TELEDEX®

Y SERIES EXA100

USER GUIDE

Wireless AP Router

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 compatible.
- 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 the manual's instruction for wiring, which should comply with article 725 and article 300 in the 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

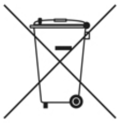
- Disconnect the power line from the device before servicing.
- Power supply specifications are clearly stated in Appendix B—Specifications.

COPYRIGHT

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

NOTE: 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 center 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

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

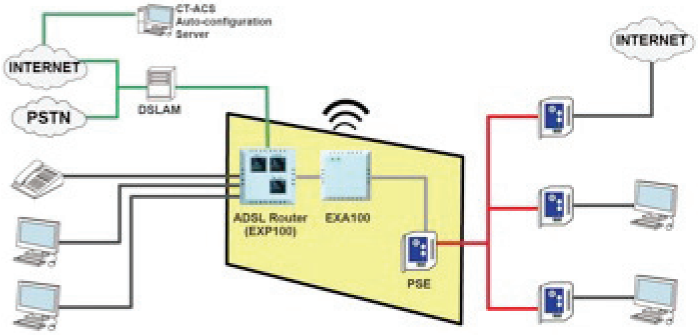
The EXA100 is customized for hotel or business environment applications. Its power can be supplied by DC-Jack or punch connector from Power over Ethernet Device and ADSL Router (EXP100). Hence it can provide several kinds of application methods to combine the wireless easily. It also provides state of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

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/PoE power in)

1.2 Application

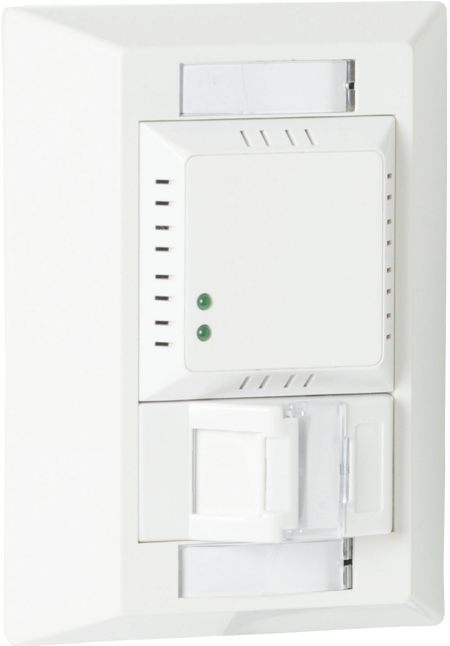
The following diagram depicts typical applications of the EXA100.



Chapter 2 Installation

2.1 Front Panel

The figure below shows the front panel of the device.

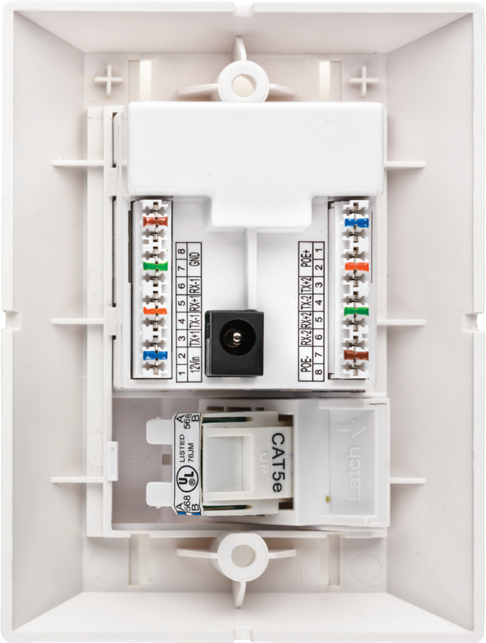


2.2 LED Status

LED	Status	Descriptions
Power	Solid OFF	System is powered 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 or CLI
	Solid ON	Wi-Fi is operational
	Flashing	Data transmission through Wi-Fi

2.3 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.

2.4 Reset Button

Restore the default parameters of the device by pressing the Reset button for ten seconds while the unit is powered.

Chapter 3 Web User Interface

This section describes how to access the device via the web user interface (WUI) using an Internet browser.

3.1 Default Settings

The factory default settings of this device are summarized below.

- LAN IP address: DHCP (no fixed default address)
- DHCP IP address is discoverable via your DHCP client logs or via the Administration server
- Administrative access (username: **root,** password: **12345**)

3.1.1 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 ten seconds until the power indicates LED blinking or by clicking the Restore Default Configuration option in the Restore Settings screen.

Using this mode you are able to connect to the WAPs wireless signal then simply log into the default STATIC IP to manage it's settings.

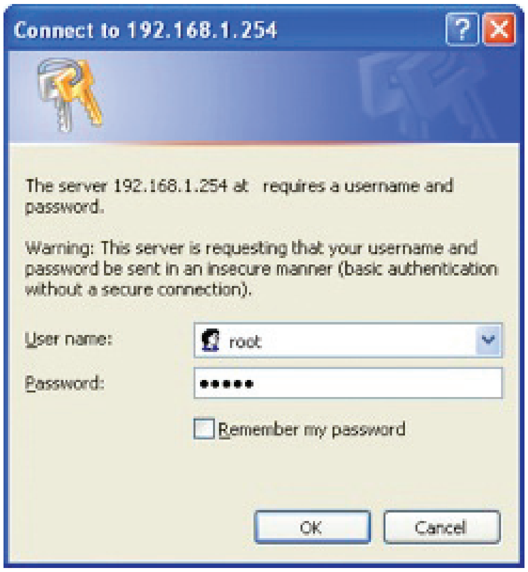
3.2 DHCP Login Procedure

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

STEP 1: Log onto the WAP's WiFi SSID then start the Internet browser and enter the DHCP awarded IP address in the Web address field. For example, if the DHCP awarded 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 LAN port of the device and not the WAN port, 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.



Connect to 192.168.1.254

The server 192.168.1.254 at requires a username and password.

Warning: This server is requesting that your username and password be sent in an insecure manner (basic authentication without a secure connection).

User name: root

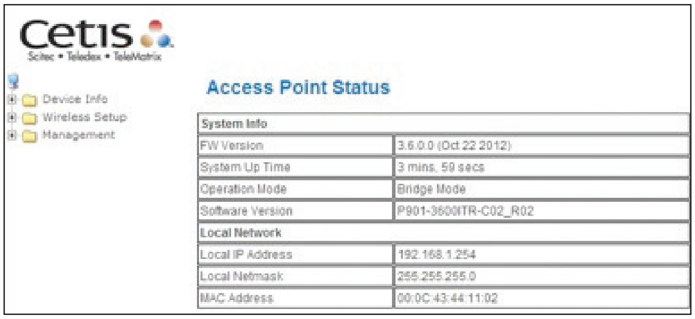
Password: •••••

☐ Remember my password

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

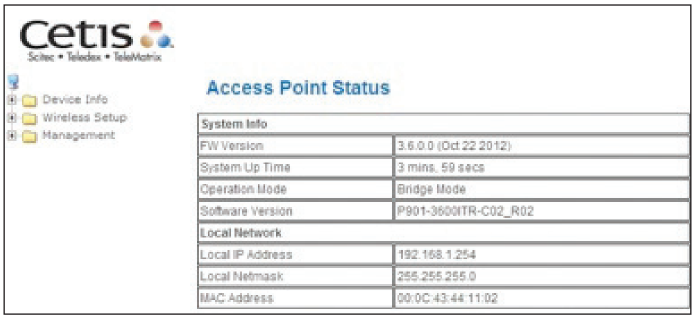
Chapter 4 Device Information

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.

