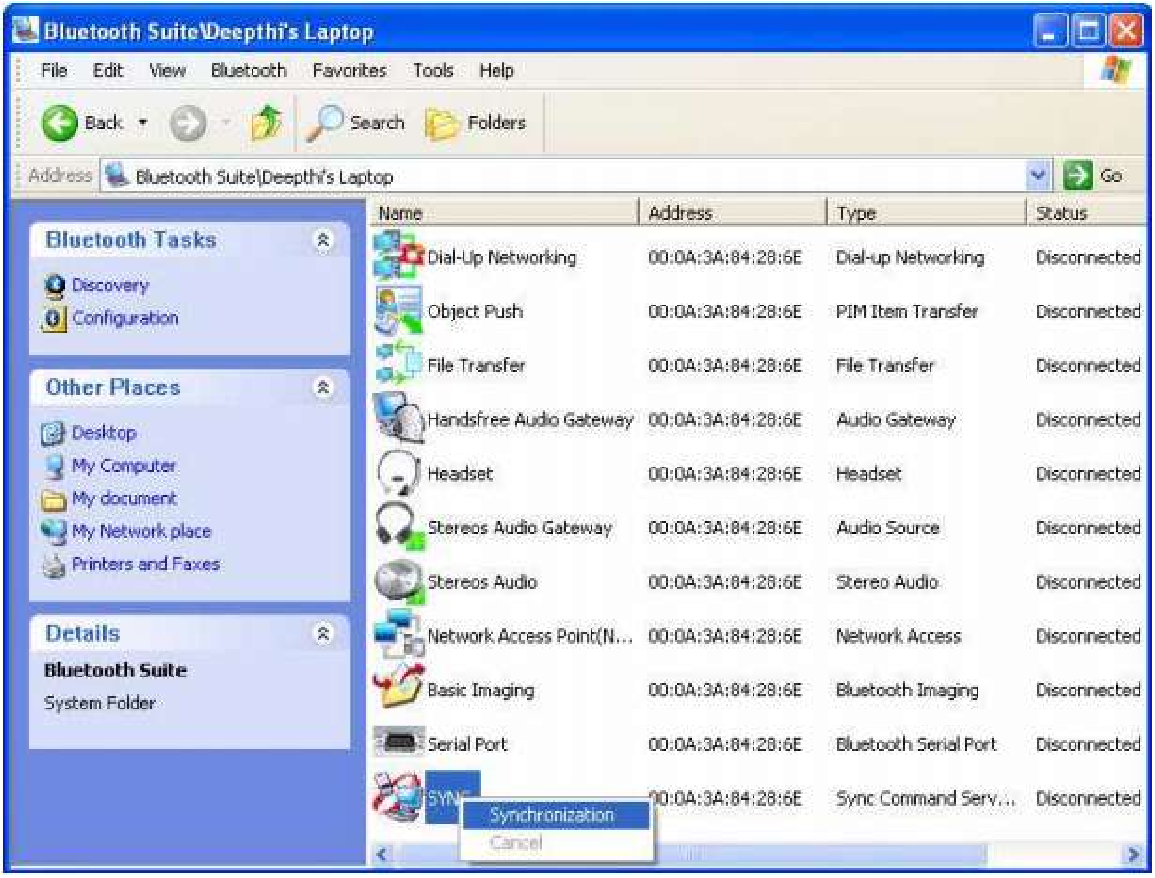
☑ Save as Trusted Device

Figure 10-3. **Bluetooth Devices Pairing**

7. You will see the passcode prompt. Enter the passcode (default is 0000) for the selected device and click **OK**.

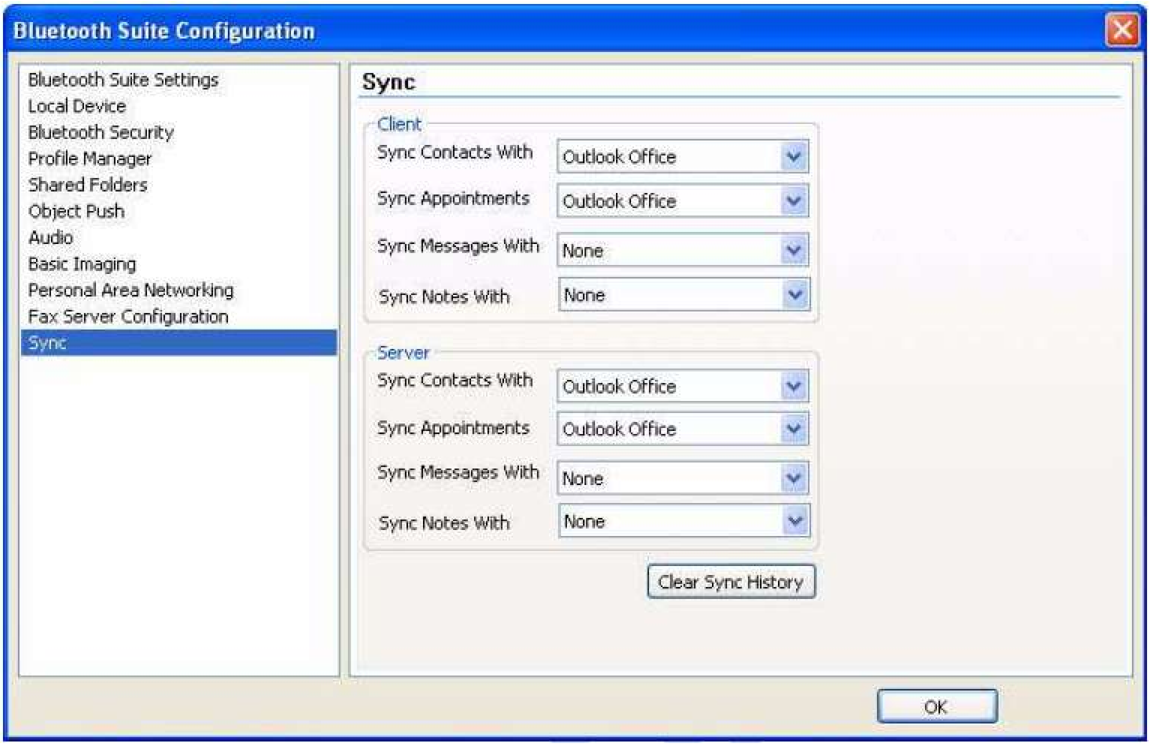
NOTE: The default code shown is 0000. Refer to the documentation of your device to find out the passcode of your device and how to change it.

8. Right click the **SYNC** icon on My Bluetooth Place under the specified device screen and choose **Synchronization** option. See Figure 10-4.



Name	Address	Type	Status
Dial-Up Networking	00:0A:3A:84:28:6E	Dial-up Networking	Disconnected
Object Push	00:0A:3A:84:28:6E	PIM Item Transfer	Disconnected
File Transfer	00:0A:3A:84:28:6E	File Transfer	Disconnected
Handsfree Audio Gateway	00:0A:3A:84:28:6E	Audio Gateway	Disconnected
Headset	00:0A:3A:84:28:6E	Headset	Disconnected
Stereos Audio Gateway	00:0A:3A:84:28:6E	Audio Source	Disconnected
Stereos Audio	00:0A:3A:84:28:6E	Stereo Audio	Disconnected
Network Access Point(N...	00:0A:3A:84:28:6E	Network Access	Disconnected
Basic Imaging	00:0A:3A:84:28:6E	Bluetooth Imaging	Disconnected
Serial Port	00:0A:3A:84:28:6E	Bluetooth Serial Port	Disconnected
SYNC	00:0A:3A:84:28:6E	Sync Command Serv...	Disconnected

Figure 10-4. **Bluetooth Synchronization**
It displays the Sync screen which allows you to specify sync parameters for both client and server. See Figure 10-5.



