4Ports+Wireless

User Manual

Important Safety Instructions

Please read these instructions carefully:

1. Unplug the ADSL2+ Router Ethernet Adaptor from the wall outlet before cleaning. Do not use liquid cleaners or aerosol cleaners. Use a damp cloth for cleaning.
2. Do not use the ADSL2+ Router Ethernet Adaptor near water.
3. Make sure the working platform is flat. Do not put heavy objects on the ADSL2+Router.
4. Use the AC/DC power adapter that matches the ADSL2+ Router.
5. Disconnect the power supply and all wires from the ADSL2+ Router in lightning storm, to avoid lightning strike.
6. Take water proof measures during the storage, transportation and running of the ADSL2+ Router.
7. Avoid direct sunlight.

Note: When the ADSL2+ Router is used for a long time, temperature of the shell will rise. This is normal.

Table of Contents

Chapter 1 Overview

Thank you for purchase of the ADSL2+ Router device. This device is a well-designed high-speed wireless ADSL2+ Router. This User Manual will show you how to install and set up the ADSL2+ Router.

1.1 System Features

The ADSL2+ Router provides the following functions:

- Four 10/100 Ethernet ports
- Friendly GUI for web configuration
- Support Single-Session IPSec and PPTP Pass-Through for Virtual Private Network (VPN)
- Several popular games are already pre-configured. Just enable the game and the port settings are automatically configured
- Configurable as a DHCP Server on Your Network
- Compatible with virtually all standard Internet applications
- Industry standard and interoperable DSL interface
- Address Filtering, DMZ Hosting, and Much More
- Simple web based status page displays a snapshot of your system configuration, and links to the configuration pages
- Downloadable flash software upgrades
- Support for up to 8 Permanent Virtual Circuits (PVC)
- Support for up to 8 PPPoE sessions

1.2 Supporting protocols

- ITU G.992.1 (G.DMT) Annex A
- ITU G.992.2 (G.LITE)
- ANSI T1.413 Issue 2
- ITU G.992.3 (ADSL2)
- ITU G.992.5 (ADSL2+)

1.3 Encapsulation supports

- RFC 1483 bridge
- RFC 1483 router
- Classical IP over ATM (RFC 1577)
- PPP over ATM (RFC 2364)
- PPP over Ethernet (RFC 2516)

1.4 System requirements

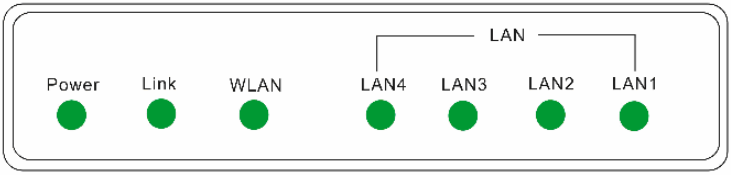
Recommended system requirements are:

- Pentium 233MHZ or above
- Memory: 64MB or above
- 10M Base-T Ethernet or above
- WIN9X WIN2000 WINXP WINME WINNT
- Ethernet Network Interface Card

Please collect the following information from your ADSL2+ service provider. This information will be very helpful for your ADSL2+ configuration. To keep a record for reference, you can fill in the column as below:

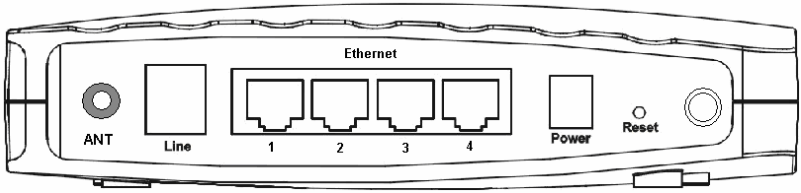
VPI	
VCI	
Encapsulation: VCMUX or LLC	
Protocol	
Standard	
User name	
Password	
Password protocol	

1.5 LED Status Description



Indicator	Status	Description
Power	OFF	Power not supplied
	ON	Power supplied
Link	Blink	DSL traffic is flowing
	Quick Blink	DSL line is training
WLAN	Quick Blink	DSL line is training
	ON	DSL line is connected
LAN (1-4)	ON	Ethernet line is connected
	Blink	Ethernet traffic is flowing

1.6 Rear Panel Layout Description



Interface	Description
Switch	Power on/off switch
Reset	Modem Reset button .Press and hold around 10s to reset the hardware. Modem's LED will be all on then all off except the Power LED, and the modem will auto restart. This action will recover the modem's default configuration.
Power socket	Plug in for power adaptor
LAN(1~4)	LAN interface for connecting to computer or Switch
Line	ADSL2+ connector for connecting to ADSL2+ telephone line

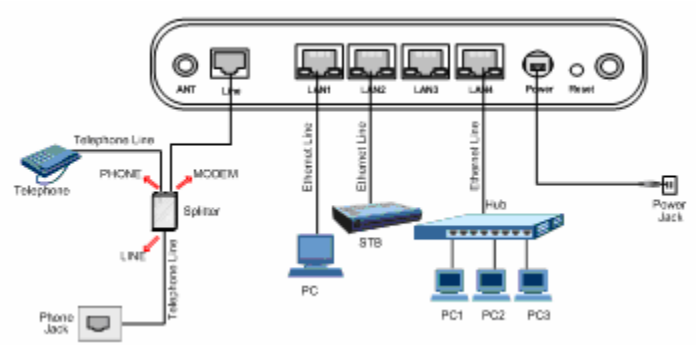
Chapter 2 Installation

2.1 ADSL2+ MODEM Installation

Please connect your ADSL2+ Router to computer as the following description:

If connecting to the splitter,

- Connect the “Line” splitter to wall jack using one telephone cable
- Use the other telephone cable to connect “MODEM” port of the splitter and “LINE” port of the modem. The “phone” port of the splitter can be use to connect the telephone and the splitter by a telephone cable.
- Use Ethernet cable to connect “LAN” port of the modem and “LAN” port of your computer.



