



AirEther™ SB54/BR54/SC54 USER MANUAL



Corporate Headquarters
Inscape Data Corporation
1620 Oakland Road D101
San Jose, CA 95131 USA

<http://www.inscapedata.com>
Tel: 408 392-9800
1-888-267-4507
Fax: 408 392-9812

Revision 1.5b
Firmware Version 1.29 RC8-h

FCC Notice

NOTE: 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 distance 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.

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

The antenna(s) used for this transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

The manufacturer is not responsible for any radio or TV interference caused by unauthorized modifications to this equipment. Such modifications could void the user's authority to operate the equipment.

PRODUCT NOTES

CAUTION: Please make note of your user name, password, serial number, and MAC Addresses before installation. After configuration, resetting of the user name and password is not permitted due to security reasons. If password and user names are lost, the user will need to ship the unit to Inscape Data for factory hardware reset. Please contact Inscape Data Technical Support if further questions arise.

Please check our website at www.inscapedata.com often for the most current product software and user manual updates.

Revision History:

Version 1.5b Added Support for BR54.

Version 1.5a Updated page 19 & 20, ODU port and mounting bracket diagram.

TABLE OF CONTENTS

1	PRODUCT SUMMARY	6
2	NETWORK TOPOLOGY	7
2.1	AP AND AP CLIENT MODE (SB54 & BR54 ONLY)	7
2.2	AP CLIENT (SC54 ONLY).....	8
2.3	BRIDGE AND MULTIPLE BRIDGE MODE (SB54 & BR54 ONLY).....	9
2.4	REPEATER MODE (SB54 & BR54 ONLY)	10
2.5	CPE ROUTER MODE (SB54 & BR54 ONLY)	11
2.6	INSTALLATION DIAGRAM	12
2.7	POE INJECTOR AND CABLE LENGTH CONSIDERATION.....	14
2.8	LED DEFINITION	14
3	EQUIPMENT CONFIGURATION USING HTTP BROWSER	15
3.1.1	<i>Start Setup by Browser</i>	15
4	WEB MANAGEMENT INTERFACE	16
4.1	STATUS.....	17
4.1.1	<i>System</i>	17
4.1.2	<i>Wireless</i>	18
4.1.3	<i>Security</i>	19
4.1.4	<i>IP Setting</i>	20
4.2	NETWORK	20
4.2.1	<i>Wireless Settings</i>	20
4.2.1.1	AP mode (SB54 & BR54 only).....	21
4.2.1.2	Bridge Mode (SB54 & BR54 only).....	23
4.2.1.3	Multiple Bridge Mode (SB54 & BR54 only).....	25
4.2.1.4	AP Client mode (SB54 & BR54)	27
4.2.1.5	AP Client Mode (SC54)	29
4.2.1.6	CPE Router mode (SB54 & BR54 Only).....	31
4.2.1.7	Repeater Mode (SB54 & BR54 Only)	33
4.2.2	<i>IP Settings</i>	37
4.2.3	<i>Antenna Settings</i>	38
4.2.4	<i>DHCP Settings</i>	39
4.3	DEVICE	40
4.3.1	<i>Bandwidth</i>	40
4.3.2	<i>Firmware Upgrade</i>	41

- 4.3.3 *Reboot*..... 42
- 4.3.4 *Backup/Restore* 43
- 4.3.5 *Hostname*..... 44
- 4.4 SECURITY..... 45
 - 4.4.1 *Access Control* 45
 - 4.4.2 *SNMP*..... 46
 - 4.4.3 *Password Settings*..... 47
- 4.5 LOCALIZATION 48
 - 4.5.1 *Network Time Protocol (NTP)* 48
 - 4.5.2 *Country Code*..... 49
- 5 WIRELESS COMPATIBILITY 50**
 - 5.1 FULLY COMPATIBLE 50
 - 5.2 SEMI-COMPATIBLE 50
 - 5.3 NOT COMPATIBLE 50
- 6 WIRELESS NETWORK PLANNING 51**
 - 6.1 SITE SURVEY..... 51
 - 6.2 PLANNING RADIO PATH..... 51
 - 6.3 ANTENNA HEIGHT..... 53
 - 6.4 ANTENNA TYPES..... 54
 - 6.5 ANTENNA CABLE..... 55
 - 6.6 WEATHER CONSIDERATION 55
- 7 THE WIRELESS TECHNOLOGY 56**
- 8 IEEE 802.11 WIRELESS NETWORK ARCHITECTURE 60**
- 9 APPENDIX..... 63**
 - 9.1 GLOSSARY 63
 - 9.2 SB54 & BR54 DEFAULT & DISPLAY VALUES 66
 - 9.3 SC54 DEFAULT & DISPLAY VALUES 67
 - 9.4 BR54 DEFAULT & DISPLAY VALUES 68
 - 9.5 TECHNICAL SPECIFICATION 69
 - 9.6 PRODUCT HARDWARE INSTALLATION GUIDELINE..... 72
 - 9.7 HARDWARE INSTALLATION GUIDE 74
 - 9.8 WARRANTY 76

1 Product Summary

Inscape Data's AirEther™ all weather SB54 & BR54 Dual Band Multi-Functional Base Station and AirEther all weather SC54 Dual Band Wireless Client Bridge are the industries best cost performing and all-in-one 2.4 GHz and 5GHz license free digital wireless transmission system. The AirEther dual band systems are standard based high power, i.e., 400mW, wireless system compliant to the IEEE 802.11 a/b/g specification with an integrated 12dBi panel antenna and an external antenna connector. The users can select to use an external 2.4GHz or 5GHz antenna based on his or her particular application. The SB54 & BR54 and SC54 wireless systems are ideal for transmission of IP based video and data devices wirelessly from few hundred meters up to several miles. Government strength AES wireless encryption, power over Ethernet port, IP68 all weather rating, and long distance OFDM digital wireless algorithm are just a few of the many standard features of the SB54 & BR54/SC54 product line and are ideal for Internet service providers, network professionals, and remote security monitoring applications where hard wiring is difficult. With increased memory hardware and CPU processing speed, the SB54 & BR54 is the industries most powerful, cost competitive, IEEE 802.11 a/b/g compliant outdoor access point.

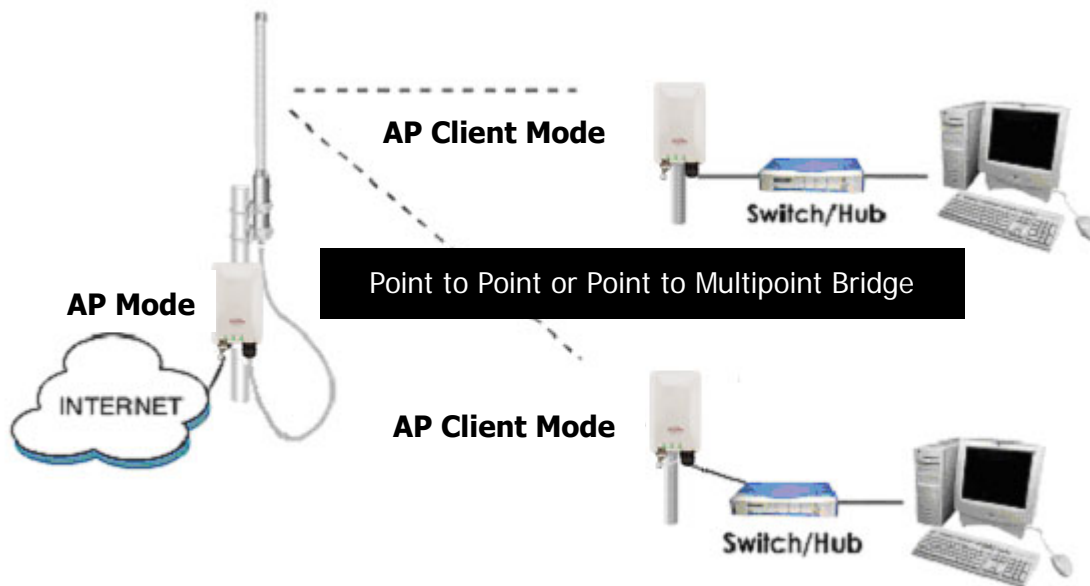
Product Model Specific Feature Matrix

Model	SB54	BR54	SC54
Integrated Antenna Gain	12 dBi	12 dBi	12 dBi
Integrated Antenna Frequency	2.4 ~ 2.5 GHz	5.1 ~ 5.8 GHz	2.4 ~ 2.5 GHz
External Antenna Connector Frequency	2.4 ~ 2.5 GHz 5.1 ~ 5.8 GHz	2.4 ~ 2.5 GHz 5.1 ~ 5.8 GHz	2.4 ~ 2.5 GHz 5.1 ~ 5.8 GHz

2 Network Topology

2.1 AP and AP Client Mode (SB54 & BR54 Only)

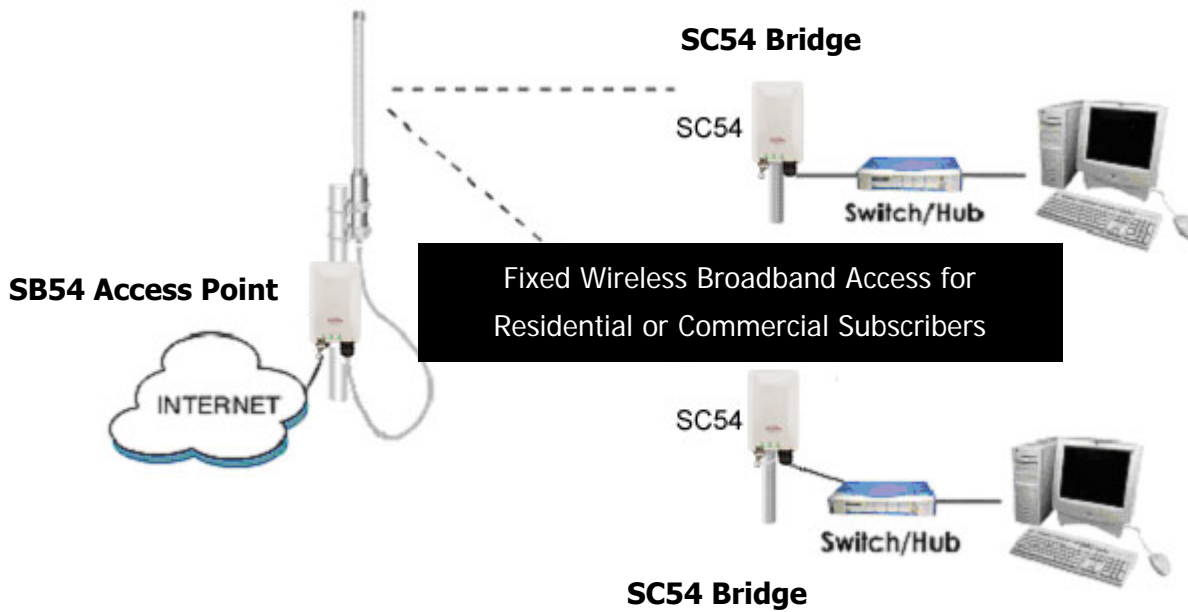
AP Mode and AP Client Mode allow the SB54 & BR54 units to form a wireless point-to-point or point-to-multipoint 802.1d network bridge. With this topology one SB54 & BR54 in AP mode function as the central unit and one or more SB54 & BR54s function as remote unit(s). Once linked, network resources maybe shared or offered between the SB54 & BR54 AP units with the SB54 & BR54 client units.



The topology diagram shown reflects SB54 & BR54's modes of configuration. New configurations maybe available due to periodic new firmware release. The diagrams shown in this manual are used for illustration purposes and may not reflect the most current configuration.

2.2 AP Client (SC54 Only)

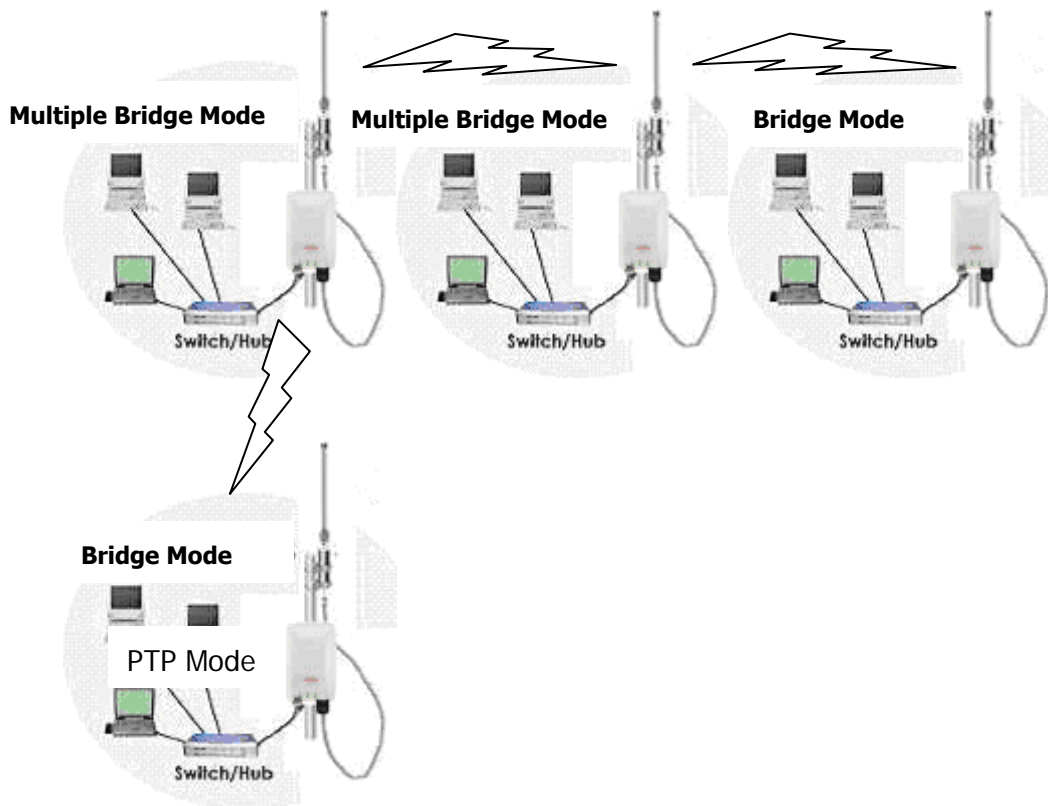
AP Client mode offered on the SC54 unit provides wired-to-wireless Bridge function for the fixed wireless broadband access market. Inscape Data's SC54 may link up to Inscape Data's SB54 & BR54 access point wirelessly to provide last mile connectivity for residential or commercial broadband internet subscribers. Users may enable up-stream and down-stream bandwidth controls on the SC54 product to provide service level tiers to maximize bandwidth usage.



2.3 Bridge and Multiple Bridge Mode (SB54 & BR54 Only)

The bridge and multiple bridge modes are a modification to the 802.11 wireless distribution standards that allows the SB54 & BR54 to communicate with one or more SB54 & BR54s without allowing for stations to connect. The maximum SB54 & BR54 peer communication is eight. This feature allows users to create a single channel transparent bridge to a large area without the need for a dedicated backhaul link. The tradeoff is overall security and throughput is greatly affected for all interlinking LAN segments. Bridge mode supports WEP encryption and multiple bridge mode supports no encryption.

Bridge or multiple bridge modes are not recommended for use with secure wireless applications or when wireless security is a high priority. AP and AP client bridge modes of the SB54 & BR54 described in the previous sections are recommended when high security is desired.

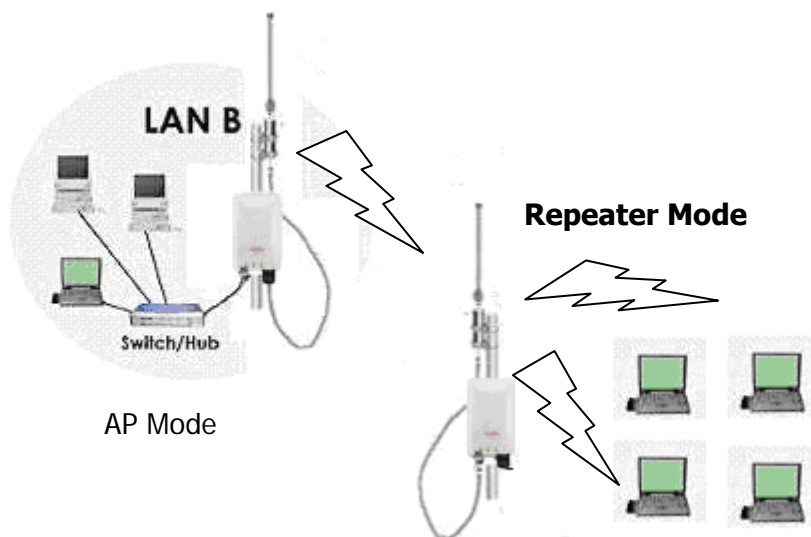


NOTE: Bridge or Multiple bridge mode may not be compatible with third party access points. Due to the slight variations of each vendor's access point implementation, Inscapa Data cannot guarantee compatibility when using third party access point with SB54 & BR54's bridge or multiple bridge modes.

2.4 Repeater Mode (SB54 & BR54 Only)

The repeater mode is a modification to the 802.11 standards that allow the SB54 & BR54 to function as an access point and client simultaneously. This feature allows users to spread coverage to a large area without the need of a backhaul link. The tradeoff is the overall throughput is greatly affected for all users of the access points linked.

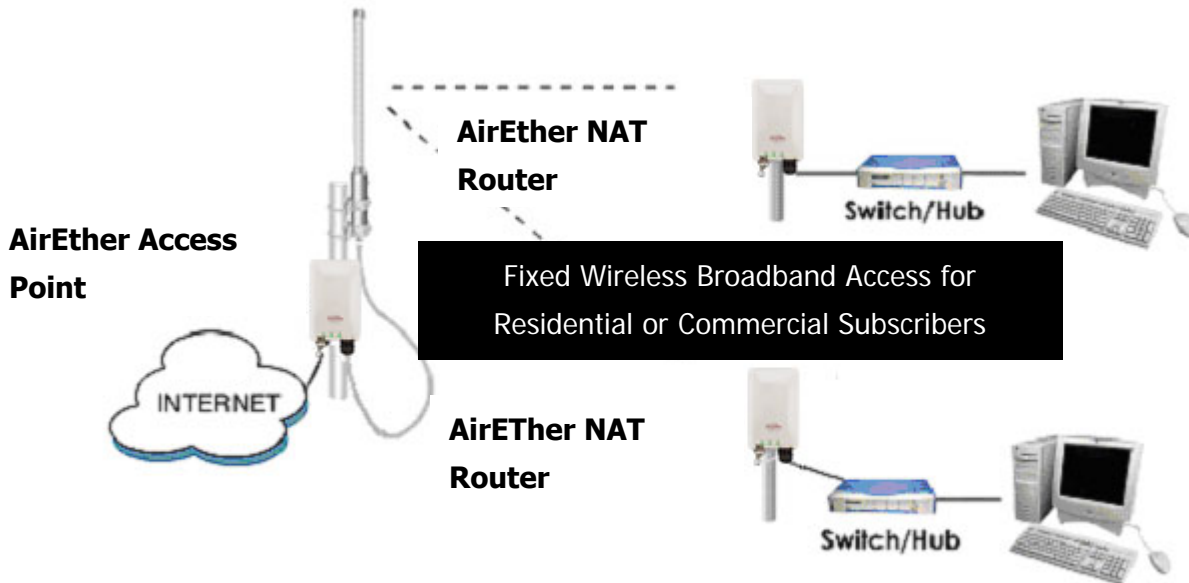
Repeater mode is not recommended with large numbers of clients or when throughput needs to be maximized. Repeater mode should not be used for time sensitive application like voice over IP (VoIP) and IP Video. In both cases, a dedicated point to point link should be used. In areas of low density and mild spectral interference, repeater mode can allow the extension of wireless network coverage into an area at a very low cost.



NOTE: Repeater mode may not be compatible with third party access points not using the Atheros radio chipset. Due to the slight variations of each vendor's access point implementation, Inscope Data cannot guarantee compatibility when using third party access points with SB54 & BR54's configured in repeater mode.

2.5 CPE Router Mode (SB54 & BR54 Only)

CPE Router mode offered on the SB54 & BR54 units provide wired-to-wireless NAT routing function for the fixed wireless broadband access market. Inscap Data's SB54 & BR54 may link up to Inscap Data's SB54 & BR54 access point wirelessly to provide last mile connectivity for residential or commercial broadband internet subscribers. NAT routing offers internet connection sharing with only one IP address. Users may enable DHCP server to locally serve IP schemes to the broadband subscribers. Up-stream and down-stream bandwidth control features also allow service providers to limit bandwidth based on service levels.