Sync

Client

Sync Contacts With: Outlook Office
Sync Appointments: Outlook Office
Sync Messages With: None
Sync Notes With: None

Server

Sync Contacts With: Outlook Office
Sync Appointments: Outlook Office
Sync Messages With: None
Sync Notes With: None

Figure 10-5. **Selecting Items to Synchronize**

9. Select the Sync items under the server and client that you wish to synchronize and click **OK**.

The selected items will be synchronized.

Advanced Status Information
Click the Advanced button on the Current Status tab of the Atheros Client Utility to see advanced information about the program and its operations. The Current Status tab does not require any configuration. The following table describes the items found on the Advanced Status screen.

Network Name (SSID) Displays the wireless network name.
Configure the network name on the General tab.

Server Based
Authentication
Shows whether server based authentication is used.
Data Encryption Displays the encryption type the driver is using. Configure the

encryption type on the Security tab.
Authentication Type Displays the authentication mode.
Configure the authentication mode on the General tab.

Message Integrity

Check
Shows whether MIC is enabled. MIC prevents bit-flip attacks on encrypted packets.

Associated AP Name Displays the name of the access point the wireless adapter is associated to.

Associated AP IP
Address

Shows the IP address of the access point the wireless adapter is associated to.

Associated AP MAC
Address
Displays the MAC address of the access point the wireless adapter is associated to.

Power Save Mode Shows the power save mode. Power management is disabled in ad hoc mode.
Configure the power save mode on the Advanced tab.

Current Power Level Displays the transmit power level rate in mW.

Current Signal Strength Shows the current signal strength in dBm.

Current Noise Level Displays the current noise level in dBm.

Up Time Shows how long the client adapter has been receiving power (in hours:minutes:seconds). If the adapter runs for more than 24 hours, the display shows in days:hours:minutes:seconds.

802.11b Preamble Displays the 802.11b preamble format.
Configure the preamble format on the Advanced tab.
Current Receive Rate Shows the current receive rate in Mbps.
Current Transmit Rate Displays the current transmit rate in Mbps.
Channel Shows the currently connected channel.
Frequency Displays frequency the station is using.
Channel Set Shows the current channel set.

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 or more 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.

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.

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.

This device and its antenna(s) must not be co-located or operating in conjunction with any other antenna or transmitter.

For product available in the USA/Canada market, only channel 1~11 can be operated. Selection of other channels is not possible.

IMPORTANT NOTE:

This module is intended for OEM integrator. The OEM integrator is still responsible for the FCC compliance requirement of the end product, which integrates this module.

20cm minimum distance has to be able to be maintained between the antenna and the users for the host this module is integrated into. Under such configuration, the FCC radiation exposure limits set forth for an population/uncontrolled environment can be satisfied.

Any changes or modifications not expressly approved by the manufacturer could void the user's authority to operate this equipment.

USERS MANUAL OF THE END PRODUCT:

In the user’s manual of the end product, the end user has to be informed to keep at least 20cm separation with the antenna while this end product is installed and operated. The end user has to be informed that the FCC radio-frequency exposure guidelines for an uncontrolled environment can be satisfied. The end user has to also be informed that any changes or modifications not expressly approved by the manufacturer could void the user's authority to operate this equipment. If the size of the end product is smaller than 8x10cm, then additional FCC part 15.19 statement is required to be available in the user’s manual: This device complies with Part 15 of 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.

LABEL OF THE END PRODUCT:

The final end product must be labeled in a visible area with the following " Contains TX FCC ID: E8H-AR5B22 ". (The other project ID: " Contains TX FCC ID: E8H-AR5B22 ") If the size of the end product is larger than 8x10cm, then the following FCC part 15.19 statement has to also be available on the label: This device complies with Part 15 of 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.