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 display at startup.



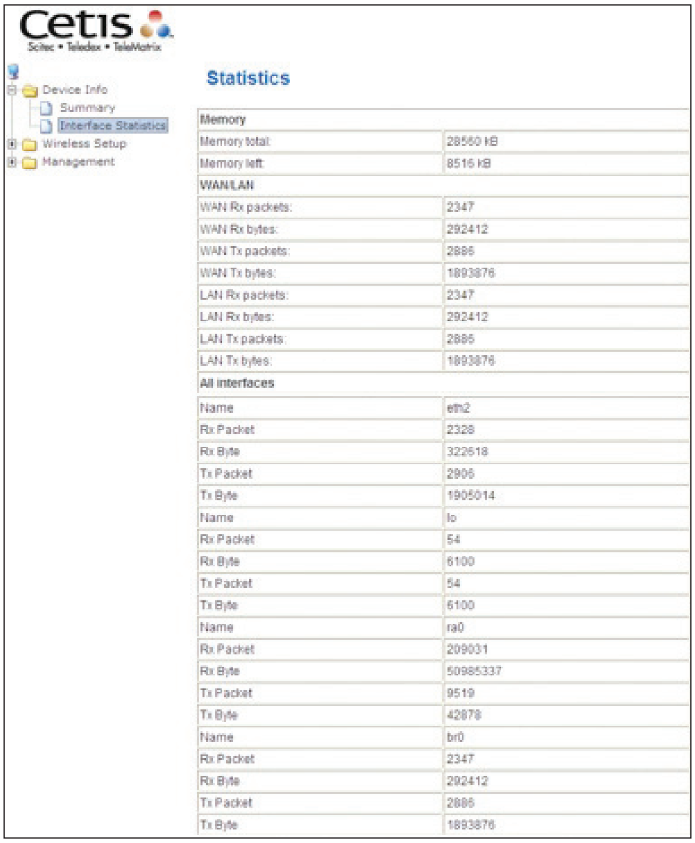
Access Point Status

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.



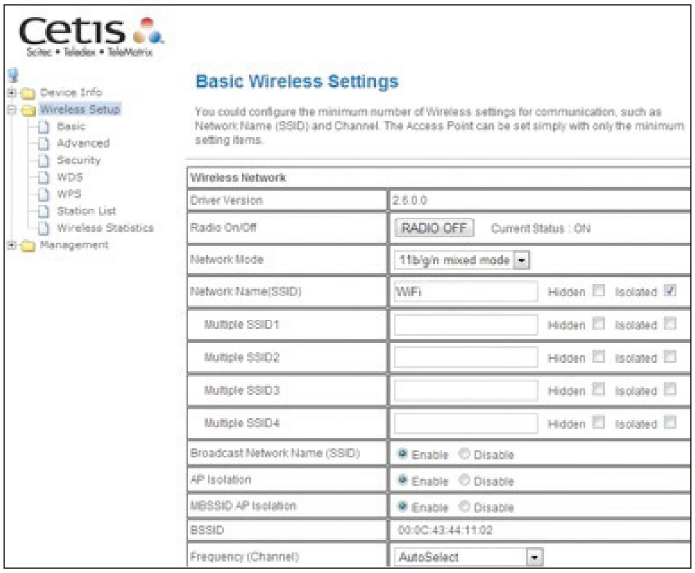
Statistics

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.



Basic Wireless Settings

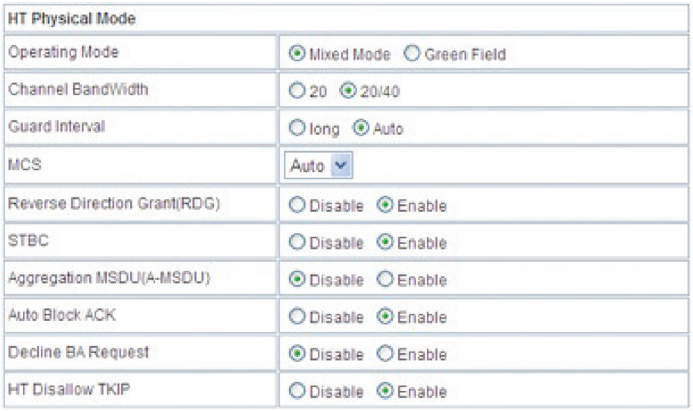
You could configure the minimum number of Wireless settings for communication, such as Network Name (SSID) and Channel. The Access Point can be set simply with only the minimum setting items.

Wireless Network	
Driver Version	2.6.0.0
Radio On/Off	RADIO OFF Current Status : ON
Network Mode	11b/g/n mixed mode
Network Name(SSID)	WiFi Hidden □ Isolated ☑
Multiple SSID1	Hidden □ Isolated □
Multiple SSID2	Hidden □ Isolated □
Multiple SSID3	Hidden □ Isolated □
Multiple SSID4	Hidden □ Isolated □
Broadcast Network Name (SSID)	● Enable ○ Disable
AP Isolation	● Enable ○ Disable
MBSSID AP Isolation	● Enable ○ Disable
BSSID	00:0C:43:44:11:02
Frequency (Channel)	AutoSelect

5.1.1 WIRELESS NETWORK

Field	Description
Driver Version	Displays the version of the driver.
Radio On/ Off	Enable or disable the wireless LAN.
Network Mode	There are 5 modes: 11b only, 11g only,11n only,11b/g mixed mode, and 11b/g/n mixed mode.
Network Name (SSID)	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.
Multiple SSID 0/1/2/3/4	This router supports multiple SSIDs called Guest SSIDs or Virtual Access Points.
Broadcast Network Name (SSID)	Select Enable to globally allow the SSID broadcast on the network, so that the STA can find it. Otherwise, the STA cannot find it. Each SSID can also have their SSID individually modified by clicking the "Hidden" check box beside the SSID.
AP Isolation	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.
MBSSID AP Isolation	Enable or disable MBSSID AP Isolation. This function will allow/disallow packets to cross between different SSIDs.
BSSID	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.
Frequency (Channel)	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.

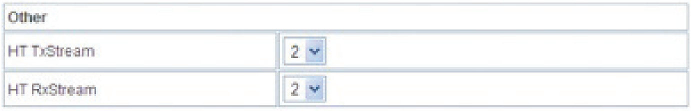
5.1.2 HT PHYSICAL MODE



HT Physical Mode	
Operating Mode	● Mixed Mode ○ Green Field
Channel BandWidth	○ 20 ● 20/40
Guard Interval	○ long ● Auto
MCS	Auto
Reverse Direction Grant(RDG)	○ Disable ● Enable
STBC	○ Disable ● Enable
Aggregation MSDU(A-MSDU)	● Disable ○ Enable
Auto Block ACK	○ Disable ● Enable
Decline BA Request	● Disable ○ Enable
HT Disallow TKIP	○ Disable ● Enable

Field	Description
Operating Mode	Two modes: Mixed Mode and Green Field. Default is Mixed Mode.
Channel BandWidth	Set the channel bandwidth of wireless radio 20 MHz and 20/40 MHz. Default is 20/40 MHz.
Guard Interval	Guard Interval is used to avoid distinct transmissions affecting each another. Choose from Long Guard and Auto. Default is Auto.
MCS	Modulation and Coding Scheme Range From 1 to 15, 32, and Auto. Default is Auto.
Reverse Direction Grant(RDG)	Enable or disable Reverse Direction Grant (RDG). Default is Enable.
STBC	Enable or disable STBC. Default is Enable.
Aggregation MSDU(A-MSDU)	Enable or disable Aggregation MSDU(A-MSDU). Default is Disable.
Auto Block ACK	Enable or disable Auto Block ACK. Default is Enable.
Decline BA Request	Enable or disable Decline BA Request. Default is Disable.
HT Disallow TKIP	Enable or disable HT Disallow TKIP. Default is Enable.

