

**Texas Instruments Software**

## **Network Support Package**

---

# **Residential Gateway User Guide**

Applies to Product Release: 3.7.1  
Publication Number: NSP-001584/Revision: A  
Publication Date: May 2006



---

Texas Instruments Incorporated  
20450 Century Boulevard  
Germantown, MD 20874 USA

---

## Copyright and Contact Information

---

### Document Copyright

Publication Title: Residential Gateway User Guide

Publication Number: NSP-001584

Revision: A

© 1998-2006 Texas Instruments Incorporated

All Rights Reserved. Reproduction, adaptation, or translation without prior written permission is prohibited, except as allowed under the copyright laws.

### Software Copyright

Product Name: Network Support Package

Product Release: 3.7.1

© 1998-2006 Texas Instruments Incorporated

All Rights Reserved.

## Notices and Trademarks

---

### Important Notice

Texas Instruments Incorporated reserves the right to make changes to its products or discontinue any product or service without notice, and to advise customers to obtain the latest version of relevant information to verify, before placing orders, that the information being relied upon is current and complete. All products are sold subject to the terms and conditions of sale supplied at the time of order acknowledgement, including those pertaining to warranty, patent infringement, and limitation of liability.

Customers are responsible for their applications using Texas Instruments Software.

### Notice of Proprietary Information

Information contained herein is subject to the terms of the Non-disclosure Agreement between Texas Instruments Incorporated and your company, and is of a highly sensitive nature and is confidential and proprietary to Texas Instruments Incorporated. It shall not be distributed, reproduced or disclosed orally or in written form, in whole or in part, to any party other than the direct recipients without the express written consent of Texas Instruments Incorporated.

Telogy Software, VLYNQ, PIQUA, wONE, PBCC, Uni-DSL, Dynamic Adaptive Equalization, TurboDSL Packet Accelerator, interOps Test Labs, TurboDOX, and INCA are trademarks of Texas Instruments Incorporated.

All other brand names and trademarks mentioned in this document are the property of Texas Instruments Incorporated or their respective owners, as applicable.





---

---

# Preface

---

---

## About This Manual

The Residential Gateway User Guide is a task-oriented document that contains procedures for configuring DSL and wireless LAN using the RG Web GUI.

The manual contains information that will be of interest to engineers and product managers of ODM/OEMs, TI's residential gateway (RG) customers.

## How to Use This Manual

This manual is organized as follows:

Chapter	Contents
Chapter 1 " <a href="#">Residential Gateway Overview</a> " on page 1-1	Provides an introduction to RG features and instructions on how to install and set up an RG platform.
Chapter 2 " <a href="#">Setup</a> " on page 2-1	Describes how to configure WAN and LAN on the RG.
Chapter 3 " <a href="#">Advanced</a> " on page 3-1	Describes the advanced features of the RG and provides instructions on how to enable/disable each feature.
Chapter 4 " <a href="#">Wireless LAN (WLAN)</a> " on page 4-1	Describes the WLAN features of the RG and how to configure the RG as an access point.
Chapter 5 " <a href="#">Tools</a> " on page 5-1	Describes the command, management, and debugging tools the RG offers and explains how to use them.
Chapter 6 " <a href="#">Status</a> " on page 6-1	Provides network connection status, statistics, and log information of the RG.

## Document Conventions

This document uses the following conventions:

- Commands and keywords are in **boldface** font.
- Arguments for which you supply values are in *italic* font.
- Terminal sessions and information the system displays are in screen font.
- Information you must enter is in **boldface screen font**.
- Elements in square brackets ([ ]) are optional.

Notes use the following conventions:



**Note**—Means reader take note. Notes contain helpful suggestions or references to material not covered in the publication.

---

The information in a caution or a warning is provided for your protection. Please read each caution and warning carefully.



**CAUTION**—Indicates the possibility of service interruption if precautions are not taken.

---



**WARNING**—Indicates the possibility of damage to equipment if precautions are not taken.

---

## Related Documents from Texas Instruments

- *Quick Start Guide*
- *NMM Command Reference Manual*
- *XML Provisioning Developer Guide*
- *AP-DK Web-based Configuration Utility User's Guides*



# Document Revision History

---

---

---

Release	Chapter	Description of Change
3.7.1	Setup	<ul style="list-style-type: none"><li>Deleted CDVT field from PPPoE, PPPoA, Static, DHCP, Bridge, and CLIP Connection Setup pages.</li><li>Added data flow diagrams for PPPoE, PPPoA, Static, DHCP, Bridge, and CLIP Connections.</li><li>Added DHCP server data flow diagram.</li></ul>
	Advanced	<ul style="list-style-type: none"><li>Added UPnP data flow diagram.</li><li>Added SNTP client functionality diagram.</li><li>Added IGMP proxy data flow diagram.</li><li>Changed the Policy Routing page name to Policy Database. Added source and destination port ranges to the Policy Database page.</li></ul>
	WLAN	<ul style="list-style-type: none"><li>Deleted VLAN ID field on the Wireless Setup page.</li><li>Deleted VLAN ID and added Hide this SSID field on the Multiple SSID page.</li><li>Added Select an SSID field on the Wireless Management page to allow one access list created for each SSID.</li><li>Changed default value of Radio Calibration Interval field on the Wireless Advanced page.</li></ul>
	Status	<ul style="list-style-type: none"><li>Added QoS - TCA NTCA Status page.</li><li>Changed Product Information page to show multiple DSL MAC addresses.</li></ul>

Release	Chapter	Description of Change
3.7.0	Setup	Added 2.3.7 <a href="#">"Two-Step PVC"</a> on page 2-32
		Updated 2.3.10 <a href="#">"Modem Setup"</a> on page 2-34
		Updated Table 2-1 <a href="#">"PPP Settings Field Descriptions"</a> on page 2-9
	Advanced	Added 3.6 <a href="#">"TR-069"</a> on page 3-14
		Added 3.11 <a href="#">"TR-068 WAN Access"</a> on page 3-32
		Added 3.14 <a href="#">"Dynamic DNS Client"</a> on page 3-37
		Deleted IP QoS Page
		Added 3.18 <a href="#">"QoS"</a> on page 3-52, which includes: <ul style="list-style-type: none"> <li>• 3.18.1 <a href="#">"Ingress"</a> on page 3-55</li> <li>• 3.18.2 <a href="#">"Egress"</a> on page 3-66</li> <li>• 3.18.3 <a href="#">"WLAN QoS Support"</a> on page 3-69</li> <li>• 3.18.4 <a href="#">"Shaper"</a> on page 3-69</li> </ul>
		Added 3.19 <a href="#">"Policy Database"</a> on page 3-74
		Added 3.22 <a href="#">"Voice Provision"</a> on page 3-86
	WLAN	Deleted WLAN QoS
Tools	Updated 5.6 <a href="#">"Update Gateway Page"</a> on page 5-8	
3.6.1	Setup	Updated 2.3.10 <a href="#">"Modem Setup"</a> on page 2-34
		Updated 2.4.1 <a href="#">"LAN Configuration"</a> on page 2-37
	Advanced	Deleted <a href="#">"Voice"</a>
		Added 3.15 <a href="#">"IGMP Proxy Page"</a> on page 3-39
		Deleted <a href="#">"Multicast"</a>
	WLAN	Added 4.4 <a href="#">"Multiple SSID"</a> on page 4-9
		Added 4.7 <a href="#">"WDS"</a> on page 4-18
		Updated 4.3 <a href="#">"Wireless Configuration Page"</a> on page 4-7
		Updated 4.5 <a href="#">"Wireless Security Page"</a> on page 4-11
	Status	Updated 4.6 <a href="#">"Wireless Management"</a> on page 4-16
Added 6.10 <a href="#">"WDS Report"</a> on page 6-14		
3.6.0C	All	First issue



# Contents

---

<i>Copyright and Contact Information</i> .....	ø-ii
<i>Notices and Trademarks</i> .....	ø-iii
<i>Preface</i> .....	ø-v
<i>About This Manual</i> .....	ø-v
<i>How to Use This Manual</i> .....	ø-v
<i>Document Conventions</i> .....	ø-vi
<i>Related Documents from Texas Instruments</i> .....	ø-vi
<i>Document Revision History</i> .....	ø-vii
<i>List of Figures</i> .....	ø-xiii
<i>List of Tables</i> .....	ø-xvii
<i>List of Procedures</i> .....	ø-xix

## Chapter 1

---

<i>Residential Gateway Overview</i> .....	1-1
1.1 Introduction .....	1-2
1.1.1 Features .....	1-2
1.2 Your Residential Gateway at a Glance .....	1-4
1.2.1 Ports and Buttons .....	1-4
1.2.2 LED Descriptions .....	1-4
1.2.3 LED States .....	1-5
1.3 Installing your Residential Gateway .....	1-6
1.4 Setting up your Residential Gateway .....	1-7
1.4.1 Log in to your Residential Gateway .....	1-7
1.4.2 Home Page .....	1-8

## Chapter 2

---

<i>Setup</i> .....	2-1
2.1 Main Setup Page .....	2-2
2.1.1 Wide Area Network Connection .....	2-2
2.1.2 Local Area Network Connection .....	2-2
2.2 Configuring the WAN .....	2-3
2.3 Set up a WAN Connection .....	2-4
2.3.1 PPPoE Connection Setup .....	2-4
2.3.2 PPPoA Connection Setup .....	2-13
2.3.3 Static Connection Setup .....	2-18
2.3.4 DHCP Connection Setup .....	2-22
2.3.5 Bridged Connection Setup .....	2-25
2.3.6 CLIP Connection Setup .....	2-29
2.3.7 Two-Step PVC .....	2-32
2.3.8 Modify an Existing Connection .....	2-33

2.3.9 Delete an Existing Connection .....	2-33
2.3.10 Modem Setup .....	2-34
2.3.11 Multi Mac Support.....	2-35
2.4 LAN Setup .....	2-37
2.4.1 LAN Configuration.....	2-37
2.4.2 Ethernet Switch Configuration .....	2-46
2.5 Hidden Page .....	2-48
2.6 Log Out Page.....	2-49

## Chapter 3

<i>Advanced</i> .....	3-1
3.1 Advanced Tab Main Page .....	3-2
3.2 Voice Page .....	3-4
3.3 UPnP Page .....	3-6
3.4 SNTP Page .....	3-8
3.5 SNMP Page.....	3-11
3.6 TR-069 .....	3-14
3.7 Port Forwarding Page .....	3-16
3.7.1 DMZ Settings Page .....	3-20
3.7.2 Custom Port Forwarding Page .....	3-21
3.8 IP Filters Page .....	3-24
3.8.1 Custom IP Filters Page .....	3-26
3.9 LAN Clients Page .....	3-28
3.10 LAN Isolation Page .....	3-31
3.11 TR-068 WAN Access .....	3-32
3.12 Bridge Filters Page .....	3-34
3.13 Web Filters Page .....	3-36
3.14 Dynamic DNS Client.....	3-37
3.15 IGMP Proxy Page .....	3-39
3.15.1 Configure a WAN Interface as the Upstream IGMP Proxy:.....	3-41
3.15.2 Configure a LAN interface as the Upstream Interface.....	3-43
3.16 Static Routing Page .....	3-45
3.17 Dynamic Routing Page .....	3-48
3.18 QoS.....	3-52
3.18.1 Ingress.....	3-55
3.18.2 Egress.....	3-66
3.18.3 WLAN QoS Support.....	3-69
3.18.4 Shaper .....	3-69
3.19 Policy Database .....	3-74
3.20 Web Access Control Page.....	3-81
3.21 SSH Access Control Page .....	3-83

3.22 Voice Provision.....	3-86
3.22.1 Voice Parameters Page .....	3-87

**Chapter 4**

<i>Wireless LAN (WLAN)</i> .....	4-1
4.1 Wireless Main Page.....	4-2
4.2 Wireless Setup Page .....	4-3
4.2.1 User Isolation.....	4-4
4.2.2 Save Your Changes .....	4-5
4.3 Wireless Configuration Page .....	4-7
4.4 Multiple SSID.....	4-9
4.5 Wireless Security Page.....	4-11
4.5.1 Wireless Security - WEP .....	4-11
4.5.2 Wireless Security - 802.1x .....	4-13
4.5.3 Wireless Security - WPA .....	4-14
4.6 Wireless Management.....	4-16
4.6.1 Access List.....	4-16
4.6.2 Associated Stations .....	4-17
4.7 WDS .....	4-18
4.8 Wireless Statistics Page .....	4-20
4.9 Hidden Pages .....	4-21
4.9.1 Wireless Production 1.....	4-21
4.9.2 Wireless Channel Range .....	4-22
4.9.3 Wireless Production 2.....	4-23
4.9.4 Wireless Advanced.....	4-24

**Chapter 5**

<i>Tools</i> .....	5-1
5.1 Tools Main Page.....	5-2
5.2 System Commands Page .....	5-3
5.3 Remote Log - Router Page .....	5-4
5.4 Remote Log - Voice Page .....	5-6
5.5 User Management Page .....	5-7
5.6 Update Gateway Page.....	5-8
5.7 Ping Test Page .....	5-11
5.8 Modem Test Page .....	5-13
5.9 Hidden Pages .....	5-16
5.9.1 Gateway System Information Page .....	5-16
5.9.2 Remote Log Settings Page .....	5-17

**Chapter 6**

---

<i>Status</i>	6-1
6.1 Status Main Page .....	6-2
6.2 Network Statistics Page.....	6-3
6.3 Connection Status Page .....	6-6
6.4 DDNS Update Status.....	6-7
6.5 DHCP Clients Page .....	6-9
6.6 QoS - TCA NTCA Status Page.....	6-10
6.7 Modem Status Page .....	6-11
6.8 Product Information Page .....	6-12
6.9 System Log Page .....	6-13
6.10 WDS Report.....	6-14

**Appendix A**

---

<i>Acronyms</i>	A-1
-----------------	-----

---

## List of Figures

---

Figure 1-1	Log In Page . . . . .	1-7
Figure 1-2	Home Page . . . . .	1-9
Figure 2-1	Main Setup Page . . . . .	2-2
Figure 2-2	PPPoE Data Flow . . . . .	2-4
Figure 2-3	PPPoE Encapsulation Diagram . . . . .	2-5
Figure 2-4	PPPoE Packet Encapsulation Diagram . . . . .	2-5
Figure 2-5	New Connection Setup - PPPoE . . . . .	2-6
Figure 2-6	WAN Connection Setup - PPPoE1 . . . . .	2-7
Figure 2-7	System Commands . . . . .	2-8
Figure 2-8	Status - Connection Status . . . . .	2-8
Figure 2-9	PPPoA Data Flow . . . . .	2-13
Figure 2-10	PPPoA Encapsulation Diagram . . . . .	2-13
Figure 2-11	PPPoA Packet Encapsulation Diagram . . . . .	2-14
Figure 2-12	PPPoA Connection Setup . . . . .	2-14
Figure 2-13	WAN Connection Setup - PPPoA1 . . . . .	2-16
Figure 2-14	Static Data Flow . . . . .	2-18
Figure 2-15	Static Connection Encapsulation Diagram . . . . .	2-19
Figure 2-16	Static Connection Setup . . . . .	2-19
Figure 2-17	WAN Connection Setup - Static1 . . . . .	2-20
Figure 2-18	DHCP Data Flow . . . . .	2-22
Figure 2-19	DHCP Encapsulation Diagram . . . . .	2-22
Figure 2-20	DHCP - Voice Connection Setup . . . . .	2-23
Figure 2-21	WAN Connection Setup - DHCP1 . . . . .	2-24
Figure 2-22	Bridge Data Flow . . . . .	2-25
Figure 2-23	Bridged Connection Setup . . . . .	2-26
Figure 2-24	Bridged Connection Encapsulation Diagram . . . . .	2-26
Figure 2-25	WAN Connection Setup - Bridge1 . . . . .	2-27
Figure 2-26	Static Data Flow . . . . .	2-29
Figure 2-27	CLIP Connection Setup . . . . .	2-29
Figure 2-28	WAN Connection Setup - CLIP1 . . . . .	2-31
Figure 2-29	Two Step PVC Page . . . . .	2-32
Figure 2-30	Modem Setup Page . . . . .	2-35
Figure 2-31	LAN Configuration 1 (Default) . . . . .	2-37
Figure 2-32	RG Routing - LAN Groups (A) . . . . .	2-38
Figure 2-33	LAN Configuration 2 . . . . .	2-39
Figure 2-34	RG Routing - LAN Groups (B) . . . . .	2-39
Figure 2-35	LAN Configuration 3 . . . . .	2-40
Figure 2-36	GRG Routing - LAN Groups (C) . . . . .	2-41
Figure 2-37	LAN Group Configuration Page . . . . .	2-42
Figure 2-38	DHCP Server Data Flow . . . . .	2-44
Figure 2-39	Example of a DHCP Relay configuration . . . . .	2-44
Figure 2-40	External DHCP Options . . . . .	2-45
Figure 2-41	Ethernet Switch Configuration . . . . .	2-47
Figure 2-42	Firewall/NAT Services . . . . .	2-48

---

Figure 2-43	Log Out Page .....	2-49
Figure 3-1	Advanced Main (on AR7VW Platform).....	3-3
Figure 3-2	Voice Page .....	3-4
Figure 3-3	UPnP Data Flow.....	3-6
Figure 3-4	UPnP Page.....	3-7
Figure 3-5	SNTP Client Functionality .....	3-8
Figure 3-6	SNTP Page.....	3-8
Figure 3-7	SNMP Agent Diagram.....	3-11
Figure 3-8	SNMP Management.....	3-11
Figure 3-9	TR-069 Page .....	3-14
Figure 3-10	Port Forwarding Page.....	3-16
Figure 3-11	Port Forwarding - View An Existing Rule .....	3-18
Figure 3-12	Port Forwarding - User Category .....	3-18
Figure 3-13	Rule Management .....	3-19
Figure 3-14	Port Forwarding - DMZ Settings Page.....	3-20
Figure 3-15	Custom Port Forwarding Page.....	3-22
Figure 3-16	IP Filters Page.....	3-24
Figure 3-17	IP Filters - User Category .....	3-25
Figure 3-18	Custom IP Filters.....	3-27
Figure 3-19	LAN Clients .....	3-28
Figure 3-20	LAN Clients with Dynamic Address .....	3-29
Figure 3-21	LAN Clients with Static Address .....	3-29
Figure 3-22	LAN Isolation .....	3-31
Figure 3-23	TR-068 WAN Access Page .....	3-32
Figure 3-24	Bridge Filters Page.....	3-34
Figure 3-25	Web Filters Page .....	3-36
Figure 3-26	Dynamic DNS Client .....	3-37
Figure 3-27	IGMP Proxy Data Flow.....	3-40
Figure 3-28	IGMP Proxy Page.....	3-40
Figure 3-29	Enable IGMP Proxy: WAN = Upstream.....	3-41
Figure 3-30	IGMP Proxy Page (WAN = Upstream) .....	3-42
Figure 3-31	Enable IGMP Proxy: LAN = Upstream .....	3-43
Figure 3-32	IGMP Proxy Page (LAN = Upstream) .....	3-44
Figure 3-33	Static Routing Page (Default).....	3-45
Figure 3-34	Static Routing - LAN with Subnet .....	3-46
Figure 3-35	Static Routing (with One Entry).....	3-47
Figure 3-36	Dynamic Routing Page.....	3-48
Figure 3-37	Dynamic Routing - LAN with Subnets.....	3-50
Figure 3-38	QoS Network .....	3-52
Figure 3-39	QoS Flow Diagram.....	3-54
Figure 3-40	Ingress Page - Untrusted .....	3-55
Figure 3-41	Ingress Page - Layer 2 .....	3-56
Figure 3-42	Ingress Page - Layer 3 .....	3-58
Figure 3-43	Ingress Page - Static.....	3-60
Figure 3-44	Policy Database Page - Ingress Payload Database Configuration.....	3-61
Figure 3-45	Ingress Payload Database Configuration Example 1 .....	3-64

Figure 3-46	Ingress Payload Database Rule 1 .....	3-65
Figure 3-47	Egress Page - No Egress .....	3-66
Figure 3-48	Egress Page - Layer2 .....	3-67
Figure 3-49	Egress Page - Layer 3.....	3-68
Figure 3-50	Shaper Page .....	3-70
Figure 3-51	Shaper Page - HTD Queue Discipline Enabled.....	3-71
Figure 3-52	Shaper Page - Low Latency Queue Discipline Enabled.....	3-72
Figure 3-53	Shaper Page - PRIOWRR Enabled .....	3-73
Figure 3-54	Policy Database Configuration Page.....	3-74
Figure 3-55	Policy Routing Configuration Example 1 .....	3-76
Figure 3-56	Policy Database Rule 1 .....	3-78
Figure 3-57	Policy Routing Configuration Example 2 .....	3-79
Figure 3-58	Policy Routing Configuration Example 3 .....	3-79
Figure 3-59	Web Access Control Page .....	3-81
Figure 3-60	SSH Access Control Page.....	3-83
Figure 61	Create New SSH Connection Using Tera term .....	3-84
Figure 3-62	Voice Provision Page.....	3-86
Figure 3-63	Voice Parameters Page (SIP Build) .....	3-87
Figure 3-64	Voice Parameters Page (MGCP Build) .....	3-88
Figure 4-1	Wireless Main.....	4-2
Figure 4-2	Wireless Setup Page .....	4-3
Figure 4-3	User Isolation .....	4-5
Figure 4-4	Wireless Configuration Page .....	4-7
Figure 4-5	Configure Multiple SSID (Default).....	4-9
Figure 4-6	Configure Multiple SSID (New) .....	4-10
Figure 4-7	Wireless Security - None.....	4-11
Figure 4-8	Wireless Security Page- WEP.....	4-12
Figure 4-9	Wireless Security - 802.1x .....	4-14
Figure 4-10	Wireless Security - WPA .....	4-15
Figure 4-11	Wireless Management - Access List.....	4-16
Figure 4-12	Wireless Management - Associated Stations .....	4-17
Figure 4-13	WDS.....	4-18
Figure 4-14	Network Statistics Page - Wireless .....	4-20
Figure 4-15	Wireless Hidden 1.....	4-21
Figure 4-16	Wireless Channel Range.....	4-23
Figure 4-17	Wireless Production 2.....	4-24
Figure 4-18	Wireless Advanced.....	4-25
Figure 5-1	Tools Main Page .....	5-2
Figure 5-2	System Commands Page (Admin and user) .....	5-3
Figure 5-3	System Commands Page (router).....	5-3
Figure 5-4	Remote Log Page.....	5-4
Figure 5-5	Remote Log - Voice Settings Page .....	5-6
Figure 5-6	User Management Page.....	5-7
Figure 5-7	Update Gateway Page .....	5-8
Figure 5-8	Update Gateway - Restarting Page .....	5-9
Figure 5-9	Ping Test Page.....	5-11

