

# EXA100 Wireless AP Router User Manual

Version A1.0, November 29, 2012

---



## Preface

This manual provides information related to the installation and operation of this device. The individual reading this manual is presumed to have a basic understanding of telecommunications terminology and concepts.

## Important Safety Instructions

With reference to unpacking, installation, use, and maintenance of your electronic device, the following basic guidelines are recommended:

Do not use or install this product near water, to avoid fire or shock hazard. For example, near a bathtub, kitchen sink or laundry tub, or near a swimming pool. Also, do not expose the equipment to rain or damp areas (e.g. a wet basement).

Do not connect the power supply cord on elevated surfaces. Allow it to lie freely. There should be no obstructions in its path and no heavy items should be placed on the cord. In addition, do not walk on, step on, or mistreat the cord.

Use only the power cord and adapter that are shipped with this device. This product is intended to be supplied by a UL Listed Power Supply with marked with "L.P.S.", or "Limited Power Source", and output rated 12 Vdc, minimum 1.0A.

To safeguard the equipment against overheating, make sure that all openings in the unit that offer exposure to air are not blocked.

Avoid using a telephone (other than a cordless type) during an electrical storm. There may be a remote risk of electric shock from lightening. Also, do not use the telephone to report a gas leak in the vicinity of the leak. Never install telephone wiring during stormy weather conditions.

The equipment is to be connected only to PoE networks without routing to the outside plant.

Following instruction or similar in the manual wiring method should comply article 725 and article 300 in national electrical code for class 2 circuit and wiring in duct.

All the installation should performed by qualified personnel.

### CAUTION:

To reduce the risk of fire, use only No. 26 AWG or larger telecommunication line cord.

Always disconnect all telephone lines from the wall outlet before servicing or disassembling this equipment.



### WARNING

Disconnect the power line from the device before servicing.

Power supply specifications are clearly stated in [Appendix B – Specifications](#)

## Copyright

Copyright© 2012 Cetus Corporation. All rights reserved. The information contained herein is proprietary to Cetus Corporation. No part of this document may be translated, transcribed, reproduced, in any form, or by any means without the prior written consent of Cetus Corporation.

This program is free software: you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation, either version 3 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program. If not, see <http://www.gnu.org/licenses/>

<b>NOTE:</b> This document is subject to change without notice.
---

## Protect Our Environment



This symbol indicates that when the equipment has reached the end of its useful life, it must be taken to a recycling centre and processed separate from domestic waste.

The cardboard box, the plastic contained in the packaging, and the parts that make up this router can be recycled in accordance with regionally established regulations. Never dispose of this electronic equipment along with your household waste; you may be subject to penalties or sanctions under the law. Instead, please be responsible and ask for disposal instructions from your local government.

# Table of Contents

Chapter 1 Introduction .....	5
1.1 Features .....	5
1.2 Application.....	6
Chapter 2 Installation .....	7
Chapter 3 Web User Interface.....	9
3.1 Default Settings .....	9
3.2 IP Configuration .....	9
3.3 Login Procedure.....	11
Chapter 4 Device Information .....	14
4.1 Statistics.....	15
Chapter 5 Wireless Setting .....	16
5.1 Basic.....	16
5.2 Advanced .....	19
5.3 Security .....	21
5.4 WDS .....	23
5.5 WPS.....	26
5.6 Station List .....	28
5.7 AP Wireless Statistics.....	29
Chapter 6 Management - Configuration Backup.....	30
6.1 Management IP .....	30
6.2 LED Control.....	31
6.3 SNMP Agent.....	32
6.4 TR-069 Client .....	33
6.5 Update Software.....	35

6.6 Reboot .....	37
6.7 Configuration .....	38
6.7.1 Backup Settings.....	38
6.7.2 Update Settings.....	38
6.7.3 Restore Default .....	39
Appendix A - Pin Assignments .....	40
Appendix B – Specifications.....	41
Appendix C –Parameter Rules .....	43

# Chapter 1 Introduction

The EXA100 is a Wi-Fi AP module which can be inserted into wall-mounted customized housing. The EXA100 is an 802.11n (300Mbps) Wireless AP and is backward compatible with existing 802.11b (11Mbps) and 11g (54Mbps) equipment.

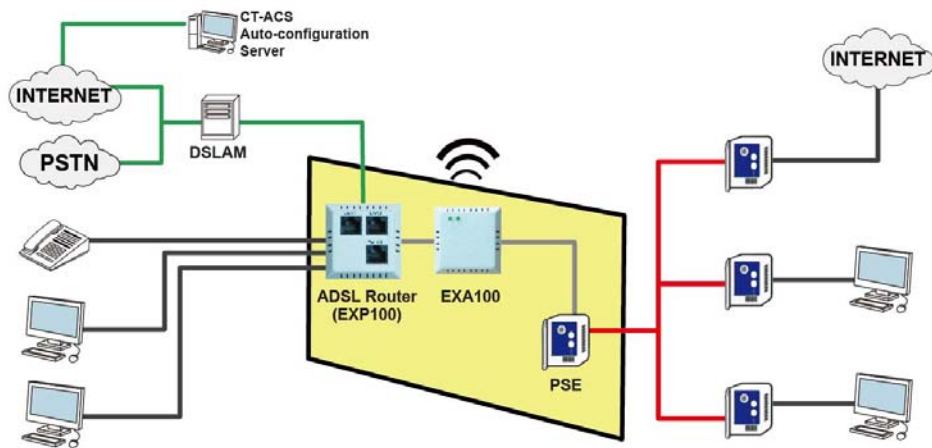
The EXA100 is customized for Hotel environment applications. It is integrated to be power supplied by DC-Jack or punch connector from Power over Ethernet Device and ADSL Router (EXP100). Hence it can provide several kinds of application methods to combine the wireless easily. It also provides state of the art security features such as 64/128 bit WEP encryption and WPA/WPA2 encryption, Firewall, and VPN pass through.

## 1.1 Features

- Wireless 802.11n access point – up to 300Mbps
- 2 LAN ports (punch by IDC connector)
- Browser based interface for configuration and management: OS independent and easy to use
- Support CLI command to access Wireless AP
- Full wireless security – WEP, WPA, WPA2
- Power Supply for 3 options (DC-Jack / ADSL power in / PSE power in )

## 1.2 Application

The following diagrams depict typical applications of the EXA100.



# Chapter 2 Installation

## FRONT PANEL



The figure below shows the front panel of the device.

### LED Status

LED	Status	Descriptions
Power	Solid OFF	System is power off or system status is abnormal or disabling 'LED ON' in web UI.
	Solid ON	System is operational
Wireless Link	Solid OFF	Wi-Fi is disabled or disabling 'LED ON' in web UI.
	Solid ON	Wi-Fi is operational
	Flashing	Data transmission through Wi-Fi



## **REAR PANEL**

The figure below shows the rear panel of the device.



**Caution 1:** If the device fails to power up, or it malfunctions, first verify that the power cords are connected securely and then power it on again. If the problem persists, contact technical support.

**Caution 2:** Before servicing or disassembling this equipment, disconnect all power cords and telephone lines from their outlets.

### **Reset Button**

Restore the default parameters of the device by pressing the Reset button for 5 to 10 seconds.

## Chapter 3 Web User Interface

This section describes how to access the device via the web user interface (WUI) using an Internet browser such as Internet Explorer (version 5.0 and later).

### 3.1 Default Settings

The factory default settings of this device are summarized below.

LAN IP address: 192.168.1.254  
LAN subnet mask: 255.255.255.0  
Administrative access (username: **root** , password: **12345** )  
User access (username: **user**, password: **user**)  
Remote (WAN) access (username: **support**, password: **support**)

#### **Technical Note**

During power on, the device initializes all settings to default values. It will then read the configuration profile from the permanent storage section of flash memory. The default attributes are overwritten when identical attributes with different values are configured. The configuration profile in permanent storage can be created via the web user interface or telnet user interface, or other management protocols. The factory default configuration can be restored either by pushing the reset button for more than five seconds until the power indicates LED blinking or by clicking the Restore Default Configuration option in the Restore Settings screen.