5.1.3 OTHER

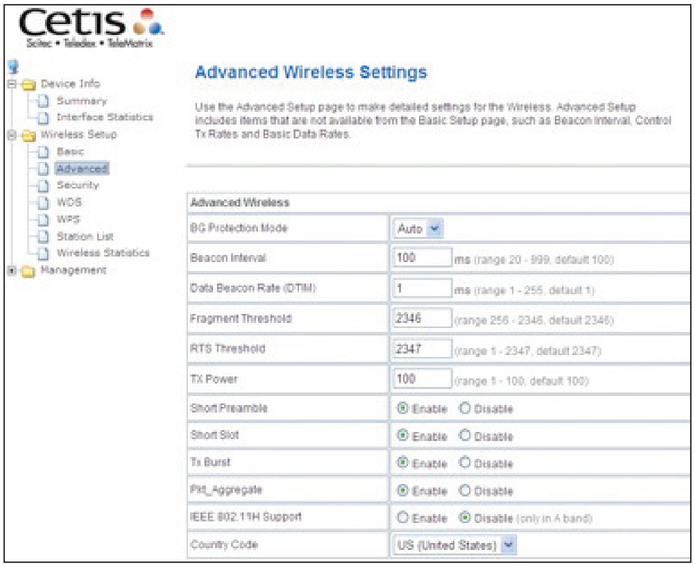


Other	
HT TxStream	2
HT RxStream	2

Field	Description
HT TxStream	Stream numbers transmits.
HT RxStream	Stream numbers receives.

5.2 Advanced

Use this page to edit 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.



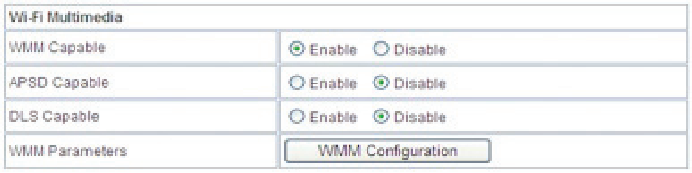
Advanced Wireless Settings

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	● Enable ○ Disable
Short Slot	● Enable ○ Disable
Tx Burst	● Enable ○ Disable
Pkt_Aggregate	● Enable ○ Disable
IEEE 802.11H Support	○ Enable ● Disable (only in A band)
Country Code	US (United States)

5.2.1 ADVANCED WIRELESS

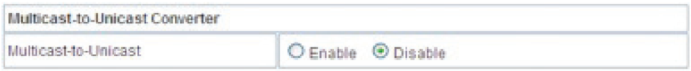
Field	Description
BG Protection Mode	It provides 3 options, including Auto, On, and Off. The default BG protection mode is **Auto.**
Beacon Interval	The interval time range is between 20 ms and 999 ms for each beacon transmission. The default value is 100 ms.
Date Beacon Rate (DTM)	The DTM range is between 1 ms and 255 ms. The default value is 1 ms.
Fragment Threshold	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.
RTS Threshold	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.
Tx Power	The Tx Power range is between 1 and 100. The default value is 100.
Short Preamble	Select Disable or Enable.
Short Slot	Select Disable or Enable.
Tx Burst	Select Disable or Enable.
Pkt_Aggregate	Select Disable or Enable.
IEEE802.1 H Support	Select Disable or Enable.
Country Code	Select the region which you are in. It provides six regions in the drop-down list.



Wi-Fi Multimedia	
WMM Capable	● Enable ○ Disable
APSD Capable	○ Enable ● Disable
DLS Capable	○ Enable ● Disable
WMM Parameters	WMM Configuration

5.2.2 WIFI MULTIMEDIA

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



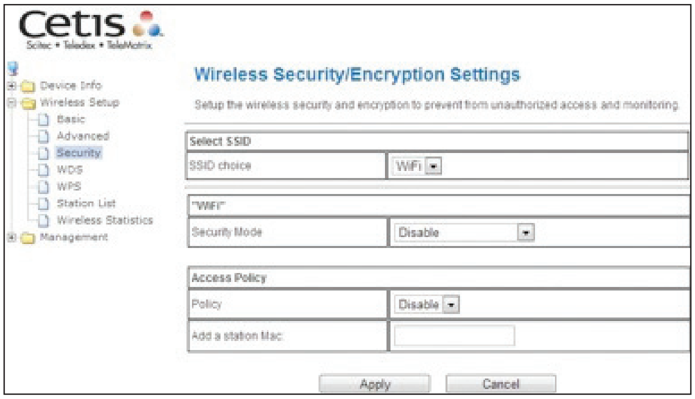
Multicast-to-Unicast Converter	
Multicast-to-Unicast	○ Enable ● Disable

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.



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	

5.3.1 SELECT SSID

SSID Choice: Select SSID from the drop-down list.

5.3.2 SECURITY MODE

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

5.3.3 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.

5.3.4 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

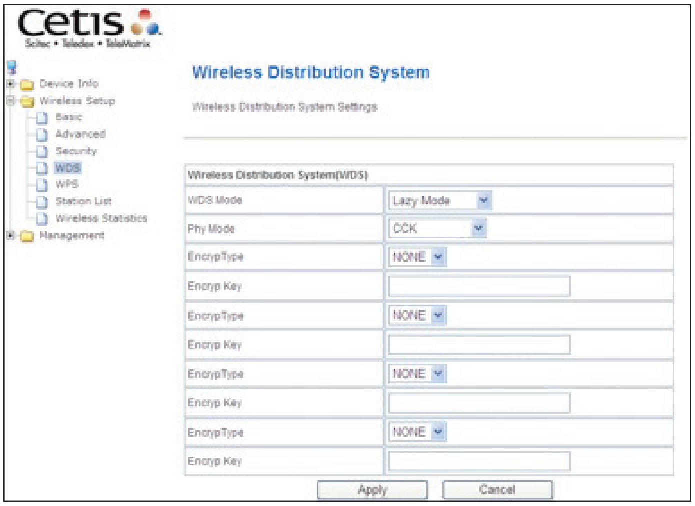
5.4.1 WIRELESS DISTRIBUTION SYSTEM (WDS)

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

- **Disable**

Select Disable to disable the WDS mode.