2.6 Installation Diagram

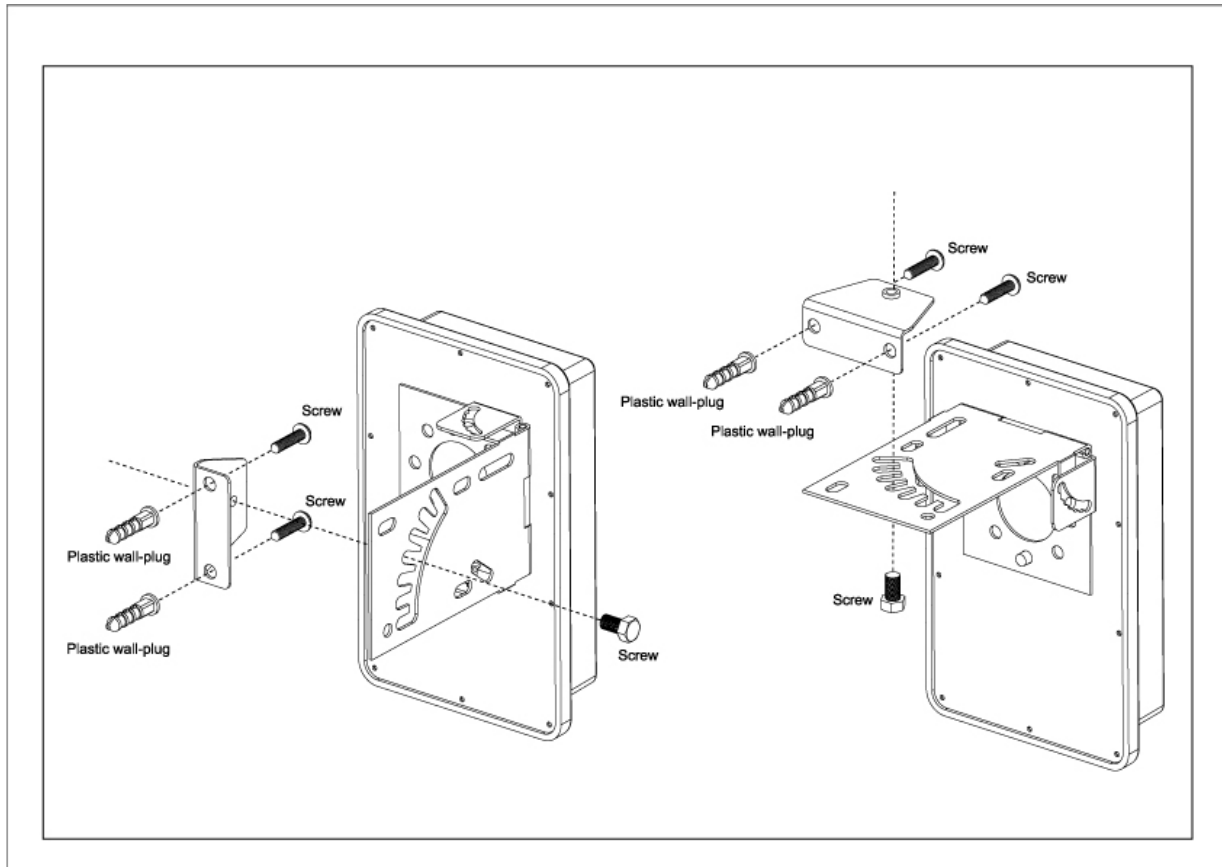


SB54, BR54, and SC54 Installation Diagram

CAUTION: The PIP 100's ODU port has data and power while the RJ 45 port is data only. Please be sure to connect the ODU port of the PIP100 to the SB54 & BR54 or SC54 and the RJ45 port to the Hub/Router/Computer.

Attention:

- Ethernet Cable distance should not exceed 100 meters.
- Make sure the wiring is correct. In 10Mbps operation, Category 3/4/5 cable can be used for connection. To reliably operate your network at 100Mbps, you must use Category 5 cable, or better Data Grade.



1. SYSTEM STATUS LED
 - a. PWR – Power Light
 - b. WLAN
 - i. AP Client / CPE Router / Bridge / Multibridge – Associated or Not Associated
 - ii. AP / Repeater – Wireless Activity. Fast blinking LED means more activity.
 - c. LAN – Network Link or No Link
2. 2.4/5 GHz External Antenna Connector. Type N Female.
3. Weatherproof PoE Port (RJ45 Jack)
4. Embedded 12 dBi directional antenna with 40 degree vertical and horizontal 3 dB beam-width. Point in this direction to maximize alignment of your antenna.

2.7 PoE Injector and Cable Length Consideration

Inscape Data products offer Power over Ethernet (PoE) capabilities and most models include PoE injectors the package. It is highly recommended to use the proper designated PoE injector for Inscape Data PoE capable products. Inscape Data has PoE radios and IP video surveillance cameras using 12VDC, 48VDC, and 802.3af power schemes. Using the wrong injector or power supply may lower the products performance or in most cases damage the product. When making your PoE cables, please adhere to TIA/EIA 568B telecommunication cabling standard.

Please also consider the length of PoE cable versus voltage drop chart below. Using longer PoE cable length may require higher voltage DC Injector to support proper operation of the radio.

PoE Cable Attenuation Table

PoE Cable Length	Voltage Drop
25m	- 3VDC
50m	- 6VDC
75m	- 9VDC
100m	- 12VDC

2.8 LED Definition

MODE	AP, Bridge, Multibridge, Repeater Mode	AP Client, CPE Router Mode
PWR	Power On/Off	Power On/Off
WLAN	TX Activity	Associated to AP & TX Activity
LAN	LAN Connection & Activity	LAN Connection & Activity

3 Equipment Configuration Using HTTP Browser

❖ Verify the IP address setting

You need to configure your PC's network settings to obtain an IP address. Computers use IP addresses to communicate with each other across a network, such as the Internet.

1. From the taskbar, click the **“Start”** button; select **“Settings > Control Panel”**. From there, double-click the **“Network connections”** icon.
2. Right click the **“Local Area Connection”** icon, and select **“Properties”**. Click on the **“TCP/IP”** for the applicable Ethernet adapter. Then, click the **“Properties”** button.
3. Click the **“IP Address”** tab, select **“USE the following IP address”**, enter **192.168.1.x** (Note: **x** could be from 1 to 254) in the **“IP Address”** field and **255.255.255.0** in the **“Subnet Mask”** field, and then click **“OK”** button.

Attention: Use the IP addresses in this section as an example only. The goal is to configure your PC to be in the same sub-network as the equipment you are configuring. Please consult a network administrator if there are any questions on setting up a PC's IP address.

3.1.1 Start Setup by Browser...

1. After getting the correct connection, start the web browser (make sure you disable the proxy) and enter **192.168.x.x (x represent the IP Address for the outdoor unit)** in the **Address** field. Press **Enter**.

THE DEFAULT SB54 & BR54 IP ADDRESS IS 192.168.1.20

2. Enter the factory default value for **User name** and **Password** as follow:
User Name: **“root”**
Password: **“root”**
Then click the **“OK”** button.
3. You will enter the SB54 & BR54 or SC54 configuration homepage.

CAUTION: Please make note of your user name and password carefully. Resetting of the user name and password is not permitted via software due to security reasons. Tampering with the unit in any way will void your product warranty. Hardware resetting of the unit to regain access can only be performed by Inscope Data.

4 Web Management Interface

The Web management interface is an easy to use method for managing the SB54 & BR54 and SC54 units. Once you log in to the SB54 & BR54 or SC54 unit, you may configure it for the following modes to fit your application.

Product	Operation Mode	Application
SB54 & BR54	Access Point, Bridge, AP Client, Multibridge, Repeater, CPE Router	Access Point, Point to Multipoint Bridge, Subscriber Access
SC54	AP Client	Broadband Wireless Subscriber Access

4.1 Status

System status provides pertinent information on the current configuration of the wireless equipment.

4.1.1 System

Shows host name, HTTP configuration web port assignment, Country Code, Device Up time, Firmware Version, Wireless MAC Address, Ethernet MAC Address, and Device Temperature.

The screenshot shows a web browser window titled "High Power WLAN Outdoor Access Point Management interface - Mozilla Firefox". The address bar shows the URL "http://192.168.100.191/01_status_01.php". The page header includes the InscapeData logo and the text "AirEther™ SB54 Dual Band Outdoor Wireless Base Station". A navigation menu contains tabs for "Status", "Network", "Device", "Security", and "Localization", with a "Logout" button on the right. The "Status" tab is active, displaying "System Information" in a table format.

System Information	
Hostname	AirEther
Web port	80
Country Code	Japan
Uptime	1 day
Firmware ver.	1.29-rc8-h
Wireless dev. MAC addr.	00:24:F3:01:00:03
Wired dev. MAC addr.	00:24:F3:01:00:02
Device temperature	41.5 °C 106.7 °F

At the bottom of the page, a status bar displays "Hostname: AirEther 23:59, May 22nd, 2009".

4.1.2 Wireless

The wireless section displays current wireless setting, including operation mode, ESSID, Band, Channel, Enabled Features, Signal Strength of Connected Device, and Security Settings.

The screenshot shows a web browser window titled "High Power WLAN Outdoor Access Point Management interface - Mozilla Firefox". The address bar shows the URL "http://192.168.100.191/01_status_02.php". The page header includes the InscapeData logo and the product name "AirEther™ SB54 Dual Band Outdoor Wireless Base Station". A navigation menu at the top includes "Status", "Network", "Device", "Security", "Localization", and "Logout". The "Status" section is active, displaying "Wireless Information" in a table format.

Wireless Information	
Mode	Access Point (Client List)
ESSID	repeaterTest1234567890
Band	802.11g
Channel	2.422 GHz (Channel 3)
4-addr. Headers	On
Isolate	Off
WMM	On
Encryption	psk/aes
Distance	0
RSSI	55(59%)

At the bottom of the interface, the status bar shows "Hostname: AirEther 00:02, May 23rd, 2009".

4.1.3 Security

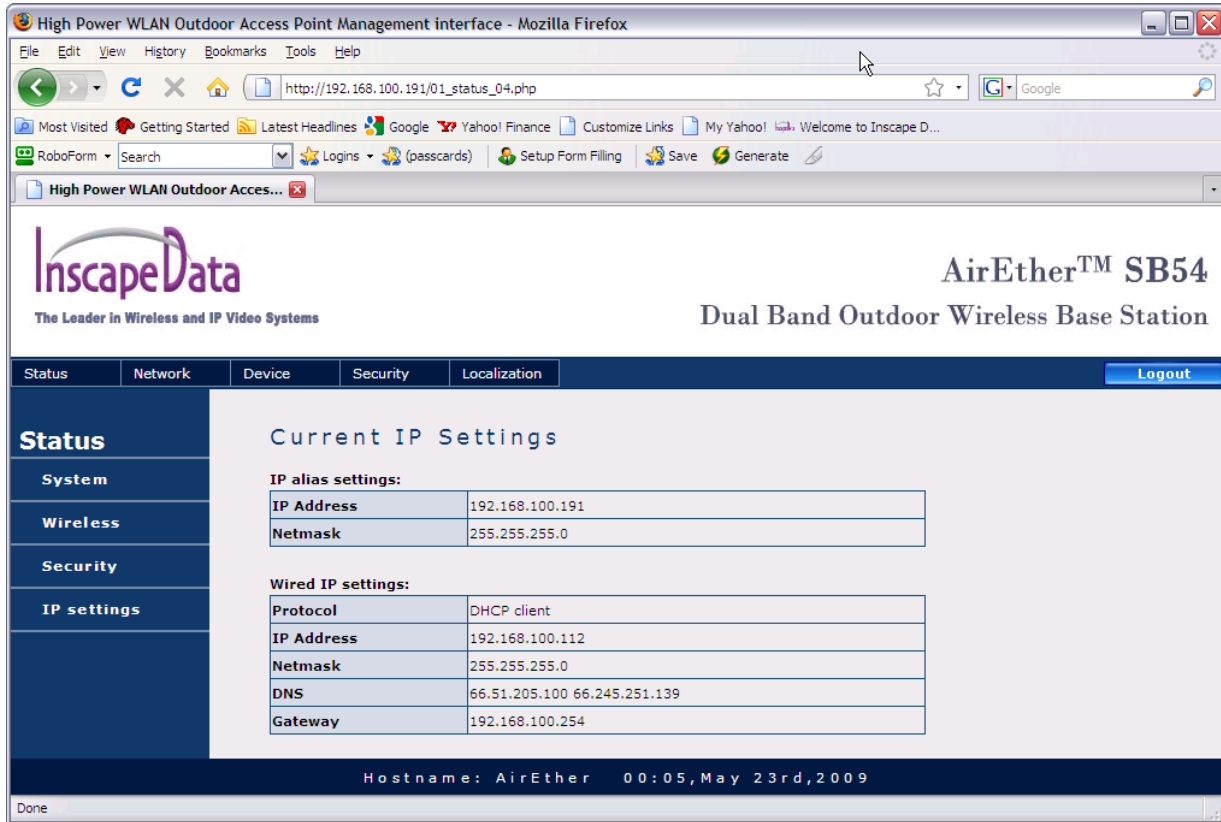
The security section displays access control or SNMP information.

The screenshot shows a web browser window titled "High Power WLAN Outdoor Access Point Management interface - Mozilla Firefox". The address bar shows the URL "http://192.168.100.191/01_status_03.php". The page header includes the InscapeData logo and the text "The Leader in Wireless and IP Video Systems" on the left, and "AirEther™ SB54 Dual Band Outdoor Wireless Base Station" on the right. A navigation menu at the top contains "Status", "Network", "Device", "Security", "Localization", and a "Logout" button. The "Security" tab is selected, and the main content area displays "Security Information" with a table showing "Access Control" set to "None" and "SNMP" set to "Enable". A status bar at the bottom indicates "Hostname: AirEther 00:04, May 23rd, 2009".

Security Information	
Access Control	None
SNMP	Enable

4.1.4 IP Setting

Shows current network settings



4.2 Network

Network Page will show the settings for the Wireless Modes, IP Setting, Antenna Selection, and DHCP.

4.2.1 Wireless Settings

This configuration page allows you to setup your SB54 & BR54 or SC54 unit to the desired wireless operation mode.

Product	Operation Mode	Application
SB54 & BR54	Access Point, Bridge, AP Client, Multibridge, Repeater, CPE Router	Access Point, Point to Multipoint Bridge, Subscriber Access
SC54	AP Client	Broadband Wireless Subscriber Access

To configure the SB54 & BR54/SC54 system, the user should set proper information per the following section.

4.2.1.1 AP mode (SB54 & BR54 only)

The default operation mode is Access Point. This connects your 802.11 compliant wireless PCs and devices to a wired network.

Network Function Settings	
<input checked="" type="radio"/> Access Point <input type="radio"/> Bridge <input type="radio"/> Multiple Bridge <input type="radio"/> AP Client <input type="radio"/> CPE Router	
SSID	AirEther <input type="checkbox"/> Hide SSID
Frequency Band	<input checked="" type="radio"/> Auto <input type="radio"/> 11a <input type="radio"/> 11b only <input type="radio"/> 11g only <input type="radio"/> 11b/g
4-Address Headers	<input checked="" type="radio"/> ON <input type="radio"/> OFF
Isolate	<input type="radio"/> ON <input checked="" type="radio"/> OFF
WMM	<input checked="" type="radio"/> ON <input type="radio"/> OFF
Channel	1 (2.412 GHz) ▼
Distance	0 M (1-50000, 0 is for indoor use.)
Encryption	None ▼
<input type="button" value="Apply"/>	

Once the network mode, Access Point, is selected, the user will have to change any network functions required by the network mode described as follow:

- SSID:** Enter a unique SSID name specified by your network administrator, default is AirEther. The SSID is the unique name shared among all points in a wireless network. The SSID must be identical for all points in the wireless network. It is case-sensitive and must not exceed 32 alphanumeric characters, which may be any keyboard character. Make sure this setting is the same for all points in your wireless network.
- Frequency Band:** Options available are Auto, 11a, 11b only, 11g only, or mixed 11b/g network. Selecting Auto allows the SB54 & BR54 unit to select the base available frequency band for operation. It is recommended to lock in to 11a or 11g modes. For WIFI access, 11b/g maybe desired to allow older 802.11b WIFI stations to connect. For your reference 802.11a "11a operates on the 5 GHZ band while 802.11b or 802.11g operates on the 2.4 GHz band. If using internal 12 dBi 2.4 GHz antenna, antenna 1, only 11b, 11g, or 11b/g option is available. Selecting 11a while antenna 1 is selected may damage your SB54 & BR54 product.
- Hide SSID:** If "Hide SSID" is selected, the AP, i.e., SB54 & BR54 Base Station will be invisible from client's site survey and it will provide better privacy to prevent intruders from accessing the wireless service.

- **4-Address Headers:** Select ON to enable 802.1d Transparent Bridge functionality. If this is selected, ON, then 4-Address Headers on the SC54 Wireless Client Bridge should also be enabled, ON. Default configuration is ON. Turning 4-Address Headers OFF will enable MAC Address translation. Leave this option ON if you are not too sure about this feature.
- **Isolate:** If this is ON, it will prohibit communications among the SC54 or Wireless Client. That is, one SC54 will not be able to communicate with another SC54 through an SB54 & BR54 configured as a access point.
- **WMM:** Select ON to enable the QoS (Quality of Service) feature. This WMM feature is one of IEEE 802.11 standards. WMM prioritizes traffic according to four Access Categories, i.e., voice, video, best effort, and background.
- **Transmit Power:** Transmit power control limits the Tx power output. The default is FULL power. Options available are $\frac{1}{2}$, $\frac{1}{4}$, $\frac{1}{8}$, and $\frac{1}{16}$. Selecting certain countries will limit the TX output power to conform to its local regulatory domain.
- **Channel:** Enter a frequency channel number specified or used by your wireless network. Select the appropriate channel from the list provided to correspond with your network settings. All points in your wireless network must use the same channel in order to function correctly. Stay with default setting if you do not have special request on channel selection.
- **Distance:** Enter the distance between the AP, i.e., SB54 & BR54 Base Station, and the SC54 Wireless Client or another SB54 & BR54 functioning as an AP client unit. Enter the longest distance between all linked equipment into every unit of the wireless link.

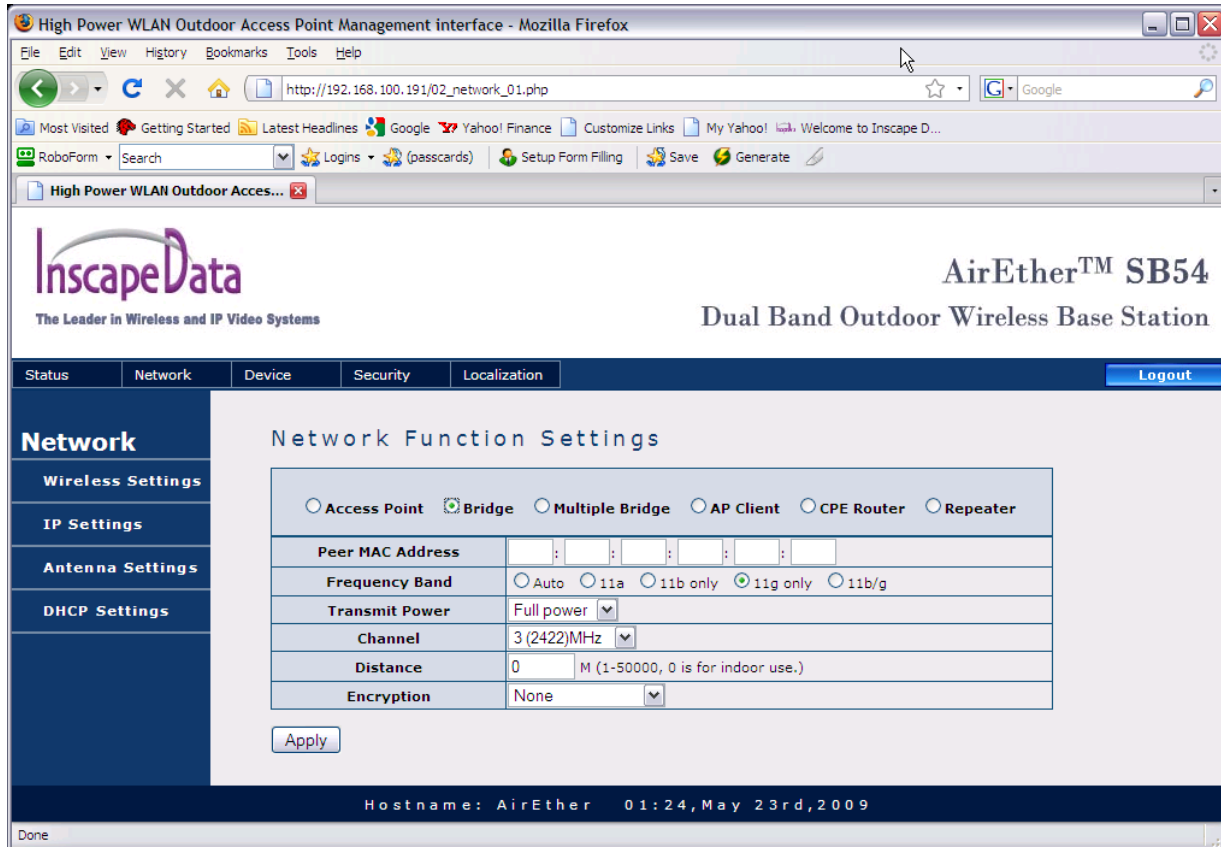


NOTE: The distance number should be greater than or equal to the real distance. An incorrect distance value will impact or degrade the performance of the wireless link.

- **Encryption:** NONE, WEP, WPA, or WPA2. The wireless security settings configure the security of your wireless network. There are three wireless security mode options supported by the Access Point: WEP, WPA-PSK and WPA2-PSK. (WPA stands for Wi-Fi Protected Access, which is a security standard stronger than WEP encryption. WEP stands for Wired Equivalent Privacy.). Once you setup the AP to work in security mode, all wireless stations will also need to have corresponding settings. System default setting is “No Security”.

4.2.1.2 **Bridge Mode (SB54 & BR54 only)**

In the Bridge mode, the WLAN MAC address of the peer device is needed to make a wireless bridge link.



- **Peer MAC Address:** Enter the WLAN MAC address of another Wireless Bridge, SB54 & BR54.
- **Frequency Band:** Options available are Auto, 11a, 11b only, 11g only, or mixed 11b/g network. Selecting Auto allows the SB54 & BR54 unit to select the base available frequency band for operation. It is recommended to lock in to 11a or 11g modes. For WIFI access, 11b/g maybe desired to allow older 802.11b WIFI stations to connect. For your reference 802.11a "11a operates on the 5 GHz band while 802.11b or 802.11g operates on the 2.4 GHz band. If using the internal 12 dBi 2.4 GHz antenna, antenna 1, only 11b, 11g, or 11b/g option is available. Selecting 11a while antenna 1 is selected may damage your SB54 & BR54 product.
- **Transmit Power:** Transmit power control limits the Tx power output. The default is FULL power. Options available are ½, ¼, 1/8, and 1/16. Selecting certain countries will limit the TX output power to conform to its local regulatory domain.