### 3.2 IP Configuration

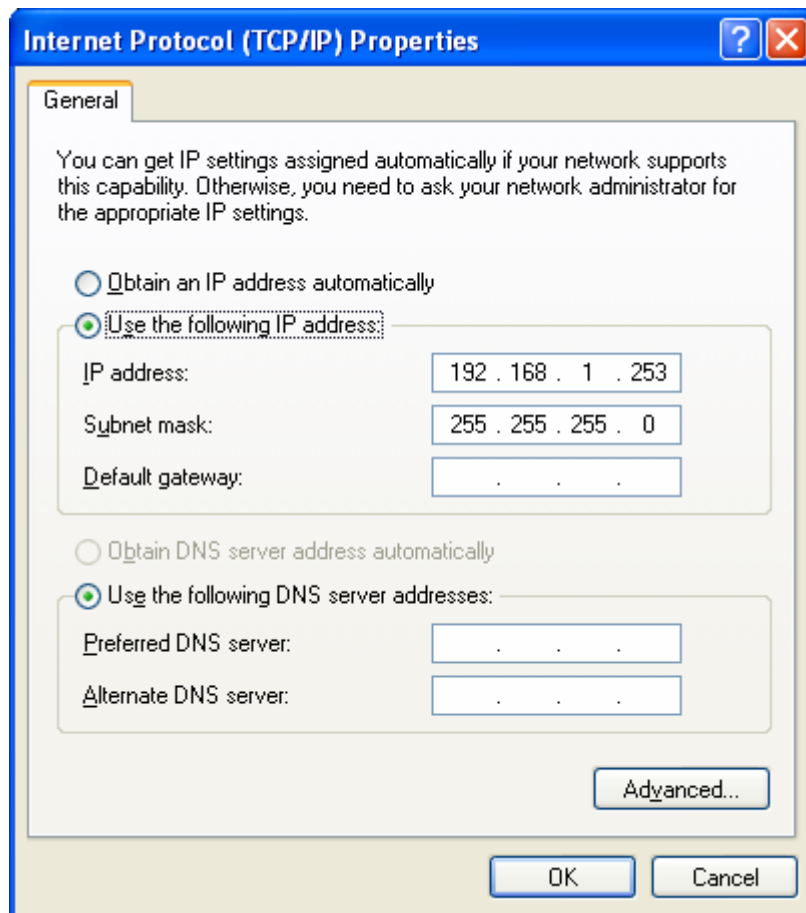
#### **STATIC IP MODE**

In static IP mode, you assign IP settings to your PC manually.

Follow these steps to configure your PC IP address to use subnet 192.168.1.x.

<p><b>NOTE:</b> The following procedure assumes you are running Windows XP. However, the general steps involved are similar for most operating systems (OS). Check your OS support documentation for further details.</p>
---

- STEP 1:** From the Network Connections window, open Local Area Connection (You may also access this screen by double-clicking the Local Area Connection icon on your taskbar). Click the **Properties** button.
- STEP 2:** Select Internet Protocol (TCP/IP) **and click the** Properties button.
- STEP 3:** Change the IP address to the 192.168.1.x (1<x<255) subnet with subnet mask of 255.255.255.0. The screen should now display as shown below.



- STEP 4:** Click **OK** to submit these settings.

## 3.3 Login Procedure

Perform the following steps to login to the web user interface.

**NOTE:** The default settings can be found in [3.1 Default Settings](#).

**STEP 1:** Start the Internet browser and enter the default IP address for the device in the Web address field. For example, if the default IP address is 192.168.1.254, type <http://192.168.1.254>.

**NOTE:** For local administration (i.e. LAN access), the PC running the browser must be attached to the Ethernet, and not necessarily to the device.  
For remote access (i.e. WAN), use the IP address shown on the

Chapter 4 Device Information screen and login with remote username and password.

**STEP 2:** A dialog box will appear, such as the one below. Enter the default username and password, as defined in [section 3.1 Default Settings](#).



Click **OK** to continue.

**NOTE:** The login password can be changed later (see [8.6.1 Passwords](#)).

**STEP 3:** After successfully logging in for the first time, you will reach this screen.



### Access Point Status

System Info	
FW Version	3.6.0.0 (Oct 22 2012)
System Up Time	3 mins, 59 secs
Operation Mode	Bridge Mode
Software Version	P901-3600ITR-C02_R02
Local Network	
Local IP Address	192.168.1.254
Local Netmask	255.255.255.0
MAC Address	00:0C:43:44:11:02

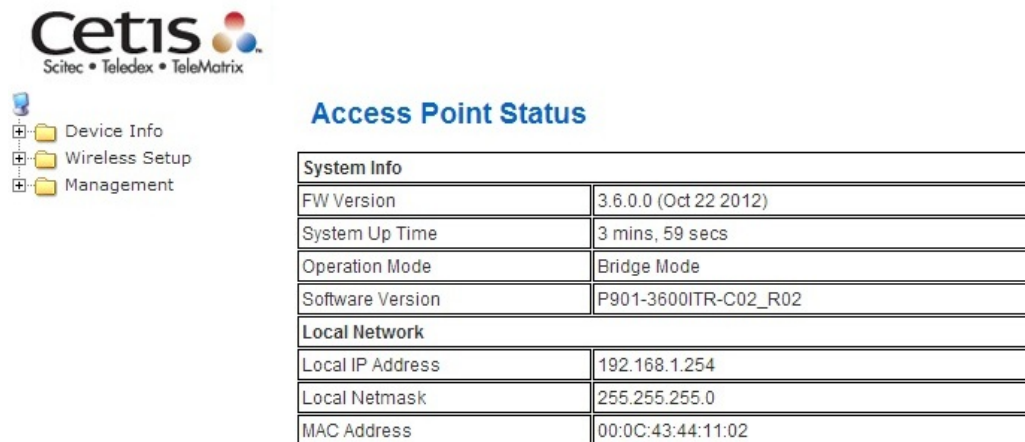
## Chapter 4 Device Information

The web user interface window is divided into two frames, the main menu (at left) and the display screen (on the right). The main menu has several options and selecting each of these options opens a submenu with more selections.

**NOTE:** The menu items shown are based upon the configured connection(s) and user account privileges. For example, if NAT and Firewall are enabled, the main menu will display the NAT and Security submenus. If either is disabled, their corresponding menu(s) will also be disabled.

Device Info is the first selection on the main menu so it will be discussed first. Subsequent chapters will introduce the other main menu options in sequence.

The Access Point Status screen displays at startup.



**Cetus**  
Scitec • Teledex • TeleMatrix

- Device Info
- Wireless Setup
- Management


### Access Point Status

System Info	
FW Version	3.6.0.0 (Oct 22 2012)
System Up Time	3 mins, 59 secs
Operation Mode	Bridge Mode
Software Version	P901-3600ITR-C02_R02
Local Network	
Local IP Address	192.168.1.254
Local Netmask	255.255.255.0
MAC Address	00:0C:43:44:11:02

This screen shows software, IP settings and other related information.

## 4.1 Statistics

Select Interface Statistics from the Device Info submenu to display the following.



**Cetis**  
Scitec • Teledex • TeleMatrix

**Statistics**

**Memory**

Memory total:	28560 kB
Memory left:	8516 kB

**WAN/LAN**

WAN Rx packets:	2347
WAN Rx bytes:	292412
WAN Tx packets:	2886
WAN Tx bytes:	1893876
LAN Rx packets:	2347
LAN Rx bytes:	292412
LAN Tx packets:	2886
LAN Tx bytes:	1893876