List of Figures

---

Figure 5-10	Modem Test Page.....	5-14
Figure 5-11	Gateway System Information Page .....	5-17
Figure 5-12	Remote Log Settings Page .....	5-18
Figure 6-1	Status Main Page .....	6-2
Figure 6-2	Network Statistics Page - Ethernet.....	6-3
Figure 6-3	Network Statistics Page - USB .....	6-4
Figure 6-4	Network Statistics Page - DSL.....	6-4
Figure 6-5	Network Statistics Page - WLAN .....	6-5
Figure 6-6	Connection Status Page.....	6-6
Figure 6-7	DDNS Status Page (DDNS Client Disabled).....	6-7
Figure 6-8	DDNS Status Page (DDNS Client Enabled).....	6-8
Figure 6-9	DHCP Clients Page.....	6-9
Figure 6-10	QoS TCA NTCA Status Page.....	6-10
Figure 6-11	Modem Status .....	6-11
Figure 6-12	Product Information Page.....	6-12
Figure 6-13	System Log Page .....	6-13
Figure 6-14	WDS Report .....	6-14



---

**List of Tables**


---

Table 1-1	AR7 RG LED States .....	1-5
Table 2-1	PPP Settings Field Descriptions .....	2-9
Table 2-2	VLAN Settings Field Descriptions .....	2-11
Table 2-3	PVC Settings Field Descriptions .....	2-11
Table 2-4	PPPoA Settings Field Descriptions .....	2-17
Table 2-5	Static Settings Field Descriptions .....	2-21
Table 2-6	DHCP Settings Field Descriptions .....	2-25
Table 2-7	Bridge Settings Field Descriptions .....	2-28
Table 2-8	CLIP Settings Field Descriptions .....	2-31
Table 2-9	LAN Group Configuration Field Descriptions .....	2-42
Table 3-1	SNTP Field Descriptions .....	3-10
Table 3-2	SNMP Field Descriptions .....	3-12
Table 3-3	TR-069 Field Descriptions .....	3-15
Table 3-4	Port Forwarding Field Descriptions .....	3-16
Table 3-5	DMZ Field Descriptions .....	3-21
Table 3-6	Custom Port Forwarding Field Descriptions .....	3-22
Table 3-7	IP Filters Field Descriptions .....	3-24
Table 3-8	Custom IP Filters Field Descriptions .....	3-27
Table 3-9	LAN Clients Field Descriptions .....	3-30
Table 3-10	TR-068 WAN Access Field Descriptions .....	3-32
Table 3-11	Bridge Filters Field Descriptions .....	3-35
Table 3-12	Dynamic DNS Client Field Descriptions .....	3-38
Table 3-13	IGMP Proxy Field Descriptions .....	3-44
Table 3-14	Static Routing Field Descriptions .....	3-45
Table 3-15	Dynamic Routing Field Descriptions .....	3-49
Table 3-16	Ingress - Layer 2 Page Descriptions .....	3-56
Table 3-17	Ingress - Layer 3 Page Descriptions .....	3-58
Table 3-18	Policy Database Page QoS-related Field Descriptions .....	3-63
Table 3-19	Egress - Layer 2 Page Descriptions .....	3-67
Table 3-20	Egress - Layer 3 Page Descriptions .....	3-68
Table 3-21	WLAN QoS Settings .....	3-69
Table 3-22	Shaper Configuration Descriptions .....	3-70
Table 3-23	Policy Database Configuration Field Descriptions .....	3-74
Table 3-24	Web Access Control Field Descriptions .....	3-82
Table 3-25	SSH Access Control Field Descriptions .....	3-84
Table 3-26	Voice Provision Field Descriptions .....	3-86
Table 4-1	Wireless Setup Field Descriptions .....	4-3
Table 4-2	Configuration Field Descriptions .....	4-7
Table 4-3	Configure Multiple SSID Field Descriptions .....	4-10
Table 4-4	WEP Field Descriptions .....	4-13
Table 4-5	802.1 Field Descriptions .....	4-14
Table 4-6	WPA Field Descriptions .....	4-15
Table 4-7	WDS Field Descriptions .....	4-18
Table 4-8	Wireless Production 1 Field Descriptions .....	4-22

List of Tables

---

Table 4-9	Wireless Channel Range Field Descriptions .....	4-23
Table 4-10	Wireless Advanced Field Descriptions .....	4-26
Table 5-1	System Commands Field Descriptions .....	5-3
Table 5-2	Remote Log - Router Page Field Descriptions .....	5-5
Table 5-3	Remote Log - Voice Page Field Descriptions .....	5-6
Table 5-4	User Management Field Descriptions.....	5-7
Table 5-5	Ping Test Field Descriptions .....	5-12
Table 5-6	Modem Test Field Descriptions.....	5-14
Table 6-1	DDNS Status Field Descriptions .....	6-8

## List of Procedures

Procedure 1-1	Log In to the RG .....	1-7
Procedure 2-1	Configure Gateway for PPPoE .....	2-6
Procedure 2-2	Configure Gateway for PPPoA .....	2-15
Procedure 2-3	Configure Gateway for Static Connection .....	2-19
Procedure 2-4	Configure RG for DHCP .....	2-23
Procedure 2-5	Configure a Bridged Connection .....	2-26
Procedure 2-6	Configure Gateway for CLIP Connection .....	2-30
Procedure 2-7	Modify a WAN Connection .....	2-33
Procedure 2-8	Delete A WAN Connection .....	2-33
Procedure 2-9	LAN Configuration .....	2-38
Procedure 2-10	Log Out .....	2-49
Procedure 3-1	Configure UPnP .....	3-7
Procedure 3-2	Enable SNTP .....	3-9
Procedure 3-3	Configure TR-069 .....	3-15
Procedure 3-4	Configure Port Forwarding .....	3-17
Procedure 3-5	Enable DMZ .....	3-20
Procedure 3-6	Configure IP Filters .....	3-25
Procedure 3-7	Configure a LAN Client .....	3-28
Procedure 3-8	Configure LAN Isolation .....	3-31
Procedure 3-9	Create Temporary User Account (WAN-Side) .....	3-33
Procedure 3-10	Configure Bridge Filters .....	3-34
Procedure 3-11	Enable Dynamic DNS .....	3-37
Procedure 3-12	Enable IGMP Proxy - Configure WAN as Upstream Interface .....	3-42
Procedure 3-13	Enable IGMP Proxy - Configure a LAN Group as Upstream Interface .....	3-43
Procedure 3-14	Configure Static Routing .....	3-46
Procedure 3-15	Configure Dynamic Routing .....	3-50
Procedure 3-16	Ingress Layer 2 Priority Bits to CoS Configuration .....	3-56
Procedure 3-17	Ingress Layer 3 ToS to CoS Configuration .....	3-58
Procedure 3-18	Ingress Static Configuration .....	3-60
Procedure 3-19	Configure Ingress Payload Database .....	3-64
Procedure 3-20	Create PR rule .....	3-77
Procedure 3-21	Enable Web Access Control (WAN-Side) .....	3-81
Procedure 3-22	Enable SSH Access Control (WAN-Side) .....	3-83
Procedure 4-1	Save Your Changes .....	4-5
Procedure 4-2	Configure Multiple SSIDs .....	4-9
Procedure 4-3	Enable WEP .....	4-12
Procedure 4-4	Create an Access List .....	4-16
Procedure 4-5	Wireless Statistics .....	4-20
Procedure 5-1	Configure Remote Log Settings .....	5-4
Procedure 5-2	Update Gateway Firmware .....	5-8
Procedure 5-3	Perform a Ping Test .....	5-11
Procedure 5-4	Perform a Connectivity Test .....	5-14



# Residential Gateway Overview

---

---

---

The Residential Gateway Overview chapter discusses:

- ["Introduction"](#) on page 1-2
- ["Your Residential Gateway at a Glance"](#) on page 1-4
- ["Installing your Residential Gateway"](#) on page 1-6
- ["Setting up your Residential Gateway"](#) on page 1-7

## 1.1 Introduction

The AR7VW NSP 3.7.1 residential gateway (RG) is a high-speed WAN bridge/router that is specifically designed to connect to the Internet and to directly connect to your local area network (LAN) via universal serial bus (USB), wireless LAN (WLAN), or high speed 10/100 Mbps Ethernet. The RG also has full Network Address Translation (NAT) firewall, demilitarized zone (DMZ) services, and WLAN security support to block unwanted users from accessing your network. Quality of Service (QoS) and Policy routing (PR) are also supported.

The RG is fully compatible with PCs and Apple Macs. Voice is also supported and can be configured using the MXP command line interface, XML provisioning file, or through the webpage (limited options). The RG supports 802.11b/g and the following wireless security protocols: WEP, WPA, WPA2, and 802.1x.

### 1.1.1 Features

Here is a list of features the RG supports:

- Single, feature-reduced build in 2/8 memory footprint
- Enhanced QoS architecture (Ingress, Egress, Shaper) and Policy Routing
- IGMP over multiple PVC for video
- Secure HTTP server (HTTPS)
- PPP on-demand enhancement
- Routing (RIP v1/2, IGMP proxy, IP forwarding)
- WAN protocols (PPPoE, DHCP, StaticPPPoA, CLIP, Bridged)
- Address translation and security
  - NAT/NAPT
  - UPnP Internet gateway device (IGD)
  - Application Level Gateways (ALGs)
  - Stateful packet inspection (SPI) firewall
  - Protection against denial of service
  - Filtering
- Gateway services
  - DHCP client/server/relay
  - DNS relay/proxy
  - Dynamic DNS support
  - IGMP proxy

- Element management
  - Customer-extendible configuration manager
  - Web server and reference web pages
  - SNMP agent and standard MIB support
  - Partial support of DSL forum TR-069 (CPE WAN-side management)
  - Remote Management Clear EOC/PVC (China MII requirement)
  - Telnet, secure shell, TFTP, FTP
  - Industry-standard CLI and Linux shell
  - Diagnostics and test capabilities
- WLAN
  - Security (WEP, 802.1x, WPA, WPA2)
  - WDS
  - Multiple SSID
  - 802.11e/WMM

## 1.2 Your Residential Gateway at a Glance

Your RG has many ports, switches, and LEDs. The features are listed below.

### 1.2.1 Ports and Buttons

**Reset Button:** The **Reset** button is used to reset the RG. You may need to reset the RG if you lose network connectivity or you lose the ability to communicate with the RG via the web interface. To reset the RG, press the reset button and release. After about 30 seconds, the RG becomes operational again.

**Reset to Factory Defaults:** The **Reset to Factory Defaults** button resets the RG's configuration to its factory default settings and resets the RG. You may need to restore the RG to its factory default settings because:

- The configuration is changed.
- The software was upgraded.

If you lose the ability to communicate with the RG, you can restore the factory defaults of the RG by pressing the **Reset** button for more than 10 seconds. The RG resets to its factory defaults and after about 30 seconds the RG becomes operational again.

**LAN ports:** Connect to Ethernet network devices, such as a PC, hub, switch, or router. The RG comes with four LAN connections. Depending on the connection, you may need a cross-over cable or a straight-through cable to connect the RG to the LAN.

**Power:** Connect the AC power supply. Make sure to observe the proper power requirements. TI's AR7 RG reference designs require either 5 or 12 volts.

**USB:** Connects to a host's USB port. The RG supports both Windows-based PCs and Apple Macs via an RNDIS driver or CDC driver (included in the software).

**WAN Port:** This is the WAN interface that connects directly to your DSL line.

**Phone Port:** This allows a phone to directly connect to the RG. You do not need to add a splitter to your phone because the RG has an internal splitter.

### 1.2.2 LED Descriptions

**LAN Act/Link LED:** The LAN's **LINK** LED serves two purposes. If the LED is continuously lit, the Ethernet interface is successfully connected to a device through the Ethernet port. If the LED is flickering, it is an indication that there is connection activity.

**Power LED: On** indicates that the power is supplied to the RG.



**USB LED:** The **USB LED** serves two purposes. If the LED is continuously lit, the RG is successfully connected to a device through the port. If the LED is flickering, it is an indication that there is network activity.

**DSL LED:** The **DSL LED** serves two purposes:

- If the LED is continuously lit, the DSL is successfully connected.
- If the LED is flickering, it is an indication that the modem is training.

**PPPoE LED:** The **PPPoE LED** is off (or yellow) if no PPPoE connection is established or if the connection is not used. When the PPPoE LED is green, a PPPoE connection is established.

### 1.2.3 LED States

The LED states can help you diagnose problems with the gateway. The meaning of the RG's LED states is shown in Table 1-1 [Table 1-1](#).

**Table 1-1 AR7 RG LED States**

LED	Off	Green	Blinking	Yellow
<b>Power</b>	Power not applied	Normal operation	N/A	N/A
<b>DSL Sync</b>	Power not applied DSL line not connected	DSL line established	DSL line is training	N/A
<b>Ethernet Activity</b>	Power not applied Ethernet line not connected Wrong type of Ethernet cable used	Ethernet line is connected	Ethernet traffic is flowing	N/A
<b>USB</b>	Power not applied USB line not connected	USB line is connected	USB traffic is flowing	N/A
<b>PPPoE</b>	Power not applied No PPPoE link established	PPPoE link established	N/A	PPPoE link invalid
<b>End of Table 1-1</b>				

## 1.3 Installing your Residential Gateway

1. Locate the RG.
2. For connections to the Ethernet, DSL and USB interfaces, refer to the *Quick Start Guide*.
3. Connect the AC power adapter. Depending upon the type of network, you may want to put the power supply on an uninterruptible supply. Use only the power adapter supplied with the RG because different adapters may damage the product.

Now that the hardware installation is complete, continue on to set up your RG.

## 1.4 Setting up your Residential Gateway

This section guides you through configuring your RG. The RG is shipped with a standard default bridge configuration. Most users would want to change the RG from a bridge to a router.

Before setting up your RG, make sure you have followed the *Quick Start Guide*. You should have your computers configured for DHCP mode and have proxies disabled on your browser. If you access the router using your web browser and see a log-in redirection page instead of the Log In page, check your browser's settings to verify that JavaScript is enabled. Also, if you do not get the page shown in [Figure 1-1](#), you may need to delete your temporary Internet files by flushing the cached web pages.

### 1.4.1 Log in to your Residential Gateway

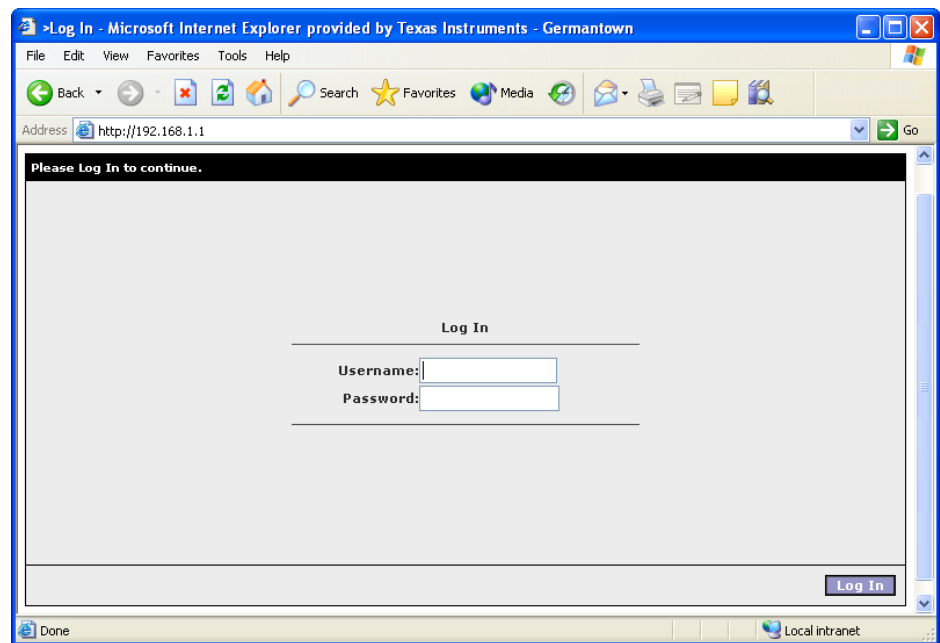
Use the following procedures to log in to your RG.

#### Procedure 1-1 Log In to the RG

##### Step – Action

- 1 Open your web browser.  
You may get an error message. This is normal. Continue on to the next step.
- 2 Type the default IP address of the RG **192.168.1.1** and press **Enter**.  
The **Log In** page appears ([Figure 1-1](#)).

**Figure 1-1 Log In Page**



**3** Enter the following information:

- **User Name:** Admin
- **Password:** Admin

**Note**—Both fields are case-sensitive. *Admin* is the default value.

**4** Click **Log In**.

The main page appears.

**Note**—The default login for **router** level access is: *router/router*. The default login for **user** level access is: *user/user*. By default, the **Admin** and **router** level accesses are enabled and the **user** level access is disabled (To learn how to enable it, refer to *XML Provisioning Developer Guide* for more information).

**Note**—The login name and password can be changed later on using the **Tools/User Management** menu options (refer to Chapter 5 “[User Management Page](#)” on page 5-7 for more information).

**End of Procedure 1-1**

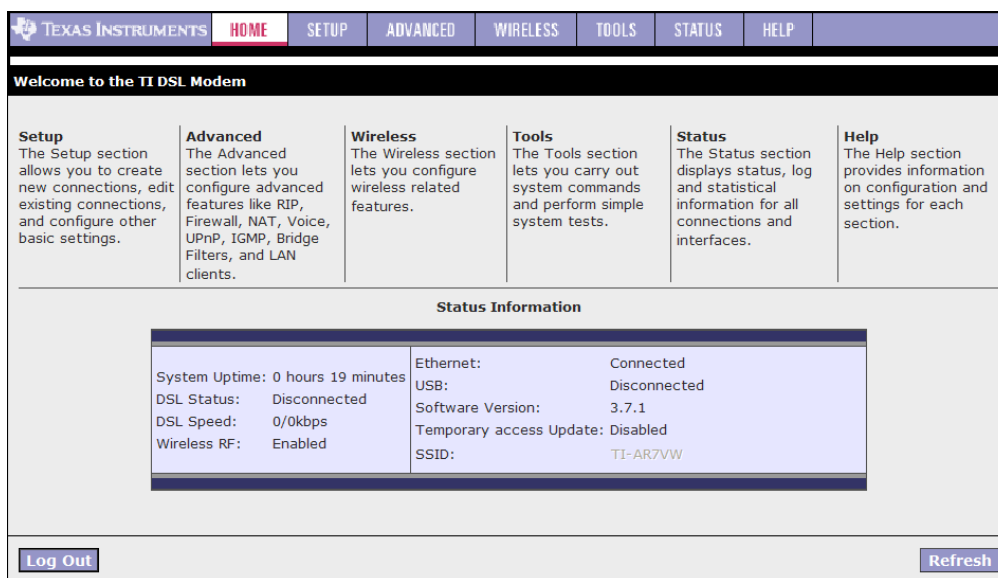
---

## 1.4.2 Home Page

The first page ([Figure 1-2](#)) is the **Home** page. From this page you can perform the following tasks:

- Setup the RG (configure the LAN and WAN connection(s)).
- Configure the advanced configuration options within the RG (security, routing, and filtering).
- Access tools that are helpful for debug purposes.
- Obtain the status of the RG.
- View the extensive online help.

Figure 1-2 Home Page



The basic layout of the **Home** page consists of a page selection list across the top of the browser window. The lower center part of the page displays the RG status, connection information, and other useful information. The center part of the display provides descriptions of the options supported on the other web interface pages.



# Setup

---

---

---

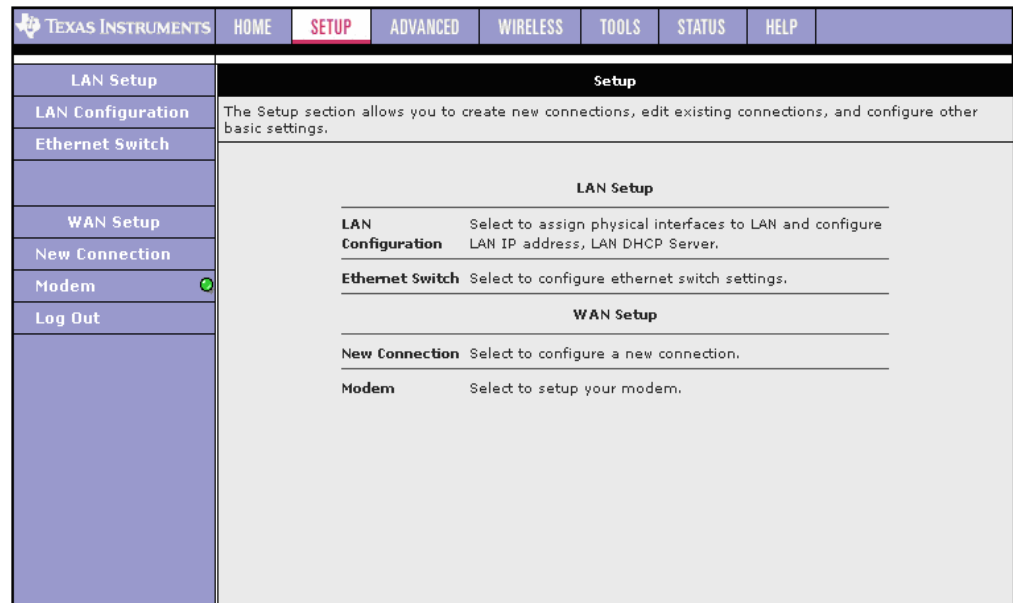
The **Setup** tab allows you to perform basic interface configuration functions. This chapter discusses:

- ["Main Setup Page"](#) on page 2-2
- ["Configuring the WAN"](#) on page 2-3
- ["Set up a WAN Connection"](#) on page 2-4
- ["LAN Setup"](#) on page 2-37
- ["Hidden Page"](#) on page 2-48
- ["Log Out Page"](#) on page 2-49

## 2.1 Main Setup Page

To set up your RG with a basic configuration, select **Setup** from the **Home** page. [Figure 2-1](#) shows the main **Setup** page. The page is divided into two subsections: WAN setup and LAN setup.