If do not need to connect to the splitter,

- Connect the modem to wall jack using one telephone cable
- Please use the Ethernet cable to connect the Ethernet port of the modem and LAN port of your computer.

Chapter 3 Configuration

3.1 Configuring computer network card IP address

Configure your network card's TCP/IP properties to Obtain an IP address automatically from modem, or set the computer's IP with the same network mask of the modem.(For example: modem's IP is 192.168.1.1/255.255.255.0,

Then you can set computer's IP to:

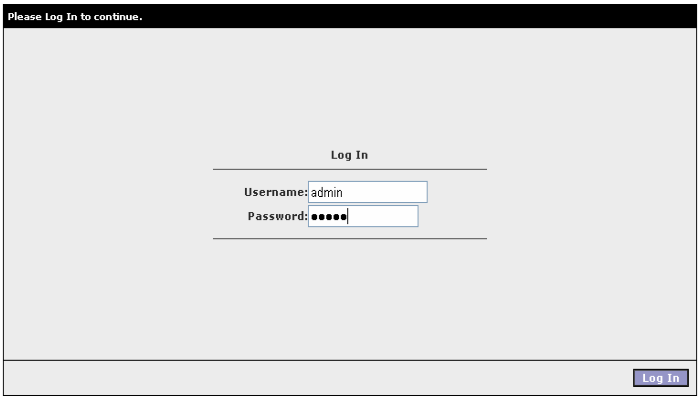
192.168.1.x/255.255.255.0.

The range for x is from 3 to 254).

3.2 Web setting interface

Open IE or Netscape Web browser, Input http://192.168.1.1(MODEM default IP address) in the address column, then click <ENTER> button, access the following setting interface:

Input user name and password, then click Login key to enter WEB setting interface.



Default setting:

IP Address: **192.168.1.1**

Subnet Mask: **255.255.255.0**

Username: **admin**

Password: **admin**

3.3 Main interface

When correct username/password has been typed, the following WINDOW will pop up:

You can realize operating as follows though the home page:

- RG configuration (though the connection between the LAN and the WAN)
- Advanced of RG configuration (security, router, filter act)
- Obtain the state of RG
- Look over help

Note—RG：Residential Gateway, refer to Modem itself here.

3.4 SETUP

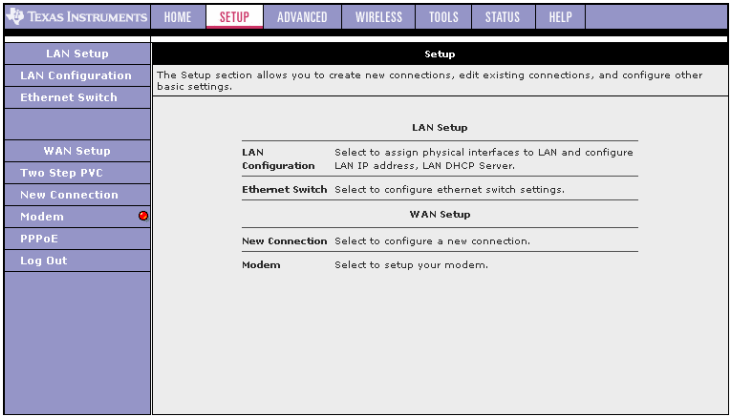
This chapter introduces the configuration of the ADSL2+ Modem through Web, including the following contents:

- LAN Setup

The local host's computers connect to LAN interface, generally set up and assign IP address in LAN the host computers of ends automatically.

- WAN Setup

Mainly set up WAN to dispose.



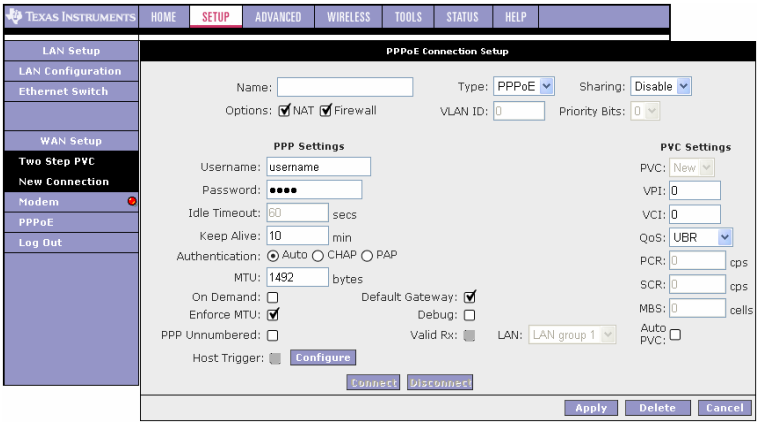
3.4.1 WAN Configuration

The RG supports and sets up to 8 different connections, if you set up many different connections, then you need to use the static behavior of RG and dynamic route function to make data transmission correct.