**All interfaces**

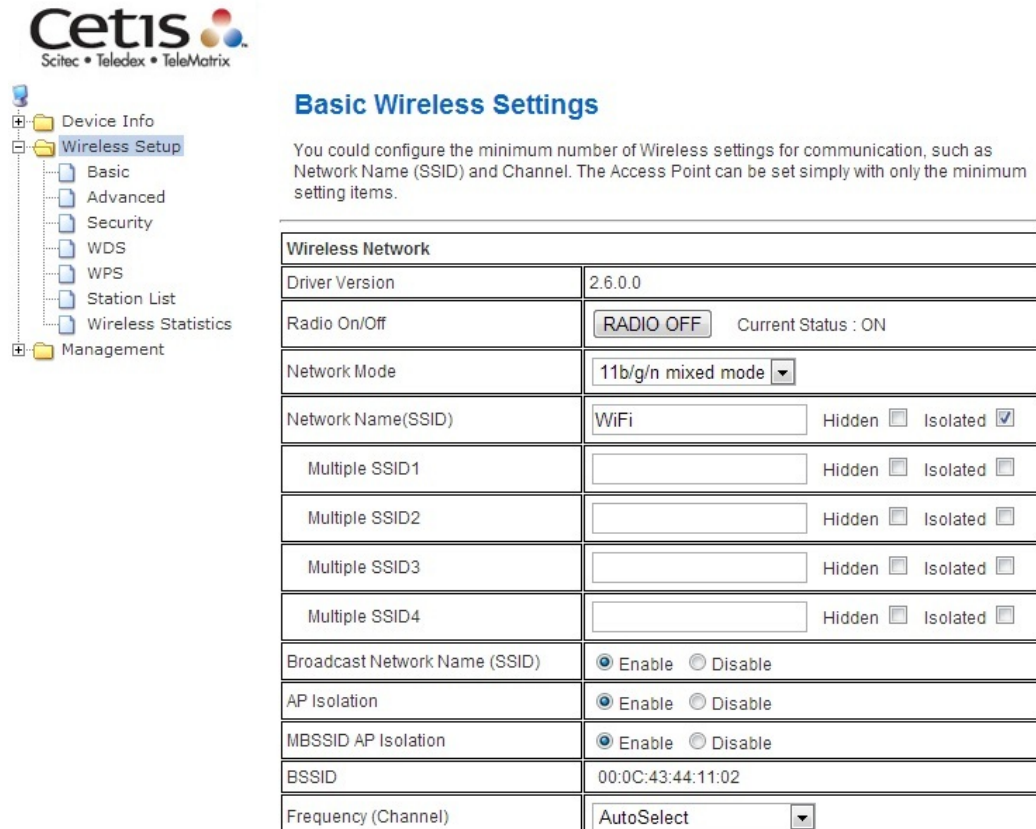
Name	eth2
Rx Packet	2328
Rx Byte	322618
Tx Packet	2906
Tx Byte	1905014
Name	lo
Rx Packet	54
Rx Byte	6100
Tx Packet	54
Tx Byte	6100
Name	ra0
Rx Packet	209031
Rx Byte	50985337
Tx Packet	9519
Tx Byte	42878
Name	br0
Rx Packet	2347
Rx Byte	292412
Tx Packet	2886
Tx Byte	1893876



# Chapter 5 Wireless Setting

## 5.1 Basic

You can configure the minimum number of wireless settings for communication, such as network name (SSID) and channel.



**Cetis**  
Scitec • Teledex • TeleMatrix

**Basic Wireless Settings**

You could configure the minimum number of Wireless settings for communication, such as Network Name (SSID) and Channel. The Access Point can be set simply with only the minimum setting items.

Wireless Network	
Driver Version	2.6.0.0
Radio On/Off	<input type="button" value="RADIO OFF"/> Current Status : ON
Network Mode	11b/g/n mixed mode ▾
Network Name(SSID)	WiFi Hidden <input type="checkbox"/> Isolated <input checked="" type="checkbox"/>
Multiple SSID1	<input type="text"/> Hidden <input type="checkbox"/> Isolated <input type="checkbox"/>
Multiple SSID2	<input type="text"/> Hidden <input type="checkbox"/> Isolated <input type="checkbox"/>
Multiple SSID3	<input type="text"/> Hidden <input type="checkbox"/> Isolated <input type="checkbox"/>
Multiple SSID4	<input type="text"/> Hidden <input type="checkbox"/> Isolated <input type="checkbox"/>
Broadcast Network Name (SSID)	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
AP Isolation	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
MBSSID AP Isolation	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
BSSID	00:0C:43:44:11:02
Frequency (Channel)	AutoSelect ▾

### Wireless Network

Field	Description
<b>Driver Version</b>	Displays the version of the driver.
<b>Radio On/Off:</b>	Enable or disable the wireless LAN.
<b>Network Mode:</b>	There are 5 modes: 11b only, 11g only, 11n only, 11b/g mixed mode, and 11b/g/n mixed mode.
<b>Network Name (SSID):</b>	The service set identification (SSID) is a unique name to identify the router in the wireless LAN. Wireless stations associating to the router must have the same SSID. Input a descriptive name. Its length is up to 32 characters.

<b>Multiple SSID 1/2/3/4:</b>	This router supports multiple SSIDs called Guest SSIDs or Virtual Access Points.
<b>Broadcast Network Name (SSID):</b>	Select Enable to allow the SSID broadcast on the network, so that the STA can find it. Otherwise, the STA cannot find it.
<b>AP Isolation:</b>	Enable or disable AP Isolation. When many clients connect to the same access point, they can access each other. If you want to disable the access between clients which connect the same access point, you can enable this function.
<b>MBSSID AP Isolation:</b>	Enable or disable MBSSID AP Isolation.
<b>BSSID:</b>	Basic Service Set Identifier. This is the assigned MAC address of the station in the access point. This unique identifier is in Hex format and can only be edited when Multi BSSID is enabled in the previous screen.
<b>Frequency (Channel):</b>	A channel is the radio frequency used by the wireless device. Channels available depend on your geographical area. You may have a choice of channels (for your region) and you should use a different channel from an adjacent AP to reduce the interference. The Interference and degrading performance occurs when radio signals from different APs overlap.

### HT Physical Mode

HT Physical Mode	
Operating Mode	<input checked="" type="radio"/> Mixed Mode <input type="radio"/> Green Field
Channel BandWidth	<input type="radio"/> 20 <input checked="" type="radio"/> 20/40
Guard Interval	<input type="radio"/> long <input checked="" type="radio"/> Auto
MCS	Auto ▼
Reverse Direction Grant(RDG)	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
STBC	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
Aggregation MSDU(A-MSDU)	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
Auto Block ACK	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
Decline BA Request	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
HT Disallow TKIP	<input type="radio"/> Disable <input checked="" type="radio"/> Enable

Field	Description
<b>Operating Mode</b>	Two modes: Mixed Mode and Green Field Default is Mixed Mode.
<b>Channel BandWidth</b>	Set the channel bandwidth of wireless radio 20MHz and 20/40 MHz Default is 20/40 MHz
<b>Guard Interval</b>	Guard Interval is used to avoid that distinct transmissions do not affect with one another. With Long Guard and Auto. Default is Auto.
<b>MCS</b>	Modulation and Coding Scheme Range From 1 to 15, 32 and Auto Default is Auto.
<b>Reverse Direction Grant(RDG)</b>	Enable or disable Reverse Direction Grant(RDG). Default is enable.
<b>STBC</b>	Enable or disable STBC. Default is enable.
<b>Aggregation MSDU(A-MSDU)</b>	Enable or disable Aggregation MSDU(A-MSDU). Default is disable.
<b>Auto Block ACK</b>	Enable or disable Auto Block ACK Default is enable.
<b>Decline BA Request</b>	Enable or disable Decline BA Request Default is disable.
<b>HT Disallow TKIP</b>	Enable or disable HT Disallow TKIP. Default is enable.

## Other

Other	
HT TxStream	2 ▼
HT RxStream	2 ▼

Field	Description
<b>HT TxStream</b>	Stream numbers transmits.
<b>HT RxStream</b>	Stream numbers receives.

## 5.2 Advanced

Use this page to make detailed settings for the AP. **Advanced Wireless Settings** page includes items that are not available in the **Basic Wireless Settings** page, such as basic data rates, beacon interval, and data beacon rate.

**Cetis**  
Scitec • Teledex • TeleMatrix

### Advanced Wireless Settings

Use the Advanced Setup page to make detailed settings for the Wireless. Advanced Setup includes items that are not available from the Basic Setup page, such as Beacon Interval, Control Tx Rates and Basic Data Rates.

Advanced Wireless	
BG Protection Mode	Auto
Beacon Interval	100 ms (range 20 - 999, default 100)
Data Beacon Rate (DTIM)	1 ms (range 1 - 255, default 1)
Fragment Threshold	2346 (range 256 - 2346, default 2346)
RTS Threshold	2347 (range 1 - 2347, default 2347)
TX Power	100 (range 1 - 100, default 100)
Short Preamble	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Short Slot	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Tx Burst	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Pkt_Aggregate	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
IEEE 802.11H Support	<input type="radio"/> Enable <input checked="" type="radio"/> Disable (only in A band)
Country Code	US (United States)

### Advanced Wireless

Field	Description
<b>BG Protection Mode:</b>	It provides 3 options, including Auto, On, and Off. The default BG protection mode is <b>Auto</b> .
<b>Beacon Interval:</b>	The interval time range is between 20ms and 999ms for each beacon transmission. The default value is 100ms.
<b>Date Beacon Rate (DTM):</b>	The DTM range is between 1ms and 255 ms. The default value is 1ms.
<b>Fragment Threshold:</b>	This is the maximum data fragment size (between 256 bytes and 2346 bytes) that can be sent in the wireless network before the router fragments the packet into smaller data frames. The default value is 2346.