- **Channel:** Enter a frequency channel number specified or used by your wireless network. Select the appropriate channel from the list provided to correspond with your network settings. All points in your wireless network must use the same channel in order to function correctly. Stay with the default settings if you do not require a specific channel selection.
- **Distance:** The distance function adjusts wireless system link timing. It is critical to enter the correct values for your wireless network. Enter a distance value according to the longest link distance between the point to point or point to multi-point in the network.



NOTE: The distance number should be greater than or equal to the real distance. An incorrect distance value will impact or degrade the performance of the wireless link.

- **Encryption:** The wireless security settings configure the security of your wireless network. WEP wireless security is available for bridge mode. WEP stands for Wired Equivalent Privacy. Once you setup the AP to work in security mode, all wireless bridges will also need to have corresponding settings. System default setting is “**No Security**”.

•

4.2.1.3 Multiple Bridge Mode (SB54 & BR54 only)

In the Multiple Bridge mode, you can link one SB54 & BR54 with multiple SB54 & BR54s using the WLAN MAC address of the SB54 & BR54s.

The screenshot displays the management interface for the AirEther™ SB54 Dual Band Outdoor Wireless Base Station. The browser window title is "High Power WLAN Outdoor Access Point Management interface - Mozilla Firefox". The address bar shows the URL "http://192.168.100.191/02_network_01.php". The page header includes the InscapeData logo and the product name "AirEther™ SB54 Dual Band Outdoor Wireless Base Station". The navigation menu includes "Status", "Network", "Device", "Security", "Localization", and "Logout". The "Network" section is expanded, showing "Wireless Settings", "IP Settings", "Antenna Settings", and "DHCP Settings". The "Network Function Settings" section is active, showing the following configuration:

<input type="radio"/> Access Point <input type="radio"/> Bridge <input checked="" type="radio"/> Multiple Bridge <input type="radio"/> AP Client <input type="radio"/> CPE Router <input type="radio"/> Repeater	
Peer 1 MAC Address	: : : : : : : :
Peer 2 MAC Address	: : : : : : : :
Peer 3 MAC Address	: : : : : : : :
Peer 4 MAC Address	: : : : : : : :
Peer 5 MAC Address	: : : : : : : :
Peer 6 MAC Address	: : : : : : : :
Peer 7 MAC Address	: : : : : : : :
Peer 8 MAC Address	: : : : : : : :
Frequency Band	<input type="radio"/> Auto <input type="radio"/> 11a <input type="radio"/> 11b only <input checked="" type="radio"/> 11g only <input type="radio"/> 11b/g
Transmit Power	Full power
Channel	3 (2422)MHz
Distance	0 M (1-50000, 0 is for indoor use.)

An "Apply" button is located below the settings table. The footer of the interface shows "Hostname: AirEther 00:59, May 23rd, 2009".

- **Peer MAC Address:** Enter the WLAN MAC address of another Wireless Bridge, SB54 & BR54, up to 8 Wireless Bridges are supported in a point to multi point bridge
- **Frequency Band:** Options available are Auto, 11a, 11b only, 11g only, or mixed 11b/g network. Selecting Auto allows the SB54 & BR54 unit to select the base available frequency band for operation. It is recommended to lock in to 11a or 11g modes. For WIFI access, 11b/g maybe desired to allow older 802.11b WIFI stations to connect. For your reference 802.11a "11a operates on the 5 GHZ band while 802.11b or 802.11g operates on the 2.4 GHZ band. If using the internal 12 dBi 2.4 GHz antenna, antenna 1,

only 11b, 11g, or 11b/g option is available. Selecting 11a while antenna 1 is selected may damage your SB54 & BR54 product.

- **Transmit Power:** Transmit power control limits the Tx power output. The default is FULL power. Options available are $\frac{1}{2}$, $\frac{1}{4}$, $\frac{1}{8}$, and $\frac{1}{16}$. Selecting certain countries will limit the TX output power to conform to its local regulatory domain.
- **Channel:** Enter a frequency channel number specified or used by your wireless network. Select the appropriate channel from the list provided to correspond with your network settings. All points in your wireless network must use the same channel in order to function correctly. Stay with default setting if you do not have special request on channel selection.
- **Distance:** The distance function adjusts wireless system link timing. It is critical to enter the correct values for your wireless network. Enter a distance value according to the longest link distance between the point to point or point to multi-point in the network.

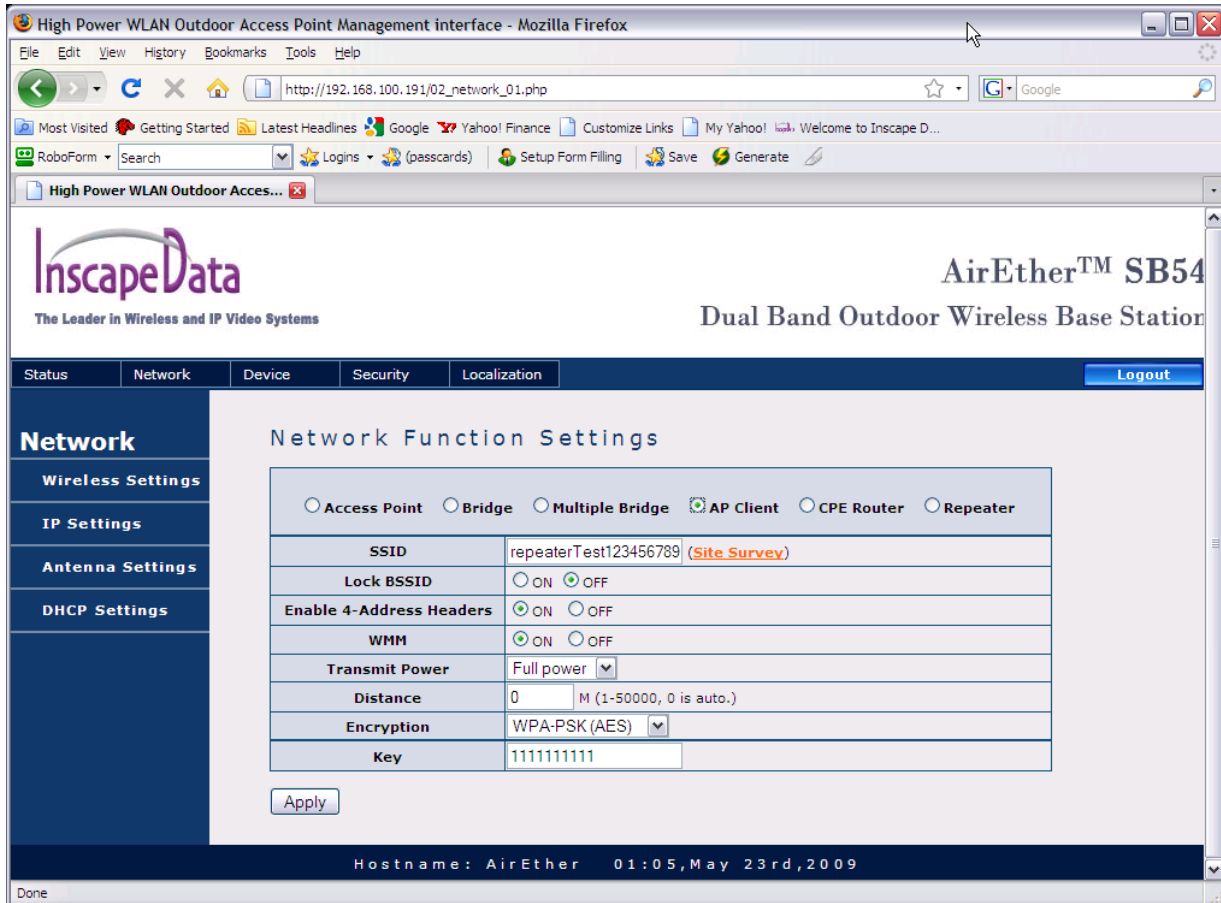


NOTE: The distance number should be greater than or equal to the real distance. An incorrect distance value will impact or degrade the performance of the wireless link.

- **Encryption:** NONE. Please note, in multiple bridge mode wireless security is not available. Use this mode only if wireless encryption is not required. System default setting is “**No Security**”.

4.2.1.4 **AP Client mode (SB54 & BR54)**

The SB54 & BR54 supports the AP Client mode to function as a point to multipoint wireless bridge. To enable the AP Client Mode, the user will select the AP Client Mode.



- **SSID:** Enter a unique SSID name specified by your network administrator, default is AirEther. The SSID is the unique name shared among all points in a wireless network. The SSID must be identical for all points in the wireless network. It is case-sensitive and must not exceed 32 alphanumeric characters, which may be any keyboard character. Make sure this setting is the same for all points in your wireless network.
- **Lock BSSID:** This will lock into the associated unit's MAC address.
- **Enable 4-Address Headers:** Select ON to enable 802.1d Transparent Bridge function. If this is selected, ON, then 4-Address Headers on the SB54 & BR54 or SC54 should also be enabled, ON. Default configuration is ON. Turning 4-Address Headers OFF will enable MAC Address translation. Leave this option ON if you are not too sure about this feature.

- **WMM:** Select ON to enable the QoS (Quality of Service) feature. This WMM feature is one of IEEE 802.11 standards. WMM prioritizes traffic according to four Access Categories, i.e., voice, video, best effort, and background.
- **Transmit Power:** Transmit power control limits the Tx power output. The default is FULL power. Options available are $\frac{1}{2}$, $\frac{1}{4}$, $\frac{1}{8}$, and $\frac{1}{16}$. Selecting certain countries will limit the TX output power to conform to its local regulatory domain.
- **Distance:** Enter the distance between the AP, i.e., SB54 & BR54 Base Station, and the SC54 Wireless Client or another SB54 & BR54 functions as an AP client unit. Enter a distance value according to the longest link distance between the point to point or point to multi-point in the network.



NOTE: The distance number should be greater than or equal to the real distance. An incorrect distance value will impact or degrade the performance or the wireless link.

- **Encryption:** NONE, or WEP, WPA, or WPA2. The wireless security settings configure the security of your wireless network. There are three wireless security mode options supported by the Access Point: WEP, WPA-PSK and WPA2-PSK. (WPA stands for Wi-Fi Protected Access, which is a security standard stronger than WEP encryption. WEP stands for Wired Equivalent Privacy.). Once you setup the AP to work in security mode, all wireless stations will also need to have corresponding settings. System default setting is “**No Security**”.

•

4.2.1.5 AP Client Mode (SC54)

The SC54 Wireless Client Bridge supports the AP Client mode. AP client mode allows subscriber broadband access. In this mode, up-stream and down-stream bandwidth control is adjustable to create service level tiers.

Network Function Settings	
<input checked="" type="radio"/> AP Client	
SSID	AirEther (Site Survey)
Lock BSSID	<input type="radio"/> ON <input checked="" type="radio"/> OFF
Enable Burst	<input type="radio"/> ON <input checked="" type="radio"/> OFF
Enable 4-Address Headers	<input type="radio"/> ON <input checked="" type="radio"/> OFF
WMM	<input type="radio"/> ON <input checked="" type="radio"/> OFF
Distance	0 M (1-50000, 0 is auto.)
Encryption	None

Apply

Hostname: AirEther 00:12,Jan 01st,2000

- **SSID:** Enter a unique SSID name specified by your network administrator, default is AirEther. The SSID is the unique name shared among all points in a wireless network. The SSID must be identical for all points in the wireless network. It is case-sensitive and must not exceed 32 alphanumeric characters, which may be any keyboard character. Make sure this setting is the same for all points in your wireless network.
- **Lock BSSID:** This will lock into the associated unit's MAC address.
- **Enable 4-Address Headers:** Select ON to enable Transparent Bridge functionality. If this is selected, ON, then 4-Address Headers on the SC54 Wireless Client Bridges should also be enabled, ON.
- **WMM:** Select ON to enable the QoS (Quality of Service) feature. This WMM feature is one of IEEE 802.11 standards. WMM prioritizes traffic according to four Access Categories, i.e., voice, video, best effort, and background.

- **Transmit Power:** Transmit power control limits the Tx power output. The default is FULL power. Options available are $\frac{1}{2}$, $\frac{1}{4}$, $\frac{1}{8}$, and $\frac{1}{16}$. Selecting certain countries will limit the TX output power to conform to its local regulatory domain.
- **Distance:** The distance function adjusts wireless system link timing. It is critical to enter the correct values for your wireless network. Enter a distance value according to the longest link distance between the point to point or point to multi-point in the network.



NOTE: The distance number should be greater than or equal to the real distance. An incorrect distance value will impact or degrade the performance of the wireless link.

- **Encryption:** NONE, WEP, WPA, or WPA2. The wireless security settings configure the security of your wireless network. There are three wireless security mode options supported by the Access Point: WEP, WPA-PSK, and WPA2-PSK. (WPA stands for Wi-Fi Protected Access, which is a security standard stronger than WEP encryption. WEP stands for Wired Equivalent Privacy.). Once you setup the AP to work in security mode, all wireless stations will also need to have corresponding settings. System default setting is “**No Security**”.

4.2.1.6 CPE Router mode (SB54 & BR54 Only)

When you select the CPE Router Mode on the SB54 & BR54, multiple SC54s or other wireless clients are able to connect to the SB54 & BR54 by Network Address Translation (NAT) and DHCP. NAT allows the sharing of a single IP address to multiple hosts behind the wireless device.

Network Function Settings	
<input type="radio"/> Access Point <input type="radio"/> Bridge <input type="radio"/> Multiple Bridge <input type="radio"/> AP Client <input checked="" type="radio"/> CPE Router	
SSID	AirEther (Site Survey)
Lock BSSID	<input type="radio"/> ON <input checked="" type="radio"/> OFF
Enable Burst	<input type="radio"/> ON <input checked="" type="radio"/> OFF
Enable 4-Address Headers	<input checked="" type="radio"/> ON <input type="radio"/> OFF
WMM	<input checked="" type="radio"/> ON <input type="radio"/> OFF
Distance	0 M (1-50000, 0 is auto.)
Encryption	None
<input type="button" value="Apply"/>	

- **SSID:** Enter a unique SSID name specified by your network administrator, default is AirEther. The SSID is the unique name shared among all points in a wireless network. The SSID must be identical for all points in the wireless network. It is case-sensitive and must not exceed 32 alphanumeric characters, which may be any keyboard character. Make sure this setting is the same for all points in your wireless network.
- **Lock BSSID:** This will lock into the associated unit's MAC address.
- **Enable 4-Address Headers:** Select ON to enable Transparent Bridge functionality. If this is selected, ON, then 4-Address Headers on the SC54 Wireless Client Bridges should also be enabled, ON.
- **WMM:** Select ON to enable the QoS (Quality of Service) feature. This WMM feature is one of IEEE 802.11 standards. WMM prioritizes traffic according to four Access Categories, i.e., voice, video, best effort, and background.

- **Transmit Power:** Transmit power control limits the Tx power output. The default is FULL power. Options available are $\frac{1}{2}$, $\frac{1}{4}$, $\frac{1}{8}$, and $\frac{1}{16}$. Selecting certain countries will limit the TX output power to conform to its local regulatory domain.
- **Distance:** The distance function adjusts wireless system link timing. It is critical to enter the correct values for your wireless network. Enter a distance value according to the longest link distance between the point to point or point to multi-point in the network.



NOTE: The distance number should be greater than or equal to the real distance. An incorrect distance value will impact or degrade the performance of the wireless link.

- **Encryption:** NONE, WEP, WPA, or WPA2. The wireless security settings configure the security of your wireless network. There are three wireless security mode options supported by the Access Point: WEP, WPA-PSK, and WPA2-PSK. (WPA stands for Wi-Fi Protected Access, which is a security standard stronger than WEP encryption. WEP stands for Wired Equivalent Privacy.). Once you setup the AP to work in security mode, all wireless stations will also need to have corresponding settings. System default setting is “**No Security**”.

4.2.1.7 Repeater Mode (SB54 & BR54 Only)

The repeater mode is a modification to the 802.11 standards that allow the SB54 & BR54 to function as an access point and client simultaneously. This feature allows users to spread coverage to a large area without the need of a backhaul link. The tradeoff is the overall throughput is greatly affected for all users of the access points linked.

Repeater mode is not recommended with large numbers of clients or when throughput needs to be maximized. Repeater mode should not be used for time sensitive application like voice over IP (VoIP) and IP Video. In both cases, a dedicated point to point link should be used. In areas of low density and mild spectral interference, repeater mode can allow the extension of wireless network coverage into an area at a very low cost.

NOTE: Repeater mode may not be compatible with third party access points not using the Atheros radio chipset. Due to the slight variation of each vendor's access point implementation, Inscope Data cannot guarantee compatibility when using third party access points with SB54 & BR54's configured in repeater mode.

High Power WLAN Outdoor Access Point Management interface - Mozilla Firefox

http://192.168.100.191/02_network_01.php

InscapeData
The Leader in Wireless and IP Video Systems

AirEther™ SB54
Dual Band Outdoor Wireless Base Station

Status Network Device Security Localization Logout

Network

Wireless Settings
IP Settings
Antenna Settings
DHCP Settings

Network Function Settings

Access Point Bridge Multiple Bridge AP Client CPE Router Repeater

Target AP SSID	<input type="text" value=""/>	(Site Survey)
Enable 4-Address Headers	<input checked="" type="radio"/> ON <input type="radio"/> OFF	
WMM	<input checked="" type="radio"/> ON <input type="radio"/> OFF	
Distance	0	M (1-50000, 0 is for indoor use.)
Encryption	None	
Transmit Power	Full power	
Local AP SSID	repeaterTest123456789	<input type="checkbox"/> Hide SSID
Frequency Band	<input type="radio"/> Auto <input type="radio"/> 11a <input type="radio"/> 11b only <input checked="" type="radio"/> 11g only <input type="radio"/> 11b/g	
Enable 4-Address Headers	<input checked="" type="radio"/> ON <input type="radio"/> OFF	
Isolate	<input type="radio"/> ON <input checked="" type="radio"/> OFF	
WMM	<input checked="" type="radio"/> ON <input type="radio"/> OFF	
Channel	3 (2422)MHz	
Encryption	WPA-PSK (AES)	
Key	1111111111	

Apply

Hostname: AirEther 01:28, May 23rd, 2009

- **Target SSID:** Enter a unique SSID of the root Access Point to associate to. The default value is AirEther. The SSID is the unique name shared among all points in a wireless network. The SSID must be identical for all points in the wireless network. It is case-sensitive and must not exceed 32 alphanumeric characters, which may be any keyboard character. Make sure this setting is the same for all points in your wireless network.
- **Enable 4-Address Headers:** Select ON to enable Transparent Bridge functionality. If this is selected, ON, then 4-Address Headers on the SC54 Wireless Client Bridges should also be enabled, ON.
- **WMM:** Select ON to enable the QoS (Quality of Service) feature. This WMM feature is one of IEEE 802.11 standards. WMM prioritizes traffic according to four Access Categories, i.e., voice, video, best effort, and background.

- **Distance:** The distance function adjusts wireless system link timing. It is critical to enter the correct values for your wireless network. Enter a distance value according to the longest link distance between the point to point or point to multi-point in the network.



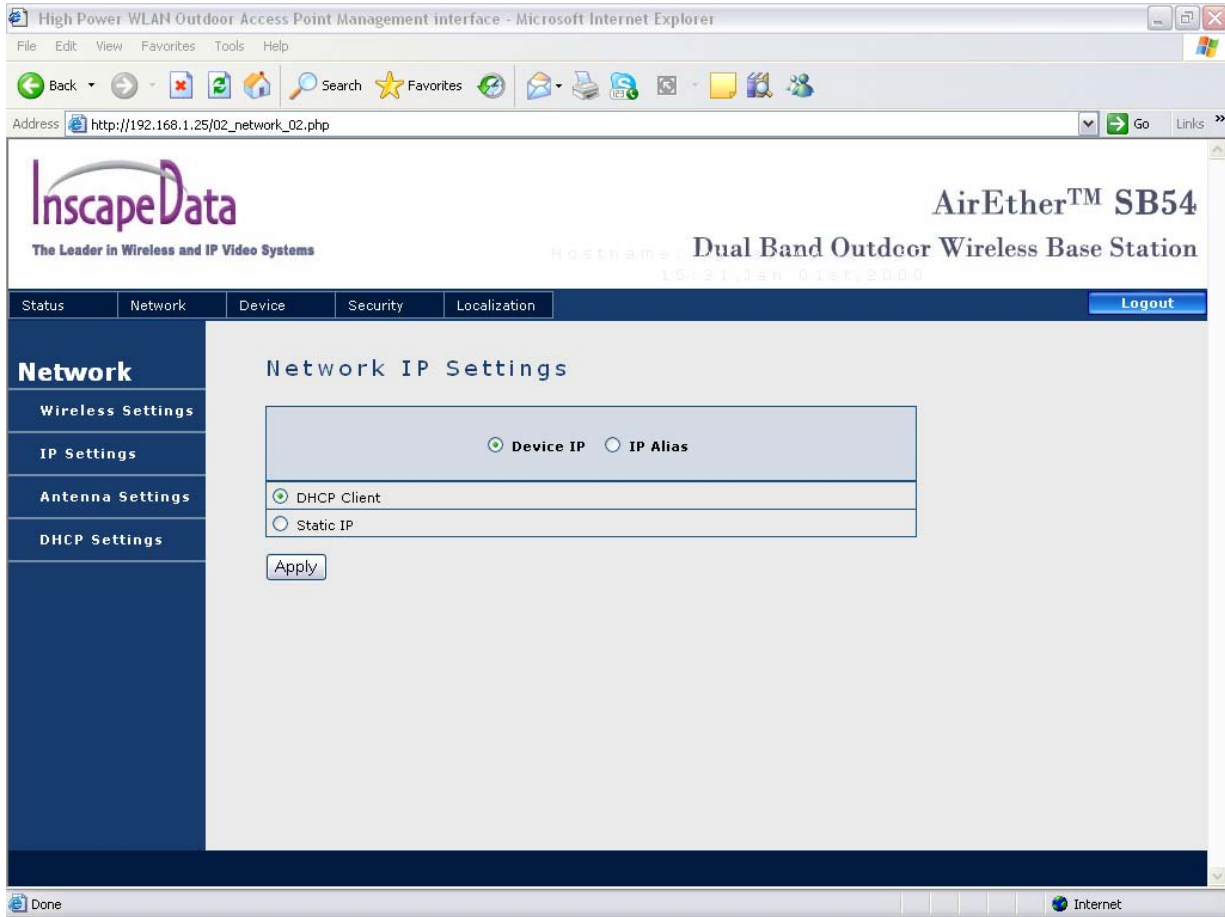
NOTE: The distance number should be greater than or equal to the real distance. An incorrect distance value will impact or degrade the performance of the wireless link.