**Figure 2-1 Main Setup Page**



Before configuring the RG, there are several concepts that you should be familiar with to better understand how your new RG works. Please take a moment to familiarize yourself with the following concepts to make the configuration easier:

- WAN
- LAN

### 2.1.1 Wide Area Network Connection

On one side of the RG is the WAN interface, also referred to as a broadband connection. This WAN connection is different for every WAN service provider. Most of the configuration you perform is for the WAN connection.

### 2.1.2 Local Area Network Connection

On the other side of the RG are LAN interfaces. This is where local hosts are connected. The RG is normally configured to automatically provide all the hosts on the LAN network with IP addresses.



## 2.2 Configuring the WAN

Before the RG passes any data between the LAN interfaces and the WAN interface, the WAN side of the RG must be configured.

You need some (or all) of the information outlined below before you can properly configure the WAN:

- Your DSL line virtual path identifier (VPI) and virtual channel identifier (VCI)
- Your DSL encapsulation type and multiplexing
- Your DSL training mode (default is MultiMode)

For **PPPoA** or **PPPoE** users, you also need these values from your ISP:

- Your username and password

For **RFC 2684 Static** connections, you may need these values from your ISP:

- Your fixed WAN IP address
- Your subnet mask
- Your default gateway
- A set of three DNS IP addresses

Since multiple users can use the RG, the RG can simultaneously support multiple connection types; hence, you must set up different profiles for each connection. The RG supports the following protocols:

- RFC 2516 PPPoE
- RFC 2364 PPPoA
- RFC 2684 Static
- Dynamic host configuration protocol (DHCP)
- Bridged
- RFC 2225 classical IP over ATM (CLIP)

You can create up to eight WAN connections.

## 2.3 Set up a WAN Connection

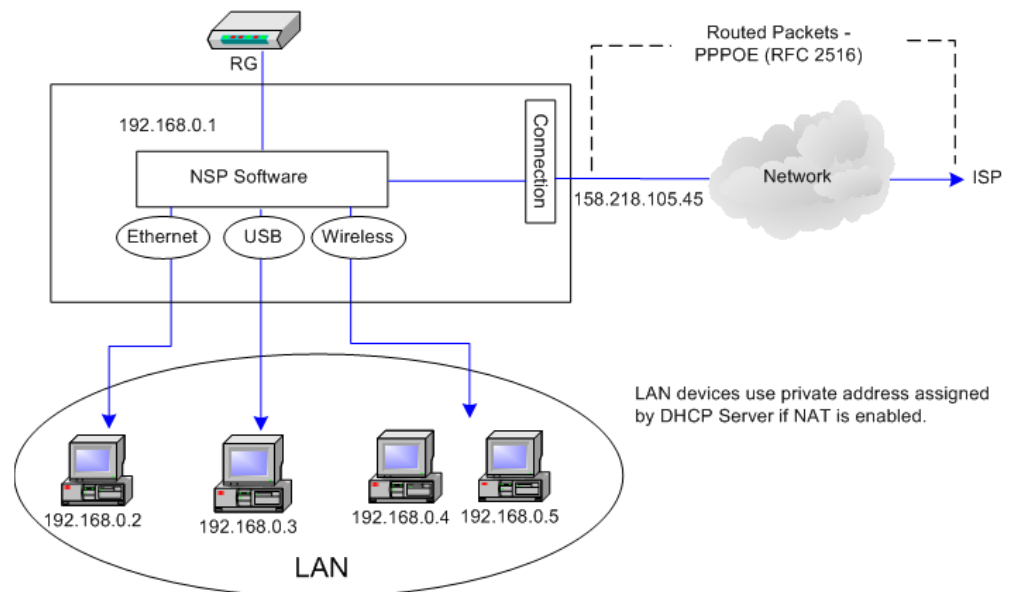
A new WAN connection is a virtual connection over the physical DSL connection. Your RG can support up to eight different (unique) virtual connections. If you have multiple different virtual connections, you may need to use the static and dynamic routing capabilities of the RG to pass data correctly.

Before you make a new WAN connection, you should make sure you have a DSL connection. There should be a green light next to the **Modem** link as shown in [Figure 2-3](#) on page 2-5.

### 2.3.1 PPPoE Connection Setup

PPP, or point-to-point protocol, is a method of establishing a network connection/session between network hosts. PPPoE is a protocol for encapsulating PPP frames in Ethernet frames and is described in RFC 2516. The data flow of a PPPoE connection is shown in [Figure 2-2](#).

**Figure 2-2 PPPoE Data Flow**



PPPoE provides the ability to connect to a network of hosts over a simple bridging access device to a remote access concentrator. With this model, each RG uses its own PPP stack. Access control, billing, and type of service control can all be done on a per-user rather than per-site basis.

The encapsulation of datagrams in a PPPoE connection is shown in [Figure 2-3](#).

**Figure 2-3 PPPoE Encapsulation Diagram**

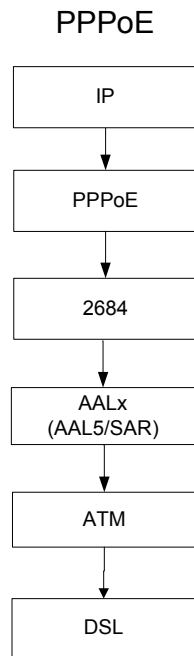


Figure 2-4 further shows the packet encapsulation and protocols used in a PPPoE connection with TCP as the transport protocol.

**Figure 2-4 PPPoE Packet Encapsulation Diagram**

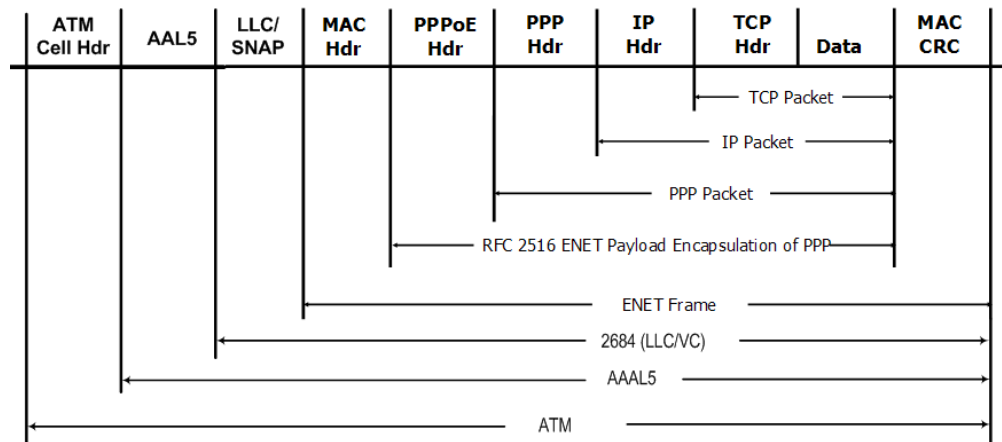


Figure 2-5 shows the default **New Connection Setup** page, which defaults to the **PPPoE Connection Setup** page. Notice this page can be logically divided into three sections. **Section A** includes settings specific to the connection type. **Section B** (VLAN settings) and **Section C** (PVC settings) remain the same for all six connection types. For other connection types, we will focus on the fields in **Section A**.

Figure 2-5 New Connection Setup - PPPoE

The screenshot shows the 'PPPoE Connection Setup' page. At the top, there is a navigation bar with 'TEXAS INSTRUMENTS', 'HOME', 'SETUP', 'ADVANCED', 'WIRELESS', 'TOOLS', 'STATUS', and 'HELP'. A left sidebar contains 'LAN Setup', 'LAN Configuration', 'WAN Setup', 'New Connection', 'Modem', and 'Log Out'. The main content area is titled 'PPPoE Connection Setup'. It features a 'Name' field, a 'Type' dropdown set to 'PPPoE', and a 'Sharing' dropdown set to 'Disable'. Below these are 'Options' for NAT and Firewall (both checked), 'VLAN ID' (0), and 'Priority Bits' (0). Section A, 'PPP Settings', includes 'Username' (username), 'Password' (masked), 'Idle Timeout' (60 secs), 'Keep Alive' (10 min), 'Authentication' (Auto selected), 'MTU' (1492 bytes), 'On Demand' (unchecked), 'Enforce MTU' (checked), 'PPP Unnumbered' (unchecked), 'Host Trigger' (unchecked), 'Default Gateway' (checked), and 'Debug' (unchecked). Section C, 'PVC Settings', includes 'PVC' (New), 'VPI' (0), 'VCI' (0), 'QoS' (UBR), 'PCR' (0 cps), 'SCR' (0 cps), 'MBS' (0 cells), and 'Auto PVC' (unchecked). At the bottom, there are 'Connect', 'Disconnect', 'Apply', 'Delete', and 'Cancel' buttons.

Use [Table 2-1](#) on page 2-9, [Table 2-2](#) on page 2-11, and [Table 2-3](#) on page 2-11 as references, and follow [Procedure 2-1](#) to configure a PPPoE connection.

### Procedure 2-1 Configure Gateway for PPPoE

#### Step – Action

- 1 At the **Setup** main page, click **New Connection**.

The default **PPPoE Connection Setup** page ([Figure 2-5](#) on page 2-6) is displayed.

- 2 In the **Name** field, enter a unique name for the PPPoE connection.

The name must not have spaces and cannot begin with numbers. In this example, the unique name is *PPPoE1*.

- 3 The **Network Address Translation** (NAT) and the **Firewall** options are enabled by default. Leave these in the default mode.

**Note**—NAT enables the IP address on the LAN side to be translated to IP address on the WAN side. If NAT is disabled, you cannot access the Internet.

- 4 If you want to enable VLAN, use [Table 2-2](#) on page 2-11 as a reference to configure the following fields:

- **Sharing:** Select VLAN to enable the **VLAN ID** and **Priority Bits** fields.
  - **VLAN ID:** Enter the VLAN ID.
  - **Priority Bits:** Select the priority bits of the VLAN.
- 5 In the **PPP Settings** section, enter values from DSL service provider or your ISP.
  - 6 In the **PVC Settings** section, enter values for the **VPI** and **VCI**.  
**Note**—Your DSL service provider or your ISP supplies these values. In this example, the DSL service provider is using 0,35.
  - 7 Select the **Quality of Service (QoS)**.  
Leave the default value if you are unsure or if the ISP did not provide this information.
  - 8 Click **Apply** to complete the connection setup. This temporarily activates this connection as shown in [Figure 2-6](#).

**Figure 2-6 WAN Connection Setup - PPPoE1**

The screenshot displays the 'PPPoE Connection Setup' configuration page. The interface includes a navigation menu on the left with options like LAN Setup, WAN Setup, and Modem. The main configuration area is divided into several sections:

- General Settings:** Name: PPPoE1, Type: PPPoE, Sharing: Disable.
- Options:** NAT and Firewall are checked. VLAN ID: 0, Priority Bits: 0.
- PPP Settings:** Username: username, Password: masked with dots, Idle Timeout: 60 secs, Keep Alive: 10 min, Authentication: Auto (selected), MTU: 1492 bytes.
- PVC Settings:** PVC: New, VPI: 0, VCI: 35, QoS: UBR, PCR: 0 cps, SCR: 0 cps, MBS: 0 cells, Auto PVC: unchecked.
- Advanced Options:** On Demand, Enforce MTU, PPP Unnumbered, Host Trigger, Default Gateway, Valid Rx, Debug, and LAN: LAN group 1.

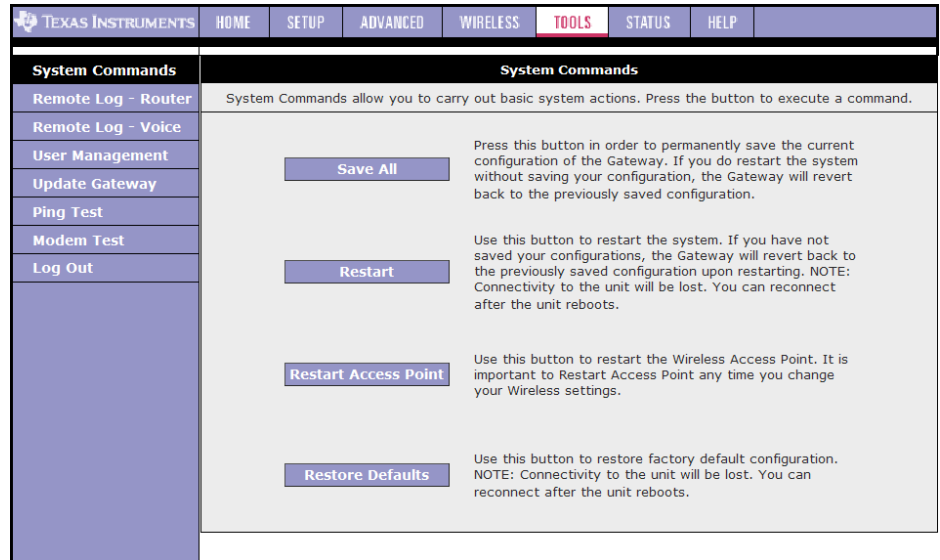
Buttons for 'Connect', 'Disconnect', 'Apply', 'Delete', and 'Cancel' are located at the bottom of the configuration area.

A new link is created for this connection in the left-hand column. You can connect, disconnect, apply, delete, or cancel this connection using the buttons at the bottom of this page.

**Note**—The changes take effect when you click **Apply**; however, if the RG configuration is not saved, these changes will be lost upon RG reboot.

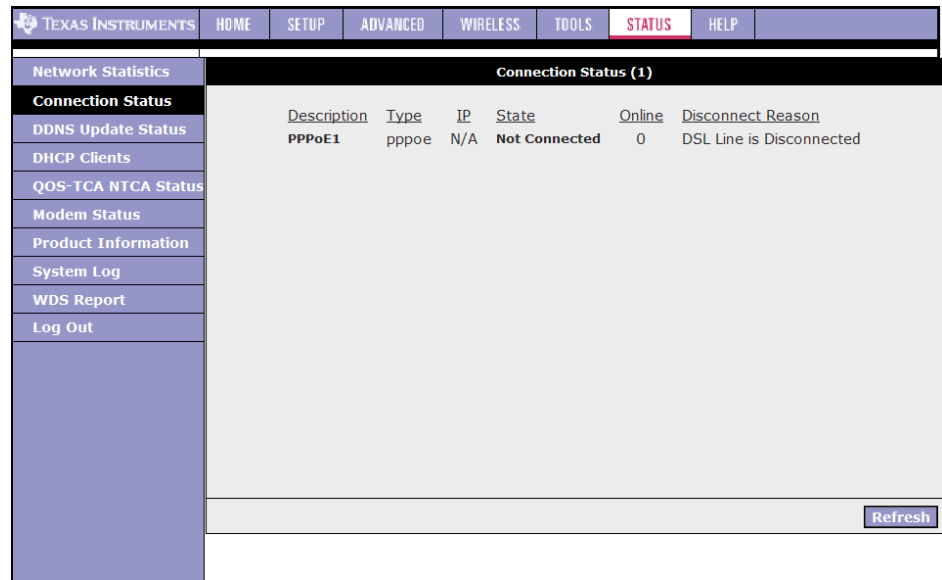
- 9 To make the change permanent, click **Tools** (at the top of the page) and select **System Commands**.

**Figure 2-7 System Commands**



- 10 On the **System Commands** page (Figure 2-7), click **Save All**.
- 11 To check the status, click **Status** (at the top of the page) and select **Connection Status**. Figure 2-8 shows the **Connection Status** page.

**Figure 2-8 Status - Connection Status**



**End of Procedure 2-1**

Table 2-1 describes the PPP settings options on the **PPPoE Connection Setup** page in Figure 2-5.

**Table 2-1 PPP Settings Field Descriptions**

Field	Definition/Description
Username	Your user name for the PPPoE access provided by your DSL service provider or your ISP. This field is alpha-numeric and the maximum length is 64 characters. It cannot start with a number. The character type restrictions do not apply for CLI-based configuration.
Password	Your password for the PPPoE access provided by your DSL service provider or your ISP. This field is alpha-numeric and the maximum length is 128 characters. The character type restrictions do not apply for CLI-based configuration.
Idle Timeout	Specifies that PPPoE connection should disconnect if the link has no activity detected for <i>n</i> seconds. This field is used in conjunction with the On-Demand feature and is enabled only when the <b>On Demand</b> field is checked. To ensure that the link is always active, enter a <i>0</i> in this field. You can also enter a value larger than <i>10 (secs)</i> .
Keep Alive	When the <b>On Demand</b> option is not enabled, this value specifies the time to wait without being connected to your provider before terminating the connection. To ensure that the link is always active, enter a <i>0</i> in this field. You can also enter any positive integer value in this field.
Authentication	Three authentication options are available: <ul style="list-style-type: none"> <li>• Auto</li> <li>• Challenge handshake authentication protocol (CHAP)</li> <li>• Password authentication protocol (PAP)</li> </ul> Microsoft CHAP v2 is also supported in the Auto and CHAP options. However, MS CHAP v1 is not supported.
MTU	Maximum transmit unit the DSL connection can transmit. It is a negotiated value that packets of no more than <i>n</i> bytes can be sent to the service provider. The PPPoE interface default MTU is <i>1492 (max)</i> and PPPoA default MTU is <i>1500 (max)</i> . The minimum MTU value is <i>64</i> .
On Demand	Enables On Demand mode. The connection disconnects if no activity is detected after the specified idle timeout value. When checked, this field enables the following fields: <ul style="list-style-type: none"> <li>• <b>Idle Timeout</b></li> <li>• <b>Host Trigger</b></li> <li>• <b>Valid Rx</b></li> </ul>
Default Gateway	If checked, this WAN connection acts as the default gateway to the Internet.
Enforce MTU	This feature is enabled by default. It forces all TCP traffic to conform with PPP MTU by changing TCP maximum segment size to PPP MTU. If it is disabled, you may have issues accessing some Internet sites.
Debug	Enables PPPoE connection debugging facilities. This option is used by ISP technical support and ODM/OEM testers to simulate packets going through the network from the WAN side.

**Table 2-1 PPP Settings Field Descriptions**

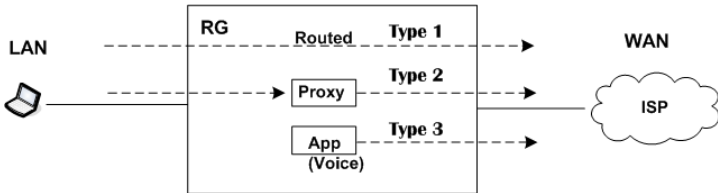
Field	Definition/Description
PPP Unnumbered	PPP Unnumbered is a special feature. It enables the ISP to designate a block of public IP addresses to the customer where it is statically assigned on the LAN side. PPP Unnumbered is, in essence, like a bridged connection.
LAN	The LAN field is associated with the PPP Unnumbered field and is enabled when the PPP Unnumbered field is checked. You can specify the LAN group the packets need to go to when the PPP Unnumbered feature is activated.
Host Trigger	<p>This field is used in conjunction with the On-Demand feature and is enabled only when the <b>On Demand</b> field is checked. There are three types of packets:</p>  <pre> graph LR     LAN[LAN] -- Type 1 (Routed) --&gt; WAN[WAN]     LAN -- Type 2 (Proxy) --&gt; RG[RG]     RG -- Type 2 (Proxy) --&gt; WAN     RG -- Type 3 (App Voice) --&gt; WAN     </pre> <ul style="list-style-type: none"> <li>LAN packets (type 1): packets routed through the RG from LAN to WAN.</li> <li>Proxied packets (type 2): packets generated by the RG after receiving packets from the LAN side, such as DNS proxy.</li> <li>Locally generated packets (type 3): Packets generated by the RG, such as Voice, SNMP, etc.</li> </ul> <p>When the On-Demand feature is enabled and Host Trigger is unchecked, only flow of type 1 packets keeps the link active, i.e., if the RG has not received type 1 packets for x amount of time (as specified in the <b>Time Out</b> field), the connection times out.</p> <p>If Host Trigger is checked, type 2 and type 3 packets can keep the link active as well. You can configure the packets using the <b>Trigger Traffic</b> page, which is accessed by clicking the <b>Configure</b> button next to <b>Host Trigger</b>. The following fields can be used to identify the traffic of type 2 and/or type 3 that will keep the link alive:</p> <ul style="list-style-type: none"> <li>Source Port (the character * is used to denote any port)</li> <li>Destination Port (the character * is used to denote any port)</li> <li>Protocol (TCP, UDP, ICMP, or Specify the protocol number)</li> </ul>
Valid Rx	<p>This field is used in conjunction with the On-Demand feature and is enabled only when the <b>On Demand</b> field is checked.</p> <p>When the <b>On-Demand</b> feature is enabled and <b>Valid Rx</b> is unchecked, only packets going from the LAN side to the WAN side keep the link active. After the RG times out, no packets can be received from the WAN side to the LAN side.</p> <p>When Valid Rx is checked, the incoming packets can keep the PPPoE WAN connection active. There is one condition though, this incoming packets should belong to a connection initiated from a LAN-side device.</p>
<b>End of Table 2-1</b>	



Table 2-2 describes the VLAN settings options.