<b>RTS Threshold:</b>	Request to send (RTS) is designed to prevent collisions due to hidden nodes. An RTS defines the biggest size data frame you can send before an RTS handshake is invoked. The RTS threshold value is between 1 and 2347. The default value is 2347. If the RTS threshold value is greater than the fragment threshold value, the RTS handshake does not occur. Because the data frames are fragmented before they reach the RTS size.
<b>Tx Power:</b>	The Tx Power range is between 1 and 100. The default value is 100.
<b>Short Preamble:</b>	Select Disable or Enable.
<b>Short Slot:</b>	Select Disable or Enable.
<b>Tx Burst:</b>	Select Disable or Enable.
<b>Pkt_Aggregate:</b>	Select Disable or Enable.
<b>IEEE802.1 H Support</b>	Select Disable or Enable.
<b>Country Code:</b>	Select the region which you are in. It provides six regions in the drop-down list.

Wi-Fi Multimedia	
WMM Capable	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
APSD Capable	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
DLS Capable	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
WMM Parameters	<input type="button" value="WMM Configuration"/>

### Wi-Fi Multimedia

Field	Description
<b>WMM Capable:</b>	Enable or disable WMM.
<b>APSD Capable:</b>	Enable or disable APSD.
<b>DLS Capable</b>	Select Disable or Enable.
<b>WMM Parameters:</b>	Click the WMM Configuration button to pop up the WMM Parameters of Access Point page. You can configure WMM parameters on the page.

Multicast-to-Unicast Converter	
Multicast-to-Unicast	<input type="radio"/> Enable <input checked="" type="radio"/> Disable

**Multicast-to-Unicast Converter:** Enable or disable Multicast-to-Unicast Converter.

After completing the settings above, click **Apply** to save the settings and make the new configuration take effect. Click **Cancel** to close without saving.

## 5.3 Security

Choose **Wireless Settings>Security** and the following page will be displayed. It allows you to modify the settings to prevent unauthorized accesses.

**Cetis**  
Scitec • Teledex • TeleMatrix

Device Info  
Wireless Setup  
Basic  
Advanced  
**Security**  
WDS  
WPS  
Station List  
Wireless Statistics  
Management

### Wireless Security/Encryption Settings

Setup the wireless security and encryption to prevent from unauthorized access and monitoring.

Select SSID	
SSID choice	WiFi ▾

"WiFi"	
Security Mode	Disable ▾

Access Policy	
Policy	Disable ▾
Add a station Mac:	<input type="text"/>

Apply Cancel

### Select SSID

**SSID choice:** Select SSID from the drop-down list.

### "default"

**Security Mode:** There are 11 options, including **Disable, OPEN, SHARED, WPAUTO, WPA, WPA-PSK, WPA2, WPA2-PSK, WPAPSKWPA2PSK, WPA1WPA2,** and **802.1X.**

### [EXAMPLE]

Take Open WEP for example. Select Open WEP from the **Security Mode** drop down-list. The following page will be displayed.

"Cetis_AP"			
Security Mode	OPENWEP ▾		
<b>Wire Equivalence Protection (WEP)</b>			
Default Key	Key 1 ▾		
WEP Keys	WEP Key 1 :	<input type="text"/>	Hex ▾
	WEP Key 2 :	<input type="text"/>	Hex ▾
	WEP Key 3 :	<input type="text"/>	Hex ▾
	WEP Key 4 :	<input type="text"/>	Hex ▾
<b>Access Policy</b>			
Policy	Disable ▾		
Add a station Mac:	<input type="text"/>		
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>			

## Cetis AP

### Security Mode:

There are 11 options, including **Disable, OPEN, SHARED, WEPAUTO, WPA, WPA-PSK, WPA2, WPA2-PSK, WPAPSKWPA2PSK, WPA1WPA2,** and **802.1X.**

### Wire Equivalence Protection (WEP)

**WEP Key (1-4):** Input the key to encrypt wireless data. To allow encrypted data transmission, the WEP Encryption Key values on all wireless stations must be the same as the router. There are four keys for your selection. The input format can either be HEX style or ASCII format, 10 and 26 HEX codes or 5 and 13 ASCII codes are required for WEP64 and WEP128 respectively.

### Access Policy

**Policy:** There are three options, including Disable, Allow, and Reject. You can choose Disable, Allow or Reject. Select Allow, only the clients whose MAC address is listed can access the router. Select Reject, the clients whose MAC address is listed are denied to access the router.

**Add a station MAC:** If you want to add a station MAC, input the MAC address of the wireless stations that are allowed or denied access to your router in this address field.

After completing the settings above, click **Apply** to save the settings and make the new configuration take effect. Click **Cancel** to close without saving.

## 5.4 WDS

### Wireless Distribution System (WDS)

**WDS Mode:** There are four options, including **Disable**, **Lazy Mode**, **Bridge Mode**, and **Repeater Mode**.

- **Disable**

Select Disable to disable the WDS mode.

- **Lazy Mode**

**Cetis**  
Scitec • Teledex • TeleMatrix

**Wireless Distribution System**  
Wireless Distribution System Settings

Wireless Distribution System(WDS)	
WDS Mode	Lazy Mode
Phy Mode	CCK
EncrypType	NONE
Encryp Key	
EncrypType	NONE
Encryp Key	
EncrypType	NONE
Encryp Key	
EncrypType	NONE
Encryp Key	

Apply Cancel

Field	Description
<b>WDS Mode:</b>	Select Lazy Mode. The EXA100WDS Lazy mode allows the other WDS bridge / repeater mode to link automatically.
<b>Phy Mode:</b>	It provides 4 options, including <b>CCK</b> , <b>OFDM</b> , <b>HTMIX</b> , and <b>GREENFIELD</b> .
<b>Encryp Type:</b>	It provides 4 options, including <b>None</b> , <b>WEP</b> , <b>TKIP</b> , and <b>AES</b> .
<b>Encryp Key:</b>	It provides 4 AP MAC Addresses. Input the MAC address of the other APs.



- **Bridge Mode/ Repeater Mode**

Wireless Distribution System(WDS)	
WDS Mode	Bridge Mode ▾
Phy Mode	CCK ▾
EncrypType	NONE ▾
Encryp Key	<input type="text"/>
EncrypType	NONE ▾
Encryp Key	<input type="text"/>
EncrypType	NONE ▾
Encryp Key	<input type="text"/>
EncrypType	NONE ▾
Encryp Key	<input type="text"/>
AP MAC Address	<input type="text"/>
AP MAC Address	<input type="text"/>
AP MAC Address	<input type="text"/>
AP MAC Address	<input type="text"/>

Field	Description
<b>WDS Mode:</b>	Select <b>Bridge</b> Mode or <b>Repeater</b> Mode.
<b>Phy Mode:</b>	It provides 4 options, including CCK, OFDM, HTMIX, and GREENFIELD.
<b>Encryp Type:</b>	It provides 4 options, including <b>None</b> , <b>WEP</b> , <b>TKIP</b> , and <b>AES</b> .
<b>AP MAC Address:</b>	It provides 4 AP MAC Addresses. Input the MAC address of the other APs.
<b>WDS (Wireless Distribution System)</b>	<p>Allows access points to communicate with one another wirelessly in a standardized way. It can also simplify the network infrastructure by reducing the amount of cabling required. Basically the access points will act as a client and an access point at the same time.</p> <p>WDS is incompatible with WPA. Both features cannot be used at the same time. A WDS link is bi-directional, so the AP must know the MAC address of the other AP, and the other AP must have a WDS link back to the AP.</p>

	<p>Dynamically assigned and rotated encryption key are not supported in a WDS connection. This means that WPA and other dynamic key assignment technologies may not be used.</p> <p>Only Static WEP keys may be used in a WDS connection, including any STAs that are associated with a WDS repeating AP.</p> <p>Input the MAC address of the other APs that you want to link to and click enable.</p> <p>Supports up to 4 point to multipoint WDS links, check Enable WDS and then enable on the MAC addresses</p>
--	---

**Example of a WDS topology:**

**AP1 <-- WDS --> Master AP (our AP) <-- WDS --> AP3 <-- WDS --> AP4**

## 5.5 WPS

You can enable or disable the WPS function on this page.



Select **Enable** from the WPS drop-down list. Click **Apply** and the following page will be displayed.

## Wi-Fi Protected Setup

You could setup security easily by choosing PIN or PBC method to do Wi-Fi Protected Setup.