- **Transmit Power:** Transmit power control limits the Tx power output. The default is FULL power. Options available are 1/2, 1/4, 1/8, and 1/16. Selecting certain countries will limit the TX output power to conform to its local regulatory domain.
- **Local AP SSID:** Enter a unique SSID name for the local wireless coverage area. This SSID should be specified by your network administrator, default is AirEther. The SSID is the unique name shared among all points in a wireless network. The SSID must be identical for all points in the wireless network. It is case-sensitive and must not exceed 32 alphanumeric characters, which may be any keyboard character. Make sure this setting is the same for all points in your wireless network.
- **Hide SSID:** If "Hide SSID" is selected, the AP, i.e., SB54 & BR54 Base Station will be invisible from client's site survey and will provide better privacy to prevent intruders from accessing the wireless service.
- **Frequency Band:** Options available are Auto, 11a, 11b only, 11g only, or mixed 11b/g network. Selecting Auto allows the SB54 & BR54 unit to select the base available frequency band for operation. It is recommended to lock in to 11a or 11g modes. For WIFI access, 11b/g maybe desired to allow older 802.11b WIFI stations to connect. For your reference 802.11a "11a operates on the 5 GHZ band while 802.11b or 802.11g operates on the 2.4 GHZ band. If using the internal 12 dBi 2.4 GHz antenna, antenna 1, only 11b, 11g, or 11b/g option is available. Selecting 11a while antenna 1 is selected may damage your SB54 & BR54 product.
- **4-Address Headers:** Select ON to enable 802.1d Transparent Bridge functionality. If this is selected, ON, then 4-Address Headers on the SC54 Wireless Client Bridge should also be enabled, ON. Default configuration is ON. Turning 4-Address Headers OFF will enable MAC Address translation. Leave this option ON if you are not too sure about this feature.
- **Isolate:** If this is ON, it will prohibit communication among the SC54 or Wireless Client. That is, one SC54 will not be able to communicate with another SC54.

- **WMM:** Select ON to enable the QoS (Quality of Service) feature. This WMM feature is one of IEEE 802.11 standards. WMM prioritizes traffic according to four Access Categories, i.e., voice, video, best effort, and background.
- **Channel:** Enter a frequency channel number specified or used by your wireless network. Select the appropriate channel from the list provided to correspond with your network settings. All points in your wireless network must use the same channel in order to function correctly. Stay with default setting if you do not have special request on channel selection.
- **Encryption:** NONE, WEP, WPA, or WPA2. The wireless security settings configure the security of your wireless network. There are three wireless security mode options supported by the Access Point: WEP, WPA-PSK, and WPA2-PSK. (WPA stands for Wi-Fi Protected Access, which is a security standard stronger than WEP encryption. WEP stands for Wired Equivalent Privacy.). Once you setup the AP to work in security mode, all wireless stations will also need to have corresponding settings. System default setting is “**No Security**”.

4.2.2 IP Settings

- **Network IP settings-** On this page you can set the IP as either DHCP or static IP. You also have the option of assigning a secondary IP address in the IP alias setting. You will also enter the subnet mask, which is the mask of a subnet in which the AP operates. Default gateway can also be entered here. This is the address needed for communication with an external network. Default



4.2.3 Antenna Settings

- **Antenna Selection** - You need to determine whether you want to use the integrated antenna or an external antenna for your device. You can set this for both transmit and receive ends. Antenna 1 will use the following built-in model specific antenna. The following table indicates the frequency of the integrated antenna and external antenna frequency options:

Model	SB54	BR54	SC54
Integrated Antenna Gain	12 dBi	12 dBi	12 dBi
Integrated Antenna Frequency	2.4 ~ 2.5 GHz	5.1 ~ 5.8 GHz	2.4 ~ 2.5 GHz
External Antenna Connector Frequency	2.4 ~ 2.5 GHz	2.4 ~ 2.5 GHz	2.4 ~ 2.5 GHz
	5.1 ~ 5.8 GHz	5.1 ~ 5.8 GHz	5.1 ~ 5.8 GHz

- **Antenna 1** – Select this option if using the integrated antenna.
- **Antenna 2** – Select this option if using external antenna.

The screenshot shows a web browser window displaying the management interface for an AirEther™ SB54 Dual Band Outdoor Wireless Base Station. The browser title is "High Power WLAN Outdoor Access Point Management interface - Microsoft Internet Explorer". The address bar shows "http://192.168.1.25/02_network_03.php".

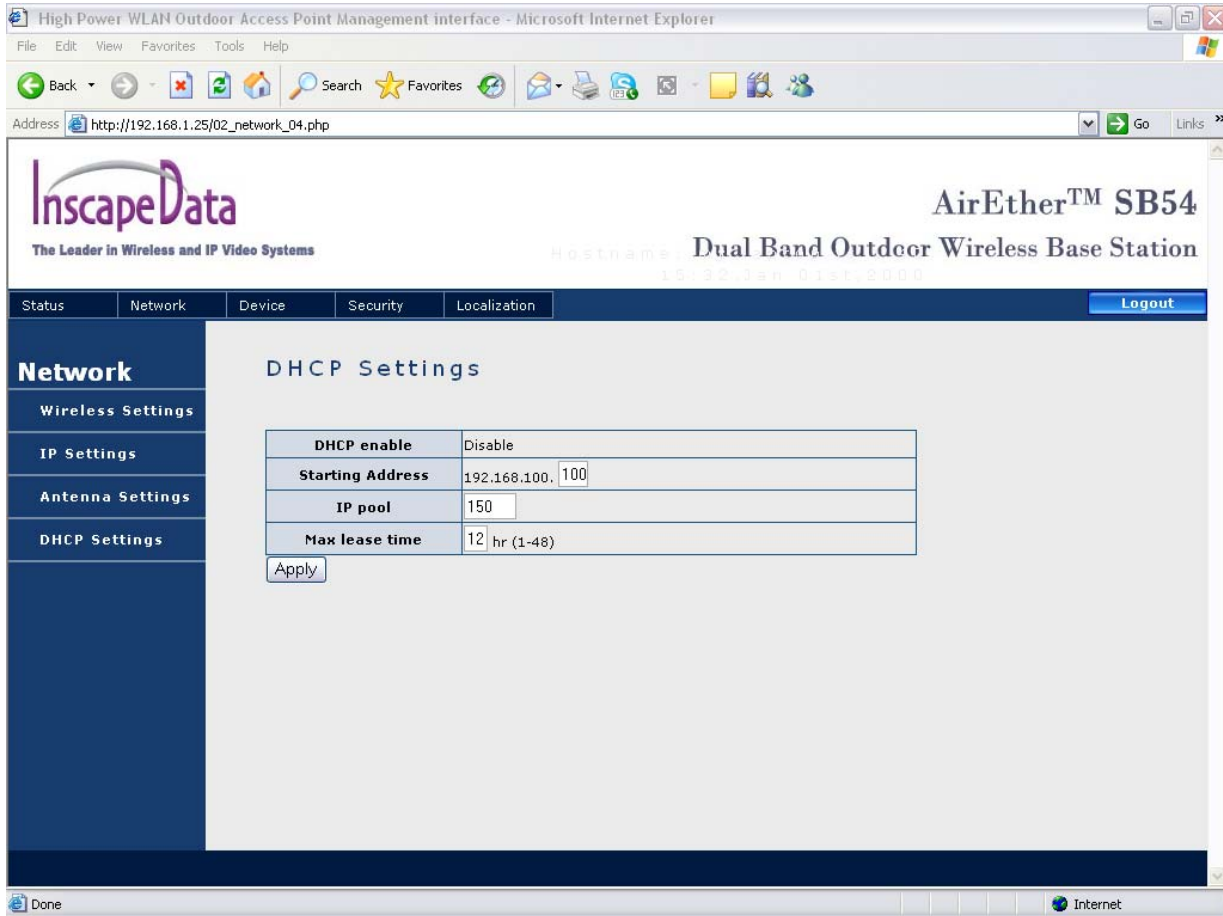
The interface features the InscapeData logo and the text "The Leader in Wireless and IP Video Systems". The device name is "AirEther™ SB54" and the model is "Dual Band Outdoor Wireless Base Station". The hostname is "192.168.1.25" and the date is "15:32:14 on 01st 2008".

The navigation menu includes "Status", "Network", "Device", "Security", "Localization", and "Logout". The "Network" menu is expanded, showing "Wireless Settings", "IP Settings", "Antenna Settings", and "DHCP Settings".

The "Antenna Selection" page is displayed, showing a radio button selection for "Antenna1" (selected) and "Antenna2". There is an "Apply" button below the selection.

4.2.4 DHCP Settings

- **DHCP Settings** - On this page you can set whether you want the unit to distribute IP addresses, which will act similar to a router. **This is only enabled in CPE router mode.**

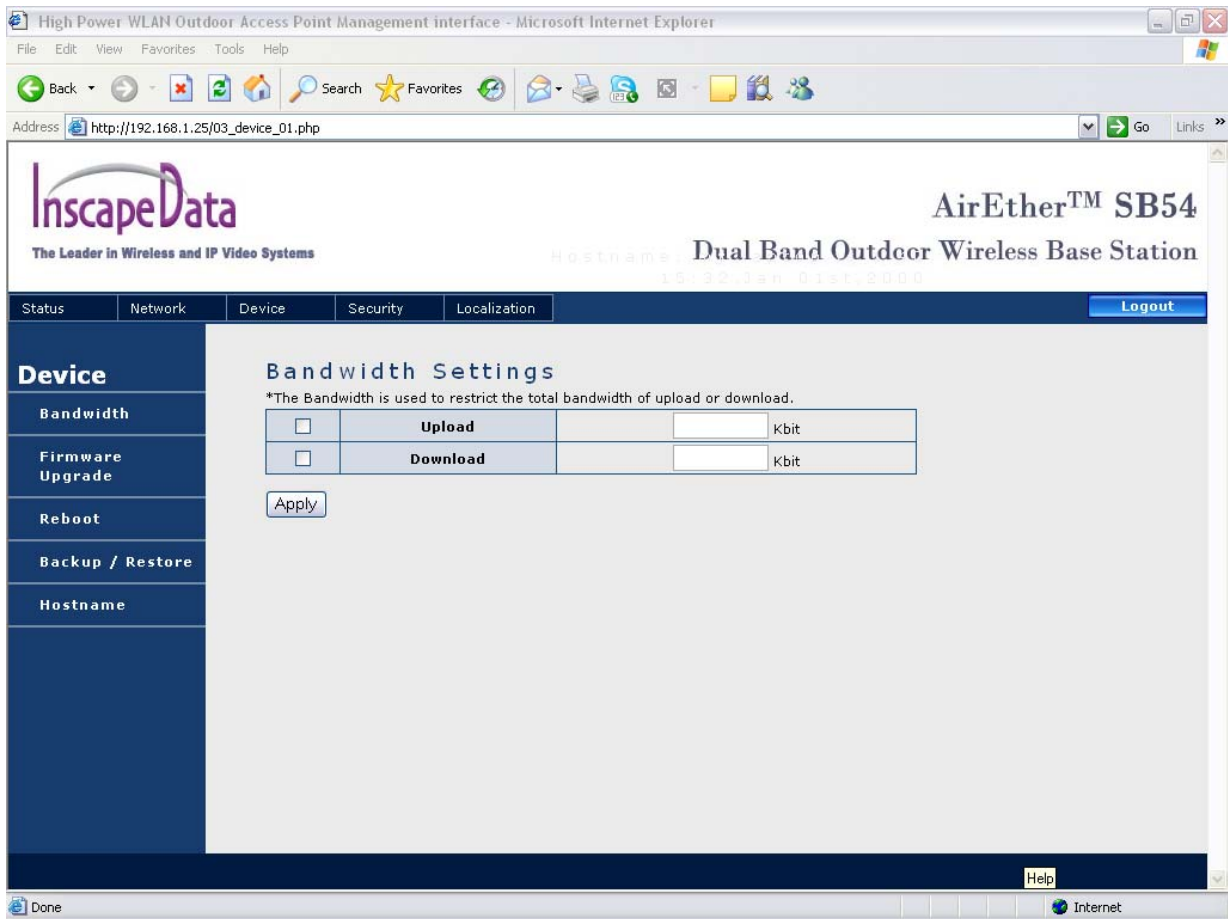


4.3 Device

Under device settings you can do a various things such as control bandwidth, Upgrade firmware, reboot the unit, backup or restore the unit, or set the hostname.

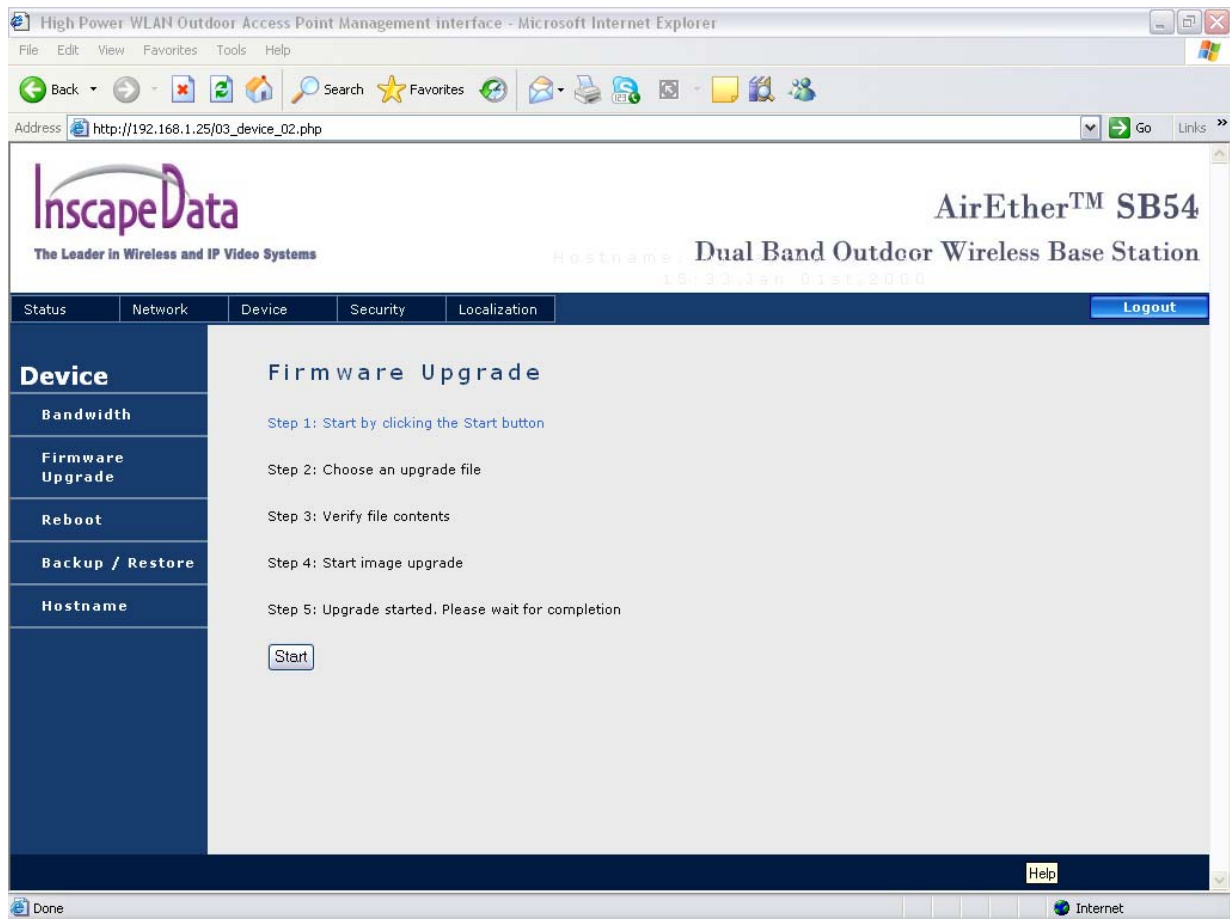
4.3.1 Bandwidth

You can set the upload and download rates for the device here. Upstream and downstream throughput maybe limited here in terms of kilobits per second.



4.3.2 Firmware Upgrade

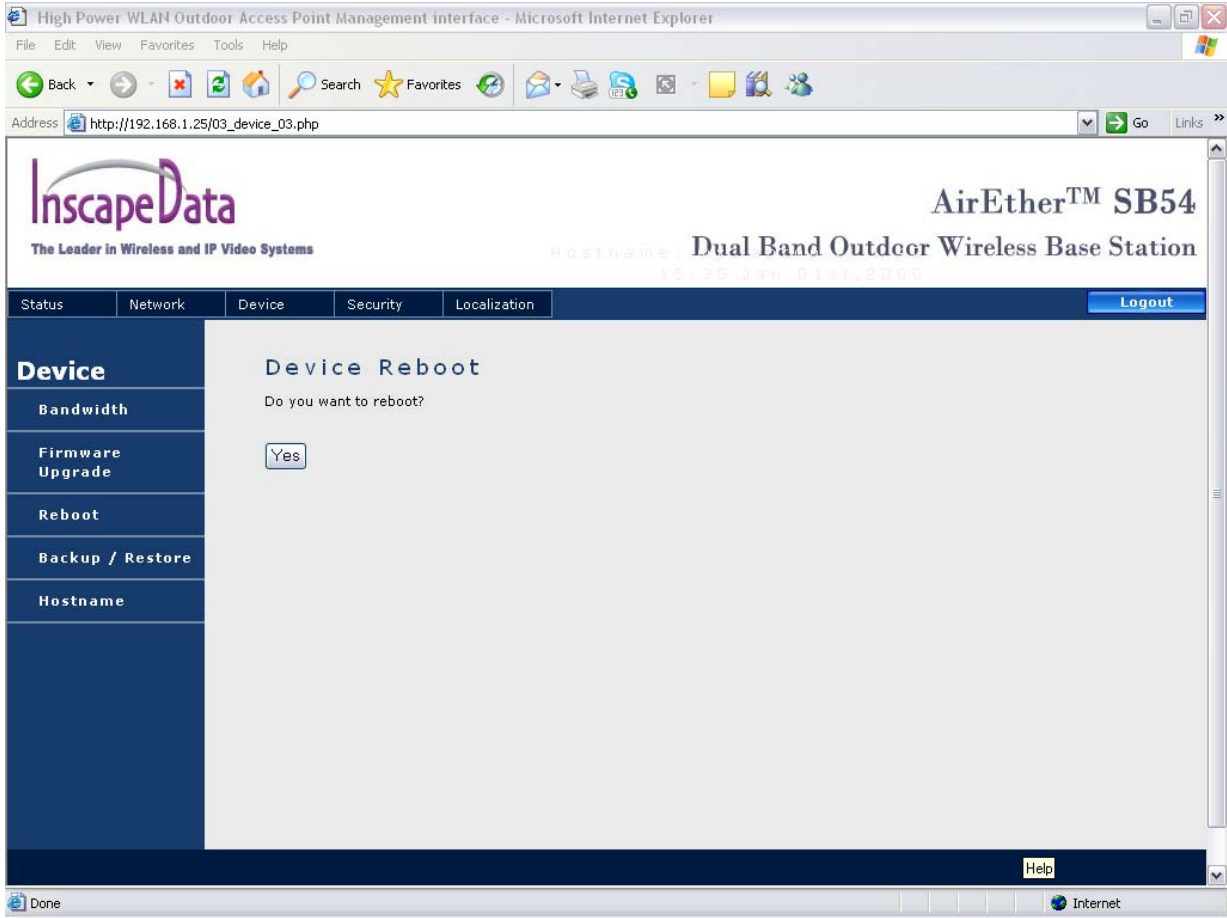
You may upgrade to the latest firmware on this page. Enter the location of the firmware upgrade file in the file path field, or click the “Browse” button to find the firmware upgrade file. Then click on the “Upgrade” button, and follow the on-screen instructions. The whole firmware upgrade process will take around 60 seconds. Before you upgrade, make sure you are using the correct version. Make sure to double check with your technical support representative, if available.



NOTE: Upgrading the firmware does not reset the equipment to the factory default configuration. Selecting “Restore to factory default” option in Step 5 will restore the unit to the factory default settings. With major version upgrades, restore to factory default is a must. An example to perform the factory default after firmware upgrade is from firmware version RC7-2 to RC8-h. Please check the release notes of the firmware to see if a factory firmware default is critical before proceeding.