- **Lazy Mod**e



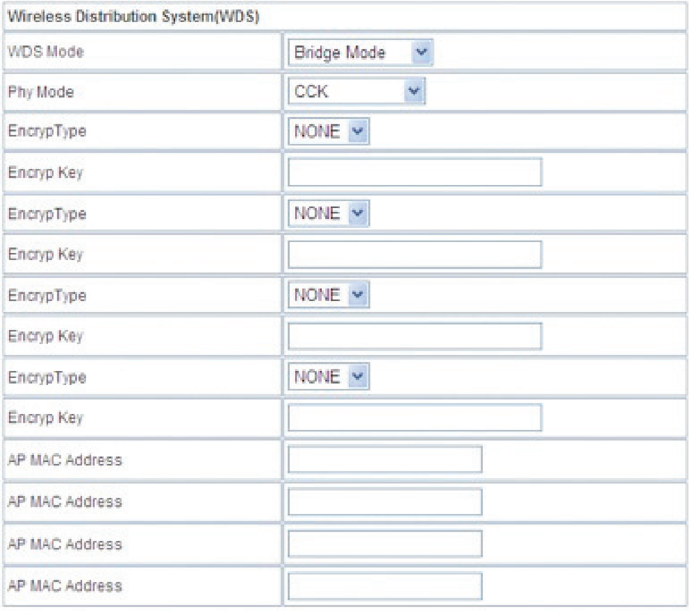
Wireless Distribution System

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	

Field	Description
WDS Mode	Select Lazy Mode. The EXA100WDS Lazy mode allows the other WDS bridge/repeater mode to link automatically.
Phy Mode	It provides 4 options, including **CCK, OFDM, HTMIX,** and **GREENFIELD.**
Encryp Type	It provides 4 options, including **None, WEP, TKIP,** and **AES.**
Encryp Key	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	
EncrypType	NONE
Encryp Key	
EncrypType	NONE
Encryp Key	
EncrypType	NONE
Encryp Key	
AP MAC Address	
AP MAC Address	
AP MAC Address	
AP MAC Address	

Field	Description
WDS Mode	Select **Bridge** Mode or **Repeater** Mode.
Phy Mode	It provides 4 options, including **CCK, OFDM, HTMIX,** and **GREENFIELD.**
Encryp Type	It provides 4 options, including **None, WEP, TKIP,** and **AES.**
AP MAC Address	It provides 4 AP MAC Addresses. Input the MAC address of the other APs.

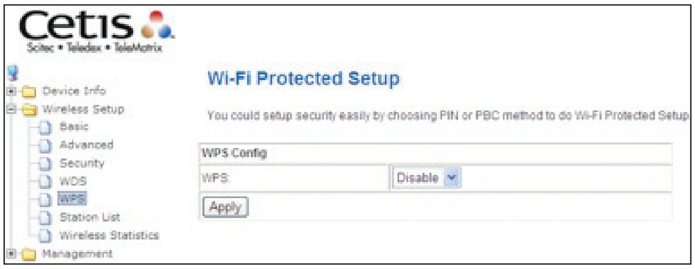
Field	Description
WDS (Wireless Distribution System)	Allows access points to communicate with one another wirelessly in a standardized way. It can also simplify the network infrastructure by reducing the amount of cabling required. Basically the access points will act as a client and an access point at the same time. 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. 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. Only Static WEP keys may be used in a WDS connection, including any STAs that are associated with a WDS repeating AP. Input the MAC address of the other APs that you want to link to and click enable. Supports up to 4 point to multipoint WDS links, check Enable WDS and then enable on the MAC addresses.

5.4.2 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.

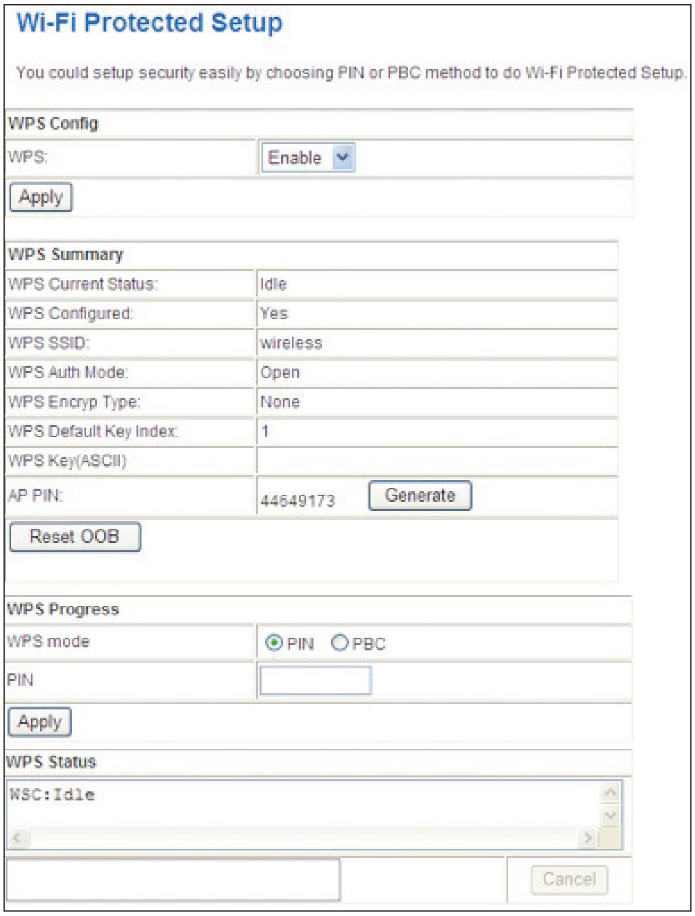


Wi-Fi Protected Setup

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

WPS Config	
WPS:	Disable

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

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

WPS Progress	
WPS mode	● PIN ○ PBC
PIN	

WPS Status

```
WSC:Idle
```

5.5.1 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.

5.5.2 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.

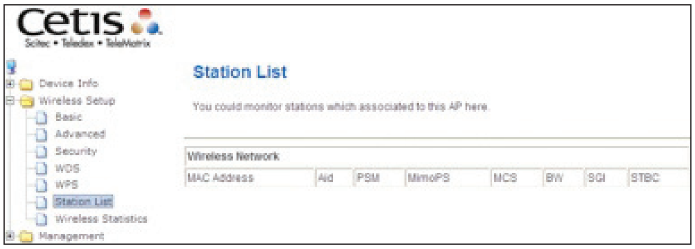
PIN: If you select PIN mode, you need to input the PIN number in the field.

5.5.3 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.



Station List

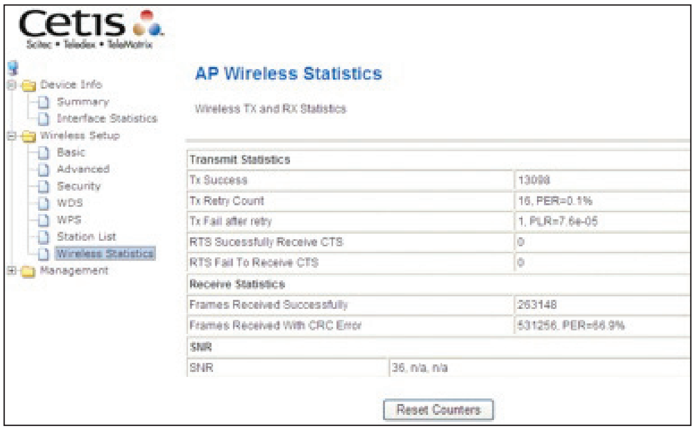
You could monitor stations which associated to this AP here.

Wireless Network

MAC Address	Aid	PSM	MimoPS	MCS	BW	SGI	STBC

5.7 AP Wireless Statistics

This page displays the Wireless Statistics (both Transmit and Receive) of the EXA100.