WPS Config	
WPS:	Enable <input type="button" value="v"/>
<input type="button" value="Apply"/>	
WPS Summary	
WPS Current Status:	Idle
WPS Configured:	Yes
WPS SSID:	wireless
WPS Auth Mode:	Open
WPS Encryp Type:	None
WPS Default Key Index:	1
WPS Key(ASCII)	
AP PIN:	44649173 <input type="button" value="Generate"/>
<input type="button" value="Reset OOB"/>	
WPS Progress	
WPS mode	<input checked="" type="radio"/> PIN <input type="radio"/> PBC
PIN	<input type="text"/>
<input type="button" value="Apply"/>	
WPS Status	
WSC: Idle <input type="button" value="v"/>	
<input type="text"/>	
<input type="button" value="Cancel"/>	

## WPS Summary

It displays the WPS information, such as WPS Current Status, WPS Configured, and WPS SSID.

Reset OOB: Reset to out of box (OoB) configuration.

## WPS Progress

**WPS mode:** There are two ways for you to enable the WPS function: **PIN, PBC**. You can use a push button configuration (PBC) on the Wi-Fi router. If there is no button, input a 4- or 8-digit PIN code. Each STA supporting WPS comes with a hard-coded PIN code.

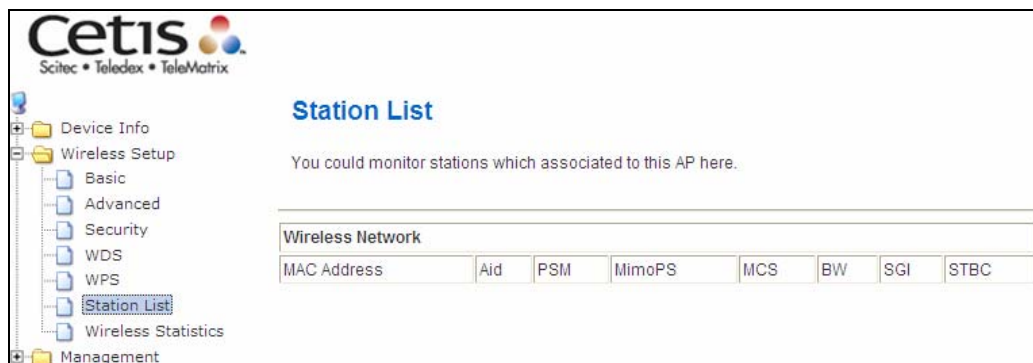
**PIN:** If you select PIN mode, you need to input the PIN number in the field.

## WPS Status

It displays the information about WPS status.

## 5.6 Station List

On this page, you can easily identify the connected wireless stations. It automatically observes the ID of the connected wireless station (if specified), MAC address, SSID, and current status.



Cetis  
Scitec • Teledex • TeleMatrix

### Station List

You could monitor stations which associated to this AP here.

Wireless Network							
MAC Address	Aid	PSM	MimoPS	MCS	BW	SGI	STBC

## 5.7 AP Wireless Statistics

This page shows the Wireless Statistics of EXA100.

**Cetus**  
Scitec • Teledex • TeleMatrix

### AP Wireless Statistics

Wireless TX and RX Statistics

Transmit Statistics	
Tx Success	13098
Tx Retry Count	16, PER=0.1%
Tx Fail after retry	1, PLR=7.6e-05
RTS Successfully Receive CTS	0
RTS Fail To Receive CTS	0

Receive Statistics	
Frames Received Successfully	263148
Frames Received With CRC Error	531256, PER=66.9%

**SNR**

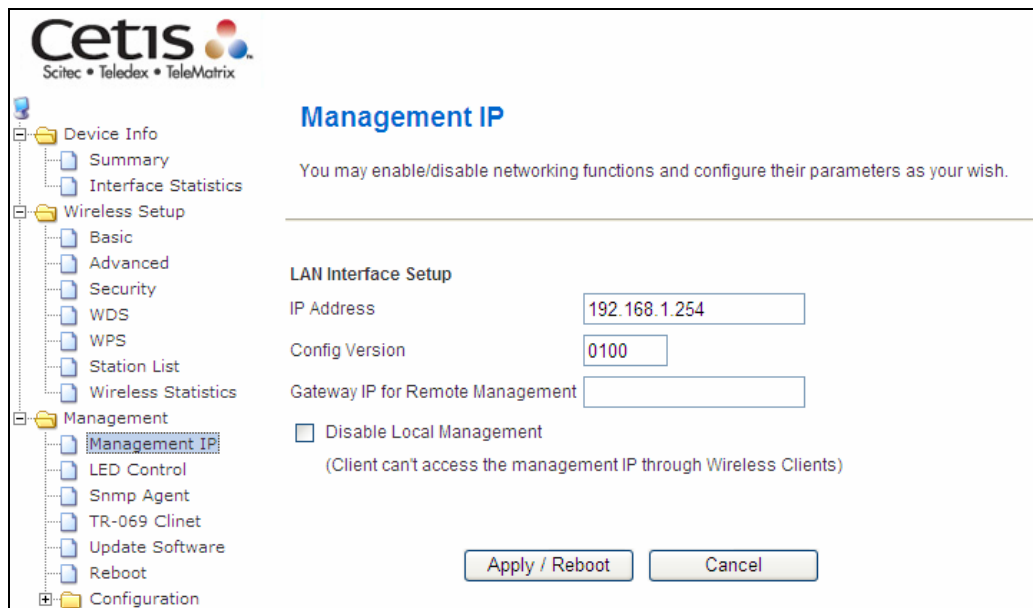
SNR	36, n/a, n/a
-----	--------------

[Reset Counters](#)

# Chapter 6 Management - Configuration Backup

To save the current configuration to a file on your PC, click **Backup Settings**. You will be prompted for backup file location. This file can later be used to recover settings on the **Update Settings** screen, as described below.

## 6.1 Management IP



### IP Address:

Web LAN IP address for management.

### Config Version:

Shows the current configuration version. The EXA100 can update the configuration automatically via TFTP server.

### Gateway IP for remote management:

### Disable Local management:

When disable the local management (ticking the checkbox ) , user can not access web page via Wireless.

## 6.2 LED Control

The screenshot shows the Cetis web interface. At the top left is the Cetis logo with the text "Scitec • Teledex • TeleMatrix". On the left is a navigation tree with folders for "Device Info", "Wireless Setup", and "Management". The "LED Control" option under "Management" is selected. The main content area is titled "LED Behavior" and contains the instruction "Turn ON/ OFF for Power and WiFi Link LED." Below this, there are two settings: "Power Led" and "Wireless Link Led", each with a dropdown menu currently set to "Disable". An "Apply" button is located below these settings.

Select Disable or Enable from the drop-down menu and click the **Apply** button.



## 6.3 SNMP Agent

Simple Network Management Protocol (SNMP) allows a management application to retrieve statistics and status from the SNMP agent in this device. Select **Enable** from the drop-down menu, configure options, and click **Apply** to activate SNMP.

**Cetis**  
SciTec • Teledex • TeleMatrix

**SNMP Settings**

Simple Network Management Protocol (SNMP) allows a management application to retrieve statistics and status from the SNMP agent in this device.

SNMP Settings	
SNMP Settings	Enable ▾
Read Community	public
Set Community	private
System Name	wireless
System Location	unknown
System Contact	unknown
Trap Manager IP	

Apply Reset

## 6.4 TR-069 Client

WAN Management Protocol (TR-069) allows an Auto-Configuration Server (ACS) to perform auto-configuration, provision, collection, and diagnostics to this device. Select desired values and click **Apply/Save** to configure TR-069 client options.

The table below is provided for ease of reference.

Field	Description
TR-069 Settings	Select <b>Enable/Disable</b> from the drop-down menu.
ACS URL	URL for the WiFi AP to connect to the ACS using the WiFi AP WAN Management Protocol. This parameter MUST be in the form of a valid HTTP or HTTPS URL. An HTTPS URL indicates that the ACS supports SSL. The “host” portion of this URL is used by the WiFi AP for validating the certificate from the ACS when using certificate-based authentication.
ACS User Name	Username used to authenticate the WiFi AP when making a connection to the ACS using the WiFi AP WAN Management Protocol. This username is used only for HTTP-based authentication of the WiFi AP.

<b>Field</b>	<b>Description</b>
ACS Password	Password used to authenticate the WIFI AP when making a connection to the ACS using the WIFI AP WAN Management Protocol. This password is used only for HTTP-based authentication of the WIFI AP.
Inform Interval	The duration in seconds of the interval for which the WIFI AP MUST attempt to connect with the ACS and call the Inform method.

## 6.5 Update Software

This option allows for firmware upgrades from a locally stored file.

**Cetis**  
Scitec • Teledex • TeleMatrix

**Update Software**

**Step 1:** Obtain an updated software image file from your ISP.  
**Step 2:** Enter the path to the image file location in the box below or click the 'Browse' button to locate the image file.  
**Step 3:** Click the 'Update Software' button once to upload the new image file.