Before setting up new WAN to connect, should confirm that you connect to DSL first, there is an indicator lamp by Modem chaining, green color specification was connected to DSL, red color specification has not been connected to.

6 kinds of different kinds of connections in all are offered to users, including: PPPoE, PPPoA, Static, DHCP, Bridge, and CLIP. Now introduce their use one by one for everybody.

3.4.1.1 Configuring PPPoE



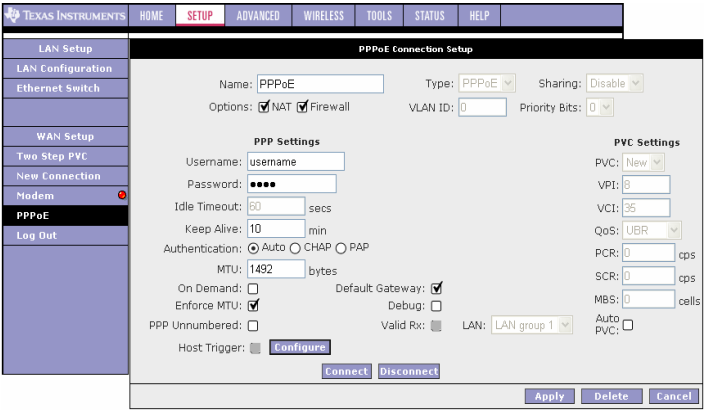
Follow the steps listed below to configure:

1. Click the “New Connection”, PPPoE that will demonstrate default connection pages.
2. Enter the Username, generally the naming rule as" type + PVC", such as PPPoE_8_35.
3. NAT and Firewall select default as the state of choosing.

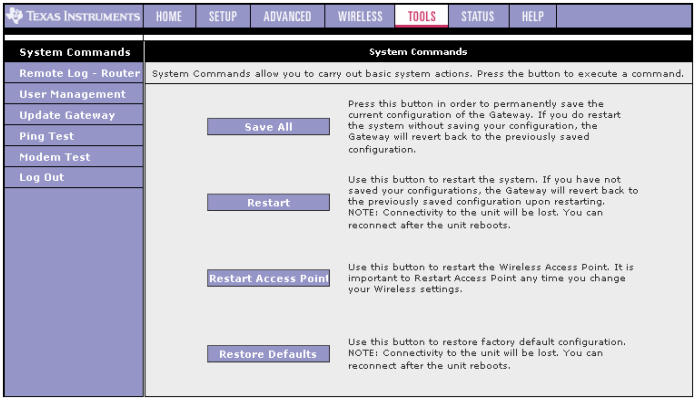
   Note—NAT can change IP address of LAN end into IP address of WAN end, if does not choose NAT to select, can not surf the Net.
4. If you want to use VLAN, draw the frame to choose VLAN under sharing, can edit the state while making VLAN id AND Priority Bits area in , inputs ID of VLAN in VLAN ID place , rank that in Priority Bits to choose to have priority for VLAN.
5. Input your DSL service provider or data of ISP provide in PPP setting area in, such as username and password.
6. Input VPI and VCI in PVC setting area in. The VPI/VCI was offered by ISP of your DSL service provider.
7. Choose QoS. If you uncertain ISP offers such information, uses default

finally.

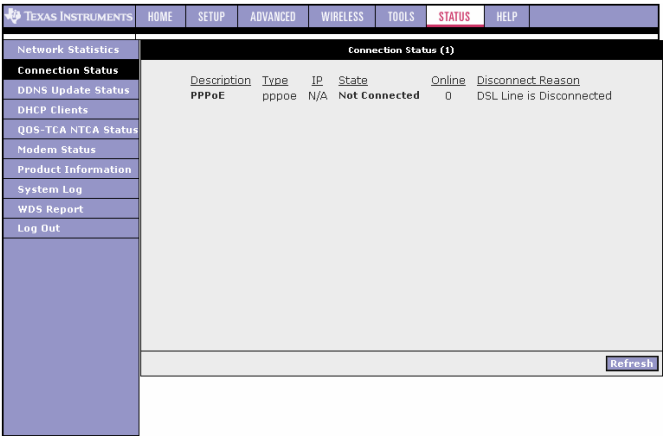
8. Click “Apply” to finish the connection .As follow:



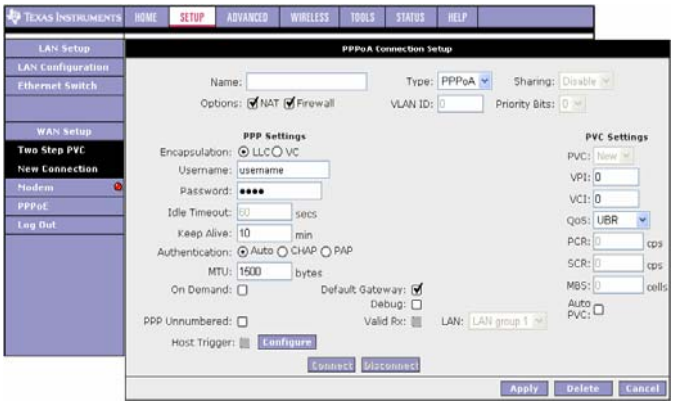
9. In order to keep setting up, click TOOLS of the page above, then choose System Commands, click Save All button to keep.