AP Wireless Statistics

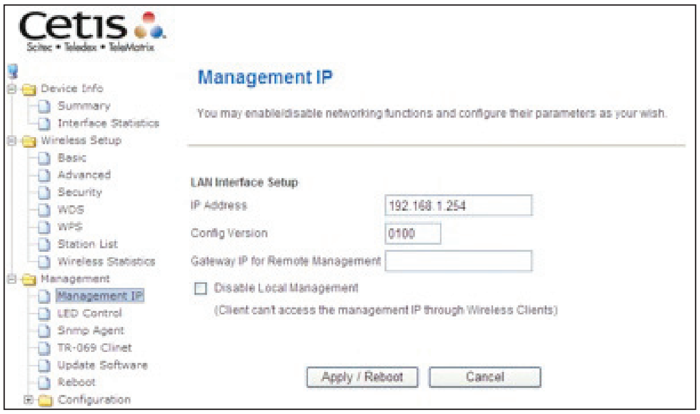
Wireless TX and RX Statistics

Transmit Statistics	
Tx Success	13098
Tx Retry Count	16, PER=0.1%
Tx Fail after retry	1, PLR=7.6e-05
RTS Sucessfully 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

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



Management IP

You may enable/disable networking functions and configure their parameters as your wish.

LAN Interface Setup

IP Address	192.168.1.254
Config Version	0100
Gateway IP for Remote Management	

□ Disable Local Management
(Client can't access the management IP through Wireless Clients)

6.1.1 IP ADDRESS

This is the Web LAN IP address for management use. Users can modify it if required.

6.1.2 CONFIG VERSION

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

6.1.3 GATEWAY IP FOR REMOTE MANAGEMENT

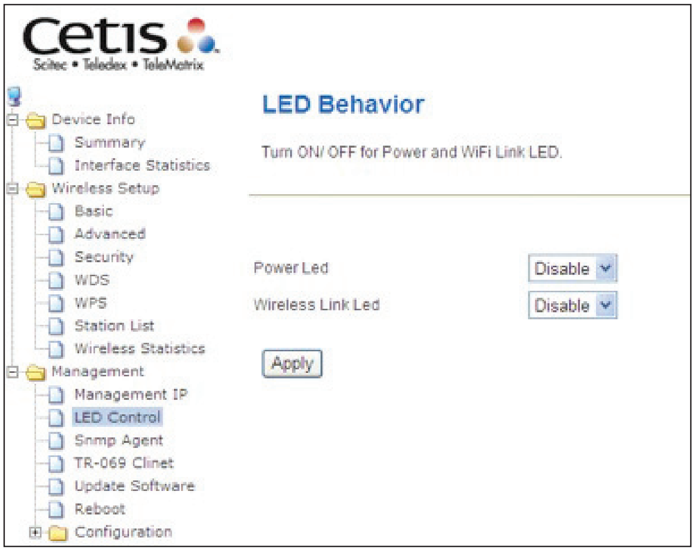
Setup the Gateway IP Address for remote management use. The Gateway IP Address must have the same network as the management IP.

6.1.4 DISABLE LOCAL MANAGEMENT

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

After completing the settings above, click **Apply/ Reboot** and EXA100 will reboot to save the settings and make the new configuration take effect. Click **Cancel** to close without saving.

6.2 LED Control



LED Behavior

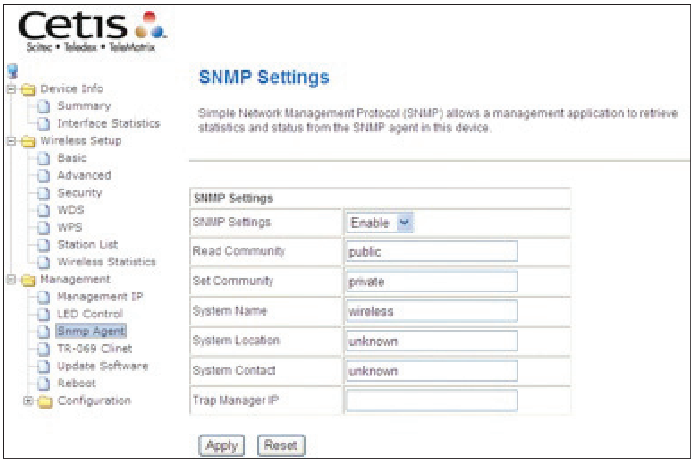
Turn ON/ OFF for Power and WiFi Link LED.

Power Led	Disable
Wireless Link Led	Disable

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.



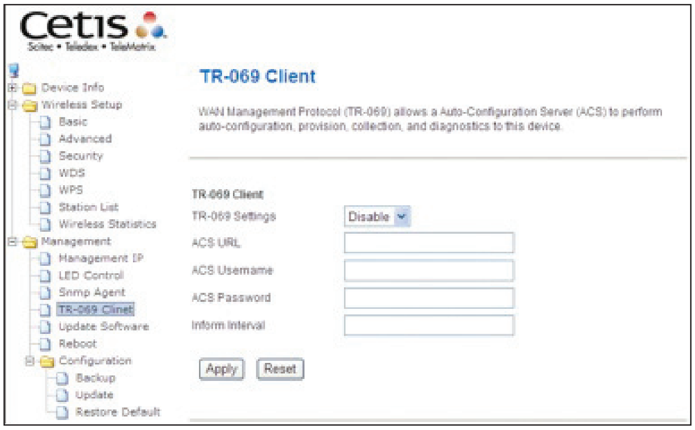
SNMP Settings

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	

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.



TR-069 Client

WAN Management Protocol (TR-069) allows a Auto-Configuration Server (ACS) to perform auto-configuration, provision, collection, and diagnostics to this device.

TR-069 Client

TR-069 Settings: Disable

ACS URL:

ACS Username:

ACS Password:

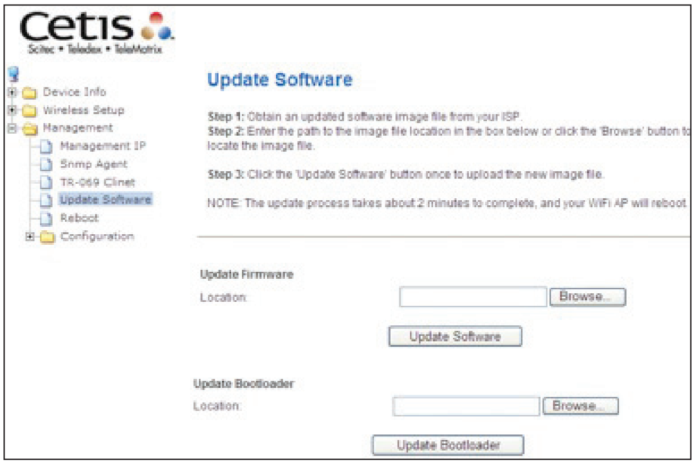
Inform Interval:

The table below is provided for ease of reference.

Field	Description
TR-069 Settings	Select **Enable/Disable** 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.
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.



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:

6.5.1 UPDATE FIRMWARE

STEP 1: Obtain an updated software image file from your ISP.

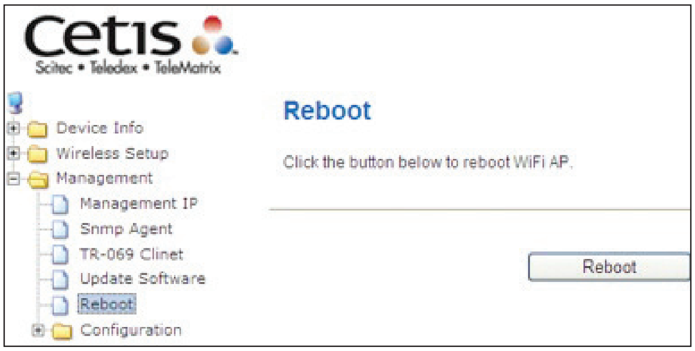
STEP 2: Enter the path and filename of the firmware image file in the **Software File Name** field or click the Browse button to locate the image file.

STEP 3: Click the **Update Software** button once to upload and install the file.