NOTE: The update process takes about 2 minutes to complete, and your WiFi AP will reboot.

**Update Firmware**  
Location:

**Update Bootloader**  
Location:

### Update Firmware

- STEP 1:** Obtain an updated software image file from your ISP.
- STEP 2:** Enter the path and filename of the firmware image file in the **Software File Name** field or click the Browse button to locate the image file.
- STEP 3:** Click the **Update Software** button once to upload and install the file.

**NOTE:** The update process will take about 2 minutes to complete. The device will reboot and the browser window will refresh to the default screen upon successful installation. It is recommended that you compare the **Software Version** on the

[Chapter 4](#) Device Information screen with the firmware version installed, to confirm the installation was successful.

## 6.6 Reboot

To save the current configuration and reboot the router, click **Save/Reboot**.

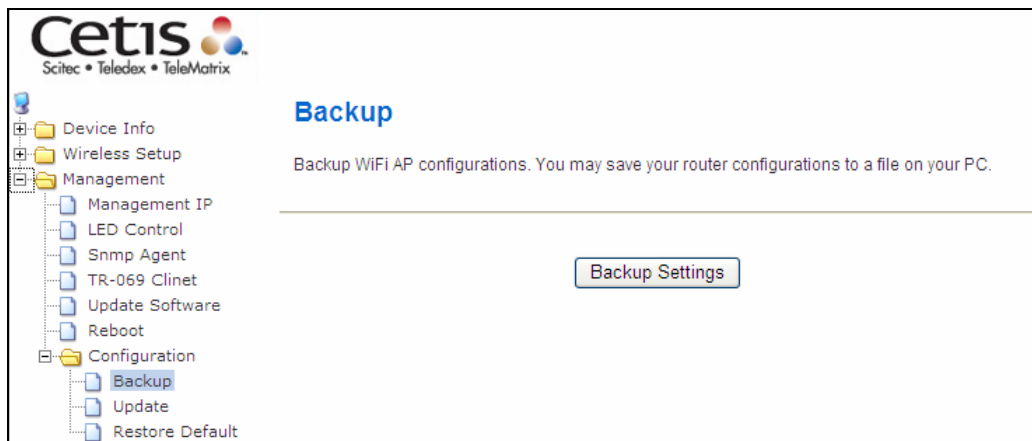


**NOTE:** You may need to close the browser window and wait for 2 minutes before reopening it. It may also be necessary, to reset your PC IP configuration.

## 6.7 Configuration

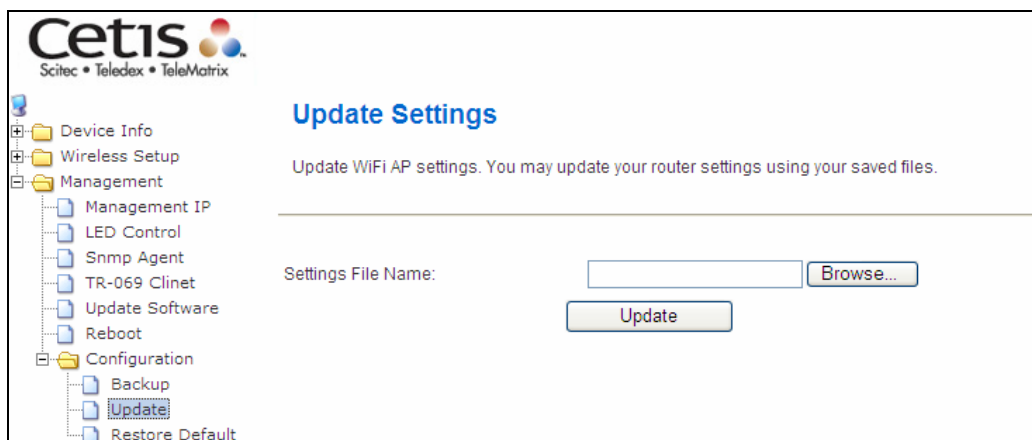
### 6.7.1 Backup Settings

To save the current configuration to a file on your PC, click **Backup Settings**. You will be prompted for backup file location. This file can later be used to recover settings on the **Update Settings** screen, as described below.



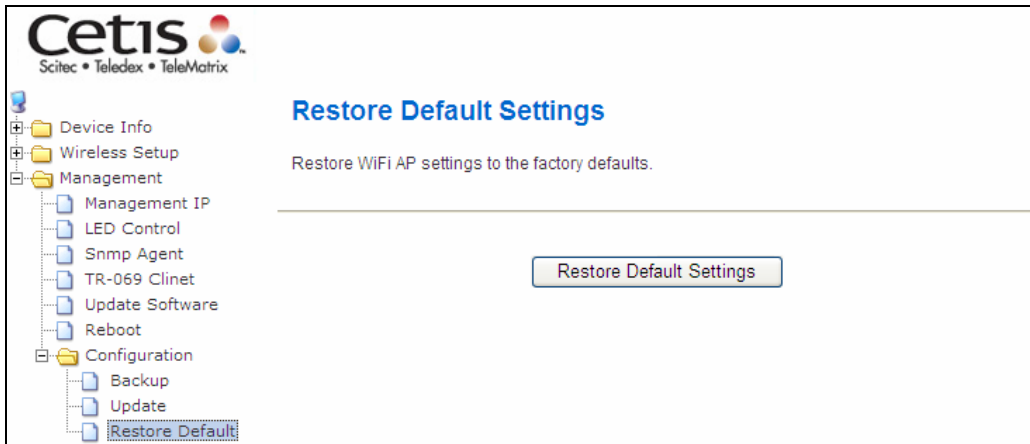
### 6.7.2 Update Settings

This option recovers configuration files previously saved using **Backup Settings**. Enter the file name (including folder path) in the **Settings File Name** box, or press **Browse...** to search for the file, then click **Update Settings** to recover settings.



### 6.7.3 Restore Default

Click **Restore Default Settings** to restore factory default settings.



After **Restore Default Settings** is clicked, close the browser and wait for 2 minutes before reopening it. It may also be necessary, to reconfigure your PC IP configuration to match any new settings.

**NOTE:** This entry has the same effect as the **Reset** button. The EXA100 board hardware and the boot loader support the reset to default. If the **Reset** button is continuously pressed for more than 5 seconds, the boot loader will erase the configuration data saved in flash memory.

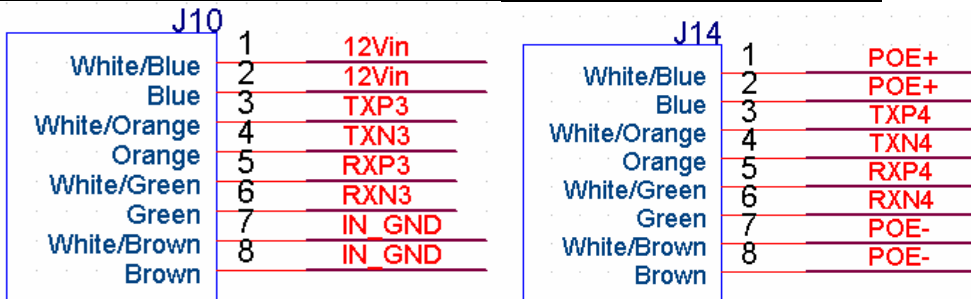


# Appendix A - Pin Assignments

## ETHERNET Ports (RJ45)

### ETHERNET LAN Ports (10/100Base-T)

Connection #	PIN #	Descriptions
J10	1	+12Vdc Input
	2	+12Vdc Input
	3	Ethernet TX (+)/LAN1
	4	Ethernet TX (-)/LAN1
	5	Ethernet RX (+)/LAN1
	6	Ethernet RX (-)/LAN1
	7	Ground
	8	Ground
J14	1	PoE (+) Input
	2	PoE (+) Input
	3	Ethernet TX (+)/LAN2
	4	Ethernet TX (-)/LAN2
	5	Ethernet RX (+)/LAN2
	6	Ethernet RX (-)/LAN2
	7	PoE (-) Input
	8	PoE (-) Input



# Appendix B – Specifications

## Hardware Interface

- Power Jack X 1,
- Two Punch IDC connectors
- Reset button X 1,
- Active LED X 2,
- Antenna internal

## LAN Interface

- IEEE 802.3, IEEE 802.3u

## ADSL

- ADSL standard ITU-T G.992.5, ITU-T G.992.3, ITU-T G.992.1, ANSI T1.413 Issue 2,
- G.992.5 (ADSL2+):
- G.992.3 (ADSL2):
- G.DMT