**Table 2-2 VLAN Settings Field Descriptions**

Field	Definition/ Description
Sharing	The following options are available: <ul style="list-style-type: none"> <li>• <b>Disable:</b> Disables connection sharing.</li> <li>• <b>Enable:</b> Enables connection sharing.</li> <li>• <b>VLAN:</b> The <b>VLAN ID</b> and <b>Priority Bits</b> fields are activated when <b>VLAN</b> is selected, which enable you to create VLAN.</li> </ul>
VLAN ID	VLAN Identification. Multiple connections over the same PVC are supported, which requires the WAN network to have VLAN support and for the DSLAMS and Routers on the ISP to handle VLAN Tags.  Extended support is also available, which allows multiple connections to be placed over the single PVC without VLAN support (VLAN Tag of 0 is this special case). In this mode of operation, a received packet is flooded on all the connections that reside over it.
Priority Bits	Priority is given to a VLAN connection from 0-7. All packets sent over the VLAN connection have the Priority bits set to the configured value.
<b>End of Table 2-2</b>	

Table 2-3 describes the PVC Settings options.

**Table 2-3 PVC Settings Field Descriptions**

Field	Definition/ Description
PVC	Permanent virtual circuit. This is a fixed virtual circuit between two users. It is the public data network equivalent of a leased line. No call setup or clearing procedures are needed.
VPI	Virtual path identifier, equivalent to the virtual path connection (VPC).
VCI	Virtual channel identifier. A 16-bit field in the header of an ATM cell. The VCI, together with the VPI, is used to identify the next destination of a cell as it passes through to the ATM switch.
QoS	Quality of service, a characteristic of data transmission that measures how accurately and how quickly a message or data is transferred from a source host to a destination host over a network. The three QoS options are: <ul style="list-style-type: none"> <li>• <b>Undefined Bit Rate (UBR):</b> When UBR is selected, the PCR, SCR, and MBS fields are disabled.</li> <li>• <b>Constant Bit Rate (CBR):</b> When CBR is selected, the PCR field is enabled.</li> <li>• <b>Variable Bit Rate (VBR):</b> When VBR is selected, the PCR, SCR, and MBS fields are enabled.</li> </ul> More on QoS is covered in Chapter 3 “QoS” on page 3-52.
PCR	Peak cell rate, measured in cells/sec, is the cell rate which the source may never exceed.
SCR	Sustained cell rate, measured in cells/sec, is the average cell rate over the duration of the connection.

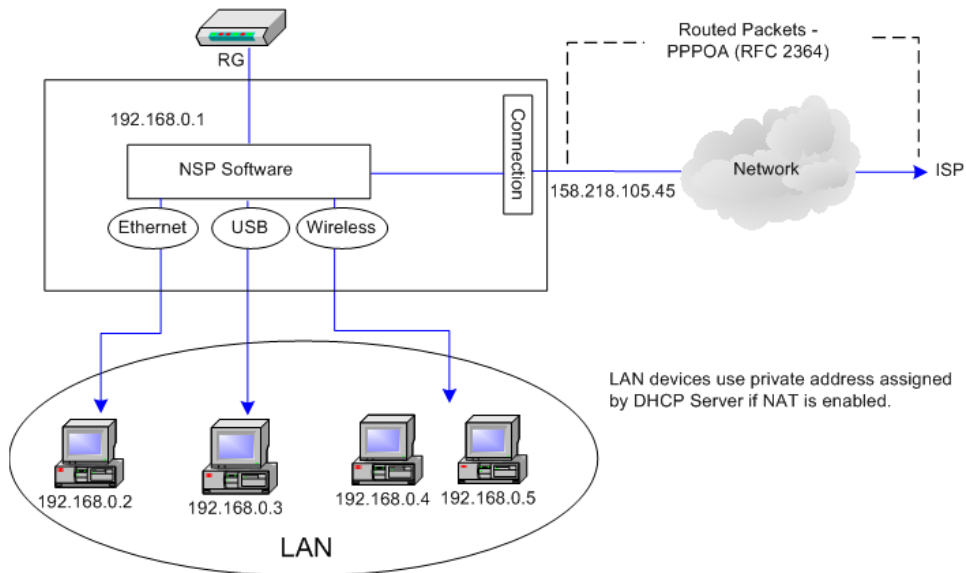
**Table 2-3 PVC Settings Field Descriptions**

Field	Definition/ Description
MBS	Maximum burst size, a traffic parameter that specifies the maximum number of cells that can be transmitted at the Peak Cell Rate.
Auto PVC	<p>Auto-Sensing permanent virtual circuit. The overall operation of the auto-sensing PVC feature relies on end-to-end OAM pings to defined PVCs. There are two groups of PVCs: customer default PVCs which are defined by the OEM/ISP and the backup PVCs. The customer default must have 0/35 as the first default PVC. The backup list of PVCs must be of the following VPI/VCI: 0/35, 8/35, 0/43, 0/51, 0/59, 8/43, 8/51, and 8/59. The list of PVCs are defined in XML and is configurable. The Auto-Sensing PVC feature itself is also configurable in that the auto-search mechanism can be disabled.</p> <p>Upon DSL synchronization, end-to-end OAM pings will be conducted for every defined PVCs. The result of the pings will be recorded in an array for later use to determine the usability of the particular PVC for connectivity. This list helps the PVC manage the available PVC for use, and needs to be synchronized with connections made without Auto-Sensing PVC. Update to this list is performed for any change in DSL synchronization.</p> <p>During connection establishment, the PVC module will first search through the list of defined default PVCs. If a PVC is found from the default list that is ping-able and not in use, the PVC module will update for that particular PVC as <i>in-use</i> from the list and continues processing. If a PVC is not found in the default, the backup PVC list is used. If no PVC is found again, the module will let the end-user know that no available VCC was found.</p> <p>With the connection established, the PVC is stored in flash as the connection default PVC. Therefore upon reboot, this PVC is automatically chosen as the PVC for that connection. This saved PVC in environment space of flash overrides the PVC connection saved in XML configuration space of flash for that connection. During the connection establishment processing, the saved PVC will be checked to see whether a connection can be made with the PVC. If the PVC is OAM ping-able, the connection process continues. If the PVC is not OAM ping-able, the search for an available PVC starts. The process of PVC selection is the same as described above.</p> <p>The list of default PVCs and backup PVCs need to be global for the management of all connections, non <i>Auto-Sensing PVC</i> connection, as well as, <i>Auto-Sensing PVC</i> connections. These lists allow the end-users to establish connectivity without keeping track of the PVC used.</p>
<b>End of Table 2-3</b>	

### 2.3.2 PPPoA Connection Setup

PPPoA is also known as RFC 2364. It is a method of encapsulating PPP packets in ATM cells that are carried over the DSL line. The data flow of a PPPoA connection is shown in Figure 2-9.

**Figure 2-9 PPPoA Data Flow**



PPP, or point-to-point protocol, is a method of establishing a network connection/session between network hosts. It usually provides a mechanism of authenticating users. Logical link control (LLC) and virtual circuit (VC) are two different methods of encapsulating the PPP packet. Contact your ISP to determine which encapsulation is being used on your DSL connection. The encapsulation of datagrams in a PPPoA connection is shown in Figure 2-10.

**Figure 2-10 PPPoA Encapsulation Diagram**

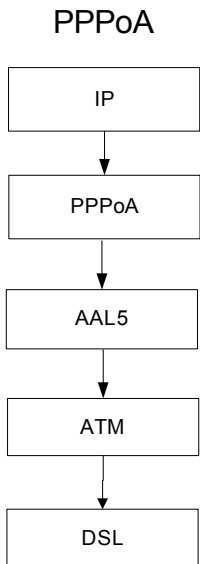


Figure 2-11 further shows the encapsulation and protocols used in a PPPoA connection with TCP as the transport protocol.

Figure 2-11 PPPoA Packet Encapsulation Diagram

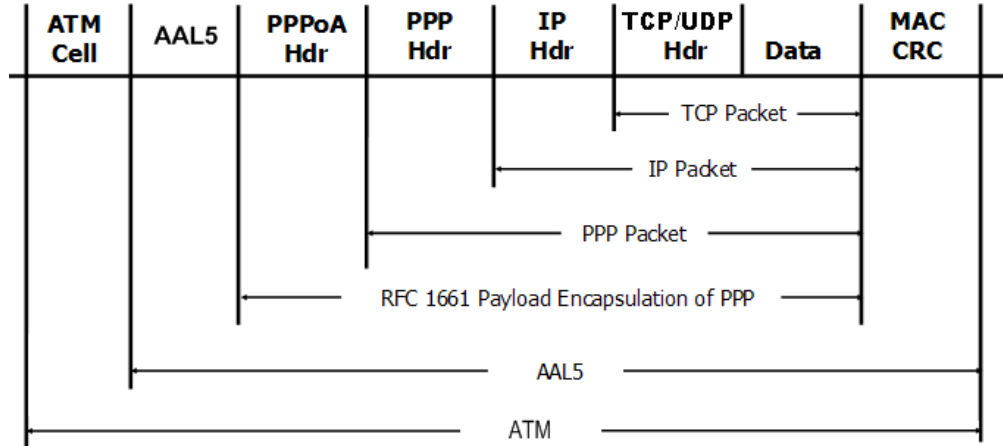


Figure 2-12 shows the default PPPoA Connection Setup page.

Figure 2-12 PPPoA Connection Setup

Navigation: TEXAS INSTRUMENTS | HOME | **SETUP** | ADVANCED | WIRELESS | TOOLS | STATUS | HELP

Left Menu: LAN Setup | LAN Configuration | WAN Setup | **New Connection** | Modem | Log Out

**PPPoA Connection Setup**

Name: [ ] Type: PPPoA Sharing: Disable

Options:  NAT  Firewall VLAN ID: 0 Priority Bits: 0

**PPP Settings**

Encapsulation:  LLC  VC

Username: username Password: [ ]

Idle Timeout: 60 secs Keep Alive: 10 min

Authentication:  Auto  CHAP  PAP

MTU: 1500 bytes

On Demand:  Default Gateway:  Debug:

PPP Unnumbered:  Valid Rx:  LAN: LAN group 1

Host Trigger:  **Configure**

**PVC Settings**

PVC: New VPI: 0 VCI: 0

QoS: UBR PCR: 0 cps SCR: 0 cps MBS: 0 cells Auto PVC:

Buttons: Connect Disconnect Apply Delete Cancel

Use [Table 2-4](#) on page 2-17, [Table 2-2](#) on page 2-11, and [Table 2-3](#) on page 2-11 as references, and follow [Procedure 2-2](#) to configure a PPPoA connection.

### Procedure 2-2 Configure Gateway for PPPoA

---

#### Step – Action

- 1** On the **Setup** main page, click **New Connection**.  
The default **PPPoE Connection Setup** page ([Figure 2-5](#) on page 2-6) is displayed.
- 2** From **Type** drop-down box, select **PPPoA**.  
The default **PPPoA Connection Setup** page ([Figure 2-12](#) on page 2-14) is displayed.
- 3** Enter a unique name for the PPPoA connection in the **Name** field.  
The name must not have spaces and cannot begin with numbers. In this example, the unique name is *PPPoA1*.
- 4** The **Network Address Translation** (NAT) and the **Firewall** options are enabled by default. Leave these in the default mode.
- 5** If you want to enable VLAN, use [Table 2-2](#) on page 2-11 as a reference to configure the following fields:
  - **Sharing**: Select VLAN to enable the **VLAN ID** and **Priority Bits** fields.
  - **VLAN ID**: Enter the VLAN ID.
  - **Priority Bits**: Select the priority bits of the VLAN.
- 6** In the **PPP Settings** section, select the encapsulation type (LLC or VC).  
**Note**—If you are not sure, just use the default mode.
- 7** In the **PVC Settings** section, enter values for the **VPI** and **VCI**.  
**Note**—Your DSL service provider or your ISP supplies these values. In this example, the DSL service provider is using *0,32*.
- 8** Select the **Quality of Service** (QoS). Leave the default value if you are unsure or if the ISP did not provide this information.  
The **PCR**, **SCR**, and **MBS** fields are enabled/disabled depending on the **QoS** selection. Enter the values provided by the ISP or leave the defaults.
- 9** Click **Apply** to complete the connection setup. This temporarily activates this connection as shown in [Figure 2-13](#).

**Figure 2-13 WAN Connection Setup - PPPoA1**

The screenshot shows the 'PPPoA Connection Setup' configuration page. The left-hand column contains a navigation menu with the following items: LAN Setup, LAN Configuration, WAN Setup, New Connection, Modem, PPPoA1, and Log Out. The main configuration area is titled 'PPPoA Connection Setup' and includes the following fields and options:

- Name: PPPoA1
- Type: PPPoA
- Sharing: Disable
- Options:  NAT  Firewall
- VLAN ID: 0
- Priority Bits: 0
- PPP Settings:
  - Encapsulation:  LLC  VC
  - Username: username
  - Password: ••••
  - Idle Timeout: 60 secs
  - Keep Alive: 10 min
  - Authentication:  Auto  CHAP  PAP
  - MTU: 1500 bytes
  - On Demand:
  - Default Gateway:
  - Debug:
  - Valid Rx:
  - Host Trigger:  [Configure](#)
- PVC Settings:
  - PVC: New
  - VPI: 0
  - VCI: 32
  - QoS: UBR
  - PCR: 0 cps
  - SCR: 0 cps
  - MBS: 0 cells
  - Auto PVC:

Buttons at the bottom include [Connect](#), [Disconnect](#), [Apply](#), [Delete](#), and [Cancel](#).

A new link has been created for this connection in the left-hand column. You can connect, disconnect, apply, delete, or cancel this connection using this page by clicking the **Connection Name** to return to its **Connection Setup** page.

**Note**—The changes take effect when you click **Apply**; however, if the RG configuration is not saved, these changes will be lost upon RG reboot.

- 10 To make the change permanent, click **Tools** (at the top of the page) and select **System Commands**.
- 11 At the **System Commands** page (Figure 2-7 on page 2-8), click **Save All**.
- 12 To check the status, click **Status** (at the top of the page) and select **Connection Status**.

**End of Procedure 2-2**

Table 2-4 describes the PPP setting options on the PPPoA Connection Setup page in Figure 2-12 on page 2-14.

**Table 2-4 PPPoA Settings Field Descriptions**

Field	Definition/Description
Encapsulation	The technique used by layered protocols in which a layer adds header information to the protocol data unit (PDU) from the layer above. As an example, in Internet terminology, a packet would contain a header from the data link layer, followed by a header from the network layer (IP), followed by a header from the transport layer (TCP), followed by the application protocol data. Two options are provided: <i>Logical Link Control (LLC)</i> and <i>Virtual Channel (VC)</i> .
Username	Your user name for the PPPoA access provided by your DSL service provider or your ISP. This field is alpha-numeric and the maximum length is 64 characters. It cannot start with a number. The character type restrictions do not apply for CLI-based configuration.
Password	Your password for the PPPoA access provided by your DSL service provider or your ISP. This field is alpha-numeric and the maximum length is 128 characters. The character type restrictions do not apply for CLI-based configuration.
Idle Timeout	Specifies that the PPPoA connection should disconnect if the link has no activity detected for <i>n</i> seconds. This field is used in conjunction with the <b>On Demand</b> feature. To ensure that the link is always active, enter a <i>0</i> in this field. You can also enter a value larger than <i>10 (secs)</i> .
Keep Alive	When the <b>On Demand</b> option is not enabled, this value specifies the time to wait without being connected to your provider before terminating the connection. To ensure that the link is always active, enter a <i>0</i> in this field. You can also enter any positive integer value in this field.
Authentication	Three authentication options are available: <ul style="list-style-type: none"> <li>• Auto</li> <li>• Challenge Handshake Authentication protocol (CHAP)</li> <li>• Password Authentication Protocol (PAP)</li> </ul> Microsoft CHAP v2 is also supported in the Auto and CHAP options. However, MS CHAP v1 is not supported.
MTU	Maximum transmit unit the DSL connection can transmit. It is a negotiated value that packets of no more than <i>n</i> bytes can be sent to the service provider. The PPPoE interface default MTU is <i>1492 (max)</i> and PPPoA default MTU is <i>1500 (max)</i> . The minimum MTU value is <i>64</i> .
On Demand	Enables On Demand mode. The connection disconnects if no activity is detected after the specified <b>Idle Timeout</b> value.
Default Gateway	If checked, this WAN connection acts as the default gateway to the Internet.
Debug	Enables PPPoA connection debugging facilities. This allows the ISP technical support and ODM/OEM testers to simulate packets going through from WAN side.

**Table 2-4 PPPoA Settings Field Descriptions**

Field	Definition/Description
PPP Unnumbered	PPP Unnumbered is a special feature. It enables the ISP to designate a block of public IP addresses to the customer where it is statically assigned on the LAN side. PPP Unnumbered is, in essence, like a bridged connection.
LAN	The LAN group associated with the PPP Unnumbered field. The packets need to go through specific LAN group when the PPP Unnumbered feature is activated. By selecting a LAN group in this field, it enables the <b>PPP IP Address</b> field in the configuration page of this particular LAN group. To view a <b>LAN Group Configuration</b> page, go to <a href="#">Figure 2-37</a> on page 2-42. For more information on LAN Groups, go to 2.4.1 “ <a href="#">LAN Configuration</a> ” on page 2-37.
<b>End of Table 2-4</b>	

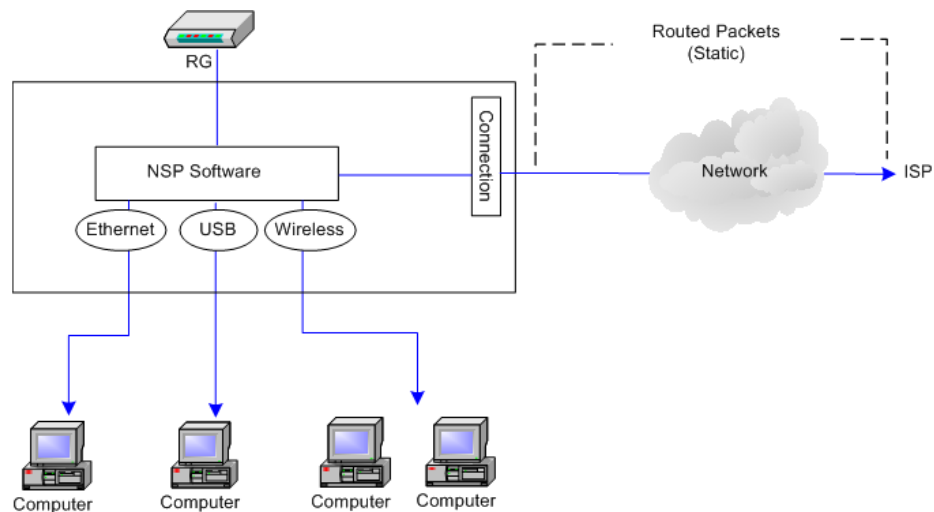
For VLAN field descriptions, please refer to [Table 2-2](#) on page 2-11.

For PVC field descriptions, please refer to [Table 2-3](#) on page 2-11.

### 2.3.3 Static Connection Setup

Static connection type is used whenever a known static IP address is assigned to the RG. The data flow of a Static connection is shown in [Figure 2-14](#).

**Figure 2-14 Static Data Flow**

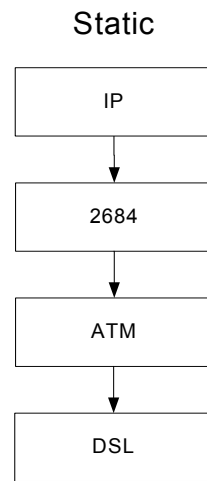


Additional addressing information such as the subnet mask and the default gateway must also be specified. Up to three domain name server (DNS) addresses can be identified. These servers resolve the name of the computer to the IP address mapped to it and thus enable you to access other web servers by typing the symbolic name (host name).



The encapsulation of datagrams in a static connection is shown in [Figure 2-15](#).

**Figure 2-15 Static Connection Encapsulation Diagram**



Use [Table 2-5](#) on page 2-21, [Table 2-2](#) on page 2-11, and [Table 2-3](#) on page 2-11 as references and follow [Procedure 2-3](#) to configure a static connection.

### Procedure 2-3 Configure Gateway for Static Connection

#### Step – Action

- 1 At the **Setup** main page, click **New Connection**.

The default **PPPoE Connection Setup** page ([Figure 2-5](#) on page 2-6) is displayed.

- 2 At the **Type** field select **Static**.

The **Static Connection Setup** page ([Figure 2-16](#)) is displayed.

**Figure 2-16 Static Connection Setup**

The screenshot shows the 'Static Connection Setup' page. The left sidebar contains navigation options: LAN Setup, LAN Configuration, WAN Setup, New Connection (highlighted), Modem, and Log Out. The main content area is titled 'Static Connection Setup' and includes the following fields and options:

- Name: [Text Input]
- Type: Static (dropdown)
- Sharing: Disable (dropdown)
- Options:  NAT,  Firewall
- VLAN ID: [Text Input: 0]
- Priority Bits: [Text Input: 0]
- Static Settings:
  - Encapsulation:  LLC,  VC
  - IP Address: [Text Input: 0.0.0.0]
  - Mask: [Text Input]
  - Gateway: [Text Input]
  - Default Gateway: [Text Input]
  - DNS 1: [Text Input]
  - DNS 2: [Text Input]
  - DNS 3: [Text Input]
  - Mode:  Bridged,  Routed
- PVC Settings:
  - PVC: [Text Input: New]
  - VPI: [Text Input: 0]
  - VCI: [Text Input: 0]
  - QoS: UBR (dropdown)
  - PCR: [Text Input: 0] cps
  - SCR: [Text Input: 0] cps
  - MBS: [Text Input: 0] cells
  - Auto PVC:

Buttons at the bottom right: Apply, Delete, Cancel.