NOTE: The update process will take about two 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.**



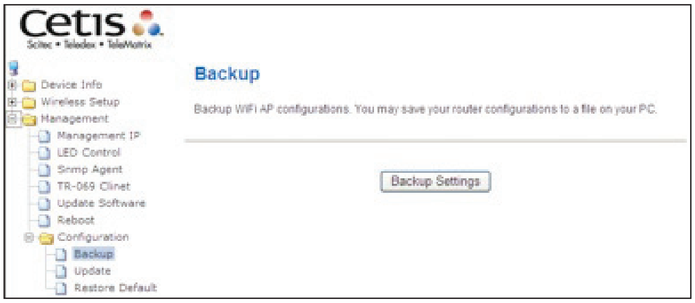
Click the button below to reboot WiFi AP.

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

6.7 Configuration

6.7.1 BACKUP SETTINGS

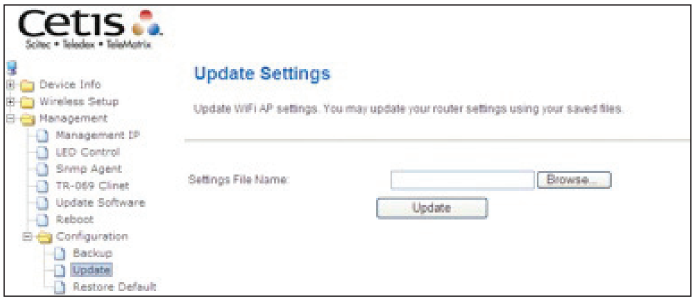
To save the current configuration to a file on your PC, click **Backup Settings.** You will be prompted for backup file location. This file can later be used to recover settings on the **Update Settings** screen, as described below.



Backup WiFi AP configurations. You may save your router configurations to a file on your PC.

6.7.2 UPDATE SETTINGS

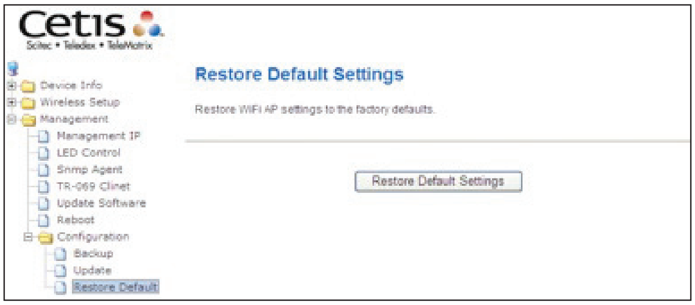
This option recovers configuration files previously saved using **Backup Settings.** Enter the file name (including folder path) in the **Settings File Name** box, or press **Browse...** to search for the file, then click **Update Settings** to recover settings.



Update WiFi AP settings. You may update your router settings using your saved files.

6.7.3 RESTORE DEFAULT

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



Restore WiFi AP settings to the factory defaults.

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.

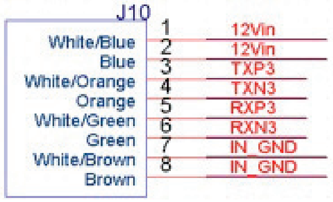
NOTE: This entry has the same effect as the **Reset** button. The EXA100 board hardware and the boot loader support the reset to default. If the **Reset** button is continuously pressed for more than 5 seconds, the boot loader will erase the configuration data saved in flash memory.

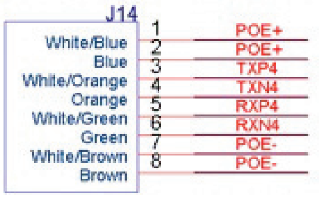
Appendix A—Pin Assignments

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

NOTE: 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=0	0: disable 1: enable	0
	Network Name(SSID)		SSID1=wireless		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=0 AutoChannelSelect=1		
	Network Mode-11b/g mixed mode		WirelessMode=0 FixedTxMode=OFDM		0
	Network Mode-11b only		WirelessMode=1 FixedTxMode=CCK		1
	Network Mode-11g only		WirelessMode=4 FixedTxMode=OFDM		4
	Network Mode-11b/g/n mixed mode		WirelessMode=9 FixedTxMode=HT		9
		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
	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

	Setting Parameters in Web GUI		**Settings Parameters in Config File**	**Value**	**Default**
Basic Wireless Setting		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	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

	Setting Parameters in Web GUI		Settings Parameters in Config File	Value	Default
Advanced Wireless Settings	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	0: disable 1: enable	1
		APSD Capable	APSDCapable=0		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

	Setting Parameters in Web GUI		Settings Parameters in Config File	Value	Default
Advanced Wireless Settings		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-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	(SSID1;SSID2;SSID3;SSID4;SSID5) keyType: 0 - 1 0: Hex 1: ASCII	KeyStr1=blank KeyType=0,0,0,0,0
		WEP Key 2	Key2Str1= Key2Type=0		
		WEP Key 3	Key3Str1= Key3Type=0		
		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

	Setting Parameters in Web GUI		Settings Parameters in Config File	Value	Default
Advanced Wireless Settings		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=OPEN EncrypType=WEP		

	Setting Parameters in Web GUI		Settings Parameters in Config File	Value	Default
Advanced Wireless Settings		802.1x WEP	IEEE8021X=		blank
		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
	Policy		AccessPolicy0=0	0: Disable 1: Allow 2: Reject	0
	Add a station Mac		AccessControlList0=		blank
Wireless Distribution System	WDS Mode-Disable		WdsEnable=0		0
	WDS Mode-Lazy Mode		WdsEnable=4		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=2		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=3		3
		Phy Mode	WdsPhyMode=	CCK;CCK;CCK;CCK OFDM;OFDM;OFDM;OFDM HTMIX;HTMIX;HTMIX;HTMIX GREENFIELD;GREENFIELD;GREENFIELD;GREENFIELD	CCK;CCK;CCK;CCK

	Setting Parameters in Web GUI		Settings Parameters in Config File	Value	Default
Wireless Distribution System		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	SNMPWRITCOMM=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	TR69ACSurl=		blank
	ACS Username	TR69Username=		blank
	ACS Password	TR69Password=		blank
	Inform Interval	TR69InformInterval=		blank

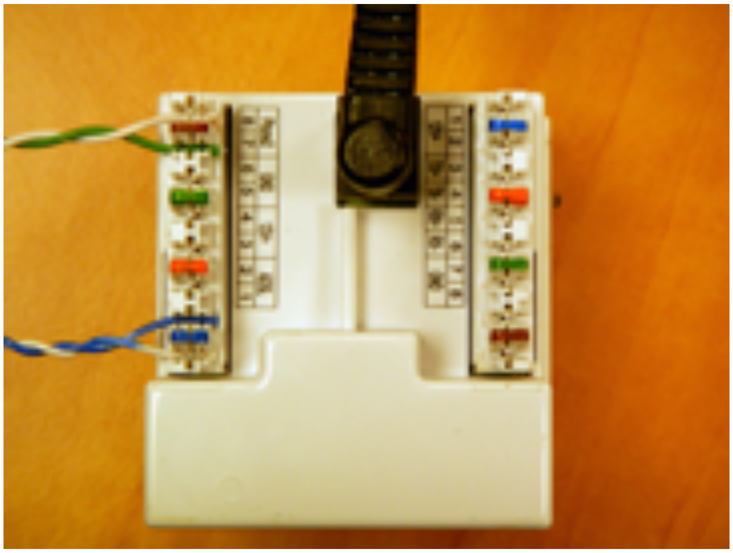
Appendix D—Y Series Wiring Examples

The Y-Series has multiple wiring possibilities and options.
This document covers only a few of the most requested and common applications.