## WLAN

- IEEE 802.11n, backward compatible with 802.11g/b
- 64, 128-bit Wired Equivalent Privacy (WEP) Data Encryption
- 11 Channels (US, Canada)/ 13 Channels (Europe)/ 14 Channels (Japan)
- Up to 300 Mbps data rate
- WPA / WPA2
- IEEE 802.1x
- RF operating frequency: 2.412-2.497 GHz (2.4 GHz ISM Band)
- ddRF output power: 15dBm
- Antenna gain: 2dBi

## Bridge Functions

- IEEE 802.1d
- VLAN support
- Spanning Tree Algorithm
- IGMP Proxy

## Management

- SNMP, Telnet, Web-based management, Configuration backup and restoration
- RFC1213 Management information base for Network management of TCP/IP-based internets : MIB-II
- Software upgrade via HTTP

## Power Supply

- Input: 100 - 240 Vac
- Vac/ 50-60Hz
- Output: 12 Vdc / 1 A

## Certifications

- EN 55022 + EN55024
- EN 300328
- EN 301489-1 / -17
- EN 60950-1
- Power Saving
- WEEE
- RoHS
- REACH

## Packing Accessories:

- Module x 3
- Quarter Blank spec x 2
- KeyStone Jack x 1
- Connector Switch x 1
- QIG for troubleshooting
- Water-proof sealed PE bag (for ATU-R&QIG) x 1

<b>NOTE:</b> Specifications are subject to change without notice
--

## Appendix C –Parameter Rules

	Setting parameters in Web GUI	Settings parameters in Config file	value	default	
Basic Wireless Setting	Radio On/Off	RadioOff= <b>0</b>	0: disable 1: enable	0	
	Network Name(SSID)	SSID1= <b>wireless</b>		wireless	
	Multiple SSID1	SSID2=		blank	
	Multiple SSID2	SSID3=		blank	
	Multiple SSID3	SSID4=		blank	
	Multiple SSID4	SSID5=		blank	
	Hidden	HideSSID=	(SSID1;SSID2;SSID3;SSID4;SSID5) 0: disable 1: enable(hide)	0;1;1;1;1	
	Isolated	NoForwarding=	(SSID1;SSID2;SSID3;SSID4;SSID5) 0: disable 1: enable	1;0;0;0;0	
	Frequency (Channel)	Channel= <b>0</b> AutoChannelSelect= <b>1</b>			
	Network Mode-11b/g mixed mode	WirelessMode= <b>0</b> FixedTxMode= <b>OFDM</b>		0	
	Network Mode-11b only	WirelessMode= <b>1</b> FixedTxMode= <b>CCK</b>		1	
	Network Mode-11g only	WirelessMode= <b>4</b> FixedTxMode= <b>OFDM</b>		4	
	Network Mode-11b/g/n mixed mode	WirelessMode= <b>9</b> FixedTxMode= <b>HT</b>		9	
		Operating Mode	HT_OpMode= <b>0</b>	0: Mixed Mode 1: Green Field	0
		Channel BandWidth	HT_BW= <b>1</b>	0: 20 1: 20/40	1
		Guard Interval	HT_GI= <b>1</b>	0: long 1: Auto	1
		MCS	HT_MCS= <b>33</b>	(SSID1;SSID2;SSID3;SSID4;SSID5) from: 1-15 and 32 33: Auto	33
		Reverse Direction Grant(RDG)	HT_RDG= <b>1</b>	0: disable 1: enable	1
		STBC	HT_STBC= <b>1</b>		1
		Aggregation MSDU(A-MSDU)	HT_AMSDU= <b>0</b>		0
		Auto Block ACK	HT_AutoBA= <b>1</b>		1
	Decline BA Request	HT_BADecline= <b>0</b>	0		
	HT Disallow TKIP	HT_DisallowTKIP= <b>1</b>	1		

	Network Mode-11n only(2.4G)		WirelessMode=6		6
	Operating Mode	HT_OpMode=0	0: Mixed Mode 1: Green Field		0
	Channel BandWidth	HT_BW=1	0: 20 1: 20/40		1
	Guard Interval	HT_GI=1	0: long 1: Auto		1
	MCS	HT_MCS=33	(SSID1;SSID2;SSID3;SSID4;SSID5) from: 1-15 and 32 33: Auto		33
	Reverse Direction Grant(RDG)	HT_RDG=1	0: disable 1: enable		1
	STBC	HT_STBC=1			1
	Aggregation MSDU(A-MSDU)	HT_AMSDU=0			0
	Auto Block ACK	HT_AutoBA=1			1
	Decline BA Request	HT_BADecline=0			0
	HT Disallow TKIP	HT_DisallowTKIP=1			1
	HT TxStream	HT_TxStream=2		from: 1-2	
	HT RxStream	HT_RxStream=2	from: 1-2		2
Advanced Wireless Settings	BG Protection Mode	BGProtection=0	0: Auto 1: On 2: Off		0
	Beacon Interval	BeaconPeriod=100	range 20 - 999		100
	Data Beacon Rate (DTIM)	DtimPeriod=1	range 1 - 255		1
	Fragment Threshold	FragThreshold=2346	range 256 - 2346		2346
	RTS Threshold	RTSThreshold=2347	range 1 - 2347		2347
	TX Power	TxPower=100	range 1		100
	Short Preamble	TxPreamble=1	0: disable 1: enable		1
	Short Slot	ShortSlot=1			1
	Tx Burst	TxBurst=1			1
	Pkt_Aggregate	PktAggregate=1			1
IEEE 802.11H Support	IEEE80211H=0			0	

Country Code		CountryRegion=0 CountryRegionABand=7 CountryCode=US	US: CountryRegion=0 CountryRegionABand=7 CountryCode=US JP: CountryRegion=5 CountryRegionABand=6 CountryCode=JP FR: CountryRegion=1 CountryRegionABand=2 CountryCode=FR TW: CountryRegion=0 CountryRegionABand=8 CountryCode=TW IE: CountryRegion=1 CountryRegionABand=1 CountryCode=IE HK: CountryRegion=1 CountryRegionABand=0 CountryCode=HK NONE: CountryRegion=5 CountryRegionABand=7 CountryCode=	US
WMM Capable		WmmCapable=1		1
	APSD Capable	APSDCapable=0	0: disable 1: enable	0
	DLS Capable	DLSCapable=0		0
Multicast-to-Unicast		M2UEnabled=0		0
Security Mode-Disable		AuthMode=OPEN EncrypType=NONE		
Security Mode-OPENWEP		AuthMode=OPEN EncrypType=WEP		
	Default Key	DefaultKeyID=1	(SSID1;SSID2;SSID3;SSID4;SSID5) from: 1-4	1,1,1,1,1
	WEP Key 1	Key1Str1= Key1Type=0	(SSID1;SSID2;SSID3;SSID4;SSID5) keyType: 0 - 1 0: Hex 1: ASCII	KeyStr1=blank KeyType=0
	WEP Key 2	Key2Str1= Key2Type=0		
	WEP Key 3	Key3Str1= Key3Type=0		
	WEP Key 4	Key4Str1= Key4Type=0		
Security Mode-SHAREDWEP		AuthMode=SHARED EncrypType=WEP		
	Default Key	DefaultKeyID=1	(SSID1;SSID2;SSID3;SSID4;SSID5) from: 1-4	1,1,1,1,1
	WEP Key 1	Key1Str1= Key1Type=0	(SSID1;SSID2;SSID3;SSID4;SSID5) keyType: 0 - 1	KeyStr1=blank