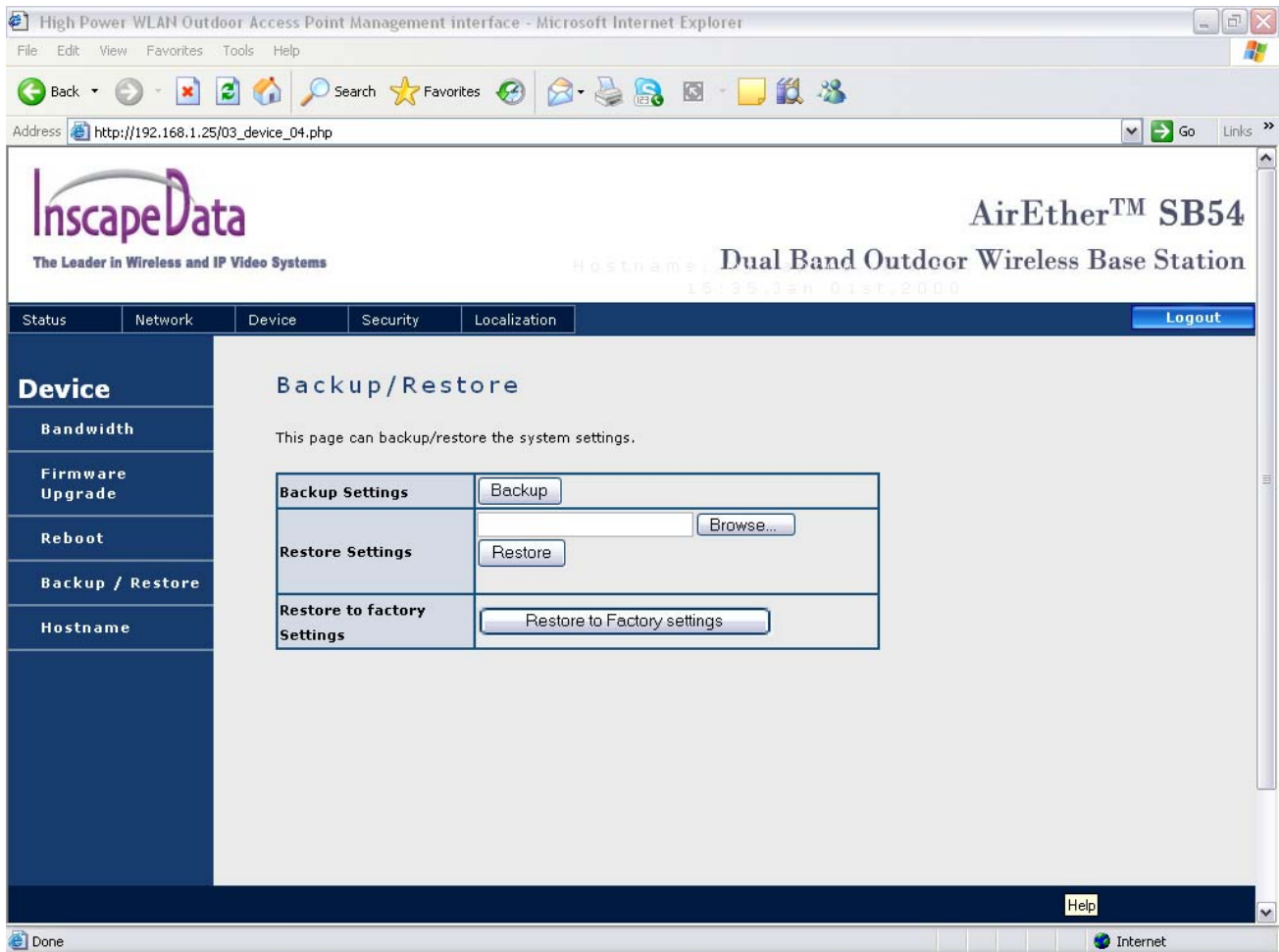
4.3.3 Reboot

You can reboot the system on this page.



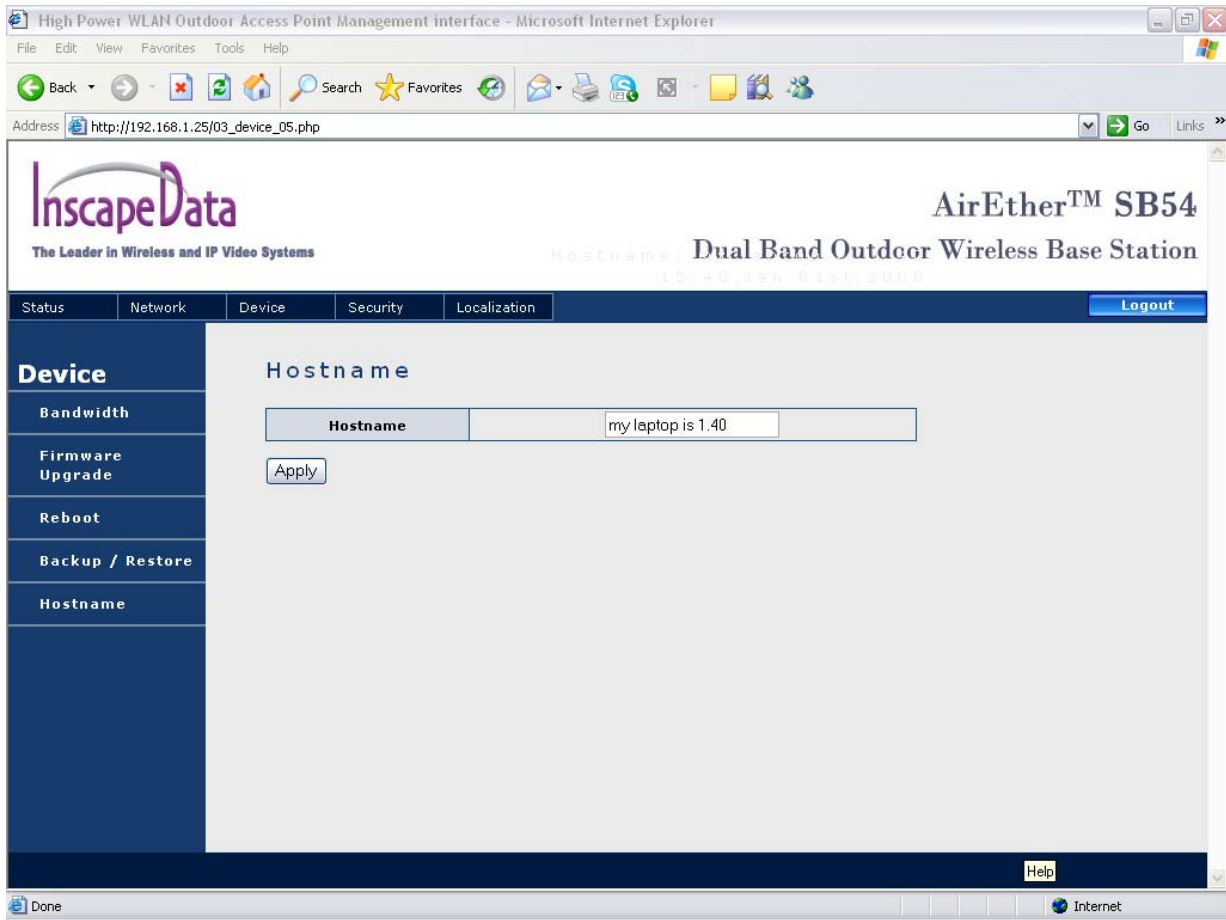
4.3.4 Backup/Restore

You can **Backup/Restore**, **Upgrade firmware** and **Reboot** the system in following pages.



- **Backup the current settings to a file** – Click on the “**Backup**” button the system will prompt you where to save the backup file. You can choose the directory to save your configuration file.
- **Restore settings from a backup file** – Here you can restore the configuration file from a previous saved back up.
- **Restore factory default setting** – Be very careful before restoring the system back to default as you will lose all current settings immediately.

If you execute this function it will display **192.168.1.20** in the **IP Address** field and **255.255.255.0** in the **Subnet Mask** field. **Please make note of your user name and password carefully.** **Hardware resetting of the unit to regain access can only be done by Inscape Data.**



4.3.5 Hostname

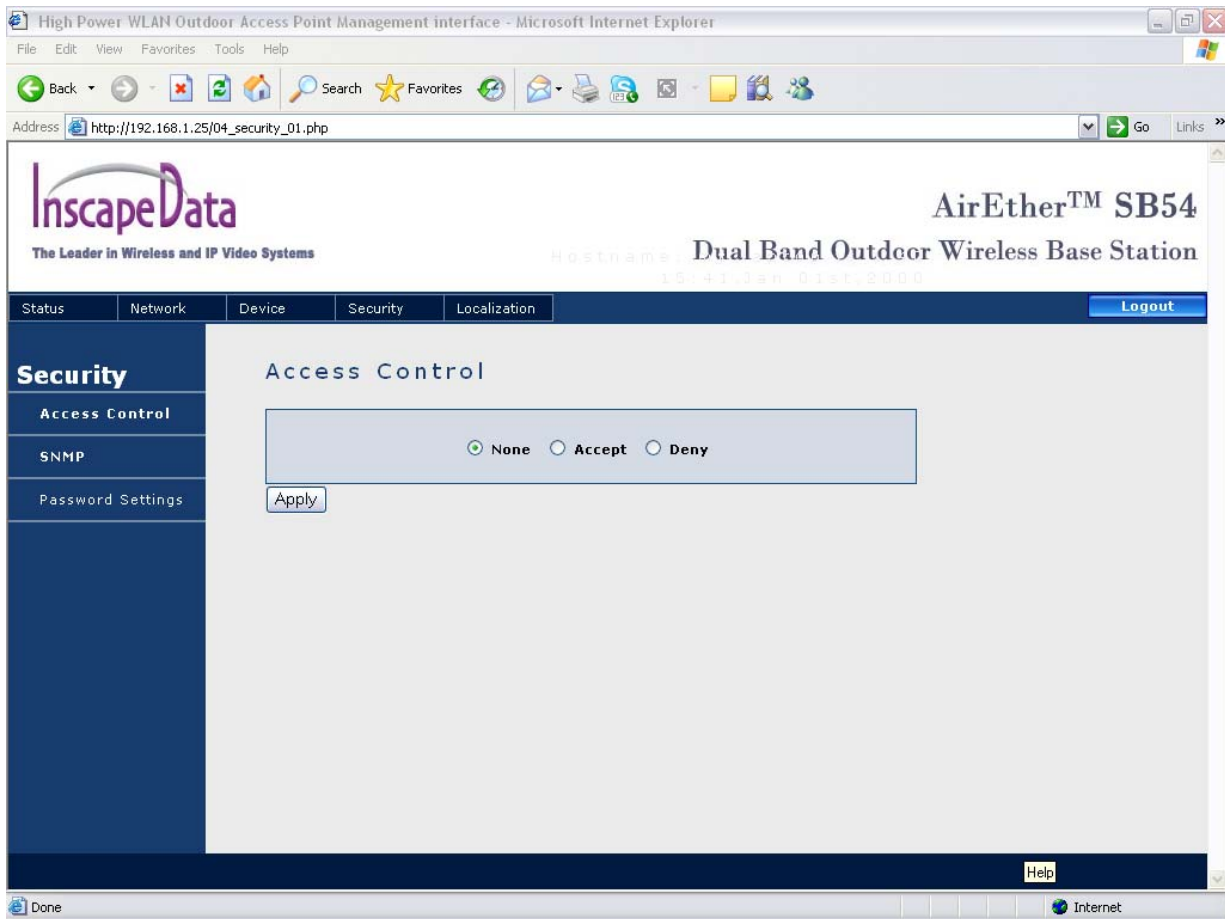
Here you may provide a specific name to identify your device in the network. This can be any name you choose.

4.4 Security

The security settings page will allow you to either enable or disable security settings.

4.4.1 Access Control

You can control how you want to filter connections to the device by MAC address. You can choose none, accept, or deny. Accept will allow the MAC addresses entered to connect while Deny will not allow the MAC addresses entered. This feature is available in AP mode only, and it applies only to wireless devices connecting with your station. You cannot restrict access of clients connected via Ethernet ports.



4.4.2 SNMP

SNMP stands for Simple Network Management Protocol. It is used in network management systems to monitor network-attached devices for conditions that warrant administrative attention. SNMP exposes management data in the form of variables on the managed systems, which describe the system configuration. These variables can then be queried and set by SNMP software applications.

The screenshot shows the InscapeData web interface for the AirEther™ SB54 Dual Band Outdoor Wireless Base Station. The main navigation bar includes tabs for Status, Network, Device, Security, and Localization, along with a Logout button. The Security section is active, and the SNMP Settings page is displayed. The form includes the following elements:

- Enable SNMP
- Read Only(RO) section:
 - Source / Hostname: Allow all, Deny all, Specific IP/Hostname
 - Community Name: public
- Read and Write(RW) section:
 - Source / Hostname: Allow all, Deny all, Specific IP/Hostname
 - Community Name: private
- Apply button

For SNMP management software to properly communicate with the access point the **SNMP** agent must first be enabled and the Network Management Station must submit a valid community string for authentication. Select **SNMP** Enable and enter data into the fields as described below. When you are finished, click “**Apply**”. See the following table for description of each SNMP items.

Setting	Description
SNMP	Enables or disables SNMP.
Contact Location	Sets the location string that describes the system location. Maximum length is 255 characters.
Community Name (Read Only)	Specifies a community string with read-only access. Authorized management stations are able to retrieve MIB objects. Maximum length is 32 characters.
Community Name (Read Write)	Specifies a community string with read-write access. Authorized management stations are able to both retrieve and modify MIB objects. Maximum length is 32 characters.
Trap Destination IP Address	Enter the IP address of the trap manager that will receive these messages.
Trap Destination Community Name	Enter the community name of the trap manager that will receive these messages.

4.4.3 Password Settings

This page will allow you to set the user name and password for the device. This password will be used when logging into the configuration page of the device. ***The default user name and password is root and root respectively.***

The screenshot displays the InscapeData web interface for the AirEther™ SB54 Dual Band Outdoor Wireless Base Station. The top navigation bar includes links for Status, Network, Device, Security, and Localization, with a Logout button on the right. The Security section is active, showing the Password Settings page. The page contains a table with the following fields:

Current User Name	root
New User Name	<input type="text"/>
New Password	<input type="text"/>
Confirmed Password	<input type="text"/>

Below the table is an button. The footer of the page displays the hostname as AirEther and the date as 20:14, Jun 03rd, 2009.

4.5 Localization

4.5.1 Network Time Protocol (NTP)

Here you can set the device to obtain the time from a valid internet time server. You will need to input the internet time server information. You can use up to 2 different time servers on this page.

The screenshot shows the web interface for the AirEther™ SB54 Dual Band Outdoor Wireless Base Station. The page title is "AirEther™ SB54 Dual Band Outdoor Wireless Base Station". The navigation menu includes "Status", "Network", "Device", "Security", "Localization", and "Logout". The sidebar on the left has "Localization" selected, with sub-options for "NTP" and "Country Code". The main content area is titled "Network Time Protocol" and contains the following configuration fields:

First NTP server IP/Hostname	pool.ntp.org	port	123
Second NTP server IP/Hostname	ntp.ubuntu.com	port	123
TimeZone Setting	GMT+0		

Below the table is an "Apply" button. At the bottom of the page, the status bar displays "Hostname: AirEther 20:18, Jun 03rd, 2009".

4.5.2 Country Code

Here you can set the country code as Wildcard, ETSI, Japan, and United States. Please choose the regulatory domain that is most suitable for your wireless deployment region. Using Wildcard disables transmit power control (TCP) and operates the unit at maximum TX Power output. Operating the wireless device outside of the allowed TX power is not advised. It not only disrupts other valid wireless networks, it is Illegal!

The screenshot displays the web interface for the AirEther™ SB54 Dual Band Outdoor Wireless Base Station. The top left features the InscapeData logo with the tagline "The Leader in Wireless and IP Video Systems". The top right identifies the device as "AirEther™ SB54 Dual Band Outdoor Wireless Base Station". A navigation bar includes tabs for "Status", "Network", "Device", "Security", "Localization", and a "Logout" button. The "Localization" tab is active, showing a sidebar with "Localization", "NTP", and "Country Code" options. The main content area is titled "Country Code Settings" and contains a "Current Country" dropdown menu currently set to "United States". An "Apply" button is located below the dropdown. The dropdown menu is open, showing the following options: "WILDCARD", "ETSI(2)", "ETSI(1)", "Japan", and "United States". The footer of the interface displays "Hostname: AirEther 20:19, Jun 03rd, 2009".

5 Wireless Compatibility

Not all access points are created equal. Certain manufacturers may deviate from standard product implementation and integrated proprietary means to achieve wireless transmission and still label their product standard product. This section will address in in-house compatibility comment and real world feedback.

5.1 Fully compatible

The following wireless vendor equipment requires no special configuration to achieve full wireless link performance.

None

5.2 Semi-compatible

The following wireless vendor equipment requires extra configuration settings to achieve full or compromised wireless link performance.

Vendor	Model	Comment
Cisco	Aironet Series AP Bridge	These products do not support 4-address header. Disable 4-address header in the Inscape Data SB54, BR54, and SC54 products to achieve compatibility at the sacrifice of 802.1d transparent bridge. MAC translation bridge is enabled.
Consumer Branded Access Point	Most	Most of these products do not support 4-address header. Disable 4-address header in the Inscape Data SB54, BR54, and SC54 products to achieve compatibility at the sacrifice of 802.1d transparent bridge. MAC translation bridge is enabled.

5.3 Not Compatible

The following wireless vendor equipment are not compatible with Inscape Data AirEther SB54, BR54, and SC54 products.

None

6 Wireless Network Planning

6.1 Site Survey

You need to consider the following operating and environmental conditions when performing a site survey:

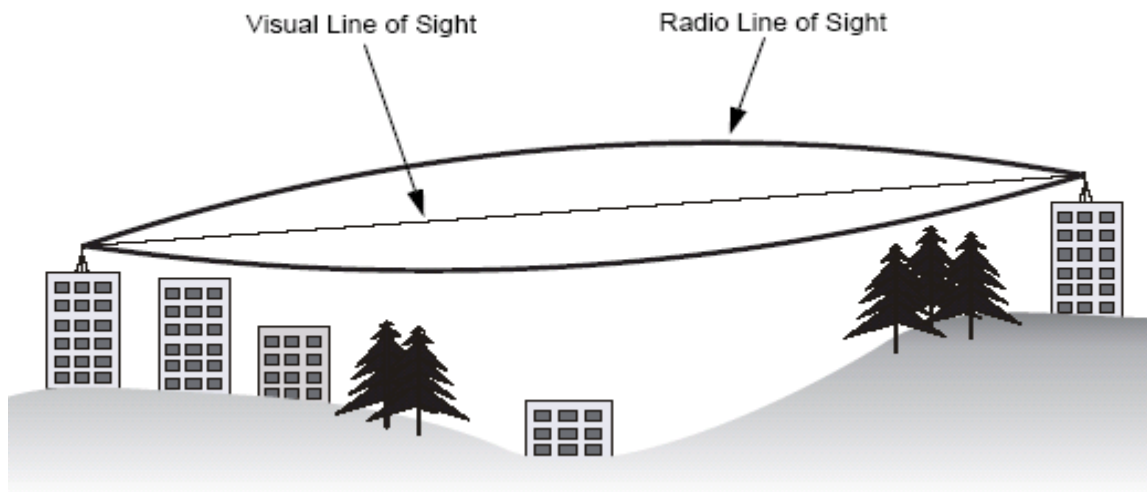
- **Data rates** – The sensitivity and the radio range are inversely proportional to data rates. Therefore, the maximum radio range is achieved at the lowest workable data rate, and a decrease in receiver threshold sensitivity occurs as the radio data rate increases.
- **Antenna type and placement** – A proper antenna configuration is a critical factor in maximizing radio range. As a general rule, the radio range increases in proportion to antenna gain and height.
- **Physical environment** - Clear or open areas provide better radio range than closed or filled areas. Clear Line-of-Sight (LOS) is required to establish a good and reliable wireless link.
- **Obstructions** - Metal shelving or a steel pillar can hinder devices. Avoid placing these devices in locations where obstructions are between the sending and receiving antennas.

6.2 Planning Radio Path

For wireless communication, the Line-of-Sight (LOS) will be the major concern in establishing a wireless link. This evaluated procedure is to reduce any obstructions and to avoid the multiple-path signal degrading the communication quality.

The first requirement is the Line-of-Sight (LOS) between Antennas on both sides. The radio Line-of-Sight concept is the area along the radio linking path through which the bulk of the radio signal power travels. The area is known as the first Fresnel Zone of the radio link. The radio link, should avoid being obstructed by obstacles in its path, including the ground within 60% of the first Fresnel Zone.

The following figure illustrates the concept of a good radio Line-of-Sight.



Picture 30 Line-of-Sight (LOS)

If there is any obstacle in the radio path, there may still be a radio link, but the quality and signal strength will be affected. Ensuring the maximum clearance from objects in a path is important. For long-distance links, the radio signals may be lost partially due to non-LOS issue.

As we setup the radio path for the wireless bridge link, we need to consider these factors:

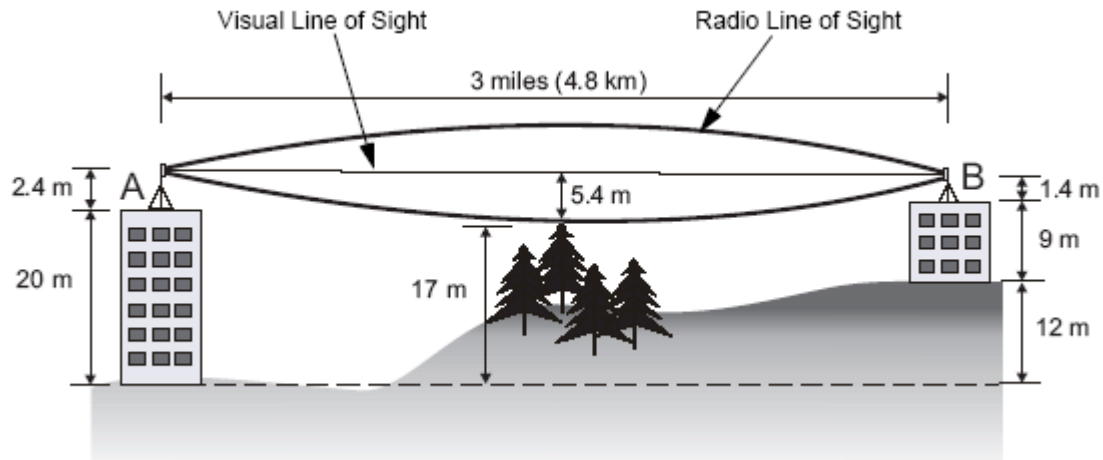
- Avoid any partial Line-of-Sight between the antennas.
- Be aware of trees that may be near the path or obstruct the path.
- Make sure there is enough clearance from buildings and that is no obstruction or blocking the path.
- Check the land topology between the antennas by using topographical maps, aerial photos, or even satellite images.
- Avoid a path that may have temporary blockage due to the moving objects, such as cars, trains, or aircrafts.