10. Click “STATUS” of the page above; choose Connection Status to check the connection state. As following:



3.4.1.2 Configuring PPPoA

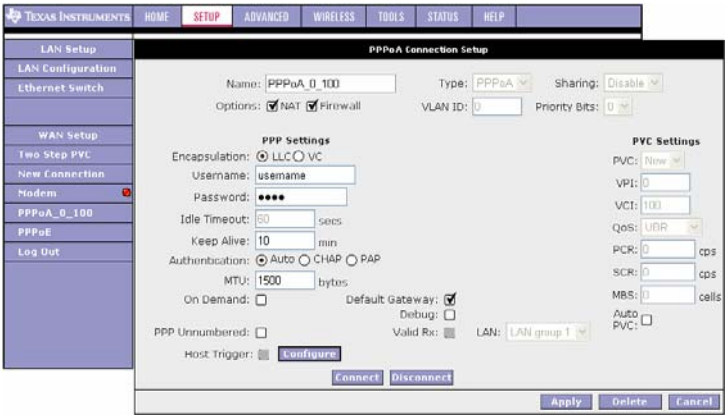


Follow the steps listed below to configure:

1. Click the “New Connection”, PPPoA that will demonstrate default connection pages.
2. Choose the PPPoA in the frame of drawing under the Type.
3. Enter the Username, generally the naming rule as “type + PVC ", such as PPPoA_0_100.
4. NAT and Firewall select default as the state of choosing.

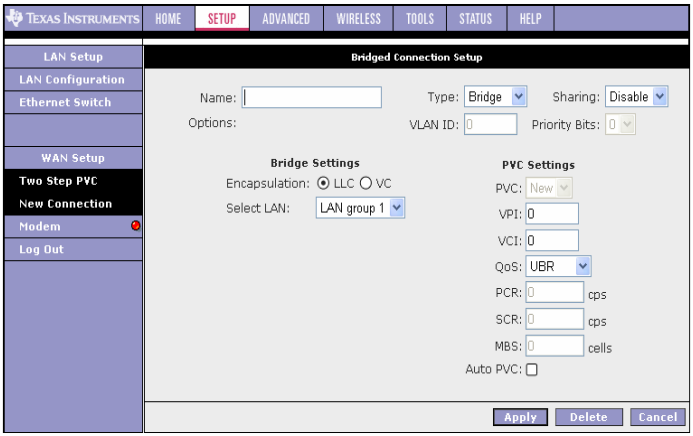
Note—NAT can change IP address of LAN end into IP address of WAN end, if does not choose NAT to select, can not surf the Net.

5. If you want to use VLAN, draw the frame to choose VLAN under sharing, can edit the state while making VLAN id AND Priority Bits area in , inputs ID of VLAN in VLAN ID place, rank that in Priority Bits to choose to have priority for VLAN.
6. Choose encapsulation type: LLC or VC in PPP setting area in. If don't confirm, use the default. Then enter your Username and Password.
7. Input VPI/VCI in PVC setting area in. The VPI/VCI was offered by your DSL service provider and ISP service provider.
8. Choose the QoS.
9. Click the "Apply" to finish the connection. As following:



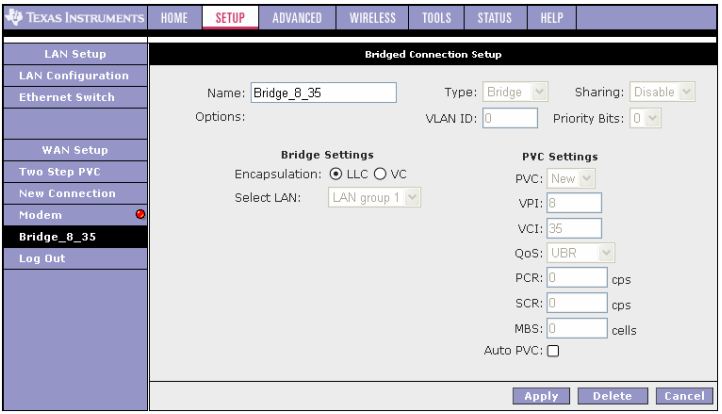
10. Remember to keep and set up, otherwise all modification is lost after RG is opened again next time. Go to System Commands page in TOOLS page, click Save All.
11. Click "STATUS" of the page above; choose "Connection Status" can check the connection state.