	WEP Key 2	Key2Str1= Key2Type=0	0: Hex 1: ASCII	KeyType=0
	WEP Key 3	Key3Str1= Key3Type=0		
	WEP Key 4	Key4Str1= Key4Type=0		
Security Mode-WEPAUTO		AuthMode=WEPAUTO EncrypType=WEP		
	Default Key	DefaultKeyID=1	(SSID1;SSID2;SSID3;SSID4;SSID5) from: 1-4	1,1,1,1,1
	WEP Key 1	Key1Str1= Key1Type=0		
	WEP Key 2	Key2Str1= Key2Type=0	(SSID1;SSID2;SSID3;SSID4;SSID5) keyType: 0 - 1	KeyStr1=blank KeyType=0,0,0,0,0
	WEP Key 3	Key3Str1= Key3Type=0	0: Hex 1: ASCII	
	WEP Key 4	Key4Str1= Key4Type=0		
Security Mode-WPA		AuthMode=WPA		
	WPA Algorithms	EncrypType=	(SSID1;SSID2;SSID3;SSID4;SSID5) TKIP or AES	
	Key Renewal Interval	RekeyInterval=3600	(SSID1;SSID2;SSID3;SSID4;SSID5) 0 - 4194303	3600
	IP Address	RADIUS_Server=		blank
	Port	RADIUS_Port=1812	(SSID1;SSID2;SSID3;SSID4;SSID5)	1812
	Shared Secret	RADIUS_Key1= RADIUS_Key2= RADIUS_Key3= RADIUS_Key4= RADIUS_Key5=		
	Session Timeout	session_timeout_interval=0	(SSID1;SSID2;SSID3;SSID4;SSID5)	0
Security Mode-WPA-PSK		AuthMode=WPAPSK		
	WPA Algorithms	EncrypType=	(SSID1;SSID2;SSID3;SSID4;SSID5) TKIP or AES	
	Pass Phrase	WPAPSK1= WPAPSK2= WPAPSK3= WPAPSK4= WPAPSK5=		
	Key Renewal Interval	RekeyInterval=3600	(SSID1;SSID2;SSID3;SSID4;SSID5) 0 - 4194303	3600
Security Mode-WPA2		AuthMode=WPA2		
	WPA Algorithms	EncrypType=	(SSID1;SSID2;SSID3;SSID4;SSID5) TKIP or AES	
	Key Renewal Interval	RekeyInterval=3600	(SSID1;SSID2;SSID3;SSID4;SSID5) 0 - 4194303	3600

	PMK Cache Period	PMKCachePeriod=10		10
	Pre-Authentication	PreAuth=0		0
	IP Address	RADIUS_Server=	(SSID1;SSID2;SSID3;SSID4;SSID5)	blank
	Port	RADIUS_Port=1812	(SSID1;SSID2;SSID3;SSID4;SSID5)	1812
	Shared Secret	RADIUS_Key1= RADIUS_Key2= RADIUS_Key3= RADIUS_Key4= RADIUS_Key5=		blank
	Session Timeout	session_timeout_interval=0	(SSID1;SSID2;SSID3;SSID4;SSID5)	0
Security Mode-WPA2-PSK		AuthMode=WPA2PSK		
	WPA Algorithms	EncrypType=	(SSID1;SSID2;SSID3;SSID4;SSID5) TKIP or AES	
	Pass Phrase	WPAPSK1= WPAPSK2= WPAPSK3= WPAPSK4= WPAPSK5=		
	Key Renewal Interval	RekeyInterval=3600	(SSID1;SSID2;SSID3;SSID4;SSID5) 0 - 4194303	3600
Security Mode-WPAPSKWPA2PSK		AuthMode=WPAPSKWPA2PSK		
	WPA Algorithms	EncrypType=	(SSID1;SSID2;SSID3;SSID4;SSID5) TKIP or AES	
	Pass Phrase	WPAPSK1= WPAPSK2= WPAPSK3= WPAPSK4= WPAPSK5=		
	Key Renewal Interval	RekeyInterval=3600	(SSID1;SSID2;SSID3;SSID4;SSID5) 0 - 4194303	3600
Security Mode-WPA1WPA2		AuthMode=WPA1WPA2		
	WPA Algorithms	EncrypType=	(SSID1;SSID2;SSID3;SSID4;SSID5) TKIP or AES	blank
	Key Renewal Interval	RekeyInterval=3600	(SSID1;SSID2;SSID3;SSID4;SSID5) 0 - 4194303	3600
	IP Address	RADIUS_Server=	(SSID1;SSID2;SSID3;SSID4;SSID5)	blank
	Port	RADIUS_Port=1812	(SSID1;SSID2;SSID3;SSID4;SSID5)	1812
	Shared Secret	RADIUS_Key1= RADIUS_Key2= RADIUS_Key3= RADIUS_Key4= RADIUS_Key5=		blank
	Session Timeout	session_timeout_interval=0	(SSID1;SSID2;SSID3;SSID4;SSID5)	0



	Security Mode-802.1x		AuthMode= <b>OPEN</b> EncrypType= <b>WEP</b>		
		802.1x WEP	IEEE8021X=		blank
		IP Address	RADIUS_Server=	(SSID1;SSID2;SSID3;SSID4;SSID5)	blank
		Port	RADIUS_Port= <b>1812</b>	(SSID1;SSID2;SSID3;SSID4;SSID5)	1812
		Shared Secret	RADIUS_Key1= RADIUS_Key2= RADIUS_Key3= RADIUS_Key4= RADIUS_Key5=		blank
		Session Timeout	session_timeout_interval= <b>0</b>	(SSID1;SSID2;SSID3;SSID4;SSID5)	0
	Policy		AccessPolicy0= <b>0</b>	0: Disable 1: Allow 2: Reject	0
	Add a station Mac		AccessControlList0=		blank
Wireless Distribution System	WDS Mode-Disable		WdsEnable= <b>0</b>		0
	WDS Mode-Lazy Mode		WdsEnable= <b>4</b>		4
		Phy Mode	WdsPhyMode=	CCK;CCK;CCK;CCK OFDM;OFDM;OFDM;OFDM HTMIX;HTMIX;HTMIX;HTMIX GREENFIELD;GREENFIELD;GREENFIELD; GREENFIELD	CCK;CCK;CCK; CCK
		EncrypType	WdsEncrypType=	(SSID1;SSID2;SSID3;SSID4;SSID5) NONE · WEP · TKIP · AES	NONE
		Encryp Key	Wds0Key= Wds1Key= Wds2Key= Wds3Key=		blank
	WDS Mode-Bridge Mode		WdsEnable= <b>2</b>		2
		Phy Mode	WdsPhyMode=	CCK;CCK;CCK;CCK OFDM;OFDM;OFDM;OFDM HTMIX;HTMIX;HTMIX;HTMIX GREENFIELD;GREENFIELD;GREENFIELD; GREENFIELD	CCK;CCK;CCK; CCK
		EncrypType	WdsEncrypType=	(SSID1;SSID2;SSID3;SSID4;SSID5) NONE · WEP · TKIP · AES	NONE
		Encryp Key	Wds0Key= Wds1Key= Wds2Key= Wds3Key=		blank
		AP MAC Address	WdsList=		blank
	WDS Mode-Repeater Mode		WdsEnable= <b>3</b>		3
	Phy Mode	WdsPhyMode=	CCK;CCK;CCK;CCK OFDM;OFDM;OFDM;OFDM HTMIX;HTMIX;HTMIX;HTMIX GREENFIELD;GREENFIELD;GREENFIELD; GREENFIELD	CCK;CCK;CCK; CCK	

		EncrypType	WdsEncrypType=	(SSID1;SSID2;SSID3;SSID4;SSID5) NONE · WEP · TKIP · AES	NONE
		Encryp Key	Wds0Key= Wds1Key= Wds2Key= Wds3Key=		blank
		AP MAC Address	WdsList=		blank
Wi-Fi Protected Setup	WPS		WscModeOption=7	default is 7 7=enable 0=disable	7

Setting parameters	Web GUI	Config file	value	default
Management IP	IP Address	lan_ipaddr=192.168.1.254		192.168.1.254
	Gateway IP for Remote Management	lan_gateway=0.0.0.0		0.0.0.0
	Disable Local Management	lan_filter=0	0: disable 1: enable	0
	Config Version	ConfigVersion=0100		0100
LED Behavior	Power Led	PwrLedEnabled=0	0: disable 1: enable	0
	Wireless Link Led	WlanLinkLedEnabled=0		0
SNMP Settings	SNMP Settings	SNMPEnabled=1	0: disable 1: enable	1
	Read Community	SNMPREADCOMM=public		public
	Set Community	SNMPWRITECOMM=private		private
	System Name	SNMPpsysname=wireless		wireless
	System Location	SNMPpsyslocation=unknown		unknown
	System Contact	SNMPpsyscontact=unknown		unknown
	Trap Manager IP	SNMPtrap=0.0.0.0		0.0.0.0
TR-069 Client	TR-069 Settings	TR69Enabled=0	0: disable 1: enable	0
	ACS URL	TR69ACUrl=		blank
	ACS Username	TR69Username=		blank
	ACS Password	TR69Password=		blank
	Inform Interval	TR69InformInterval=		blank

### **FCC Interference Statement**

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

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

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

1. This device may not cause harmful interference
2. This device must accept any interference received, including interference that may cause undesired operation.

### **FCC Radiation Exposure Statement**

To comply with the FCC RF exposure compliance requirements, this device and its antenna must not be co-located or operating to conjunction with any other antenna or transmitter.

This equipment should be installed and operated with minimum distance 20cmbetween the radiator & your body

<p><b>FCC Caution:</b> The changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.</p>
--