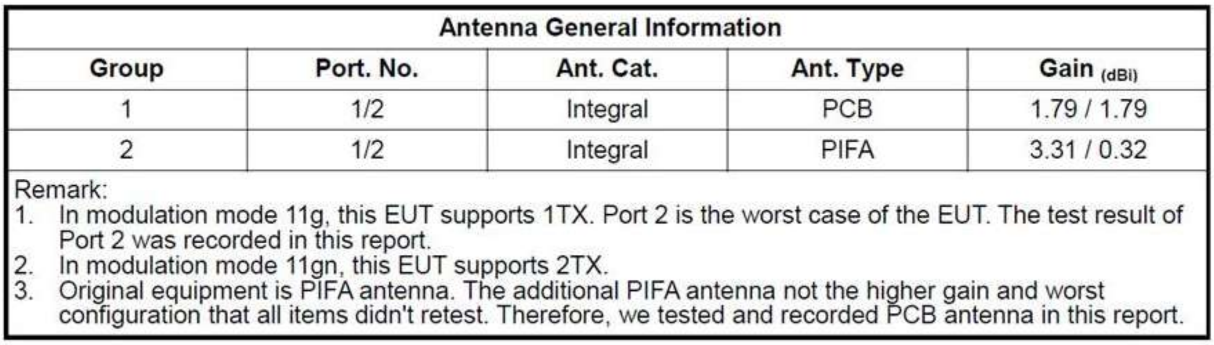
Professional installation

Section 15.204(b) states that an approved "transmission system" must always be marketed as a complete system including the antenna.

APPENDIX:

1). Antenna List

For 2.4GHz Band:

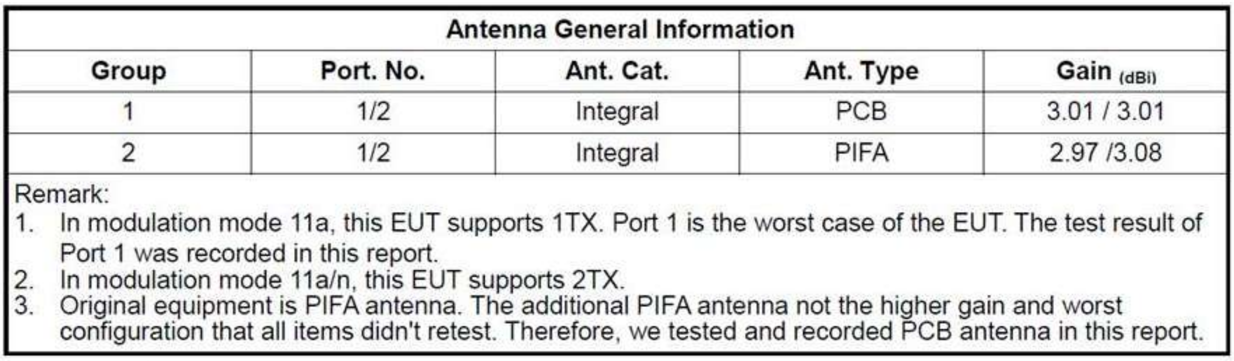


Antenna General Information				
Group	Port. No.	Ant. Cat.	Ant. Type	Gain (dBi)
1	1/2	Integral	PCB	1.79 / 1.79
2	1/2	Integral	PIFA	3.31 / 0.32

Remark:

1. In modulation mode 11g, this EUT supports 1TX. Port 2 is the worst case of the EUT. The test result of Port 2 was recorded in this report.
2. In modulation mode 11gn, this EUT supports 2TX.
3. Original equipment is PIFA antenna. The additional PIFA antenna not the higher gain and worst configuration that all items didn't retest. Therefore, we tested and recorded PCB antenna in this report.

For 5GHz Band:



Antenna General Information				
Group	Port. No.	Ant. Cat.	Ant. Type	Gain (dBi)
1	1/2	Integral	PCB	3.01 / 3.01
2	1/2	Integral	PIFA	2.97 /3.08

Remark:

1. In modulation mode 11a, this EUT supports 1TX. Port 1 is the worst case of the EUT. The test result of Port 1 was recorded in this report.
2. In modulation mode 11a/n, this EUT supports 2TX.
3. Original equipment is PIFA antenna. The additional PIFA antenna not the higher gain and worst configuration that all items didn't retest. Therefore, we tested and recorded PCB antenna in this report.