Typical ADSL 2+ wiring examples

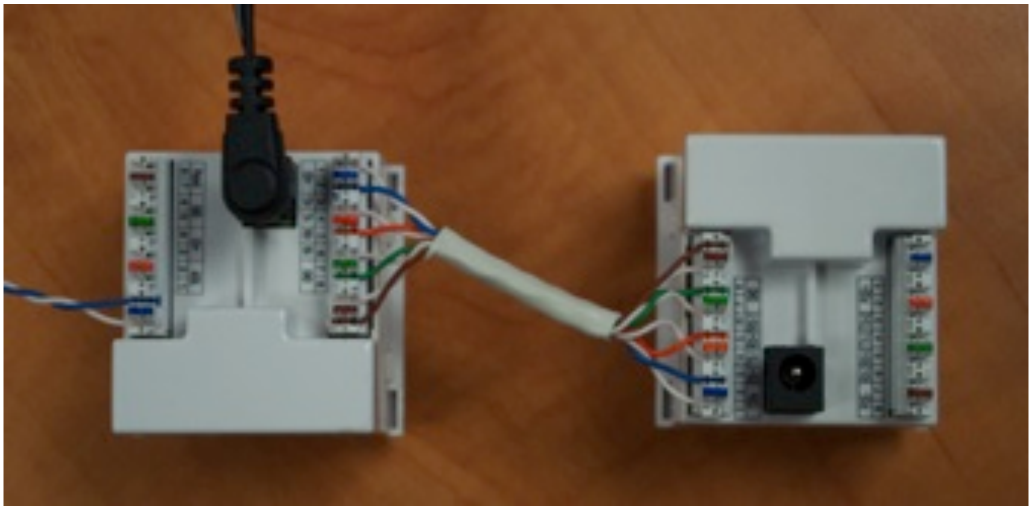
ADSL2+ (With one extra Analog Line) --> CPE (2 analog lines)

In this example, an ADSL2+ wire pair (blue and white) connects to the EXP100 (CPE).
Power is supplied to the CPE by the PSU.



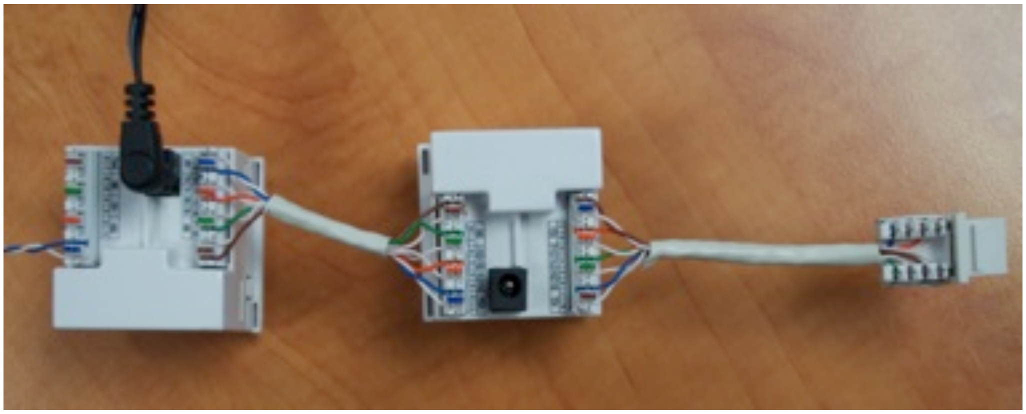
ADSL 2+ --> CPE (one analog line)--> CAT5 --> WAP

In this example, an ADSL2+ wire pair (blue and white) connects to the EXP100 (CPE).
Power is supplied to the CPE by the PSU. CAT5 cable carries Ethernet connectivity from the EXP100 (CPE) to the EXA100 Wireless Access Point (WAP).



ADSL 2+ --> CPE (one analog line)--> CAT5 --> WAP --> CAT5 --> RJ45 connector

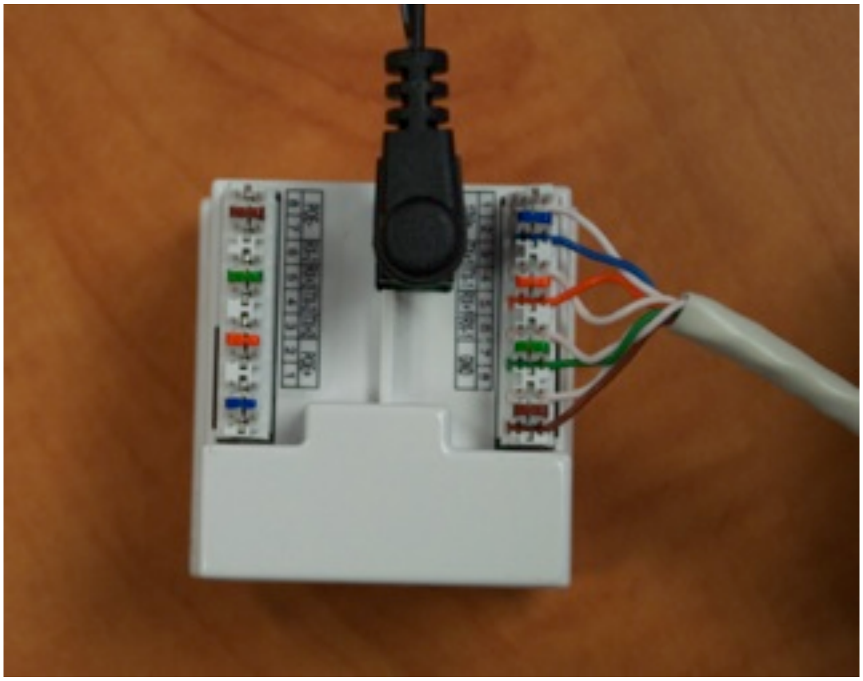
In this example, an ADSL2+ wire pair (blue and white) connects to the EXP100 (CPE).
Power is supplied by the PSU. CAT5 cable carries Ethernet connectivity from the EXP100 (CPE) to the EXA100 Wireless Access Point (WAP). and another CAT5 splice connects to the supplied RJ45 connector for the wall mount keystone.



Typical WAP ONLY wiring examples (12VDC Powered)

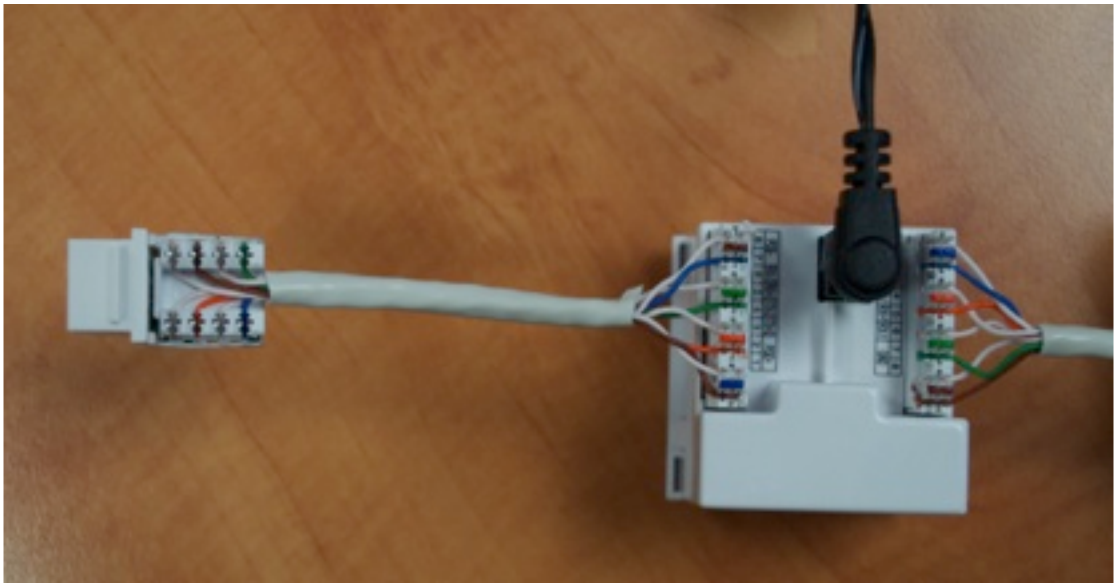
CAT5 (non-POE) --> (12VDC powered) WAP --> CAT5 --> RJ45 connector