3.4.1.2 Configuring Bridge



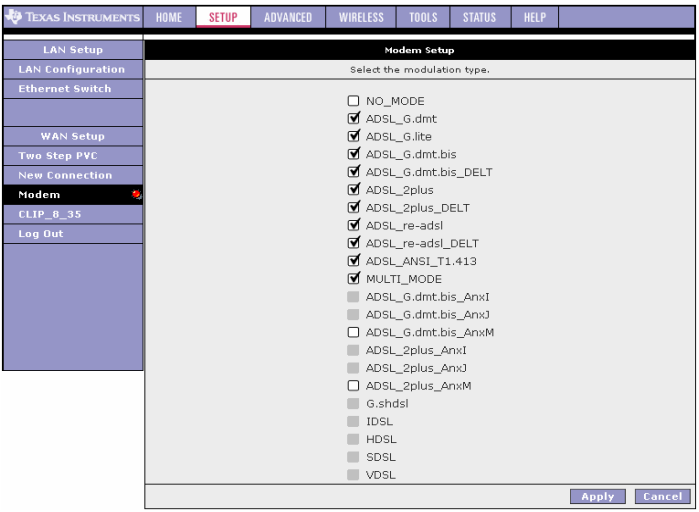
Following the steps listed below to configure:

1. Click the “New Connection,”PPPoE that will demonstrate default connection pages.
2. Choose Bridge in the frame of drawing under the Type, will show that Bridge connection pages.
3. Enter the Username, generally the naming rule as “type + PVC”, such as Bridge_8_35.
4. Choose encapsulation type: LLC or VC in Bridge setting area in. If don’t confirm, use the default.
5. Input VPI/VCI in PVC setting area in.
6. Choose QoS.
7. Click “Apply” to finish the connection.



8. Remember to keep and set up, otherwise all modification is lost after RG is opened again next time. Go to System Commands page in TOOLS page, click Save All.

9. Click “STATUS” of the page above; choose Connection Status can check the connection.



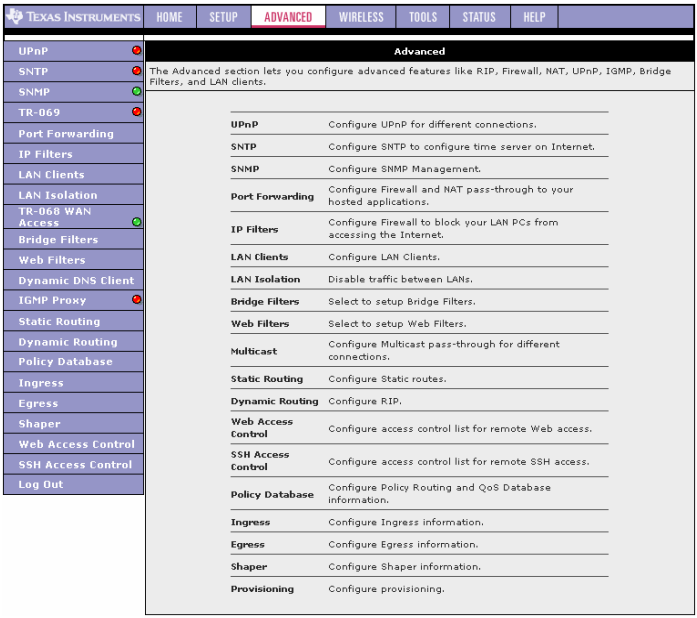
3.5 ADVANCED

3.5.1 Advanced the main page

Use the advanced page; you can dispose the connection that has already existed advanced. Include:

- Use UPNP, SNTP, IP, QoS, RIP, access control, broadcast the function
- In order to connect which assigns IP QoS
- Manage the interface of LAN, dataflow and filtering

Must set up a WAN at least to connect before carrying out WAN to configure advanced, must define one LAN group at least before carrying out LAN to configure advanced.



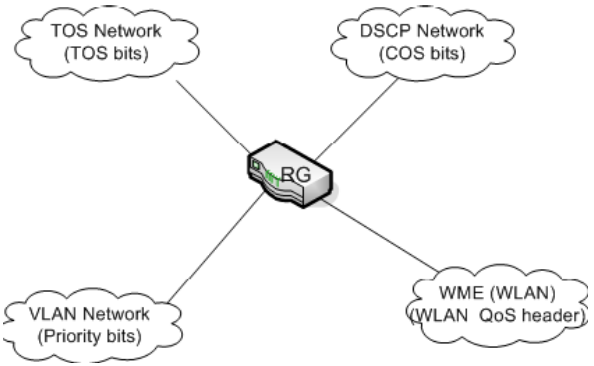
3.5.2 Configuring QoS

Quality of service (QoS) is an important feature for this release. The QoS

Framework allows network administrators to configure the routers to meet the real time requirements for voice and video.

Different QoS marking is used in different network:

- ToS network: ToS bits in the IP header
- VLAN network: Priority bits in the VLAN header
- DSCP network: Uses only 5 bits of the CoS
- WLAN: WLAN QoS header



The QoS framework is supported on all the above domains. How do you make them talk to each other? How can you make sure the priority from one network is carried over to another network? Class of service (CoS) is introduced as the common language for the QoS mappings. When QoS is enabled, the RG has full control over packets from the time they enter the RG till they leave the RG. This is how it works: The domain mapping (ToS bits, priority bits, etc.) of a packet needs to be translated to CoS when the packet enter the RG, and vice versa, the CoS of a packet needs to be translated back to the domain mapping when the packet leaves the RG.