6.3 Antenna Height

A reliable wireless link usually depends on a clear radio Line-of-Sight between the antennas on both sides. The minimum height determined by the link distance, obstacles that may be in the path, topology of the terrain, and the curvature of the earth (for links over 2 miles). For long-distance links, the mast or pole may need to be constructed to attain the minimum required height. The following table estimates the required minimum clearance above the ground or path obstruction.

Total Link Distance	Max Clearance for 60% of First Fresnel Zone at 5.8 GHz	Approximate Clearance for Earth Curvature	Total Clearance Required at Mid-point of Link
0.25 mile (402 m)	4.5 ft (1.4 m)	0	4.5 ft (1.4 m)
0.5 mile (805 m)	6.4 ft (1.95 m)	0	6.4 ft (1.95 m)
1 mile (1.6 km)	9 ft (2.7 m)	0	9 ft (2.7 m)
2 miles (3.2 km)	12.7 ft (3.9 m)	1 ft (0.3 m)	13.7 ft (4.2 m)
3 miles (4.8 km)	15.6 ft (4.8 m)	2 ft (0.6 m)	17.6 ft (5.4 m)
4 miles (6.4 km)	18 ft (5.5 m)	3 ft (0.9 m)	21 ft (6.4 m)
5 miles (8 km)	20 ft (6.1 m)	4 ft (1.2 m)	24 ft (7.3 m)
7 miles (11.3 km)	24 ft (7.3 m)	8 ft (2.4 m)	32 ft (9.7 m)
9 miles (14.5 km)	27 ft (8.2 m)	14 ft (4.3 m)	41 ft (12.5 m)
12 miles (19.3 km)	31 ft (9.5 m)	24 ft (7.3 m)	55 ft (16.8 m)

Table 2 Estimated LOS Clearances



Picture 31 Antenna Height

For example, the wireless link between building A and building B is 3 miles (4.8 km). There is a tree-covered hill in between. From the table above, it can be seen that for a three-mile link and the object clearance required at the mid-point is 5.4 m (17.6 ft). The tree-covered hill height is at an elevation of 17 m (56 ft), so the antennas linked at both sides needs to be at least 22.4 m (73 ft) high. The building A is six stories high or 20 m (66 ft), so the mast or pole with 2.4 m (7.9 ft) must be constructed on its roof to meet the required antenna height. The building B is only three stories high or 9 m (30 ft), but it is located at an elevation that is 12 m (39 ft) higher than the building A. A mast or pole is required to mount an antenna at the required height 1.4 m (4.6ft) on the roof of building B.

6.4 Antenna Types

Each antenna must have the FCC approval for use in a wireless link. The antennas provide Omni directional, directional, or sector coverage and support various communication distances. Antennas are available with different gain ratings and coverage areas. Inscape Data offers a broad selection of 2.4GHz and 5GHz antennas for the SB54 & BR54 and SC54 product line to meet the needs of your wireless applications. For further details, please visit Inscape Data's website, <http://www.inscapedata.com/antennas.htm>.

6.5 Antenna Cable

A quality low loss antenna cable improves signal loss and offers long term reliability. The antenna cable connector should N-Type Male on both ends. To further minimize signal loss, short antenna cable runs of 1 meter or 3 feet is recommended. Since unlicensed wireless power is very valuable, minimizing loss can increase your link performance. When calculating wireless path loss, please include the antenna cable loss. Please check Inscape Data's website on quality matching antenna cables.

6.6 Weather Consideration

Weather and seasonal related considerations may affect your wireless link and performance. If your deployment region experiences more rain, storms, lightning, and wind, plan to increase the system operating margin to accommodate the larger signal fluctuations to maintain a reliable wireless link. Plan your wireless link ahead to accommodate for natural vegetation growths. For example, a tree not in line of site this year may encroach into the Fresnel zone.

7 The Wireless Technology

In an Era of IP network explosion, the license-exempt wireless communication platform has expanded its role beyond simple voice communication. It has reached the mass market segment to provide a reliable alternative to hardwiring for voice over IP, IP TV, and security applications, to name a few. There are several great reason why wireless is a preferred medium over hard wiring; Wireless is economical, faster time to deployment, secure, and reliable. In many cases, wireless is the only option.

License exempt wireless is available worldwide in several frequency bands. The most popular and uniformly accepted is ISM 2.4GHz and 5GHz frequency bands. The 2.4 GHz frequency allocation, 2.40GHz to 2.4835GHz, and 5GHz, 5.15GHz to 5.85GHz, are adequate for voice and data communication therefore usage of cordless telephones and wireless computer access points worldwide find their homes in these bands. Among other license free bands, not all are uniformly acceptable worldwide. National restrictions may limit or omit the use of certain frequency bands from one country to another. The following map provides a rough overview of license free frequencies supported or not supported world wide.



Figure 1. License Free Bands of the World – a rough overview

When considering wireless communication for data and video security applications, there are two wireless technology options, proprietary or standardized. The install base for proprietary wireless technology is small and costly relative to standardized wireless technology based on Wi-Fi (802.11). In 1999, 802.11b boosted speed to 11 Mbps using DSSS. The 1 and 2 Mbps DSSS modes were retained so that devices could throttle down to lower speeds when signals became weak. Using the orthogonal FDM (OFDM) transmission method, two higher-speed standards followed 802.11b that provided up to 54 Mbps: 802.11a transmits in the 5 GHz frequency range and is not backward compatible with 11b, but, 11g transmits in the same 2.4 GHz range and is compatible with 11b. If 11b and 11g devices are communicating, it is done at the slower 11b speed. Wi-Fi is well proven and readily available since late 1998. It is also one of the most successful industry standards in history. Wi-Fi is experiencing rapid advancement with newer extensions released to enhance wireless performance.

WiMax is another wireless standard rapidly gaining ground and holds lots of promise for the licensed bands. However, the industry anticipates cost effective WiMax equipment to emerge within a few years. Inscap Data's long range wireless equipment based on WiFi is available today and brings a host of benefits to the security market. Table I provides a rough overview of license free band characteristics and use of each band if available in your deployment region.

License Free Frequency	Equipment Cost	Allowable Tx Power	Channel Bandwidth	Data Rate	Non-Line-of-Site Support	Purpose
315/433 MHz	Good	Good	Poor	Poor	Excellent	Voice
900 MHz	Good	Good	Poor	Poor	Very Good	Voice/Data
2.4 GHz	Excellent	Good	Very Good	Very Good	Good	Voice/Data/Video
5.x GHz	Very Good	Good	Very Good	Very Good	Good	Voice/Data/Video
24 GHz	Poor	Very Good	Very Good	Very Good	Poor	Data/Video
60 GHz	Poor	Excellent	Excellent	Excellent	Poor	Data/Video
FSO/Laser	Very Poor	Excellent	Excellent	Excellent	Very Poor	Data/Video

Table I. License Free Frequency Review (FSO, Free Space Optics)

Illegal or improper use of license free radio equipment is a federal offense and extreme care should be considered when using it in your country. Confirm with national authorities when in doubt if a particular frequency band is considered license free or when a new frequency band will be available in your region. The following table provides information on fourteen regional spectrum management authorities and their websites.

Country / Region	National Spectrum Authority	Website
Australia	Australian Communications and Media Authority	www.acma.gov.au
Brazil	Agencia Nacional de Telecomunicações	www.anatel.gov.br
Canada	Industry Canada	www.ic.gc.ca
China	Ministry of Information Industry	www.mii.gov.cn
France	National Frequency Agency (NFA)	www.anfr.fr
Germany	Federal Network Agency Bonn, Federal Republic of Germany	www.bundesnetzagentur.de
Italy	The Communications Regulatory Authority (Agcom)	www.agcom.it
Japan	Japan Ministries of Internal Affairs and Communications	www.soumu.go.jp
South Korea	Ministry of Information and Communication	www.mic.go.kr
Russia	Ministry for Communication and Information of the Russian Federation	www.gov.ru
South Africa	The Independent Communications Authority of South Africa	www.icasa.org.za
United Arab Emirates	Supreme Committee for the Supervision of the Telecommunication Sector	www.tra.gov.ae
United Kingdom of Great Britain & Northern Ireland	Office of Communications	www.ofcom.org.uk
United States of America	Federal Communications Commission	www.fcc.gov

Table II. Country or Regional Radio Spectrum Authorities

Radio transmission power and antenna gain combinations or EIRP at specific frequencies are primary technical considerations in deploying license free radio equipment. EIRP stands for equivalent isotropic radiated power and is defined by each country's spectrum authority. In the United States, equipment operating on 2.4 GHz frequency may not exceed a maximum of 36 EIRP for point to multipoint communication as stated in the FCC part 15 rules. License free radio spectrum is a great tool for the industrial, medical, and scientific communities for the advancement of cost effective radio communication technology. After all, wireless is economical, faster time to deployment, secure, and reliable. In many deployment scenarios, wireless is the only option.

The SB54 & BR54 acts as a high performance IEEE802.11 a/b/g compliant dual band access point and also supports bridge mode to enable multiple wired Ethernet client access to wireless environments. The SC54 functions as a high performance IEEE a/b/g compliant dual band wireless client bridge. Both SB54 & BR54/SC54 support Wi-Fi Protected Access standards to provide higher levels of security for network data and communication. The SB54 & BR54/SC54 is also fully compatible with IEEE802.11 a/b/g standards, so it connects with all existing IEEE802.11 a/b/g compliant devices.

8 IEEE 802.11 Wireless Network Architecture

Inscape Data AirEther wireless access points, bridges, and clients are designed based on IEEE 802.11a/b/g wireless standards. The IEEE (Institute of Electrical and Electronics Engineers, Inc) or also pronounced as (Eye-triple-E) is the world's leading professional non-profit association for the advancement of technology. It serves the aerospace, biomedical, electric power, consumer electronics, and computers and telecommunications industry. IEEE standardization efforts are organized by projects, each of which is assigned a number. The most famous IEEE project is the IEEE 802 project to develop LAN standards. Within each project, individual working groups develop standards to address a particular facet of the problem. Working groups are also given a number, which is written after the decimal point for the corresponding projects. Ethernet, the most widely used IEEE LAN technology, was standardized by the third working group, 802.3. Wireless LANs were the eleventh working group formed, hence the name 802.11.

Within a working group, task groups form to revise particular aspects of the standard or add on to the general area of functionality. Task groups are assigned a letter beneath the working group. The case of the letter in a standards revision encodes information. Lowercase letters indicate dependent standards that cannot stand alone from their parent, while uppercase letters indicate full-fledged standalone specifications. For example, 802.11b adds new clause to 802.11, but cannot stand alone, so the "b" is written in lowercase. In contrast, the 802.1X are self-contained and standalone specifications where as 802.11n is not standalone specification.

IEEE 802 family, which is a series of specifications for LAN technologies focuses on the physical (layer 1) and data link (layer 2) of the OSI model. *Physical layer* defines all the electrical and physical specifications for devices. It defines in particular the relationship between a device and the communication medium. In other words, it defines the protocol which interconnects devices together to form a network. *Data link layer* describes the functional means to transfer data between network entities. It provides access control, device identification, error checking, and the essentials for reliable data communication. IEEE 802.11 (WLAN standard) introduces physical layer communication methods using FHSS (Frequency Hopping Spread Spectrum) and DSSS (Direct Sequence Spread Spectrum). 802.11b specifies high-rate direct-sequence layer (HR/DSSS). 802.11a describes a physical layer based on orthogonal frequency division multiplexing (OFDM). 802.11g, the newest addition provides higher data speeds using OFDM. Below is a table of data speed based on working group.

WLAN Speeds based on 802.11 working group

Working Group	Maximum Data Rate/Speed
802.11	2 mbps
802.11b	11 mbps
802.11g	54 mbps
802.11a	54 mbps
802.11n	300 mbps

802.11n also known as MIMO is a working standard to bring even higher data rate for multi-media applications. IEEE 802.11 has been readily available since 1998 offering speeds at 2 mbps and 2001 at 54 mbps. Late 2008, the introduction of 802.11n will deliver speeds in the 300 mbps range. IEEE 802.11 is one of the most successful industry standards in history. It has been experiencing exponential growth in multi-industry support and rapid advancement with newer extensions released periodically to enhance wireless performance.

802.11 Nomenclature

802.11 networks consist of four major physical components. Access points, Stations, Wireless Medium, and Distribution System.

Access Points

Access points function as media converters from one type to another. It performs the wireless-to-wired bridging function as its core functionality.

Stations/Clients

Networks are essentially built to transfer data between stations. Stations are computing devices with wireless network interfaces. Since 802.11 is fast in becoming the defacto standard for linking together consumer electronics, device with 802.11 wireless interfaces is rapidly increasing from portable handheld scanners to mobile computing.

Wireless Medium

To move data from station to station, the standard uses a wireless medium. Radio Frequency has been the most popular although Infrared (IR) is also available. The top two popular frequency usages are 2.4 GHz and 5 GHz spectrum. Although 2.4 GHz is internationally accepted spectrum for use with WLAN, 5GHz and other frequencies are also becoming popular.

Distribution System

When several access points are used to provide large network coverage area, they also need to talk to each other and track stations moving from one coverage area to another. Distribution system essentially functions as a backbone to pass data to their destination. Ethernet has been the most successful backbone network and is available in almost all IEEE 802.11 access points.

Inscape Data fixed broadband wireless products are built upon the IEEE 802.11 standard platform and through proprietary algorithms extends the network communication connectivity range beyond 50km. Users can easily access the Inscape Data AirEther outdoor wireless system's user interface to adjust for distance and performance speed of the network link. The rugged outdoor design boasts IP68 product certification and ensures reliable operation during the worst weather conditions. The table below references the Inscape Data outdoor fixed wireless broadband system and core relationship to the 802.11 Nomenclature.

IEEE 802.11 Nomenclature	Inscape Data AirEther Outdoor System	Inscape Data Model # Reference
Access Point (AP)	Access Point (AP)	SB54 & BR54 Series Product set as Access Point Mode
N/A	Bridge / Backhaul (Proprietary)	SB54 & BR54 Series product set as Bridge Mode or AP & AP Client mode.
Station	Client Bridge / Customer Premises Equipment (CPE)	CB54 Series Product
Medium	2.4 GHz 5.1 ~ 5.8 GHz	SB54 & BR54, SC54, and BR108 Series Product
Distribution System	Ethernet port (RJ45)	All Product Support Ethernet
WDS (Wireless Distribution System)	Access Point (AP) w/ firmware upgrade	SB54 & BR54 Series Product

WDS is a feature allowing access point to communicate with access point wirelessly without medium conversion from wireless to Ethernet and Ethernet back to wireless (*Industry term: back to back*). It is a great means to deploy very quickly a wireless access point network with built in distribution system for wireless internet connectivity. WDS capability is available on Inscape Data AirEther SB54 & BR54 series access point.

9 Appendix

This section will provides various references related to your product.

9.1 Glossary

802.11a - An IEEE wireless networking standard that specifies a maximum data transfer rate of 54Mbps and an operating frequency of 5GHz.

802.11b - An IEEE wireless networking standard that specifies a maximum data transfer rate of 11Mbps and an operating frequency of 2.4GHz.

802.11g - An IEEE wireless networking standard that specifies a maximum data transfer rate of 54Mbps, an operating frequency of 2.4GHz, and backward compatibility with 802.11b devices.

Adapter - A device that adds network functionality to your PC.

Ad-hoc - A group of wireless devices communicating directly with each other (peer-to-peer) without the use of an access point.

Backbone - The part of a network that connects most of the systems and networks together, and handles most of the data.

Bandwidth - The transmission capacity of a given device or network.

Beacon Interval - Data transmitted on your wireless network that keeps the network synchronized.

Bit - A binary digit.

Browser - An application program that provides a way to look at and interact with all the information on the World Wide Web.

CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance) - A method of data transfer that is used to prevent data collisions.

CTS (Clear To Send) - A signal sent by a wireless device, signifying that it is ready to send data.

Database - A collection of data that is organized so that its contents can easily be accessed, managed, and updated.

DHCP (Dynamic Host Configuration Protocol) - A networking protocol that allows administrators to assign temporary IP addresses to network computers by "leasing" an IP address to a user for a limited amount of time, instead of assigning a permanent static IP addresses.

Download - To receive a file transmitted over a network.

DSSS (Direct-Sequence Spread-Spectrum) - Frequency transmission with a redundant bit pattern resulting in a lower probability of information being lost in transit.

DTIM (Delivery Traffic Indication Message) - A message included in data packets that can increase wireless efficiency.

Encryption - Encoding data transmitted in a network.

Ethernet - IEEE standard network protocol that specifies how data is placed on and retrieved from a common transmission medium.

Firmware - The programming code that runs a networking device.

Fragmentation - Breaking a packet into smaller units when transmitting over a network medium that cannot support the original size of the packet.

Gateway - A device that interconnects networks with different, incompatible communications protocols.

Hardware - The physical aspect of computers, telecommunications, and other information technology devices.

IEEE (The Institute of Electrical and Electronics Engineers) - An independent institute that develops networking standards.

Infrastructure - A wireless network that is bridged to a wired network via an access point.

IP (Internet Protocol) - A protocol used to send data over a network.

IP Address - The address used to identify a computer or device on a network.

ISM band - Radio bandwidth utilized in wireless transmissions.

ISP (Internet Service Provider) - A company that provides access to the Internet.

LAN - The computers and networked devices that make up your local network.

MAC (Media Access Control) Address - The unique address that a manufacturer assigns to each networking device.

Network - A series of computers or devices connected for the purpose of data sharing, storage, and/or transmission between users.

Node - A network junction or connection point, typically a computer or work station.

Packet - A unit of data sent over a network.

Passphrase - Used much like a password, a passphrase simplifies the WEP encryption process by automatically generating the WEP encryption keys to be compatible with consumer type AP products.

Port - The connection point on a computer or networking device used for plugging in cables or adapters.

Roaming - The ability to take a wireless device from one access point's range to another without losing the connection.

Router - A networking device that connects multiple networks together.

RTS (Request To Send) - A networking method of coordinating large packets through the RTS Threshold setting.

Server - Any computer whose function in a network is to provide user access to files, printers, communication, and other services.

SNMP (Simple Network Management Protocol) - A widely used network monitoring and control protocol.

Software - Instructions for the computer. A series of instructions that perform a particular task is called a "program".

SOHO (Small Office/Home Office) - Market segment of professionals who work at home or in small offices.

Spread Spectrum - Wideband radio frequency technique used for more reliable and secure data transmission.

SSID (Service Set Identifier) - Your wireless network's name.

Static IP Address - A fixed address assigned to a computer or device that is connected to a network.

Subnet Mask - An address code that determines the size of the network.

Switch - 1. A data switch that connects computing devices to host computers, allowing a large number of devices to share a limited number of ports. 2. A device for making, breaking, or changing the connections in an electrical circuit.

TCP (Transmission Control Protocol) - A network protocol for transmitting data that requires acknowledgement from the recipient of data sent.

TCP/IP (Transmission Control Protocol/Internet Protocol) - A set of instructions PCs use to communicate over a network.

TKIP (Temporal Key Integrity Protocol) - A wireless encryption protocol that provides dynamic encryption keys for each packet transmitted.

Topology - The physical layout of a network.

Upgrade - To replace existing software or firmware with a newer version.

WEP (Wired Equivalent Privacy) - An optional cryptographic confidentiality algorithm specified by IEEE 802.11 that may be used to provide data confidentiality, that is subjectively equivalent to the confidentiality of a wired local area network (LAN) medium that does not employ cryptographic techniques to enhance privacy confidentiality.

WPA (Wi-Fi Protected Access) - a wireless security protocol using TKIP (Temporal Key Integrity Protocol) encryption, which can be used in conjunction with a RADIUS server.