- 3 In the **Name** field, enter a unique name for the Static connection.  
The name must not have spaces and cannot begin with numbers. In this example, the unique name is *Static1*.
- 4 The **Network Address Translation** (NAT) and the **Firewall** options are enabled by default. Leave these in the default mode.
- 5 In the **Static Settings** section, select the **Encapsulation Type** (LLC or VC).  
**Note**—If you are not sure, just use the default mode.
- 6 Based upon the information your DSL/ISP provided, enter your assigned **IP Address, Subnet Mask, Default Gateway** (if provided), and **Domain Name Services** (DNS) values (if provided).
- 7 For the static configuration, you can also select a **Bridged** connection or a **Routed** connection.
- 8 In the **PVC Settings** section, enter values for the **VPI** and **VCI**.  
**Note**—Your DSL service provider or your ISP supplies these values. In this example, the DSL service provider is using 0,35.
- 9 Select the **Quality of Service** (QoS). Leave the default value if you are unsure or if the ISP did not provide this information.  
The **PCR, SCR, and MBS** fields are enabled/disabled depending on the **QoS** selection. Enter the values provided by the ISP or leave the defaults.
- 10 Click **Apply** to complete the connection setup. This temporarily activates this connection as shown in [Figure 2-17](#).

**Figure 2-17 WAN Connection Setup - Static1**

The screenshot displays the 'Static Connection Setup' configuration page. The interface includes a navigation menu on the left with options like LAN Setup, WAN Setup, and Modem. The main configuration area is divided into several sections:
 

- General Settings:** Name: Static1, Type: Static, Sharing: Disable.
- Options:** NAT and Firewall are checked. VLAN ID: 0, Priority Bits: 0.
- Static Settings:** Encapsulation: LLC (selected), VC. IP Address: 0.0.0.0, Mask: 255.255.255.0, Gateway: 192.168.1.15, Default Gateway: (empty).
- DNS Settings:** DNS 1, 2, and 3: (empty).
- PVC Settings:** PVC: New, VPI: 0, VCI: 35, QoS: UBR, PCR: 0 cps, SCR: 0 cps, MBS: 0 cells, Auto PVC: unchecked.
- Mode:** Bridged (selected), Routed.

 At the bottom right, there are buttons for 'Apply', 'Delete', and 'Cancel'.

A new link has been created for this connection in the left-hand column. You can apply, delete, or cancel this connection using the buttons on this page.

A new link is created for this connection in the left-hand column. You can connect, disconnect, apply, delete, or cancel this connection using the buttons at the bottom of this page.

**Note**—The changes take effect when you click **Apply**; however, if the RG configuration is not saved, these changes will be lost upon RG reboot.

- 11 To make the change permanent, click **Tools** at the top of the page and select **System Commands**.
- 12 At the **System Commands** page ([Figure 2-7](#) on page 2-8), click **Save All**.
- 13 To check the status, click **Status** at the top of the page and select **Connection Status**.

#### End of Procedure 2-3

[Table 2-5](#) describes the static setting options on the **Static Connection Setup** page in [Figure 2-17](#) on page 2-20.

**Table 2-5 Static Settings Field Descriptions**

Field	Definition/Description
Encapsulation	The technique used by layered protocols in which a layer adds header information to the protocol data unit (PDU) from the layer above. As an example, in Internet terminology, a packet would contain a header from the data link layer, followed by a header from the network layer (IP), followed by a header from the transport layer (TCP), followed by the application protocol data. Two options are provided: <i>Logical Link Control (LLC)</i> and <i>Virtual Channel (VC)</i> .
IP Address	IP address of the static connection provided by the ISP.
Mask	Subnet mask provided by your ISP.
Gateway	The IP address of your gateway provided by the ISP.
Default Gateway	The IP address of the default gateway to the Internet provided by the ISP.
DNS	Domain name server IP address provided by your ISP. You can configure up to three DNS IP addresses.
Mode	Two modes are available: <i>Bridged</i> and <i>Routed</i> .
<b>End of Table 2-5</b>	

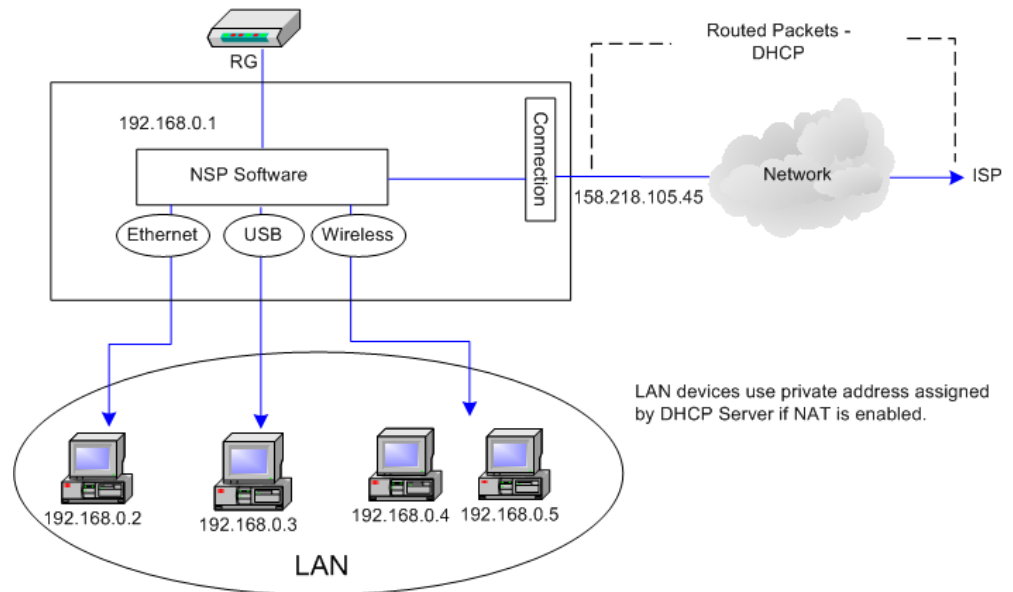
For VLAN field descriptions, please refer to [Table 2-2](#) on page 2-11.

For PVC field descriptions, please refer to [Table 2-3](#) on page 2-11.

### 2.3.4 DHCP Connection Setup

The dynamic host configuration protocol (DHCP) allows the RG to automatically obtain the IP address from the server. This option is commonly used in situations where the IP is dynamically assigned and is not known prior to assignment. The data flow of a DHCP connection is shown in Figure 2-18.

Figure 2-18 DHCP Data Flow



The encapsulation of datagrams in a DHCP connection is shown in Figure 2-19.

Figure 2-19 DHCP Encapsulation Diagram

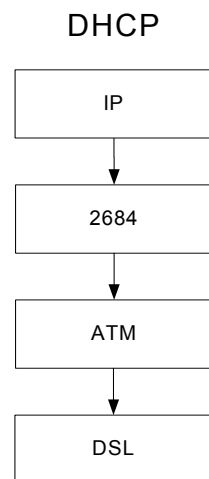


Figure 2-20 shows the default **DHCP Voice Connection Setup** page.

**Figure 2-20 DHCP - Voice Connection Setup**

The screenshot displays the 'DHCP Connection Setup' page. On the left is a navigation menu with options: LAN Setup, LAN Configuration, WAN Setup, New Connection (highlighted), Modem, and Log Out. The main content area is titled 'DHCP Connection Setup' and contains the following fields and controls:

- Name:** An empty text input field.
- Type:** A dropdown menu set to 'DHCP'.
- Sharing:** A dropdown menu set to 'Disable'.
- Options:** Checkboxes for 'NAT' and 'Firewall', both of which are checked.
- VLAN ID:** A text input field containing '0'.
- Priority Bits:** A dropdown menu set to '0'.
- DHCP Settings:**
  - Encapsulation:** Radio buttons for 'LLC' (selected) and 'VC'.
  - IP Address:** An empty text input field.
  - Mask:** An empty text input field.
  - Gateway:** An empty text input field.
  - Default Gateway:** An unchecked checkbox.
- PVC Settings:**
  - PVC:** A dropdown menu set to 'New'.
  - VPI:** A text input field containing '0'.
  - VCI:** A text input field containing '0'.
  - QoS:** A dropdown menu set to 'UBR'.
  - PCR:** A text input field containing '0' followed by 'cps'.
  - SCR:** A text input field containing '0' followed by 'cps'.
  - MBS:** A text input field containing '0' followed by 'cells'.
  - Auto PVC:** An unchecked checkbox.

At the bottom of the main content area are buttons for 'Renew' and 'Release'. At the bottom right of the entire page are buttons for 'Apply', 'Delete', and 'Cancel'.

Use [Table 2-6](#) on page 2-25, [Table 2-2](#) on page 2-11, and [Table 2-3](#) on page 2-11 as references and follow [Procedure 2-4](#) to configure a DHCP connection.

#### **Procedure 2-4 Configure RG for DHCP**

##### **Step – Action**

- 1 On the **Setup** main page, click **New Connection**.

The default **DHCP Connection Setup** page ([Figure 2-5](#) on page 2-6) is displayed.

- 2 From the **Type** drop-down box, select **DHCP**.

The default **DHCP Connection Setup** page ([Figure 2-20](#) on page 2-23) is displayed.

- 3 Enter a unique name for the DHCP connection in the **Name** field.

The name must not have spaces and cannot begin with numbers. In this example, the unique name is *DHCP1*.

- 4 The **Network Address Translation** (NAT) and the **Firewall** options are enabled by default. Leave these in the default mode.

- 5 If your DSL line is connected and your DSL/IPS provider is supporting DHCP, you can click **Renew** and the gateway retrieves an IP Address, Subnet Mask, and Gateway Address.

At any time, you can release the DHCP address by clicking **Release**, and renew the DHCP address by clicking **Renew**.

- 6 Under **PVC Settings**, enter values for the **VPI** and **VCI**.  
**Note**—Your DSL service provider or your ISP supplies these values. In this example, the DSL service provider is using 0,35.
- 7 Select the **Quality of Service (QoS)**. Leave the default value if you are unsure or if the ISP did not provide this information.  
The **PCR**, **SCR**, and **MBS** fields are enabled/disabled depending on the **QoS** selection. Enter the values provided by the ISP or leave the defaults.
- 8 Click **Apply** to complete the connection setup. This temporarily activates this connection as shown in [Figure 2-21](#).

**Figure 2-21 WAN Connection Setup - DHCP1**

The screenshot shows the 'DHCP Connection Setup' configuration page. The left sidebar contains navigation links: LAN Setup, LAN Configuration, WAN Setup, New Connection, Modem, DHCP1 (highlighted), and Log Out. The main content area is titled 'DHCP Connection Setup' and contains the following fields and controls:

- Name: DHCP1
- Type: DHCP
- Sharing: Disable
- Options:  NAT,  Firewall
- VLAN ID: 0
- Priority Bits: 0
- DHCP Settings**:
  - Encapsulation:  LLC,  VC
  - IP Address: NA
  - Mask: NA
  - Gateway: NA
  - Default Gateway:
- PVC Settings**:
  - PVC: New
  - VPI: 0
  - VCI: 35
  - QoS: UBR
  - PCR: 0 cps
  - SCR: 0 cps
  - MBS: 0 cells
  - Auto PVC:

Buttons at the bottom include Renew, Release, Apply, Delete, and Cancel.

A new link has been created for this connection in the left-hand column. You can apply, delete, or cancel this connection using the buttons on this page.

**Note**—The changes take effect when you click **Apply**; however, if the RG configuration is not saved, these changes will be lost upon RG reboot.

- 9 To make the change permanent, click **Tools** at the top of the page and select **System Commands**.
- 10 At the **System Commands** page ([Figure 2-7](#) on page 2-8), click **Save All**.
- 11 To check the status, click **Status** at the top of the page and select **Connection Status**.

**End of Procedure 2-4**

Table 2-6 describes the DHCP settings options on the **DHCP Connection Setup** page (Figure 2-20 on page 2-23).

**Table 2-6 DHCP Settings Field Descriptions**

Field	Definition/Description
Encapsulation	The technique used by layered protocols in which a layer adds header information to the protocol data unit (PDU) from the layer above. As an example, in Internet terminology, a packet would contain a header from the data link layer, followed by a header from the network layer (IP), followed by a header from the transport layer (TCP), followed by the application protocol data. Two options are provided: <i>Logical Link Control (LLC)</i> and <i>Virtual Channel (VC)</i> .
IP Address	IP address assigned by the DHCP server.
Mask	The subnet mask assigned by the DHCP server.
Gateway	The IP address of your gateway.
Default Gateway	If checked, this WAN connection acts as the default gateway to the Internet.
<b>End of Table 2-6</b>	

For VLAN field descriptions, please refer to Table 2-2 on page 2-11.

For PVC field descriptions, please refer to Table 2-3 on page 2-11.

### 2.3.5 Bridged Connection Setup

A pure bridged connection does not assign any IP address to the WAN interface. NAT and firewall rules are not enabled. This connection method makes the RG act as a bridge for passing packets between the WAN interface and the LAN interface. The data flow of a Static connection is shown in Figure 2-22.

**Figure 2-22 Bridge Data Flow**

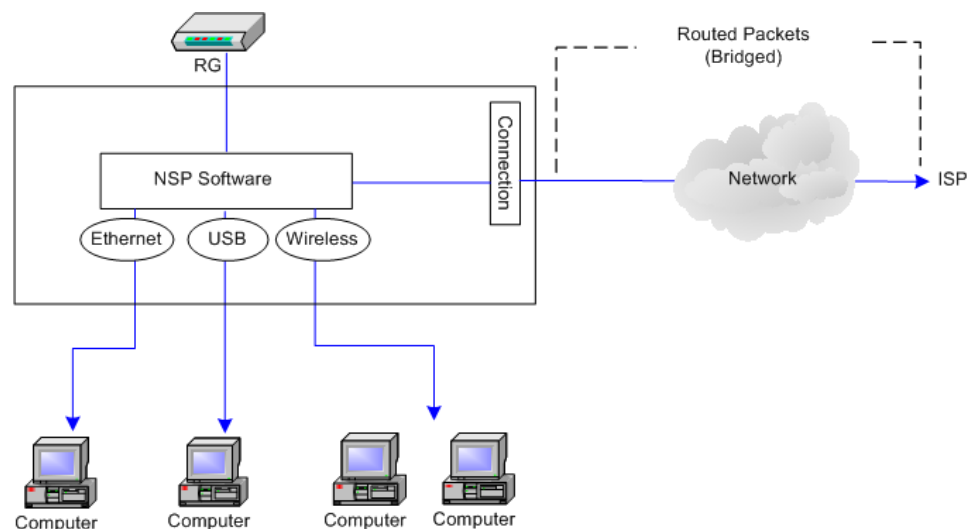
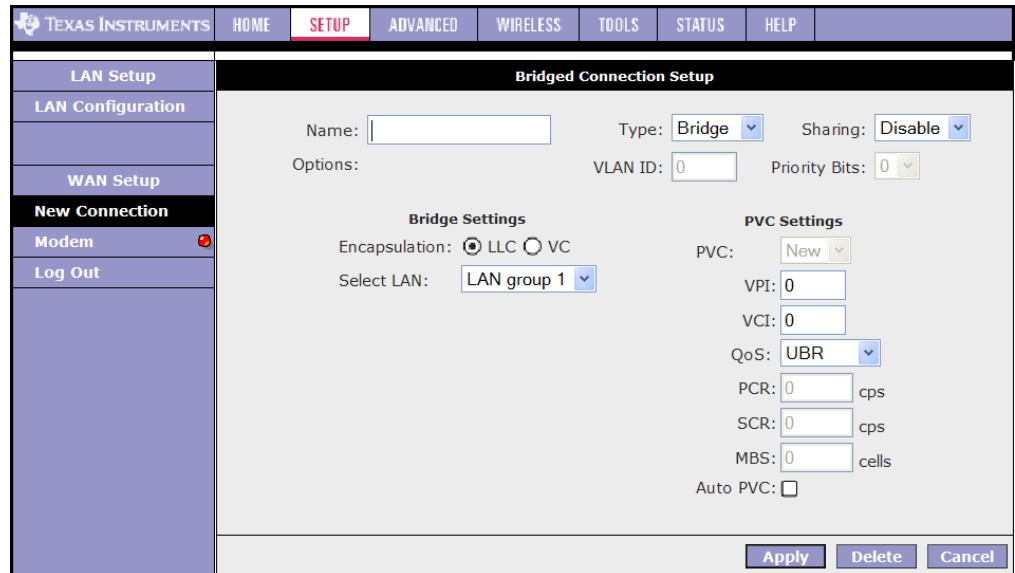


Figure 2-23 shows the default **Bridged Connection Setup** page.

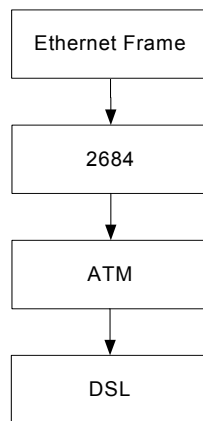
**Figure 2-23 Bridged Connection Setup**



The encapsulation of datagrams in a bridged connection is shown in Figure 2-24.

**Figure 2-24 Bridged Connection Encapsulation Diagram**

Bridged Connection



Use Table 2-7 on page 2-28, Table 2-2 on page 2-11, and Table 2-3 on page 2-11 as references and follow Procedure 2-5 to configure a bridged connection.

**Procedure 2-5 Configure a Bridged Connection**

**Step – Action**

- 1 On the **Setup** main page, click **New Connection**.

The default **PPPoE Connection Setup** page (Figure 2-5 on page 2-6) is displayed.



- 2 From **Type** drop-down box, select **Bridge**.  
The default **Bridged Connection Setup** page (Figure 2-23 on page 2-26) is displayed.
- 3 Enter a unique name for the Bridged connection in the **Name** field.  
The name must not have spaces and cannot begin with numbers. In this example, the unique name is *Bridge 1*.
- 4 The **NAT** and the **Firewall** options are enabled by default. Leave these in the default mode.
- 5 In the **Bridge Settings** section, select the **Encapsulation Type** (LLC or VC).  
**Note**—If you are not sure, just use the default mode.
- 6 In the **PVC Settings** section, enter values for the **VPI** and **VCI**.  
**Note**—Your DSL service provider or your ISP supplies these values. In this example, the DSL service provider is using 0,35.
- 7 Select the **Quality of Service (QoS)**. Leave the default value if you are unsure or if the ISP did not provide this information.  
The **PCR**, **SCR**, and **MBS** fields are enabled/disabled depending on the **QoS** selection. Enter the values provided by the ISP or leave the defaults.
- 8 Click **Apply** to complete the connection setup. This temporarily activates this connection as shown in Figure 2-25.

**Figure 2-25 WAN Connection Setup - Bridge1**

The screenshot displays the 'Bridged Connection Setup' configuration page. The interface includes a navigation menu on the left with options like LAN Setup, WAN Setup, and Modem. The main content area is titled 'Bridged Connection Setup' and contains the following fields and sections:

- Name:** Bridge1
- Type:** Bridge
- Sharing:** Disable
- Options:**
  - VLAN ID:** 0
  - Priority Bits:** 0
- Bridge Settings:**
  - Encapsulation:** LLC (selected), VC
  - Select LAN:** LAN group 1
- PVC Settings:**
  - PVC:** New
  - VPI:** 0
  - VCI:** 35
  - QoS:** UBR
  - PCR:** 0 cps
  - SCR:** 0 cps
  - MBS:** 0 cells
  - Auto PVC:**

At the bottom right, there are three buttons: **Apply**, **Delete**, and **Cancel**.

A new link has been created for this connection in the left-hand column. You can apply, delete, or cancel this connection using this page.

**Note**—The changes take effect when you click **Apply**; however, if the RG configuration is not saved, these changes will be lost upon RG reboot.

- 9 To make the change permanent, click **Tools** at the top of the page and select **System Commands**.
- 10 At the **System Commands** page (Figure 2-7 on page 2-8), click **Save All**.
- 11 To check the status, click **Status** (at the top of the page) and select **Connection Status**.

**End of Procedure 2-5**

Table 2-7 describes the bridge settings options on the **Bridged Connection Setup** page in Figure 2-23 on page 2-26.

**Table 2-7 Bridge Settings Field Descriptions**

Field	Definition/ Description
Encapsulation	The technique used by layered protocols in which a layer adds header information to the protocol data unit (PDU) from the layer above. As an example, in Internet terminology, a packet would contain a header from the data link layer, followed by a header from the network layer (IP), followed by a header from the transport layer (TCP), followed by the application protocol data. Two encapsulation options are provided: <i>Logical Link Control (LLC)</i> and <i>Virtual Channel (VC)</i> .
Select LAN	Select the LAN group for the bridged connection. The following options are available: <ul style="list-style-type: none"> <li>• LAN Group 1</li> <li>• LAN Group 2</li> <li>• LAN Group 3</li> <li>• None</li> </ul> <p>This bridged connection will be added to the selected LAN group. If you select <i>None</i>, the connection is not added to any LAN group but to the Interfaces box on the <b>LAN Configuration</b> page (Figure 2-31 on page 2-37), which can be configured to a LAN group on the same page.</p> <p>For more information on LAN Groups, go to 2.4.1 “LAN Configuration” on page 2-37.</p>
<b>End of Table 2-7</b>	

For VLAN field descriptions, please refer to Table 2-2 on page 2-11.

For PVC field descriptions, please refer to Table 2-3 on page 2-11.

### 2.3.6 CLIP Connection Setup

The Classical IP over ATM (CLIP) connection is supported on the AR7WRD platform in this release. It is not supported on the AR7VW platform.