CoS: There are 6 types of CoS (in descending priority):

- CoS1
- CoS2
- CoS3
- CoS4
- CoS5
- CoS6

The rules are:

1. CoS1 has absolute priority and is used for expedited forwarding (EF) traffic. This is always serviced till completion.
2. CoS2-CoS5 is used for assured forwarding (AF) classes. They are serviced in a strict round robin manner using the following priority scheme: CoS2 > CoS3 > CoS4 > CoS5
3. CoS6 is for best effort (BE) traffic. This is only serviced when there is no other class of service. If QoS is not enabled on your RG, all traffic will be treated as best effort.

Additional Terms There are some additional terms you should get familiarize with:

• Ingress: Packets arriving into the RG from a WAN/LAN interface.

• Egress: Packets sent from the RG to a WAN/LAN interface.

• Trusted mode: Honors the domain mapping (ToS byte, WME, WLAN user priority).

• Untrusted mode: Does not honor domain mapping. This is the default QoS setting.

• Traffic Conditioning Agreement (TCA): The TCA needs to be defined for each interface:

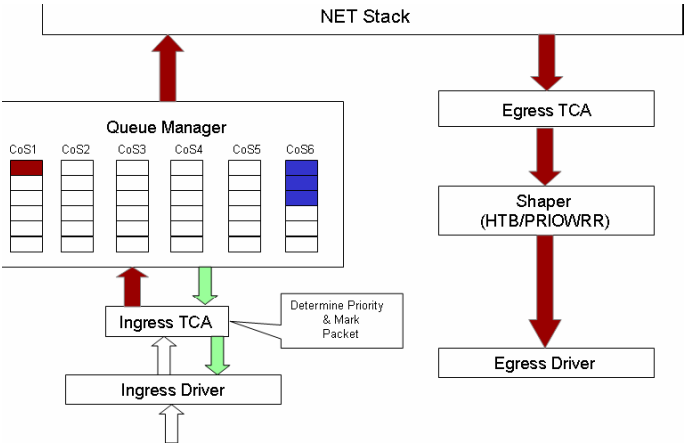
– Ingress mappings (Domain =>CoS)

– Egress Mappings (CoS => Domain)

– By default, all interfaces are in Untrusted mode.

• Shaper

As follow the figure is diagram that shows the QoS packet flow.



GUI Configuration Your RG provides the following web pages for you to configure QoS:

• **Ingress page:** The **Ingress** page allows you to translate domain mapping of an incoming packet to CoS.

• **Egress page:** The **Egress** page allows you to translate CoS of an outgoing packet to a domain mapping.

• **Shaper page:** The **Shaper** page allows you to define rules and assign bandwith for the CoS types. This page is applicable only to the Egress interface.

• **Policy Database page:** Policy Routing (PR) rules apply when you configure QoS for multiple WAN connections. The **Policy Database** page also enables you to classify packets on the basis of various fields in the packet.

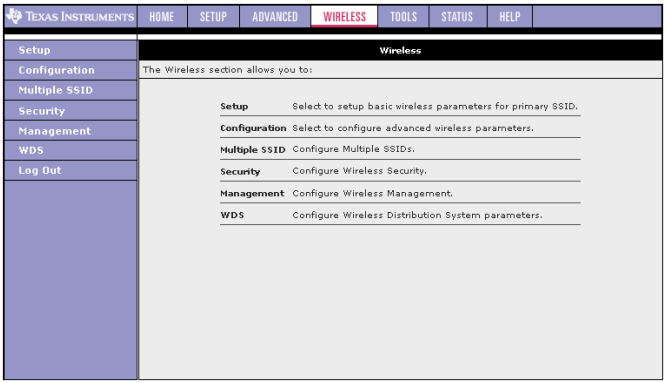
Note—The QoS/PR pages are recommended for ODM/OEMs' use only and should not be exposed to the end user.

3.6 WIRELESS

3.6.1 Wireless main page

As follow the Wireless main page, this is accessed by clicking the Wireless tab at the top of the page. This page provides access to the following wireless configuration pages:

- Setup
- Configuration
- Multiple SSID
- Security
- Management
- WDS
- Log Out



3.6.2 Wireless Setup

As follow shows the default Wireless Setup page, which is accessed by clicking the Setup link, this page provides basic access point (AP) parameter settings.

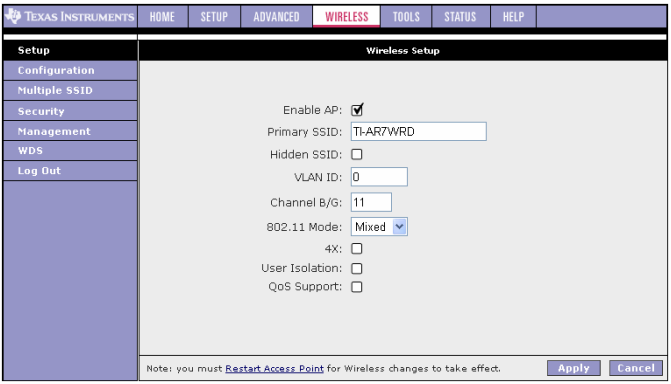


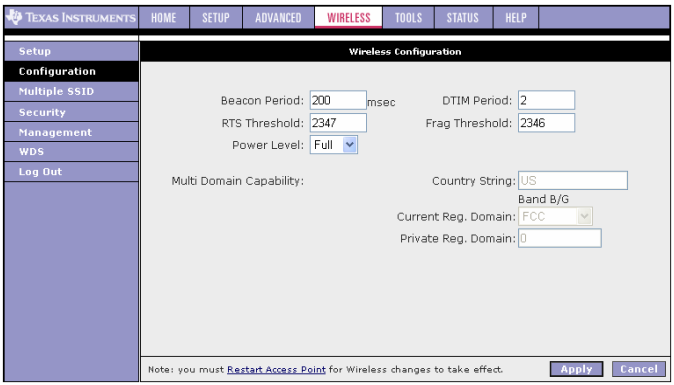
Table: Wireless Setup Field Descriptions