9.2 SB54 & BR54 Default & Display Values

Item	Values
User Name	root
Password	root
IP Alias	Disabled
Static IP Address	192.168.1.20
Subnet Mask	255.255.255.0
DHCP Client	Disabled
Default Gateway	192.168.1.1
SSID	AirEther
Frequency	802.11g
Channel	auto
Host Name	SB54 & BR54
Country Code	WILDCARD
F/W Version	To be determined

9.3 SC54 Default & Display Values

Item	Values
User Name	root
Password	root
IP Alias	Disabled
Static IP Address	192.168.1.21
Subnet Mask	255.255.255.0
DHCP Client	Disabled
Default Gateway	192.168.1.1
SSID	AirEther
Frequency	802.11g
Channel	auto
Host Name	SC54
Country Code	WILDCARD
F/W Version	To be determined

9.4 BR54 Default & Display Values

Item	Values
User Name	root
Password	root
IP Alias	Disabled
Static IP Address	192.168.1.20
Subnet Mask	255.255.255.0
DHCP Client	Disabled
Default Gateway	192.168.1.1
SSID	AirEther5
Frequency	802.11a
Channel	auto
Host Name	AirEther
Country Code	WILDCARD
F/W Version	To be determined

9.5 Technical Specification

Hardware	
Enclosure Protection	IP68 Compliant
Environmental	-40°C to +85°C
Humidity	95% @ 55°C
Frequency	2412 ~ 2484 MHz & 5.1 ~ 5.8 GHz
LAN port	1
Number of Radio	1
Operating Channels	IEEE802.11 b/g: 1~11 Channels (America), 1 ~ 13 Channels (General Europe), 1 ~ 14 Channels (Japan) IEEE802.11a: 4 Channels (Japan), 19 Channels (Europe), 13 Channels (USA)
Modulation	OFDM (64-QAM, QPSK, BPSK / DSSS (DBPSK, DQPSK, CCK)
Transmit Power 802.11a**	19dBm @ 6-24Mbps, 18dBm @ 36Mbps, 17dBm @ 48Mbps, 16dBm @ 54Mbps
Transmit Power 802.11g**	25dBm @ 6-24Mbps, 23dBm @ 36Mbps, 22dBm @ 48Mbps, 21dBm @ 54Mbps
Transmit Power 802.11b**	25dBm
Receiver Sensitivity 802.11a	-92dBm @ 6-24Mbps, -80dBm @ 36Mbps, -76dBm @ 48Mbps, -72dBm @ 54Mbps
Receiver Sensitivity 802.11g	-92dBm @ 6-24Mbps, -80dBm @ 36Mbps, -76dBm @ 48Mbps, -72dBm @ 54Mbps
Receiver Sensitivity 802.11b	-96dBm @ 1Mbps, -95dBm @ 2Mbps, -93dBm @ 5.5Mbps, -92dBm @ 11Mbps

Software	
Wireless	802.11R IEEE 802.11a IEEE 802.11 b/g Wireless Channel Support Country Selection: FCC, ETSI, Japan SSID assignment Client BSSID assignment WMM Support Bandwidth Control: UP/DOWN kbps 802.11g Only Support TPC (Transmit Power Control) Support: 5 Steps RSSI (dBm) RF Site Survey Burst Mode Maximum Range (Use of External Antenna): 50km
Security	Http User Name & Password Access Control List, i.e (None/Accept/Deny) 802.1x Support, i.e (EAP-MD5, EAP-TLS, EAP-TTLS, PEAP) Wireless Encryption: Open, Shared, WPA-PSK, WPA2-PSK, WPA & WPA2, 64bit/128bit/256bit WEP, TKIP, AES-CCMP Support Wireless Station Isolation Hide SSID
Management	Wireless Client/Station List HTTP Web Based Configuration (IE) IP Alias Configuration File Backup / Restore SNMP v1, v2c, 802.11 Mib Host Name
Configuration Retention after FW Upgrade	Yes
DHCP Client	Yes
VPN Pass Through	Yes
Network	
Protocols	TCP/IP, RTSP, UDP, IGMP, DHCP, Tags, PPPoE
Maximum Ethernet Clients Supported	64
Compliance	
	FCC,CE, ROHS, ETSI

Mechanical

Dimensions

- a. 7.5 inches
- b. 4.73 inches
- c. 1.84 inches

Interface

- 1. Status LED
- 2. Type N Antenna Interface
- 3. RJ45 Female Power over Ethernet Power



9.6 Product Hardware Installation Guideline

AirEther™ Outdoor Wireless System SB54 & BR54/SC54/BR108 Series Product Hardware Installation Guideline

NOT FOLLOWING THIS GUIDELINE MAY VOID YOUR PRODUCT WARRANTY

Inscape Data Corporation's next generation AirEther outdoor wireless system SB54 & BR54, SC54, and BR108 are high performance long range 2.4GHz and 5GHz outdoor wireless IP networking solutions. With increased data rate capabilities and robust OFDM modulation, high performance reliable wireless networking is possible and supports high-demand video, voice, and data applications. When care is taken during installation and configuration, the AirEther wireless system will operate optimally and provide long term return on your investment. Not observing care or omitting important ground contacts during installation may degrade network performance, cause system failure, or void the manufactures warranty. Please refer to the following table of required and recommended accessories:

Items	Specification	Required	Notes
PIP100 1-Port PoE DC Injector	0 ~ 48VDC	✓	Simplify installation
PES100 1-Port Ethernet Surge Suppressor	In-Line Cat 5 with 8 lines Protected or equivalent		Strongly Recommended in severe environment. Damage due to surge is not covered under manufacturer warranty!
PoE Cable	Outdoor rated Cat 5/5e STP, FTP, ScTP	✓	Shielded Twisted Pair Cable (1 to 100 meter)
LSS0001 Lightning Arrestor	In-Line Coaxial Protector or equivalent		Strongly Recommended in severe environment. Damage due to surge is not covered under manufacturer warranty!
RJ-45 Jack	Radio/Equipment Side (Unshielded) PoE Injector Side (Shielded)	✓	Shielded RJ-45 connectors used for both ends
Ground Wire	16 AWG Copper Wire (Minimum)	✓	Attached to backside of the Radio/Antenna, Antenna mast, and appropriate common Earth Ground. Product damage caused by improper or no grounding is not covered under warranty!
Torque Wrench	20kgf-cm or 1.44 lbf-ft.	✓	All nuts and bolts should not be tightened beyond specified torque setting
CAT 5/5e Cable Termination	TIA-568B Standard	✓	Improper termination will damage the device and void your warranty
Weatherproof Sealing Tape	Rubber Mastic or equivalent (i.e. Coax-Seal)	✓	Sealing of antenna and RJ45 connector at both end s required to ensure installation and equipment longevity.

Highly Recommended Accessories*

- **PES100/PIS200**

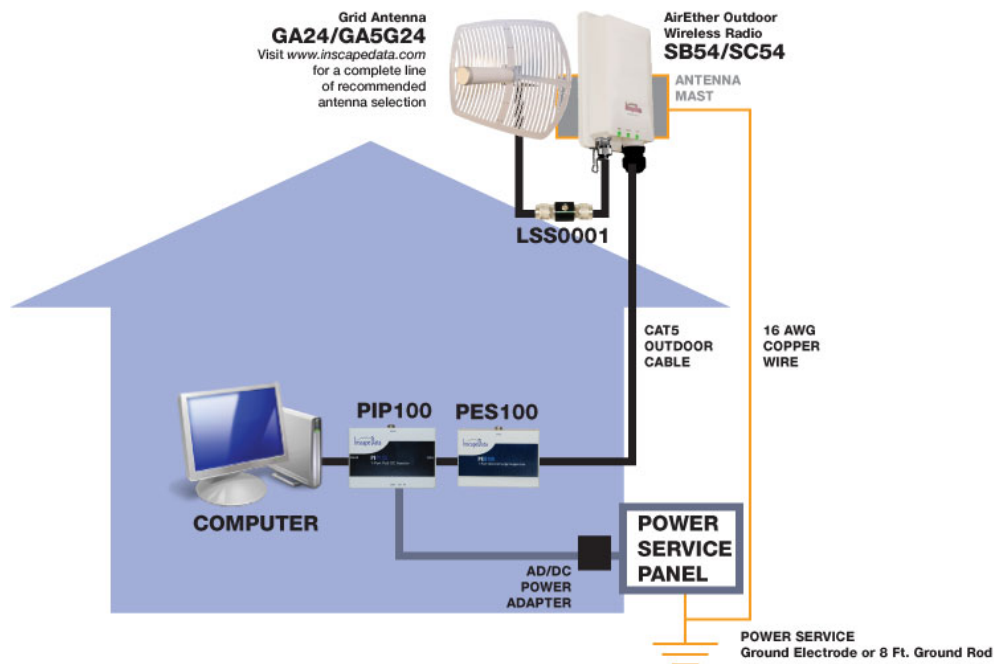
Protect Wireless Radios from Unexpected Surge Up to 132A

- **LSS0001**

Protects Antennas from Unexpected Surge Up to 600V

***Disclaimer:** INSCAPE DATA Corporation DISCLAIMS ALL WARRANTIES CONCERNING, AS TO, OR ON THE SURGE PROTECTION SYSTEM, WHETHER EXPRESS, IMPLIED, OR STATUTORY, INCLUDING WITHOUT LIMITATION WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

System Grounding Diagram



Please refer to the above system grounding diagram for your installation reference. When in doubt, refer to your country's national electric code to determine proper grounding techniques. For reference information regarding grounding the AirEther outdoor system, please check the application note directory included with your product's CDROM.

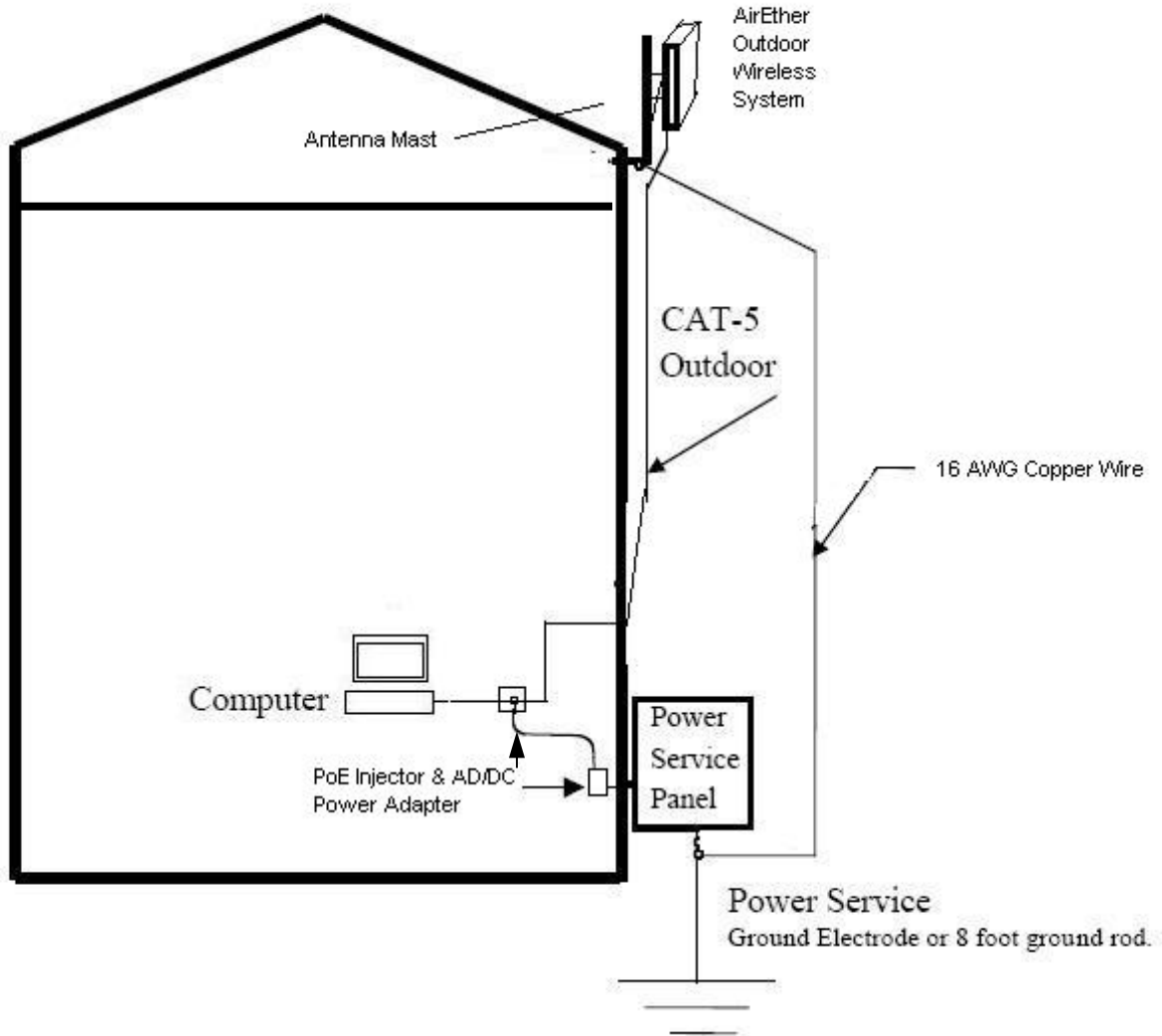
9.7 Hardware Installation Guide

NOT FOLLOWING THIS GUIDELINE MAY VOID YOUR PRODUCT WARRANTY

Inscape Data Corporation's next generation AirEther outdoor wireless system SB54 & BR54, SC54, and BR108 are high performance long range 2.4GHz and 5GHz outdoor wireless IP networking solution. With increased data rate capability and robust OFDM modulation, high performance reliable wireless network is possible and supports high-demand video, voice, and data applications. When care is taken during installation and configuration, the AirEther wireless system will operate optimally and provide long term return on your investment. Not observing care or omitting important ground contacts during installation may degrade network performance, cause system failure, or void the manufactures warranty. Please refer to the following table of required and recommended accessories:

Items	Specification	Required	Notes
PoE Cable	Outdoor rated Cat 5/5e STP, FTP, ScTP	√	Shielded Twisted Pair Cable (1 to 100 meter)
PoE Port Surge Protector	In-Line Cat 5 with 8 lines Protected or equivalent		Strongly Recommended in severe environment. Damage due to surge is not covered under manufacturer warranty!
Antenna Port Surge Protector	In-Line Coaxial Protector or equivalent		Strongly Recommended in severe environment. Damage due to surge is not covered under manufacturer warranty!
RJ-45 Jack	Radio/Equipment Side (Unshielded) PoE Injector Side (Shielded)	√	Shielded RJ-45 connectors used for both ends
Ground Wire	16 AWG Copper Wire (Minimum)	√	Attached to backside of the Radio/Antenna, Antenna mast, and appropriate common Earth Ground. Product damage caused by improper or no grounding is not covered under warranty!
Torque Wrench	20kgf-cm or 1.44 lbf-ft.	√	All nuts and bolts should not be tightened beyond specified torque setting
CAT 5/5e Cable Termination	TIA-568B Standard	√	Improper termination will damage the device and void your warranty
Weatherproof Sealing Tape	Rubber Mastic or equivalent (i.e. Coax-Seal)	√	Sealing of <u>antenna</u> and RJ45 connector at both end is required to ensure installation and equipment longevity.

Please refer to the following system grounding diagram for your installation reference. When in doubt, refer to your country's national electric code to determine proper grounding techniques. For reference information regarding grounding the AirEther outdoor system, please check the application note directory included with your product's CDROM.



9.8 WARRANTY

Inscape Data Corporation Limited Warranty and Disclaimer of Warranty

Hardware. Inscape Data Corporation, or subsidiary selling the Product (“Inscape Data”) warrants that commencing from the date of shipment to Customer (and in case of resale by a Inscape Data’s reseller, commencing not more than ninety (90) days after original shipment by Inscape Data), and continuing for a period of the longer of (a) ninety (90) days or (b) the period set forth in the warranty card accompanying the Product (if any), the Hardware will be free from defects in material and workmanship under normal use. The date of shipment of a Product by Inscape Data is set forth on the packaging material in which the Product is shipped. This limited warranty extends only to the original user of the Product. Customer’s sole and exclusive remedy and the entire liability of Inscape Data and its suppliers under this limited warranty will be, at Inscape Data’s or its service center’s option, shipment of a replacement within the warranty period and according to the replacement process described in the warranty card (if any), or if no warranty card, as described on the Inscape Data Product Warranty Policy or a refund of the purchase price if the Hardware is returned to the party supplying it to Customer, freight and insurance prepaid. Inscape Data replacement parts used in Hardware replacement may be new or equivalent to new. Inscape Data’s obligations hereunder are conditioned upon the return of affected Hardware in accordance with Inscape Data’s or its service center’s then-current Return Material Authorization (RMA) procedures.

Software. The limited warranty in the United States Federal Communications Commission Notice sets forth Inscape Data’s warranty obligations with respect to the Software.

Restrictions. The above Hardware warranty and limited warranty in the End User License Agreement (“Software warranty”) do not apply if the Software, Hardware Product or any other equipment upon which the Software is authorized by Inscape Data or its suppliers or licensors to be used (a) has been altered, except by Inscape Data or its authorized representative, (b) has not been installed, operated, repaired, or maintained in accordance with instructions supplied by Inscape Data, (c) has been subjected to abnormal physical or electrical stress, abnormal environmental conditions, misuse, negligence, or accident; or (d) is licensed for beta, evaluation, testing or demonstration purposes. The Software warranty also does not apply to (e) any temporary Software modules; (f) any Software not

posted on Inscape Data's Software Center (on InscapeData.com URL where Inscape Data makes the Software publicly available to customers); (g) any Software that Inscape Data expressly provides on an "AS IS" basis on Inscape Data's Software Center; or (h) any Software for which Inscape Data does not receive a license fee.

DISCLAIMER OF WARRANTY

EXCEPT AS SPECIFIED IN THIS WARRANTY SECTION, ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS, AND WARRANTIES INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTY OR CONDITION OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NON-INFRINGEMENT, SATISFACTORY QUALITY, NON-INTERFERENCE, ACCURACY OF INFORMATIONAL CONTENT, OR ARISING FROM A COURSE OF DEALING, LAW, USAGE, OR TRADE PRACTICE, ARE HEREBY EXCLUDED TO THE EXTENT ALLOWED BY APPLICABLE LAW AND ARE EXPRESSLY DISCLAIMED BY INSCAPE DATA, ITS SUPPLIERS AND LICENSORS. TO THE EXTENT AN IMPLIED WARRANTY CANNOT BE EXCLUDED, SUCH WARRANTY IS LIMITED IN DURATION TO THE EXPRESS WARRANTY PERIOD. BECAUSE SOME STATES OR JURISDICTIONS DO NOT ALLOW LIMITATIONS ON HOW LONG AN IMPLIED WARRANTY LASTS, THE ABOVE LIMITATION MAY NOT APPLY. THESE WARRANTIES GIVE CUSTOMER SPECIFIC LEGAL RIGHTS, AND CUSTOMER MAY ALSO HAVE OTHER RIGHTS WHICH VARY FROM JURISDICTION TO JURISDICTION. THIS DISCLAIMER AND EXCLUSION SHALL APPLY EVEN IF THE EXPRESS WARRANTY SET FORTH ABOVE FAILS OF ITS ESSENTIAL PURPOSE.

INSCAPE DATA CORPORATION

1-Year Limited Hardware Warranty Terms

The following are special terms applicable to your hardware warranty. Your formal Warranty Statement, including the warranty applicable to Inscape Data software, appears in the End User License Agreement that accompanies your Inscape Data product.

Duration of Hardware Warranty: One (1) Year

Replacement, Repair or Refund Procedure for Hardware: Inscape Data or its authorized service center will use commercially reasonable efforts to ship a replacement part after receipt of the RMA request and the RMA item. Actual delivery times may vary depending on Customer location. Inscape Data reserves the right to refund the purchase price as its exclusive warranty remedy.

To Receive a Return Materials Authorization (RMA) Number: Please go to Inscape Data's website and complete the RMA request, <http://www.inscapedata.com/rma.htm>.



Inscape Data Corporation, 1611 South Main Street, Milpitas, CA 95035 USA

**IMPORTANT: PLEASE READ THIS END USER LICENSE AGREEMENT CAREFULLY.
DOWNLOADING, INSTALLING OR USING INSCAPE DATA OR INSCAPE DATA-SUPPLIED SOFTWARE
CONSTITUTES ACCEPTANCE OF THIS AGREEMENT.**

INSCAPE DATA CORPORATION OR ITS SUBSIDIARY LICENSING THE SOFTWARE INSTEAD OF INSCAPE DATA CORPORATION (“INSCAPE DATA”) IS WILLING TO LICENSE ITS SOFTWARE TO YOU ONLY UPON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS CONTAINED IN THIS END USER LICENSE AGREEMENT PLUS ANY ADDITIONAL LIMITATIONS ON THE LICENSE SET FORTH IN A SUPPLEMENTAL LICENSE AGREEMENT ACCOMPANYING THE PRODUCT (COLLECTIVELY THE “AGREEMENT”). TO THE EXTENT OF ANY CONFLICT BETWEEN THE TERMS OF THIS END USER LICENSE AGREEMENT AND ANY SUPPLEMENTAL LICENSE AGREEMENT, THE SUPPLEMENTAL LICENSE AGREEMENT SHALL APPLY. BY DOWNLOADING, INSTALLING, OR USING THE SOFTWARE, YOU ARE BINDING YOURSELF AND THE BUSINESS ENTITY THAT YOU REPRESENT (COLLECTIVELY, “CUSTOMER”) TO THE AGREEMENT. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THE AGREEMENT, THEN INSCAPE DATA IS UNWILLING TO LICENSE THE SOFTWARE TO YOU AND (A) YOU MAY NOT DOWNLOAD, INSTALL OR USE THE SOFTWARE, AND (B) YOU MAY RETURN THE SOFTWARE (INCLUDING ANY UNOPENED CD PACKAGE AND ANY WRITTEN MATERIALS) FOR A FULL REFUND, OR, IF THE SOFTWARE AND WRITTEN MATERIALS ARE SUPPLIED AS PART OF ANOTHER PRODUCT, YOU MAY RETURN THE ENTIRE PRODUCT FOR A FULL REFUND. YOUR RIGHT TO RETURN AND REFUND EXPIRES 30 DAYS AFTER PURCHASE FROM INSCAPE DATA OR AN AUTHORIZED INSCAPE DATA RESELLER, AND APPLIES ONLY IF YOU ARE THE ORIGINAL END USER PURCHASER.

THE FOLLOWING TERMS OF THE AGREEMENT GOVERN CUSTOMER’S ACCESS AND USE OF EACH INSCAPE DATA OR INSCAPE DATA-SUPPLIED SOFTWARE (“SOFTWARE”), EXCEPT TO THE EXTENT: (A) THERE IS A SEPARATE SIGNED CONTRACT BETWEEN CUSTOMER AND INSCAPE DATA GOVERNING CUSTOMER’S USE OF THE SOFTWARE, OR (B) THE SOFTWARE INCLUDES A SEPARATE “CLICK-ACCEPT” LICENSE AGREEMENT OR THIRD PARTY LICENSE AGREEMENT AS PART OF THE INSTALLATION AND/OR DOWNLOAD PROCESS GOVERNING CUSTOMER’S USE OF THE SOFTWARE. TO THE EXTENT OF A CONFLICT BETWEEN THE PROVISIONS OF THE FOREGOING DOCUMENTS, THE ORDER OF PRECEDENCE SHALL BE (1)THE SIGNED CONTRACT, (2) THE CLICK-ACCEPT AGREEMENT OR THIRD PARTY LICENSE AGREEMENT, AND (3) THE AGREEMENT.