CLIP, defined in RFC 2225, provides the ability to transmit IP packets over an ATM network. TI's CLIP support encapsulates an IP datagram in an AAL5 PDU frame using RFC 2225 and it uses an ATM-aware version of the address resolution protocol (ATMARP). TI's CLIP support only allows support for PVCs, SVCs are not supported by the RG. The data flow of a Static connection is shown in Figure 2-14.

Figure 2-26 Static Data Flow

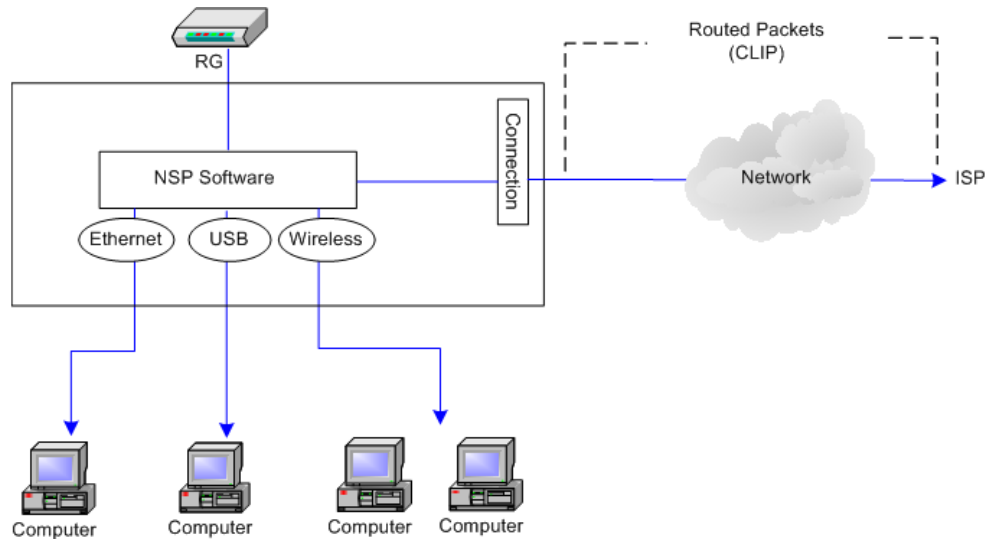
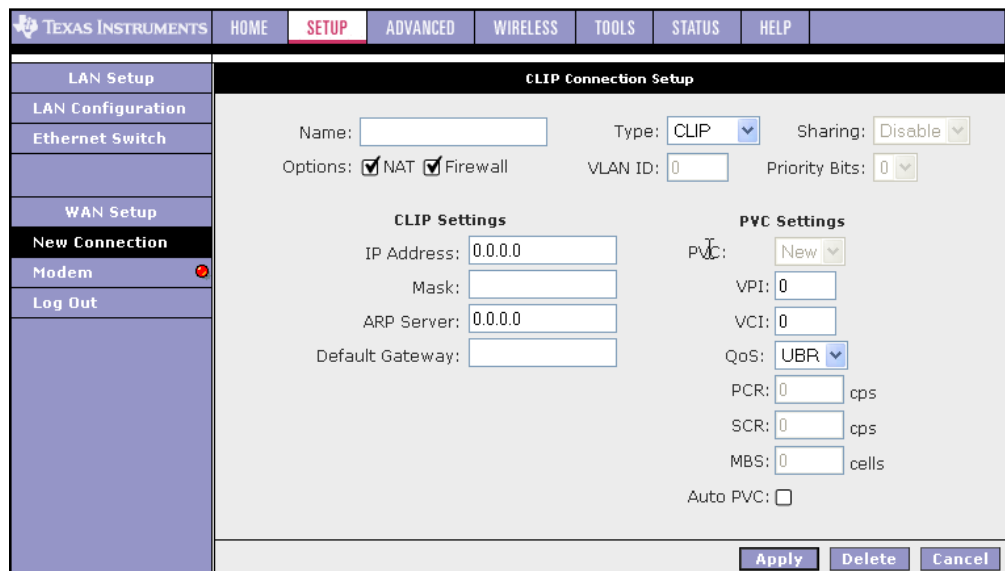


Figure 2-27 shows the default CLIP Connection Setup page.

Figure 2-27 CLIP Connection Setup



Use [Table 2-8](#) on page 2-31, [Table 2-2](#) on page 2-11, and [Table 2-3](#) on page 2-11 as references and follow [Procedure 2-6](#) to configure a CLIP connection.

---

**Procedure 2-6 Configure Gateway for CLIP Connection**

---

**Step – Action**

- 1** On the **Setup** main page, click **New Connection**.  
The default **PPPoE Connection Setup** page ([Figure 2-5](#) on page 2-6) is displayed.
- 2** From **Type** drop-down box, select **CLIP**.  
The default **CLIP Connection Setup** page ([Figure 2-27](#)) is displayed.
- 3** Enter a unique name for the static connection in the **Name** field.  
The name must not have spaces and cannot begin with numbers. In this example, the unique name is *Clip1*.
- 4** The **Network Address Translation** (NAT) and the **Firewall** options are enabled by default. Leave these in the default mode.
- 5** Based upon the information your DSL/ISP provided, enter your assigned **IP Address, Mask, ARP Server, and Default Gateway**.
- 6** In the **PVC Settings** section, enter values for the **VPI** and **VCI**.  
**Note**—Your DSL service provider or your ISP supplies these values.
- 7** Select the **Quality of Service** (QoS); leave the default value if you are unsure or if the ISP did not provide this information.  
The **PCR, SCR, and MBS** fields are enabled/disabled depending on the **QoS** selection. Enter the values provided by the ISP or leave the defaults.
- 8** Click **Apply** to complete the connection setup. This temporarily activates this connection as shown in [Figure 2-28](#).

**Figure 2-28 WAN Connection Setup - CLIP1**

The screenshot shows the 'CLIP Connection Setup' page. The left-hand navigation menu includes: LAN Setup, LAN Configuration, Ethernet Switch, WAN Setup, New Connection, Modem, and Log Out. The main content area is titled 'CLIP Connection Setup' and contains the following fields and options:

- Name: [Text Input]
- Type: CLIP (dropdown)
- Sharing: Disable (dropdown)
- Options:  NAT,  Firewall
- VLAN ID: 0 (text input)
- Priority Bits: 0 (dropdown)
- CLIP Settings**
  - IP Address: 0.0.0.0 (text input)
  - Mask: [Text Input]
  - ARP Server: 0.0.0.0 (text input)
  - Default Gateway: [Text Input]
- PVC Settings**
  - PVC: New (dropdown)
  - VPI: 0 (text input)
  - VCI: 0 (text input)
  - QoS: UBR (dropdown)
  - PCR: 0 cps (text input)
  - SCR: 0 cps (text input)
  - MBS: 0 cells (text input)
  - CDVT: 0 usecs (text input)
  - Auto PVC:

Buttons at the bottom: Apply, Delete, Cancel.

A new link has been created for this connection in the left-hand column. You can apply, delete, or cancel this connection using this page.

**Note**—The changes take effect when you click **Apply**; however, if the RG configuration is not saved, these changes will be lost upon RG reboot.

- 9 To make the change permanent, click **Tools** at the top of the page and select **System Commands**.
- 10 At the **System Commands** page (Figure 2-7 on page 2-8), click **Save All**.
- 11 To check the status, click **Status** at the top of the page and select **Connection Status**.

#### End of Procedure 2-6

Table 2-8 describes the CLIP setting options on the **CLIP Connection Setup** page in Figure 2-27 on page 2-29.

**Table 2-8 CLIP Settings Field Descriptions**

Field	Definition/Description
IP Address	IP address of the CLIP connection provided by your ISP.
Mask	Subnet mask provided by your ISP.
ARP Server	IP address of the Address Resolution Protocol (ARP) server provided by your ISP.
Default Gateway	If checked, this WAN connection acts as the default gateway to the Internet.

**End of Table 2-8**

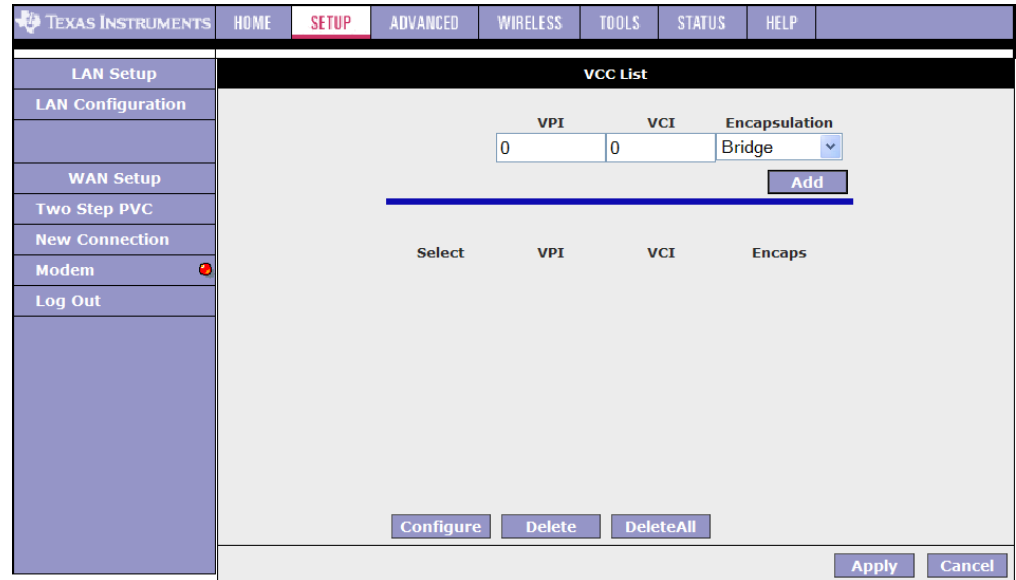
For VLAN field descriptions, please refer to Table 2-2 on page 2-11.

For PVC field descriptions, please refer to [Table 2-3](#) on page 2-11.

### 2.3.7 Two-Step PVC

The Two-step PVC feature is only available on the AR7WRD platform for this software release. It is not available on the AR7VW platform.

**Figure 2-29 Two Step PVC Page**



The Two-step PVC page ([Figure 2-29](#)) is added to support the Remote Management /Clear Embedded Operations Channel (EOC) feature, which is a China MII requirement. This page allows WAN connections to be created in two steps:

1. Create multiple PVCs with VPI , VCI values, and encapsulation types. The following encapsulation methods are supported:
  - PPPoA
  - PPPoE
  - Router 1483
  - Bridge
  - Static
  - DHCP
  - CLIP
2. Create a WAN connection from an existing PVC.

For PVC field descriptions, go to [Table 2-3 “PVC Settings Field Descriptions”](#) on page 2-11. For information on creating a specific WAN connection, go to the relevant headings in this chapter.

### 2.3.8 Modify an Existing Connection

Use the following procedures to modify a WAN connection.

---

#### Procedure 2-7 Modify a WAN Connection

---

##### Step – Action

- 1 On the **Setup** main page, select the connection you want to modify from the left-hand column.

The connections are listed as Connection 1 through Connection 8.

**Note**—Up to eight WAN connections of all types are supported.

- 2 Make modifications on the individual connection page.

**Note**—Some fields are disabled after initial creation.

- 3 Click **Apply** to temporarily activate the changes you made.

**Note**—The changes take effect when you click **Apply**; However, if the RG configuration is not saved, these changes will be lost upon RG reboot.

- 4 To make the change permanent, click **Tools** at the top of the page and select **System Commands**.

- 5 On the **System Commands** page, click **Save All**.

End of Procedure 2-7

---

### 2.3.9 Delete an Existing Connection

Use the following procedures to delete a WAN connection.

---

#### Procedure 2-8 Delete A WAN Connection

---

##### Step – Action

- 1 On the **Setup** main page, select the connection you want to modify from the left-hand column.

The connections are listed as Connection 1 through Connection 8

- 2 Click **Delete** on the particular **Connection Setup** page.

**Note**—The changes take effect when you click **Delete**; however, if the RG configuration is not saved, these changes will be lost upon RG reboot.

- 3 To make the change permanent, click **Tools** at the top of the page and select **System Commands**.

- 4 At the **System Commands** page ([Figure 2-7](#) on page 2-8), click **Save All**.

End of Procedure 2-8

---

### 2.3.10 Modem Setup

The Modem Setup page is only available in the AR7WRD platform in this release.

The **Modem Setup** page allows you to select any combination of DSL training modes including:

- NO\_MODE
- ADSL\_G.dmt (G Discrete Multi-Tone): G.dmt (G.992.1)
- ADSL\_G.lite: G.lite (G.992.2)
- ADSL\_G.dmt.bis
- ADSL\_G.dmt.bis\_DELT
- ADSL\_2plus
- ADSL\_2plus\_DELT
- ADSL\_re-adsl
- ADSL\_re-adsl\_DELT
- ADSL\_ANSI\_T1.413
- Multi\_MODE:
- ADSL\_G.dmt.bis\_AnXI (currently not supported)
- ADSL\_G.dmt.bis\_AnXJ (currently not supported)
- ADSL\_G.dmt.bis\_AnXM
- ADSL\_2plus\_AnXI (currently not supported)
- ADSL\_2plus\_AnXJ (currently not supported)
- ADSL\_2plus\_AnXM
- G.shdsl
- IDSL (currently not supported)
- HDSL (currently not supported)
- SDSL (currently not supported)
- VDSL (currently not supported)



Figure 2-30 Modem Setup Page

TEXAS INSTRUMENTS	HOME	SETUP	ADVANCED	WIRELESS	TOOLS	STATUS	HELP
LAN Setup	<b>Modem Setup</b>						
LAN Configuration	Select the modulation type.						
WAN Setup	<input type="checkbox"/> NO_MODE <input checked="" type="checkbox"/> ADSL_G.dmt <input checked="" type="checkbox"/> ADSL_G.lite <input checked="" type="checkbox"/> ADSL_G.dmt.bis <input checked="" type="checkbox"/> ADSL_G.dmt.bis_DELT <input checked="" type="checkbox"/> ADSL_2plus <input checked="" type="checkbox"/> ADSL_2plus_DELT <input checked="" type="checkbox"/> ADSL_re-adsl <input checked="" type="checkbox"/> ADSL_re-adsl_DELT <input checked="" type="checkbox"/> ADSL_ANSI_T1.413 <input checked="" type="checkbox"/> MULTI_MODE <input type="checkbox"/> ADSL_G.dmt.bis_AnXI <input type="checkbox"/> ADSL_G.dmt.bis_AnXJ <input type="checkbox"/> ADSL_G.dmt.bis_AnXM <input type="checkbox"/> ADSL_2plus_AnXI <input type="checkbox"/> ADSL_2plus_AnXJ <input type="checkbox"/> ADSL_2plus_AnXM <input type="checkbox"/> G.shdsl <input type="checkbox"/> IDSL <input type="checkbox"/> HDLSL <input type="checkbox"/> SDLSL <input type="checkbox"/> VDSL						
New Connection							
<b>Modem</b>							
Log Out							
							Apply Cancel

### 2.3.11 Multi Mac Support

This feature applies to ODM/OEMs. By default, all WAN connections use the same MAC address. When you have multiple WAN connections, you want each one of them to use a different MAC address, which can be configured in the **Environment Variable** space (manufacturing time activity). Up to eight MAC addresses are supported, which are (in the order of assignment):

- HWA\_WAN0: Assigned to the first connection created.
- HWA\_WAN1
- HWA\_WAN2
- HWA\_WAN3
- HWA\_WAN4
- HWA\_WAN5
- HWA\_WAN6
- HWA\_WAN7

The Multi Mac feature supports the following types of connections:

- Static
- DHCP

- Bridge
- PPPoE

## 2.4 LAN Setup

### 2.4.1 LAN Configuration

#### LAN Configuration

The RG provides LAN configuration for multiple LAN bridge groups. Up to five LAN bridge groups are supported. The LAN interfaces could include: Ethernet (for AR7WRD platform), Ethernet 1, Ethernet 2, Ethernet 3, Ethernet 4 (for Ar7VW platform), USB, WLAN (Primary SSID), SSID1, SSID2, and SSID3. It is possible to assign any LAN interface to any bridge group but only one group, except that the Ethernet interface needs to stay in LAN group 1. Each LAN group can then be configured with static IP address, dynamic IP address, or be unmanaged (no IP).

**Figure 2-31 LAN Configuration 1 (Default)**

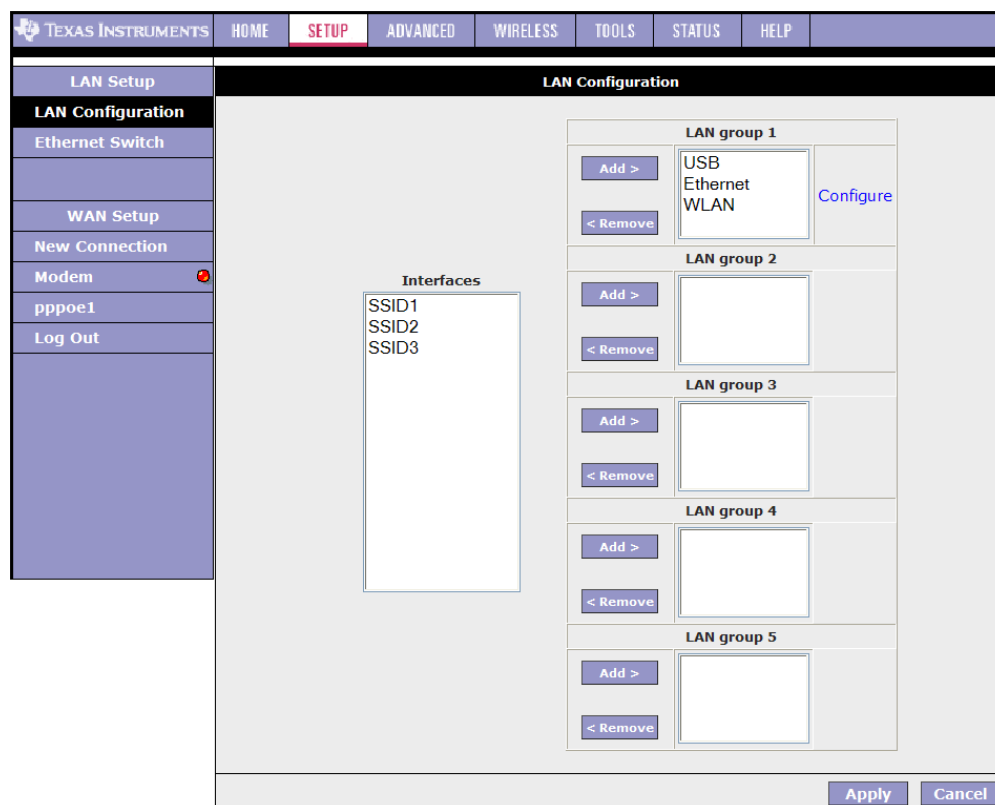


Figure 2-31 shows the default **LAN Configuration** page. The following LAN interfaces belong to a single LAN bridge group (LAN Group 1):

- USB
- Ethernet

- WLAN



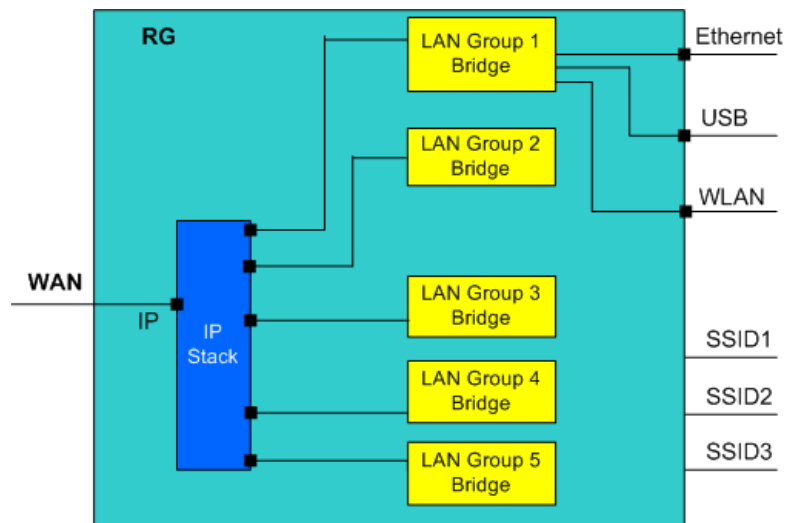
**Note**—The following interfaces are not valid until multiple SSID is enabled and the secondary SSIDs are configured:

- SSID1 (corresponds to the first secondary SSID)
- SSID2 (corresponds to the second secondary SSID)
- SSID3 (corresponds to the third secondary SSID)

For more information on how to configure multiple SSIDs, go to 4.4 “Multiple SSID” on page 4-9.

The RG performs routing between the LAN group 1 and the WAN connections as shown in [Figure 2-32](#).

**Figure 2-32 RG Routing - LAN Groups (A)**



Use [Procedure 2-9](#) to configure LAN group 2.