In this example, a CAT5 cable carrying Ethernet connectivity to the EXA100 Wireless Access Point (WAP).
Power is supplied by the PSU.



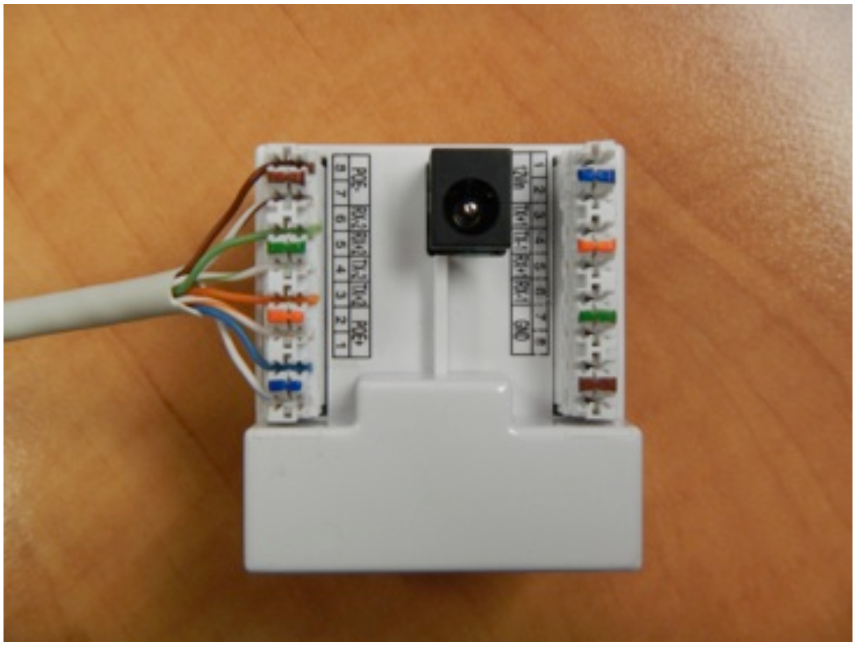
CAT5 (non-POE) --> (12VDC powered) WAP --> CAT5 --> RJ45 connector

In this example, a CAT5 cable carrying Ethernet connectivity to the EXA100 Wireless Access Point (WAP). Power is supplied by the PSU, and another CAT5 splice connects to the supplied RJ45 connector for the wall mount keystone.



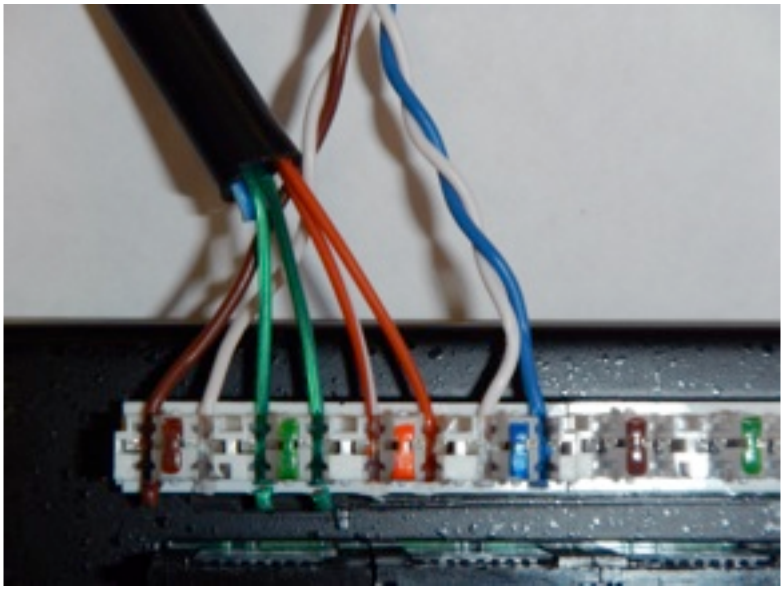
CAT5 (POE) --> (POE powered) WAP

In this example, a CAT5 cable carrying 802.3af compliant Power over Ethernet (POE) is powering the EXA100 Wireless Access Point (WAP). It is also possible, (but not pictured), to pass through the ethernet data by wiring the right side to a non-POE CAT5 keystone)



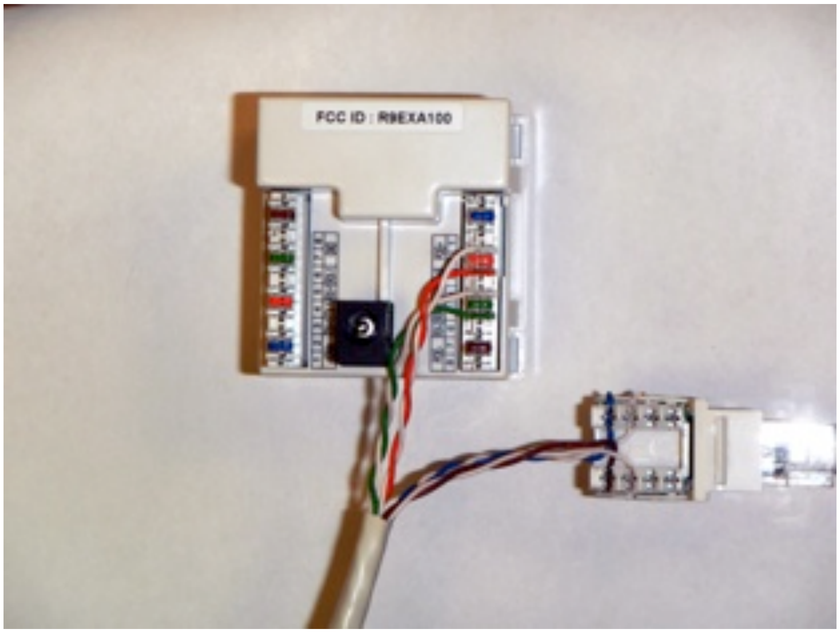
Creative WAP ONLY Wiring

CAT3 (POE) / 2 Analog--> Patch Panel --> Cat5 --> WAP and 2 analog lines



The image above shows the Green / Light Green / Orange / Light Orange used to supply both POE and data to the EXA100 WAP.

The Brown / Light Brown / Blue / Light Blue conductors represent two analog lines



Using a Cat5 cable we are able to provide both power and 10 base networking to the WAP while at the same time using the spare 4 conductors to supply 2 analog lines.

TELEDEX®

Toll Free: +1.800.462.9446
Tel: +1.719.638.8821

Email: info@teledex.com
www.teledex.com