License. Conditioned upon compliance with the terms and conditions of the Agreement, Inscape Data grants to Customer a nonexclusive and nontransferable license to use for Customer's internal business purposes the Software and the Documentation for which Customer has paid the required license fees. "Documentation" means written information (whether contained in user or technical manuals, training materials, specifications or otherwise) pertaining to the Software and made available by Inscape Data with the Software in any manner (including on CD-ROM, or on-line). In order to use the Software, Customer may be required to input a registration number or product authorization key and register Customer's copy of the Software online at Inscape Data's website to obtain the necessary license key or license file.

End User License Agreement

Customer's license to use the Software shall be limited to, and Customer shall not use the Software in excess of, a single hardware chassis or card or such other limitations as are set forth in the applicable Supplemental License Agreement or in the applicable purchase order which has been accepted by Inscape Data and for which Customer has paid to Inscape Data the required license fee (the "Purchase Order"). Unless otherwise expressly provided in the Documentation or any applicable Supplemental License Agreement, Customer shall use the Software solely as embedded in, for execution on, or (where the applicable Documentation permits installation on non-Inscape Data equipment) for communication with Inscape Data equipment owned or leased by Customer and used for Customer's internal business purposes. No other licenses are granted by implication, estoppel or otherwise.

For evaluation or beta copies for which Inscape Data does not charge a license fee, the above requirement to pay license fees does not apply.

General Limitations. This is a license, not a transfer of title, to the Software and Documentation, and Inscape Data retains ownership of all copies of the Software and Documentation. Customer acknowledges that the Software and Documentation contain trade secrets of Inscape Data or its suppliers or licensors, including but not limited to the specific internal design and structure of individual programs and associated interface information. Except as otherwise expressly provided under the Agreement, Customer shall have no right, and Customer specifically agrees not to:

- (i) transfer, assign or sublicense its license rights to any other person or entity (other than in compliance with any Inscape Data relicensing/transfer policy then in force), or use the Software on unauthorized or secondhand Inscape Data equipment, and Customer acknowledges that any attempted transfer, assignment, sublicense or use shall be void;
- (ii) make error corrections to or otherwise modify or adapt the Software or create derivative works based upon the Software, or permit third parties to do the same;
- (iii) reverse engineer or decompile, decrypt, disassemble or otherwise reduce the Software to human-readable form, except to the extent otherwise expressly permitted under applicable law notwithstanding this restriction;
- (iv) publish any results of benchmark tests run on the Software;

- (v) use or permit the Software to be used to perform services for third parties, whether on a service bureau or time sharing basis or otherwise, without the express written authorization of Inscape Data; or
- (vi) disclose, provide, or otherwise make available trade secrets contained within the Software and Documentation in any form to any third party without the prior written consent of Inscape Data. Customer shall implement reasonable security measures to protect such trade secrets.

To the extent required by applicable law, and at Customer's written request, Inscape Data shall provide Customer with the interface information needed to achieve interoperability between the Software and another independently created program, on payment of Inscape Data's applicable fee, if any. Customer shall observe strict obligations of confidentiality with respect to such information and shall use such information in compliance with any applicable terms and conditions upon which Inscape Data makes such information available.

Software, Upgrades and Additional Copies. For purposes of the Agreement, "Software" shall include (and the terms and conditions of the Agreement shall apply to) computer programs, including firmware, as provided to Customer by Inscape Data or an authorized Inscape Data reseller, and any upgrades, updates, bug fixes or modified versions thereto (collectively, "Upgrades") or backup copies of any of the foregoing. NOTWITHSTANDING ANY OTHER PROVISION OF THE AGREEMENT: (1) CUSTOMER HAS NO LICENSE OR RIGHT TO MAKE OR USE ANY ADDITIONAL COPIES OR UPGRADES UNLESS CUSTOMER, AT THE TIME OF MAKING OR ACQUIRING SUCH COPY OR UPGRADE, ALREADY HOLDS A VALID LICENSE TO THE ORIGINAL SOFTWARE AND HAS PAID THE APPLICABLE FEE FOR THE UPGRADE OR ADDITIONAL COPIES; (2) USE OF UPGRADES IS LIMITED TO INSCAPE DATA EQUIPMENT FOR WHICH CUSTOMER IS THE ORIGINAL END USER PURCHASER OR LESSEE OR OTHERWISE HOLDS A VALID LICENSE TO USE THE SOFTWARE WHICH IS BEING UPGRADED; AND (3) THE MAKING AND USE OF ADDITIONAL COPIES IS LIMITED TO NECESSARY BACKUP PURPOSES ONLY.

Proprietary Notices. Customer agrees to maintain and reproduce all copyright and other proprietary notices on all copies, in any form, of the Software in the same form and manner that such copyright and other proprietary notices are included on the Software. Except as expressly authorized in the Agreement, Customer shall not make any copies or duplicates of any Software without the prior written permission of Inscape Data.

Term and Termination. The Agreement and the license granted herein shall remain effective until terminated. Customer may terminate the Agreement and the license at any time by destroying all copies of Software and any Documentation. Customer's rights under the Agreement will terminate immediately without notice from Inscape Data if Customer fails to comply with any provision of the Agreement. Upon termination, Customer shall destroy all copies of Software and Documentation in its possession or control. All confidentiality obligations of Customer and all limitations of liability and disclaimers and restrictions of warranty shall survive termination of this Agreement. In addition, the provisions of the sections titled "U.S. Government End User Purchasers" and "General Terms Applicable to the Limited Warranty Statement and End User License Agreement" shall survive termination of the Agreement.

Customer Records. Customer grants to Inscape Data and its independent accountants the right to examine Customer's books, records and accounts during Customer's normal business hours to verify compliance with this Agreement. In the event such audit discloses non-compliance with this Agreement, Customer shall promptly pay to Inscape Data the appropriate license fees, plus the reasonable cost of conducting the audit.

Export, Re-Export, Transfer and Use Controls. The Software, Documentation and technology or direct products thereof (hereafter referred to as Software and Technology), supplied by Inscape Data under the Agreement are subject to export controls under the laws and regulations of the United States (U.S.) and any other applicable countries' laws and regulations. Customer shall comply with such laws and regulations governing export, re-export, transfer and use of Inscape Data Software and Technology and will obtain all required U.S. and local authorizations, permits, or licenses. Inscape Data and Customer each agree to provide the other information, support documents, and assistance as may reasonably be required by the other in connection with securing authorizations or licenses.

End User License Agreement

U.S. Government End User Purchasers. The Software and Documentation qualify as "commercial items," as that term is defined at Federal Acquisition Regulation ("FAR") (48 C.F.R.) 2.101, consisting of "commercial computer software" and "commercial computer software documentation" as such terms are used in FAR 12.212. Consistent with FAR 12.212 and DoD FAR Supp. 227.7202-1 through 227.7202-4, and notwithstanding any other FAR or other contractual clause to the contrary in any agreement into which the Agreement may be incorporated, Customer may provide to Government end user or, if the Agreement is direct, Government end user will acquire, the Software and Documentation with only those rights set forth in the Agreement. Use of either the Software or Documentation or both constitutes agreement by the Government that the Software and Documentation are "commercial computer software" and "commercial computer software documentation," and constitutes acceptance of the rights and restrictions herein.

Limited Warranty

Subject to the limitations and conditions set forth herein, Inscape Data warrants that commencing from the date of shipment to Customer (but in case of resale by an authorized Inscape Data reseller, commencing not more than ninety (90) days after original shipment by Inscape Data), and continuing for a period of the longer of (a) ninety (90) days or (b) the warranty period (if any) expressly set forth as applicable specifically to software in the warranty card accompanying the product of which the Software is a part (the "Product") (if any): (a) the media on which the Software is furnished will be free of defects in materials and workmanship under normal use; and (b) the Software substantially conforms to the Documentation. The date of shipment of a Product by Inscape Data is set forth on the packaging material in which the Product is shipped. Except for the foregoing, the Software is provided "AS IS". This limited warranty extends only to the Customer who is the original licensee. Customer's sole and exclusive remedy and the entire liability of Inscape Data and its suppliers under this limited warranty will be (i) replacement of defective media and/or (ii) at Inscape Data's option, repair, replacement, or refund of the purchase price of the Software, in both cases subject to the condition that any error or defect constituting a breach of this limited warranty is

reported to Inscap Data or the party supplying the Software to Customer, if different than Inscap Data, within the warranty period. Inscap Data or the party supplying the Software to Customer may, at its option, require return of the Software and/or Documentation as a condition to the remedy. In no event does Inscap Data warrant that the Software is error free or that Customer will be able to operate the Software without problems or interruptions. In addition, due to the continual development of new techniques for intruding upon and attacking networks, Inscap Data does not warrant that the Software or any equipment, system or network on which the Software is used will be free of vulnerability to intrusion or attack.

Restrictions. This warranty does not apply if the Software, Product or any other equipment upon which the Software is authorized to be used (a) has been altered, except by Inscap Data or its authorized representative, (b) has not been installed, operated, repaired, or maintained in accordance with instructions supplied by Inscap Data, (c) has been subjected to abnormal physical or electrical stress, abnormal environmental conditions, misuse, negligence, or accident; or (d) is licensed for beta, evaluation, testing or demonstration purposes. The Software warranty also does not apply to (e) any temporary Software modules; or (f) any Software for which Inscap Data does not receive a license fee.

DISCLAIMER OF WARRANTY

EXCEPT AS SPECIFIED IN THIS WARRANTY SECTION, ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS, AND WARRANTIES INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTY OR CONDITION OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NON-INFRINGEMENT, SATISFACTORY QUALITY, NON-INTERFERENCE, ACCURACY OF INFORMATIONAL CONTENT, OR ARISING FROM A COURSE OF DEALING, LAW, USAGE, OR TRADE PRACTICE, ARE HEREBY EXCLUDED TO THE EXTENT ALLOWED BY APPLICABLE LAW AND ARE EXPRESSLY DISCLAIMED BY INSCAPE DATA, ITS SUPPLIERS AND LICENSORS. TO THE EXTENT AN IMPLIED WARRANTY CANNOT BE EXCLUDED, SUCH WARRANTY IS LIMITED IN DURATION TO THE EXPRESS WARRANTY PERIOD. BECAUSE SOME STATES OR JURISDICTIONS DO NOT ALLOW LIMITATIONS ON HOW LONG AN IMPLIED WARRANTY LASTS, THE ABOVE LIMITATION MAY NOT APPLY. THIS WARRANTY GIVES CUSTOMER SPECIFIC LEGAL RIGHTS, AND CUSTOMER MAY ALSO HAVE OTHER RIGHTS WHICH VARY FROM JURISDICTION TO JURISDICTION. This disclaimer and exclusion shall apply even if the express warranty set forth above fails of its essential purpose.

General Terms Applicable to the Limited Warranty Statement, End User License Agreement, and Supplemental License Agreement

Disclaimer of Liabilities - Limitation of Liability. IF YOU ACQUIRED THE SOFTWARE IN THE UNITED STATES, LATIN AMERICA, CANADA, JAPAN OR THE CARIBBEAN, NOTWITHSTANDING ANYTHING ELSE IN THE AGREEMENT TO THE CONTRARY, ALL LIABILITY OF INSCAPE DATA, ITS AFFILIATES, OFFICERS, DIRECTORS, EMPLOYEES, AGENTS, SUPPLIERS AND LICENSORS COLLECTIVELY, TO CUSTOMER, WHETHER IN CONTRACT, TORT (INCLUDING NEGLIGENCE), BREACH OF WARRANTY OR OTHERWISE, SHALL NOT EXCEED THE PRICE PAID BY CUSTOMER TO INSCAPE DATA FOR THE SOFTWARE THAT GAVE RISE TO THE

CLAIM OR IF THE SOFTWARE IS PART OF ANOTHER PRODUCT, THE PRICE PAID FOR SUCH OTHER PRODUCT. THIS LIMITATION OF LIABILITY FOR SOFTWARE IS CUMULATIVE AND NOT PER INCIDENT (I.E. THE EXISTENCE OF TWO OR MORE CLAIMS WILL NOT ENLARGE THIS LIMIT). IF YOU ACQUIRED THE SOFTWARE IN EUROPE, THE MIDDLE EAST, AFRICA, ASIA OR OCEANIA, NOTWITHSTANDING ANYTHING ELSE IN THE AGREEMENT TO THE CONTRARY, ALL LIABILITY OF INSCAPE DATA, ITS AFFILIATES, OFFICERS, DIRECTORS, EMPLOYEES, AGENTS, SUPPLIERS AND LICENSORS COLLECTIVELY, TO CUSTOMER, WHETHER IN CONTRACT, TORT (INCLUDING NEGLIGENCE), BREACH OF WARRANTY OR OTHERWISE, SHALL NOT EXCEED THE PRICE PAID BY CUSTOMER TO INSCAPE DATA FOR THE SOFTWARE THAT GAVE RISE TO THE CLAIM OR IF THE SOFTWARE IS PART OF ANOTHER PRODUCT, THE PRICE PAID FOR SUCH OTHER PRODUCT. THIS LIMITATION OF LIABILITY FOR SOFTWARE IS CUMULATIVE AND NOT PER INCIDENT (I.E. THE EXISTENCE OF TWO OR MORE CLAIMS WILL NOT ENLARGE THIS LIMIT). NOTHING IN THE AGREEMENT SHALL LIMIT (I) THE LIABILITY OF INSCAPE DATA, ITS AFFILIATES, OFFICERS, DIRECTORS, EMPLOYEES, AGENTS, SUPPLIERS AND LICENSORS TO CUSTOMER FOR PERSONAL INJURY OR DEATH CAUSED BY THEIR NEGLIGENCE, (II) INSCAPE DATA'S LIABILITY FOR FRAUDULENT MISREPRESENTATION, OR (III) ANY LIABILITY OF INSCAPE DATA WHICH CANNOT BE EXCLUDED UNDER APPLICABLE LAW.

End User License Agreement

Disclaimer of Liabilities - Waiver of Consequential Damages and Other Losses. IF YOU ACQUIRED THE SOFTWARE IN THE UNITED STATES, LATIN AMERICA, THE CARIBBEAN OR CANADA, REGARDLESS OF WHETHER ANY REMEDY SET FORTH HEREIN FAILS OF ITS ESSENTIAL PURPOSE OR OTHERWISE, IN NO EVENT WILL INSCAPE DATA OR ITS SUPPLIERS BE LIABLE FOR ANY LOST REVENUE, PROFIT, OR LOST OR DAMAGED DATA, BUSINESS INTERRUPTION, LOSS OF CAPITAL, OR FOR SPECIAL, INDIRECT, CONSEQUENTIAL, INCIDENTAL, OR PUNITIVE DAMAGES HOWEVER CAUSED AND REGARDLESS OF THE THEORY OF LIABILITY OR WHETHER ARISING OUT OF THE USE OF OR INABILITY TO USE SOFTWARE OR OTHERWISE AND EVEN IF INSCAPE DATA OR ITS SUPPLIERS OR LICENSORS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. BECAUSE SOME STATES OR JURISDICTIONS DO NOT ALLOW LIMITATION OR EXCLUSION OF CONSEQUENTIAL OR INCIDENTAL DAMAGES, THE ABOVE LIMITATION MAY NOT APPLY TO YOU.

IF YOU ACQUIRED THE SOFTWARE IN JAPAN, EXCEPT FOR LIABILITY ARISING OUT OF OR IN CONNECTION WITH DEATH OR PERSONAL INJURY, FRAUDULENT MISREPRESENTATION, AND REGARDLESS OF WHETHER ANY REMEDY SET FORTH HEREIN FAILS OF ITS ESSENTIAL PURPOSE OR OTHERWISE, IN NO EVENT WILL INSCAPE DATA, ITS AFFILIATES, OFFICERS, DIRECTORS, EMPLOYEES, AGENTS, SUPPLIERS AND LICENSORS BE LIABLE FOR ANY LOST REVENUE, PROFIT, OR LOST OR DAMAGED DATA, BUSINESS INTERRUPTION, LOSS OF CAPITAL, OR FOR SPECIAL, INDIRECT, CONSEQUENTIAL, INCIDENTAL, OR PUNITIVE DAMAGES HOWEVER CAUSED AND REGARDLESS OF THE THEORY OF LIABILITY OR WHETHER ARISING OUT OF THE USE OF OR INABILITY TO USE SOFTWARE OR OTHERWISE AND EVEN IF INSCAPE DATA OR ITS SUPPLIERS

OR LICENSORS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

IF YOU ACQUIRED THE SOFTWARE IN EUROPE, THE MIDDLE EAST, AFRICA, ASIA OR OCEANIA, IN NO EVENT WILL INSCAPE DATA, ITS AFFILIATES, OFFICERS, DIRECTORS, EMPLOYEES, AGENTS, SUPPLIERS AND LICENSORS, BE LIABLE FOR ANY LOST REVENUE, LOST PROFIT, OR LOST OR DAMAGED DATA, BUSINESS INTERRUPTION, LOSS OF CAPITAL, OR FOR SPECIAL, INDIRECT, CONSEQUENTIAL, INCIDENTAL, OR PUNITIVE DAMAGES, HOWSOEVER ARISING, INCLUDING, WITHOUT LIMITATION, IN CONTRACT, TORT (INCLUDING NEGLIGENCE) OR WHETHER ARISING OUT OF THE USE OF OR INABILITY TO USE THE SOFTWARE, EVEN IF, IN EACH CASE, INSCAPE DATA, ITS AFFILIATES, OFFICERS, DIRECTORS, EMPLOYEES, AGENTS, SUPPLIERS AND LICENSORS, HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. BECAUSE SOME STATES OR JURISDICTIONS DO NOT ALLOW LIMITATION OR EXCLUSION OF CONSEQUENTIAL OR INCIDENTAL DAMAGES, THE ABOVE LIMITATION MAY NOT FULLY APPLY TO YOU. THE FOREGOING WAIVER SHALL NOT APPLY TO ANY LIABILITY ARISING OUT OF OR IN CONNECTION WITH: (I) DEATH OR PERSONAL INJURY, (II) FRAUDULENT MISREPRESENTATION, OR (III) INSCAPE DATA'S LIABILITY IN CONNECTION WITH ANY TERMS THAT CANNOT BE EXCLUDED UNDER APPLICABLE LAW.

For all countries referred to above, Customer agrees that the limitations of liability and disclaimers set forth herein will apply regardless of whether Customer has accepted the Software or any other product or service delivered by Inscape Data.

Customer acknowledges and agrees that Inscape Data has set its prices and entered into the Agreement in reliance upon the disclaimers of warranty and the limitations of liability set forth herein, that the same reflect an allocation of risk between the parties (including the risk that a contract remedy may fail of its essential purpose and cause consequential loss), and that the same form an essential basis of the bargain between the parties.

Controlling Law, Jurisdiction. If you acquired the Software in the United States, Latin America, or the Caribbean, the Agreement and Hardware and Software warranties (“Warranties”) are controlled by and construed under the laws of the State of California, United States of America, notwithstanding any conflicts of law provisions; and the state and federal courts of California shall have exclusive jurisdiction over any claim arising under the Agreement or Warranties. If you acquired the Software in Canada, unless expressly prohibited by local law, the Agreement and Warranties are controlled by and construed under the laws of the Province of Ontario, Canada, notwithstanding any conflicts of law provisions; and the courts of the Province of Ontario shall have exclusive jurisdiction over any claim arising under the Agreement or Warranties. If you acquired the Software in Europe, the Middle East, Africa, Asia or Oceania (excluding Australia), unless expressly prohibited by local law, the Agreement and Warranties are controlled by and construed under the laws of England, notwithstanding any conflicts of law provisions; and the English courts shall have exclusive jurisdiction over any claim arising under the Agreement or Warranties. In addition, if the Agreement is controlled by the laws of England, no person who is not a party to the Agreement shall be entitled to enforce or take the benefit of any of its terms under the Contracts (Rights of Third Parties) Act 1999. If you acquired the Software in Japan, unless expressly prohibited by local law, the Agreement and Warranties are controlled by and construed under the laws of Japan, notwithstanding any conflicts of law provisions; and the Tokyo District

Court of Japan shall have exclusive jurisdiction over any claim arising under the Agreement or Warranties. If you acquired the Software in Australia, unless expressly prohibited by local law, the Agreement and Warranties are controlled by and construed under the laws of the State of New South Wales, Australia, notwithstanding any conflicts of law provisions; and the State and federal courts of New South Wales shall have exclusive jurisdiction over any claim arising under the Agreement or Warranties. If you acquired the Software in any other country, unless expressly prohibited by local law, the Agreement and Warranties are controlled by and construed under the laws of the State of California, United States of America, notwithstanding any conflicts of law provisions; and the state and federal courts of California shall have exclusive jurisdiction over any claim arising under the Agreement or Warranties.

For all countries referred to above, the parties specifically disclaim the application of the UN Convention on Contracts for the International Sale of Goods. Notwithstanding the foregoing, either party may seek interim injunctive relief in any court of appropriate jurisdiction with respect to any alleged breach of such party's intellectual property or proprietary rights. If any portion hereof is found to be void or unenforceable, the remaining provisions of the Agreement and Warranties shall remain in full force and effect. Except as expressly provided herein, the Agreement constitutes the entire agreement between the parties with respect to the license of the Software and Documentation and supersedes any conflicting or additional terms contained in any Purchase Order or elsewhere, all of which terms are excluded. The Agreement has been written in the English language, and the parties agree that the English version will govern.

© 2007, 2008, 2009 Inscope Data Corporation, All rights reserved.