#### **Procedure 2-9 LAN Configuration**

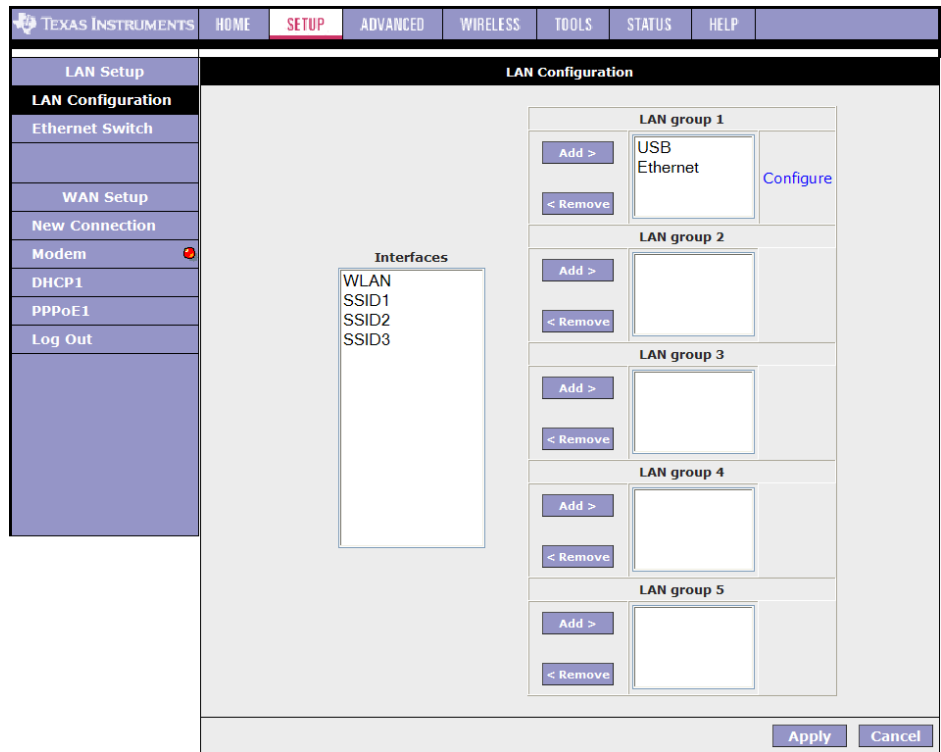
##### **Step – Action**

- 1 Select **WLAN** interface in LAN group 1 and click **Remove**.

**WLAN** moves to the **Interfaces** box on the left as shown in [Figure 2-33](#).

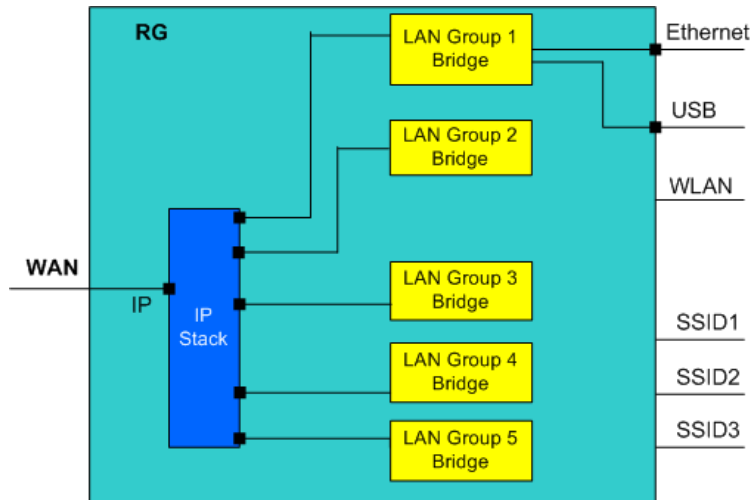
**Note**—You can configure the USB interface and WLAN interfaces to a different LAN group; however, the Ethernet interface is default in LAN group 1 and cannot be moved.

**Figure 2-33 LAN Configuration 2**



No packets are sent to the WLAN interface as it does not belong to any LAN group. This is shown in [Figure 2-34](#).

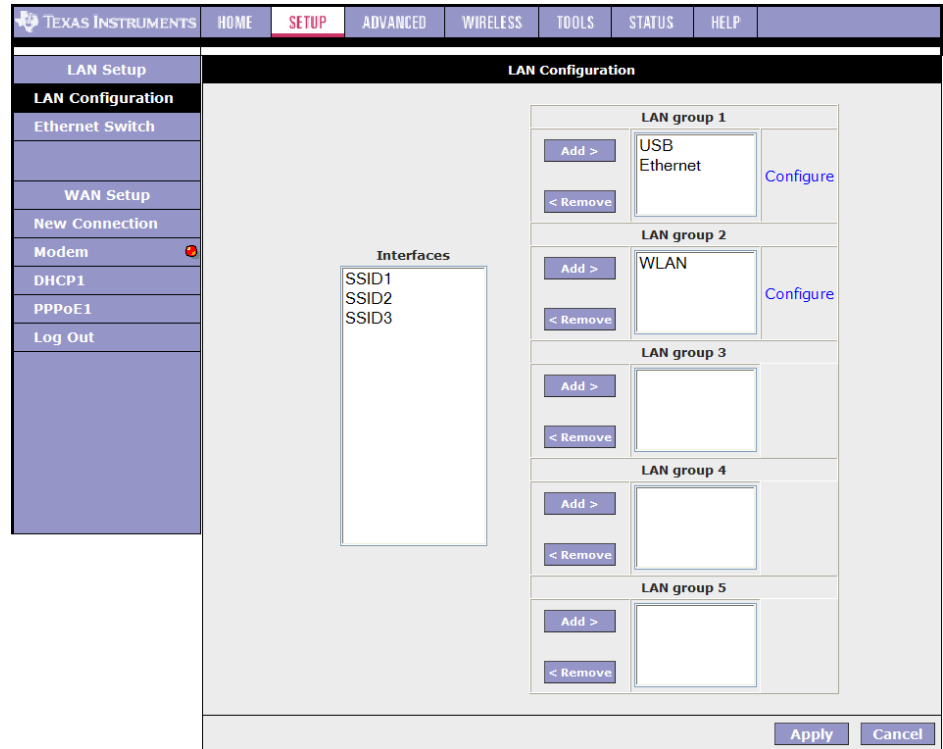
**Figure 2-34 RG Routing - LAN Groups (B)**



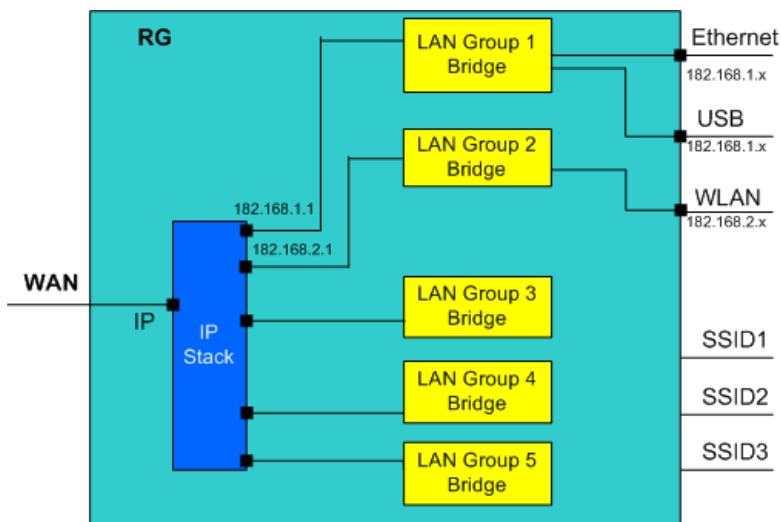
- 2 Select **WLAN** in the Interface box and click **Add** next to LAN group 2.

**WLAN** moves to LAN group 2 as shown in [Figure 2-35](#). The **Configure** link for LAN group 2 has also been generated, allowing additional configurations for the defined LAN group.

**Figure 2-35 LAN Configuration 3**



Two LAN segments have been configured as shown in [Figure 2-36](#) with two sets of IP addresses. The Ethernet and USB interfaces belong to LAN group 1 with an IP of 192.168.1.x. The WLAN interface belongs to LAN group 2 with an IP of 192.168.2.x.

**Figure 2-36 GRG Routing - LAN Groups (C)**

- 3 Click **Apply** to temporarily activate the changes.

**Note**—The changes take effect when you click **Apply**; however, if the RG configuration is not saved, these changes will be lost upon RG reboot.

- 4 To make the change permanent, click **Tools** at the top of the page and select **System Commands**.
- 5 On the **System Commands** page (Figure 2-7 on page 2-8), click **Save All**.

End of Procedure 2-9

### LAN Group Configuration

The **LAN Group Configuration** page (Figure 2-37) allows you to configure settings for each defined LAN group.

Notice that you can also view the status of advanced services that can be applied to this LAN group. A green status indicates that the services have been enabled, while a red status indicates that the service is currently disabled.

**Figure 2-37 LAN Group Configuration Page**

The screenshot shows the 'LAN Group 1 Configuration' page. On the left is a navigation menu with options: LAN Setup, LAN Configuration, WAN Setup, New Connection, Modem, and Log Out. The main area is titled 'LAN Group 1 Configuration' and contains the following sections:

- IP Settings:**
  - Unmanaged
  - Obtain an IP address automatically (includes 'Release' and 'Renew' buttons)
  - PPP IP Address
  - Use the following Static IP address (includes fields for IP Address: 192.168.1.1, Netmask: 255.255.255.0, Default Gateway: 192.168.1.1, Host Name: mygateway1, Domain: ar7)
- DHCP Settings:**
  - Enable DHCP Server (includes fields for Start IP: 192.168.1.2, End IP: 192.168.1.254, Lease Time: 3600 Seconds)
  - Assign ISP DNS, SNTIP
  - Enable DHCP Relay (includes field for Relay IP: 20.0.0.3)
  - Server and Relay Off
- Services Status:**
  - IP Filters: ●
  - Bridge Filters: ●
  - UPnP: ●
  - LAN Clients: ●
  - Static Routing: ●

At the bottom right are 'Apply' and 'Cancel' buttons.

Table 2-9 describes the LAN Group Configuration page options.

**Table 2-9 LAN Group Configuration Field Descriptions**

Category/Field	Field	Definition/Description
Unmanaged		Unmanaged is a state when the LAN group is not configured and no IP address has been assigned to the bridge.
Obtain an IP address automatically		When this function is enabled, your RG acts like a client and requests an IP address from the DHCP server on the LAN side.
	IP Address	You can retrieve/renew an IP address from the DHCP server using the <b>Release</b> and <b>Renew</b> buttons.
	Netmask	The subnet mask of your RG.
PPP IP Address		Enables/disables PPP unnumbered feature.
	IP Address	The IP address should be different from, but in the same subnet as the WAN-side IP address.
Use the following Static IP address		This field enables you to change the IP address of the RG.
	IP Address	The default IP address of the RG (as shown) is 192.168.1.1.
	Netmask	The default subnet mask of your RG is 255.255.255.0. This subnet allows the RG to support 254 users. If you want to support a larger number of users you can change the subnet mask.



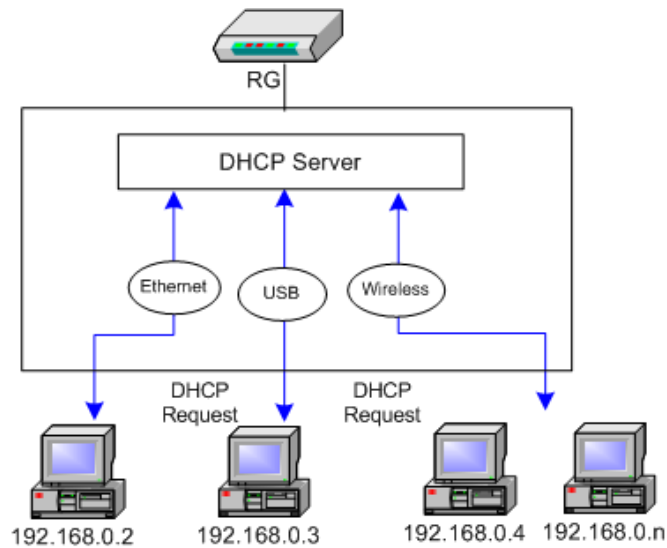
**Table 2-9 LAN Group Configuration Field Descriptions**

Category/Field	Field	Definition/Description
	Default Gateway	The default gateway is the routing device used to forward all traffic that is not addressed to a station within the local subnet. Your ISP provides you with the IP address of the default gateway.
	Host Name	The host name is used in conjunction with the domain name to uniquely identify the RG. It can be any alphanumeric word that does not contain spaces.
	Domain	The domain name is used in conjunction with the host name to uniquely identify the RG. To access the web pages of the RG you can type <i>192.168.1.1</i> (the IP address) or <i>mygateway1.ar7</i> (Host Name.Domain).
Enable DHCP Server		Enables/disables DHCP. By default, your RG has the DHCP server (LAN side) enabled. If you already have a DHCP server running on your network, you must disable one of the two DHCP servers. The DHCP server data flow is shown in <a href="#">Figure 2-38</a> on page 2-44.
	Assign ISP DNS, SNTP	Enable/disables the <b>Assign ISP DNS, SNTP</b> feature when the DHCP server of your RG has been enabled. To learn more about the <b>Assign ISP DNS, SNTP</b> feature, go to " <a href="#">Assign ISP DNS, SNTP</a> " on page 2-44.
	Start IP	The Start IP Address is where the DHCP server starts issuing IP addresses. This value must be greater than the IP address value of the RG. For example, if the IP address of the RG is <i>192.168.1.1</i> (default), then the starting IP address must be <i>192.168.1.2</i> (or higher).  Note: If you change the start or end values, make sure the values are still within the same subnet as the RG. In other words, if the IP address of the RG is <i>192.168.1.1</i> (default) and you change the DHCP start/end IP addresses to be <i>192.168.1.2/192.168.1.100</i> , you cannot communicate with the RG if your host has DHCP enabled.
	End IP	The End IP Address is where the DHCP server stops issuing IP addresses. The ending address cannot exceed a subnet limit of 254, hence the max value for the default gateway is <i>192.168.1.254</i> . If the DHCP server runs out of DHCP addresses, users do not get access to network resources. If this happens, you can increase the Ending IP address (to the limit of 254) or reduce the lease time.  Note: If you change the start or end values, make sure the values are still within the same subnet as the IP address of the RG. In other words, if the IP address of the RG is <i>192.168.1.1</i> (default) and you change the DHCP start/end IP addresses to be <i>192.168.1.2/192.168.1.100</i> , you cannot communicate with the RG if your host has DHCP enabled.
	Lease Time	The Lease Time is the amount of time that a network user is allowed to maintain a network connection to the RG using the current dynamic IP address. At the end of the Lease Time, the lease is either renewed or a new IP is issued by the DHCP server. The amount of time is in units of seconds. The default value is 3600 seconds (1 hour). The maximum value is 999999 seconds (about 278 hours).
Enable DHCP Relay		In addition to the DHCP server feature, the RG supports the DHCP relay function. When the RG is configured as DHCP server, it assigns the IP addresses to the LAN clients. When the gateway is configured as DHCP relay, it is responsible for forwarding the requests and responses negotiated between the DHCP clients and the server. See <a href="#">Figure 2-39</a> .

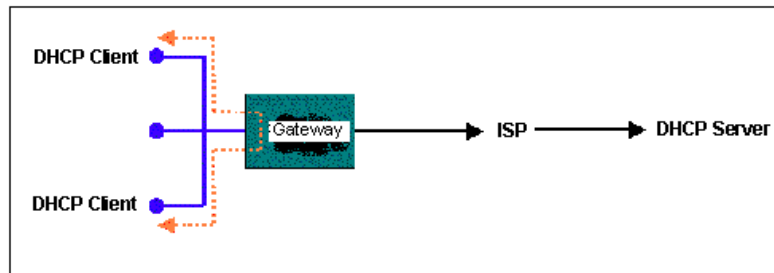
**Table 2-9 LAN Group Configuration Field Descriptions**

Category/Field	Field	Definition/Description
	Relay IP	The IP address of the DHCP relay server.
Server and Relay Off		When the DHCP server and relay functions are turned off, the network administrator must carefully configure the IP address, Subnet Mask, and DNS settings of every host on your network. Do not assign the same IP address to more than one host. Also, your RG must reside on the same subnet as all the other hosts.
<b>End of Table 2-9</b>		

**Figure 2-38 DHCP Server Data Flow**



**Figure 2-39 Example of a DHCP Relay configuration**



**Assign ISP DNS, SNTP**

When you enable the DHCP server on the LAN side, the RG dynamically assigns IP addresses to the hosts on the local network. The RG provides its own LAN IP address (192.168.1.1) as both the gateway and the DNS server (as shown in Figure 2-40).

On the WAN side, the RG receives the following data (among other data) from the ISP:

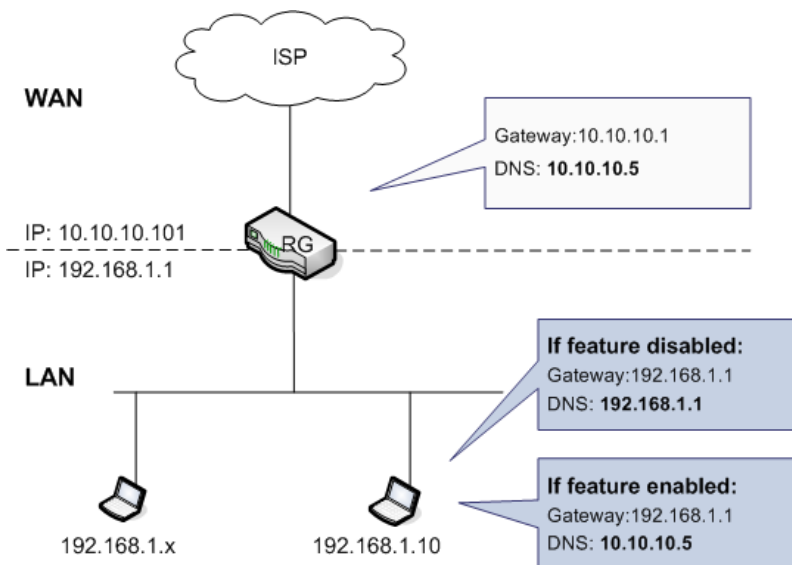
- IP: *10.10.10.101*
- Gateway: *10.10.10.1*
- DNS: *10.10.10.5*

The RG has a choice of advertising its own IP address (*192.168.1.1*) to the LAN side hosts as the DNS server, or providing the DNS that was received from the WAN side (*10.10.10.5*). This can be configured by enabling/ disabling **Assign ISP DNS SNTP** on the **LAN Group Configuration** page.



**Note**—This section only applies when you have enabled DHCP server on the **LAN Group Configuration** page (Figure 2-37 on page 2-42).

**Figure 2-40 External DHCP Options**



**The default option (feature disabled)**

As shown in Figure 2-40, when **Assign ISP DSN SNTP** is disabled, the hosts on the LAN network use the LAN IP address of the RG as the DNS. The following data is provided to the host by the DHCP server.

- IP: *192.168.1.x*
- Gateway: *192.168.1.1*
- DNS: *192.168.1.1*

### The external DHCP option (*feature enabled*)

As shown in [Figure 2-40](#), when **Assign ISP DSN SNTP** is enabled, the host on the LAN network uses the WAN side DNS. The following data is provided to the host:

- IP: 192.168.1.x
- Gateway: 192.168.1.1
- DNS: **10.10.10.5**



**Note**—If the WAN connection is also of DHCP type, the RG receives additional data from the ISP, and if **Assign ISP DSN SNTP** is enabled, the data is passed on to the LAN side hosts as well. The additional data may include (but not limited to) the following:

- Time server
- Log server
- Cookie server
- Print server
- NTP server
- WINS server

## 2.4.2 Ethernet Switch Configuration

The **Ethernet Switch Configuration** page is available in the AR7WRD SDB and not in the AR7VW SDB.

Ethernet switch port settings can be configured to meet the requirements of your LAN configuration. As seen in the drop-down menu in [Figure 2-41](#), port setting options include:

- Auto detect (default)
- 10 Mbps half duplex
- 10 Mbps full duplex
- 100 Mbps half duplex
- 100 Mbps full duplex

In the example shown, the system has auto-detected an Ethernet cable connected to LAN port 2 and assigned a port setting of 100 Mbps full duplex.

**Figure 2-41 Ethernet Switch Configuration**

	Set Value	Fallback Value
Physical Port1:	Auto	Disabled
Physical Port2:	Auto	100/Full Duplex
Physical Port3:	Auto	Disabled
Physical Port4:	Auto	Disabled

Auto  
10/Half Duplex  
10/Full Duplex  
100/Half Duplex  
100/Full Duplex

Apply Cancel

## 2.5 Hidden Page

There is a hidden page in the **Setup** section that allows you to enable and disable the firewall and NAT for all WAN connections. This feature is enabled by default. If you disable it, it is disabled for all WAN connections. If you enable it again after you have disabled, it could take sometime for the request to be processed.

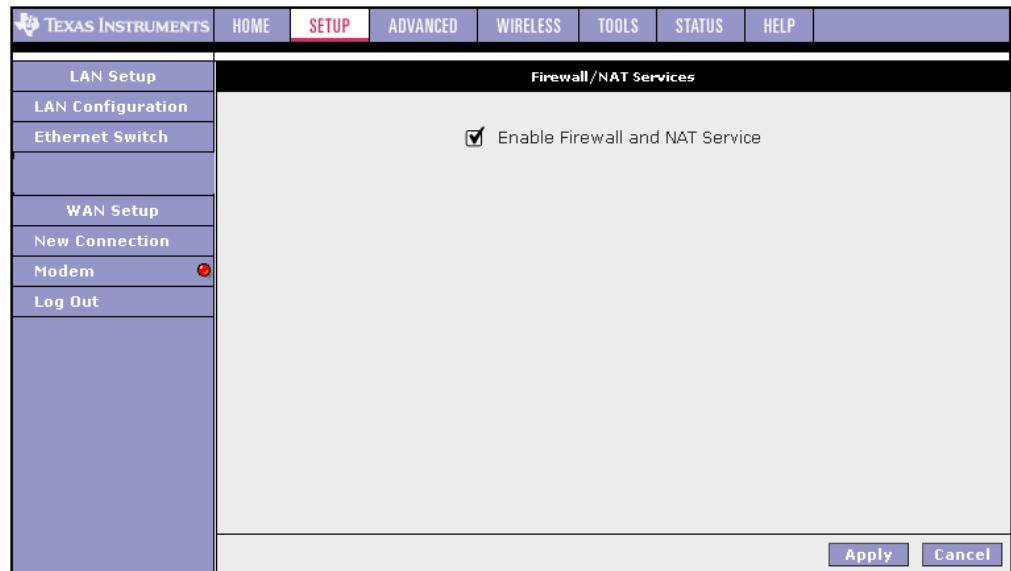


**Note**—The hidden page is to be used by ODMs/OEMs for development and debugging purposes only. Do **NOT** distribute this section to the end user.