Field	Definition
Enable	Enables/disables the access point
Primary SSID	The primary service set identifier of the AP, which is the only SSID your AP broadcasts (if hidden SSID is disabled). The default is TI-AR7VW and you can assign a unique SSID to your AP. The SSID is up to 32 characters.
Hidden SSID	Enables/disables the hidden SSID feature. When hidden SSID is enabled, the SSID is removed from the beacon frames the AP transmits, thus the AP will not be seen by any other station.
Channel B/G	The channel on which the AP and the wireless stations communicate. Different domains have different ranges of channels. For FCC in 2.4 GHz, the default channel is 11.
802.11 Mode	You can select from the following modes: **Mixed mode**: Both 802.11b and g modes are supported. The legacy supported rates information element (SRIE) contains the 802.11b legacy supported rates and the additional OFDM supported rates. Extended SRIE contains the extended supported rates, if present. Beacon & Probe Response Frames are sent in b rate.

	11b only Mode: The legacy SRIE contains only the 802.11b legacy supported rates. The extended SRIE is not present. **11b+ Mode**: Similar to the 802.11b-only mode except that 22Mbps PBCC rate/modulation is included, this is TI proprietary. **11g only Mode**: The legacy SRIE contains only the OFDM additional supported rates. The extended SRIE contains the extended supported rates, if present.
4X	Enables/disables the 4x feature for 802.11g mode. This function is TI proprietary and is only available when both TI wireless station card and TI RG are used.
User Isolation	When checked, wireless users will not be able to directly access other wireless users. More details on User Isolation are discussed.
QoS Support	Refer to WLAN QoS Support more information.

3.6.3 Wireless Configuration

You can access the Wireless Configuration page by clicking the Configuration link. This page provides the advanced wireless network parameter settings.



Note—The highlighted area relates to the multi domain capability function, which cannot be configured on this page. It is configured. For more information on the wireless hidden pages, refer to the AP-DK Web-based Configuration Utility User's Guide.

Configuration Field Descriptions

Field	Definition
Multi Domain Capability	This feature can only be configured on the page by the OEM/ODM. It is not recommended that the end users configure this feature.
Country String	This feature can only be configured on the page by the OEM/ODM. It is not recommended that the end users configure this feature.
Current Reg. Domain	This feature can only be configured on the page by the OEM/ODM. It is not recommended that the end users configure this feature.
Private Reg. Domain	This feature can only be configured on the page by the OEM/ODM. It is not recommended that the end users configure this feature.

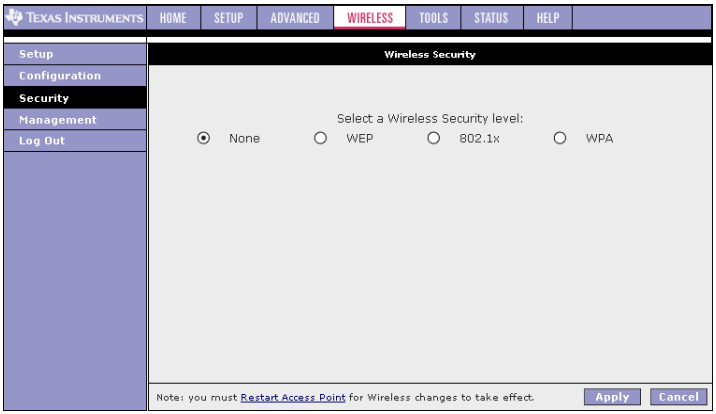
3.6.4 Wireless Security

As follow shows the default Wireless Security page, which provides the following wireless network security options.

- None: No security used.
- Wired equivalent privacy (WEP): Enable legacy stations to connect the AP.
- 802.1x: Enable stations with 802.1x capability to connect the AP.
- Wi-Fi protected access (WPA): Enable legacy stations to connect the AP.

- WPA2: Enable stations with WPA2 capability to connect the AP. This option is available under the WPA option.

Wireless Security - None



If you have multiple SSID enabled, you can assign security to each SSID. There are a few rules/limitations that you should follow:

- WEP cannot be assigned to more than one SSID.
- 802.1x cannot be assigned to more than one SSID.
- WEP and 802.1x cannot both be assigned concurrently to different SSIDs.
- When more than one SSID exists with security enabled, the Authentication type for WEP cannot be shared.

Wireless Security- WEP

WEP is a Security protocol of the WLAN; WEP provides security by encrypting the data that is sent over the WLAN.

The RG supports three levels of WEP encryption:

- 64 encryption
- 128 encryption

- 256 encryption

With WEP, the receiving station must use the same key for decryption. Each radio network interface card (NIC) and AP, therefore, must be manually configured with the same key. As the follow page shows the default setting of the WEP Wireless Secruity page.

WEP is disabled by default. As follow the steps to enable WEP on your AP.

1. Select the SSID that you want to apply security to.
2. Check Enable WEP Wireless Security.
3. Select Authentication Type.
4. Enter Encryption key and select Cipher following the instructions on the page.

   You will need to enter the same key for the first time configuration of each station.

5. To save your settings.

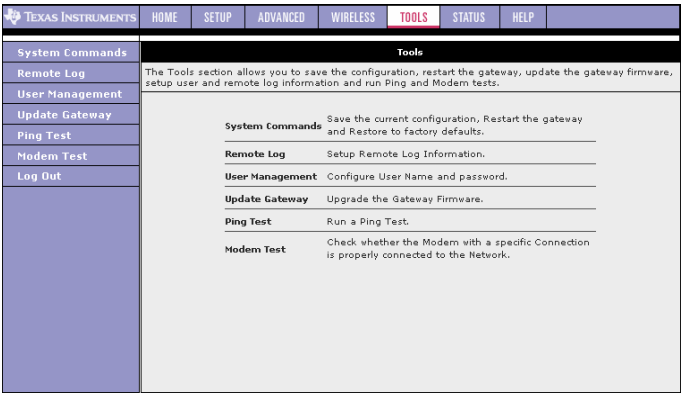
Table WEP Field Descriptions

Field	Definition
Select an SSID and its Security Level	If multiple SSID is enabled, use this drop-down menu to select the SSID that you want to apply wireless security to.

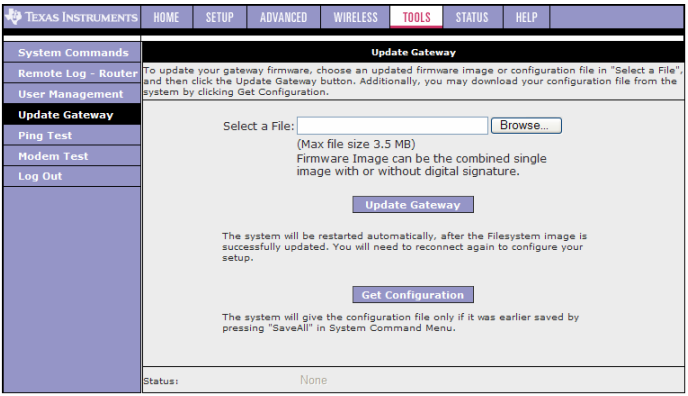
Enable WEP Wireless Security	Check this field to enable WEP wireless security on the selected SSID.
Authentication Type	Authentication algorithm to use when the security configuration is set to Legacy. When the security configuration is set to 802.1x or WPA, the authentication algorithm is always open. This field is enabled when the WEP security field is checked. There are three options: **Open** (default): In open-system authentication, the access point accepts any station without verifying its identify. **Shared**: Shared-key authentication requires a shared key (WEP encryption key) be distributed to the stations before attempting authentication. **Both**: If both is selected, the access point will perform shared-key authentication, then open-system authentication.
Encryption Key	This field is enabled when the WEP security is checked to identify the key value that is used when the security configuration is set to WEP. The key length must match the WEP cipher.
WEP Cipher	This field is enabled when the WEP security field is checked. You can select from 64 bits, 128bits and 256bits. The WEP cipher that is used when the security configuration is set to WEP. This field is not used when the security configuration is set to 802.1x and WPA.

3.7 TOOLS

3.7.1 Tools main page



3.7.2 Update Gateway



Following the steps below to configure the update the gateway soft:

1. Click the “Browse” button, select the nsp.ar7wrd.firmware.upgrade.img”.
2. Click the “Update Gateway” button.

3. The state of uploading the file will show that in the page, will act as and spread it while finishing, RG will be opened automatically again, need to land the page again.
4. Input username and password to login again.
5. If you want to confirm whether the software is upgraded correctly, go to check the edition information of the gateway to STATUS->Product Information page.
6. Use the same step to upgrade and dispose the file.(config.bin)
7. Can download config.bin of RG hard disk conduct to reach you back up too, click “Get Configuration " button, then keep .

Chapter 4 Questions & Answers

1. Question: Why all LED indicators are off?

Answer: Please check the connection between the power adaptor and the power socket and check the power switch is on or not.

2. Question: Why the ADSL will always lose the line?

Answer: a. Please don't use the telephone directly through the separator and register one's residence on the line, the telephone should be answered after the separator.

b. Please don't use the outdated ISA net card, change into a PCI net card and upgrade the driver.

c. If still can't solve that please contact your operator to solve.

3. Question: Why my computer can't connect to Internet?

Answer: a. the reliable connection of the circuit, please guarantee to connect and insert stabilizing.

b. Please confirm that VPI/VCI set up and keep the same with information that DSL operator offers.

c. Please enter the Username/Password correctly.

d. Please try to login in a lot of websites in order to confirm that isn't caused by a server trouble of one website.