The **Firewall/NAT Services** hidden page (Figure 2-42) can be accessed by replacing the pagename in the URL with “*pagename=fw\_nat*” or typing in the following address:

[http://192.168.1.1/cgi-bin/webcm?getpage=..%2Fhtml%2Fdefs%2Fstyle5/menus%2Fmenu.html&var:style=style5&var:main=menu&var:pagename=fw\\_nat&var:pagetitle=Home&var:menu=setup&var:menutitle=Setup](http://192.168.1.1/cgi-bin/webcm?getpage=..%2Fhtml%2Fdefs%2Fstyle5/menus%2Fmenu.html&var:style=style5&var:main=menu&var:pagename=fw_nat&var:pagetitle=Home&var:menu=setup&var:menutitle=Setup)

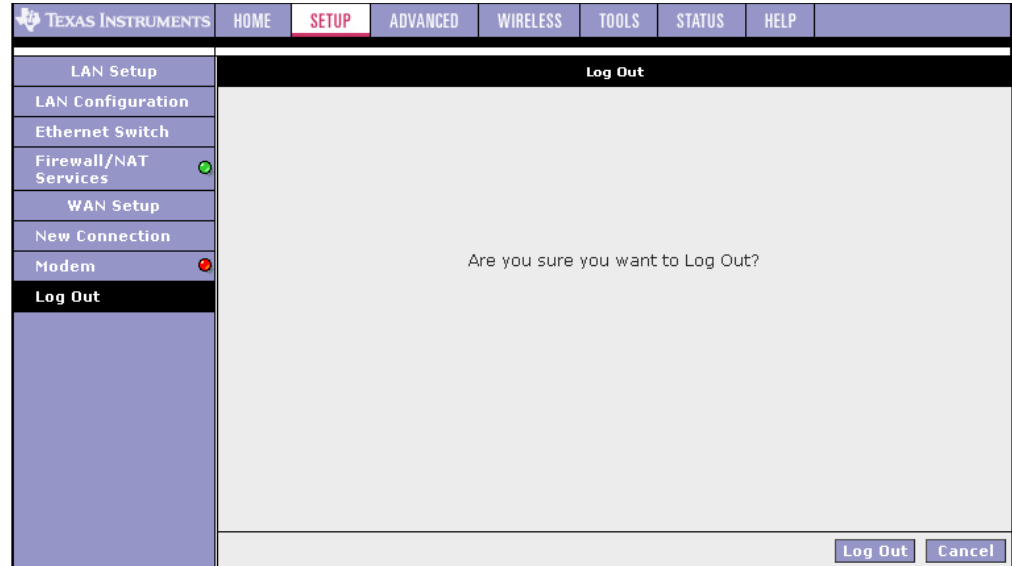
**Figure 2-42 Firewall/NAT Services**



## 2.6 Log Out Page

By clicking **Log Out**, you log out of the RG GUI (not just the Setup interface) as shown in [Figure 2-43](#).

**Figure 2-43 Log Out Page**



Use [Procedure 2-10](#) to log out.

### Procedure 2-10 Log Out

#### Step – Action

- 1 Click **Log Out** at the left-hand column.  
You are prompted to confirm the Log Out.
- 2 Confirm by clicking **Log Out** at the bottom-right corner.  
You are taken back to the **Log In** page ([Figure 1-1](#) on page 1-7).

#### End of Procedure 2-10





# Advanced

---

---

---

The **Advanced** tab allows you to perform advanced configuration functions for existing connections. This chapter discusses:

- ["Advanced Tab Main Page"](#) on page 3-2
- ["Voice Page"](#) on page 3-4
- ["UPnP Page"](#) on page 3-6
- ["SNTP Page"](#) on page 3-8
- ["SNMP Page"](#) on page 3-11
- ["TR-069"](#) on page 3-14
- ["Port Forwarding Page"](#) on page 3-16
- ["IP Filters Page"](#) on page 3-24
- ["LAN Clients Page"](#) on page 3-28
- ["LAN Isolation Page"](#) on page 3-31
- ["TR-068 WAN Access"](#) on page 3-32
- ["Bridge Filters Page"](#) on page 3-34
- ["Web Filters Page"](#) on page 3-36
- ["Dynamic DNS Client"](#) on page 3-37
- ["IGMP Proxy Page"](#) on page 3-39
- ["Static Routing Page"](#) on page 3-45
- ["Dynamic Routing Page"](#) on page 3-48
- ["QoS"](#) on page 3-52
- ["Policy Database"](#) on page 3-74
- ["Web Access Control Page"](#) on page 3-81
- ["SSH Access Control Page"](#) on page 3-83
- ["Voice Provision"](#) on page 3-86

## 3.1 Advanced Tab Main Page

The **Advanced** tab allows you to perform advanced configuration functions for existing connections including:

- Enabling and disabling of key features including voice, voice provision, UPnP, SNTP, SNMP, TR-069, RIP, access control, TR-068 WAN access, and multicasting
- QoS (ingress, egress, shaper) and policy database
- Management of LAN port interfaces, packet flow, and filtering

At least one WAN connection must be configured before implementing advanced WAN configuration features. At least one LAN group must be defined before implementing advanced LAN configuration features.

[Figure 3-1](#) shows the **Advanced** main page, which is accessed by clicking the **Advanced** tab at the top of the page. This page provides access to the following configuration pages:

- Voice (on AR7VW platform only)
- UPnP
- SNTP
- SNMP (on AR7WRD platform only)
- TR-069
- Port Forwarding
- IP Filters (per connection or LAN group)
- LAN Clients
- LAN Isolation (between LAN groups)
- TR-068 WAN Access
- Bridge Filters
- Web Filters (for all LAN users)
- Dynamic DNS Client
- IGMP Proxy
- Static Routing (on AR7WRD platform only)
- Dynamic Routing
- Policy Database
- Ingress
- Egress
- Shaper
- Web Access Control

- SSH Access Control
- Voice Provision (on AR7VW platform only)

**Figure 3-1 Advanced Main (on AR7VW Platform)**

TEXAS INSTRUMENTS		HOME	SETUP	ADVANCED	WIRELESS	TOOLS	STATUS	HELP
Voice		<b>Advanced</b>						
UPnP		The Advanced section lets you configure advanced features like RIP, Firewall, NAT, Voice, UPnP, IGMP, Bridge Filters, and LAN clients.						
SNTP								
TR-069								
Port Forwarding								
IP Filters								
LAN Clients								
LAN Isolation								
TR-068 WAN Access								
Bridge Filters								
Web Filters								
Dynamic DNS Client								
IGMP Proxy								
Static Routing								
Policy Database								
Ingress								
Egress								
Shaper								
Web Access Control								
SSH Access Control								
Voice provision								
Log Out								

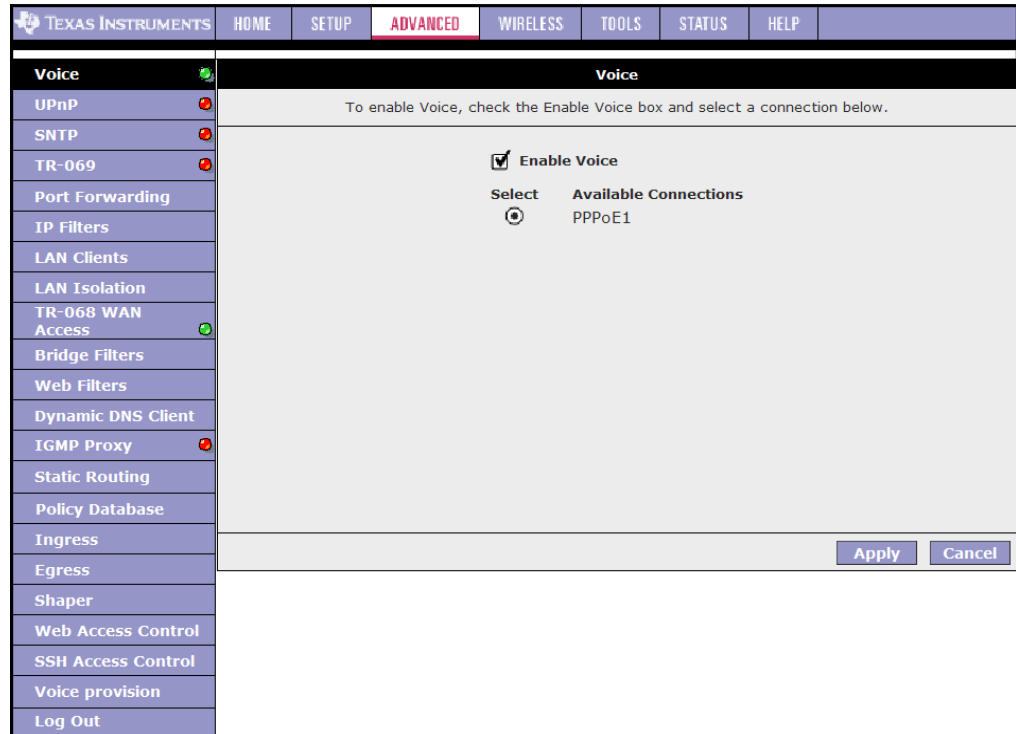
  

<b>Voice</b>	Configure Voice for different connections.
<b>UPnP</b>	Configure UPnP for different connections.
<b>SNTP</b>	Configure SNTP to configure time server on Internet.
<b>Port Forwarding</b>	Configure Firewall and NAT pass-through to your hosted applications.
<b>IP Filters</b>	Configure Firewall to block your LAN PCs from accessing the Internet.
<b>LAN Clients</b>	Configure LAN Clients.
<b>LAN Isolation</b>	Disable traffic between LANs.
<b>Bridge Filters</b>	Select to setup Bridge Filters.
<b>Web Filters</b>	Select to setup Web Filters.
<b>Multicast</b>	Configure Multicast pass-through for different connections.
<b>Static Routing</b>	Configure Static routes.
<b>Web Access Control</b>	Configure access control list for remote Web access.
<b>SSH Access Control</b>	Configure access control list for remote SSH access.
<b>Policy Database</b>	Configure Policy Routing and QoS Database information.
<b>Ingress</b>	Configure Ingress information.
<b>Egress</b>	Configure Egress information.
<b>Shaper</b>	Configure Shaper information.
<b>Provisioning</b>	Configure provisioning.

## 3.2 Voice Page

Figure 3-2 shows the default **Voice** page, which is accessed by clicking the **Voice** link. This page allows you to enable or disable voice on a single WAN connection. When voice is enabled, there is a green status indicator next to the Voice link. When voice is disabled, the status indicator is red.

Figure 3-2 Voice Page



At least one WAN connection must be configured in order to access the **Voice Setup** page. While up to eight WAN connections can be configured on your RG, only one connection can be selected to enable voice. By default, voice is automatically enabled on the first WAN connection you create. Each additional WAN connection you create is added to the list of Available Connections that are also candidates for enabling voice.

Voice-specific parameters can be configured using one of the following three methods:

1. The MXP command line interface, which is accessed from the CLI. More information about voice-specific configuration commands and parameters can be found in the *NMM Command Reference Manual*.
2. XML provisioning file. More information about XML provisioning can be found in the *XML Provisioning Developer Guide*.
3. The web pages. For more information, visit 3.22 “[Voice Provision](#)” on page 3-86.

**NMM vs. XML:**

Most of the command line configuration can be done using XML tags. An example is given below:

- **MXP command line:**

```
MXP>set tcid <tcid> rtcp enable <on|off>
```

- **XML Tag:**

```
<RTCP_ENABLE>TRUE</RTCP_ENABLE>
```

Please keep in mind, the MXP CLI-to-XML mappings may not exist for all configuration options. It is recommended that you start using XML tags because XML provisioning will be the primary configuration method moving forward.

### 3.3 UPnP Page

The NSP supports a control point for Universal plug and play (UPnP), version 1.0 and supports two key features: **NAT traversal** and **Device Identification**. This feature requires one active WAN connection. In addition, the PC should support this feature. In the presence of multiple WAN connections, select a connection on which the incoming traffic is present, for example, the default WAN connection.

Figure 3-3 shows the UPnP data flow. The UPnP application sits on top of a HTTP based socket listening for UPnP requests. With NAT Traversal, when an UPnP command is received to open ports in NAT, the application translates the request into IP tables commands to open the ports in NAT and the firewall, mapping them back to the IP address of the PC on the LAN making the request. The connection to open the ports on is given to UPnP when it starts up and is part of the configuration of the application.

For Device Identification, the application will send a description of the NSP as a control point back to the device making the request. An example of how this works is with Windows XP. You can go into the network for Windows XP and you will see the RG represented. You can then click on the RG and get access to its web pages.

Figure 3-3 UPnP Data Flow

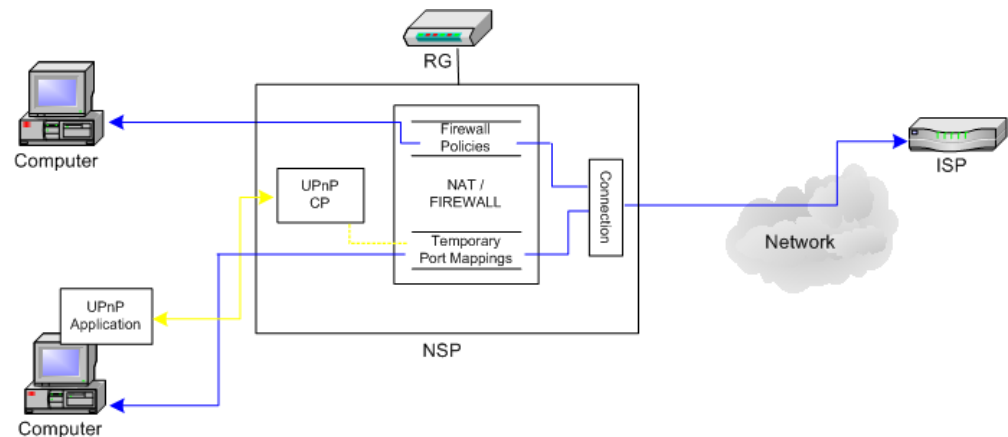


Figure 3-4 shows the default UPnP page.

**Figure 3-4 UPnP Page**

The screenshot displays the UPnP configuration interface. The top navigation bar includes 'HOME', 'SETUP', 'ADVANCED', 'WIRELESS', 'TOOLS', 'STATUS', and 'HELP'. The left sidebar lists various settings, with 'UPnP' highlighted. The main panel contains the following elements:

- UPnP** (Section Header)
- Instruction: To enable UPnP, check the Enable UPnP box and select a connection below.
- Enable UPnP
- WAN Connection: PPPoE1 (dropdown menu)
- LAN Connection: LAN group 1 (dropdown menu)
- Buttons: Apply, Cancel

Use [Procedure 3-1](#) to configure UPnP.

### Procedure 3-1 Configure UPnP

#### Step – Action

- 1 Check **Enable UPnP**.  
This enables the WAN Connection and LAN Connection fields.
- 2 Select the **WAN Connection** and **LAN Connection** that will use UPnP from the drop-down lists.
- 3 Click **Apply** to temporarily activate the settings.  
**Note**—The changes take effect when you click **Apply**; however, if the RG configuration is not saved, these changes will be lost upon RG reboot.
- 4 To make the change permanent, click **Tools** (at the top of the page) and select **System Commands**.
- 5 On the **System Commands** page ([Figure 5-2](#) on page 5-3), click **Save All**.

#### End of Procedure 3-1

## 3.4 SNTP Page

Simple network timing protocol (SNTP) is a protocol used to synchronize the system time to the public SNTP servers. It uses the UDP protocol on port 123 to communicate between clients and servers. The NSP supports SNTP client functionality in compliance with IETF RFC 2030. The system clock time in NSP can be configured by SNTP client functioning in daemon mode which issues sending client requests to the configured SNTP server addresses periodically. The NSP can be configured with the SNTP server addresses either through CLI or Web or through DHCP at boot time. Figure 3-5 shows the SNTP client functionality.

**Figure 3-5 SNTP Client Functionality**

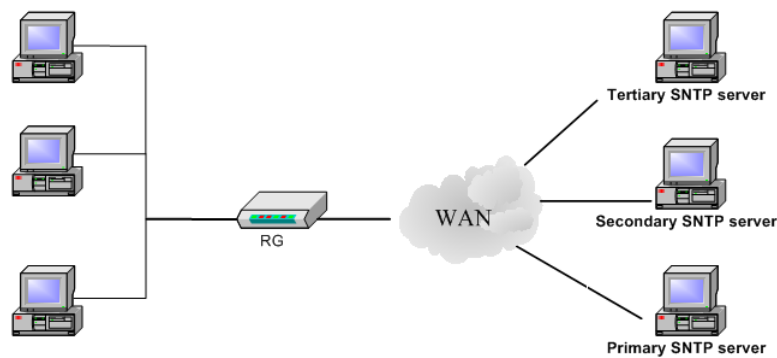


Figure 3-6 shows the default SNTP page.

**Figure 3-6 SNTP Page**

TEXAS INSTRUMENTS		HOME	SETUP	ADVANCED	WIRELESS	TOOLS	STATUS	HELP
Voice	✔	<b>SNTP</b> To enable SNTP, check the Enable SNTP box and enter a time server.  <input type="checkbox"/> Enable SNTP Primary SNTP Server: <input type="text" value="0.0.0.0"/> Secondary SNTP Server: <input type="text" value="0.0.0.0"/> Tertiary SNTP Server: <input type="text" value="0.0.0.0"/> Timeout: <input type="text" value="5"/> Secs Polling Interval: <input type="text" value="30"/> Mins Retry Count: <input type="text" value="2"/> Time Zone: <input type="text" value="(GMT-12:00) International Date Line West"/> Day Light: <input type="checkbox"/>						
UPnP	✘							
<b>SNTP</b>	✘							
TR-069	✘							
Port Forwarding								
IP Filters								
LAN Clients								
LAN Isolation								
TR-068 WAN Access	✔							
Bridge Filters								
Web Filters								
Dynamic DNS Client								
IGMP Proxy	✘							
Static Routing								
Policy Database								
Ingress								
Egress								
Shaper								
Web Access Control								
SSH Access Control								
Voice provision								
Log Out								



When the SNTP feature is enabled, your RG starts querying for the time clock information from the primary SNTP server. If it fails to get a valid response within the **Timeout** period, it makes additional attempts based on the number specified in the **Retry Count** field before moving to the Secondary SNTP server. If it fails to get a valid response from Secondary STNP server within the specified retry count, it starts querying the Tertiary SNTP server. If it fails to get a valid response from all the servers, then the program stops. Once a valid response is received from one of the servers, the program goes to sleep for number of minutes specified in the **Polling Interval** field before starting the whole process again.

Use [Procedure 3-2](#) to enable SNTP.

---

**Procedure 3-2 Enable SNTP****Step – Action**

- 1 Check **Enable SNTP**.
- 2 Use [Table 3-1](#) as a reference and configure the following fields:
  - Primary SNTP Server
  - Secondary SNTP Server
  - Tertiary SNTP Server
  - Timeout
  - Polling Interval
  - Retry Count
  - Time Zone
  - Day Light
- 3 Click **Apply** to temporarily activate the settings.

**Note**—The changes take effect when you click **Apply**; however, if the RG configuration is not saved, these changes will be lost upon RG reboot.
- 4 To make the change permanent, click **Tools** and select **System Commands**.
- 5 On the **System Commands** page ([Figure 5-2](#) on page 5-3), click **Save All**.

---

**End of Procedure 3-2**

---

Table 3-1 describes the SNTP page fields.

**Table 3-1 SNTP Field Descriptions**

Field	Definition/ Description
Primary SNTP Server	The IP address or the host name of the primary SNTP server. This can be provided by ISP or user-defined.
Secondary SNTP Server	The IP address or the host name of the secondary SNTP server. This can be provided by ISP or user-defined.
Tertiary SNTP Server	The IP address or the host name of the tertiary SNTP server. This can be provided by ISP or user-defined.
Timeout	If the RG failed to connect to a SNTP server within the <b>Timeout</b> period, it retries the connection.
Polling Interval	The amount of time between a successful connection with a SNTP server and a new attempt to connect to an SNTP server.
Retry Count	The number of times the RG tries to connect to an SNTP server before it tries to connect to the next server in line.
Time Zone	The time zone in which the RG resides.
Day Light	Check/uncheck this option to enable/disable daylight saving time (DST). Note: DST is not automatically enabled or disabled. You need to manually enable and disable it.
<b>End of Table 3-1</b>	

### 3.5 SNMP Page

The SNMP page is only available on the AR7WRD platform and not available on the AR7VW platform in this release.

Simple network management protocol (SNMP) is a troubleshooting and management protocol that uses the UDP protocol on port 161 to communicate between clients and servers. The NSP can be managed either locally or remotely by Network Management stations through SNMP protocol. SNMP access on the LAN or WAN side must be allowed to enable SNMP management.

Figure 3-7 shows the SNMP agent diagram.

Figure 3-7 SNMP Agent Diagram

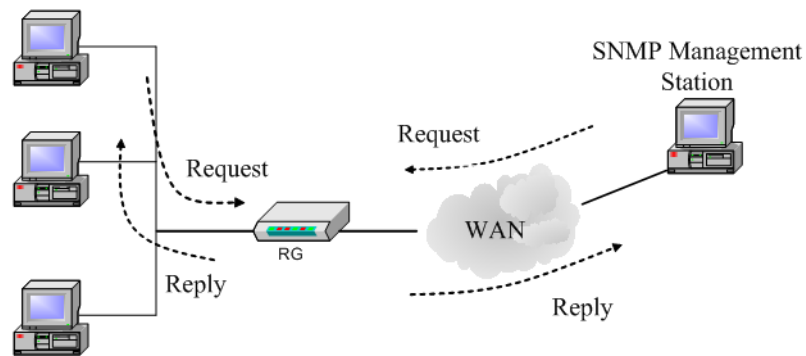
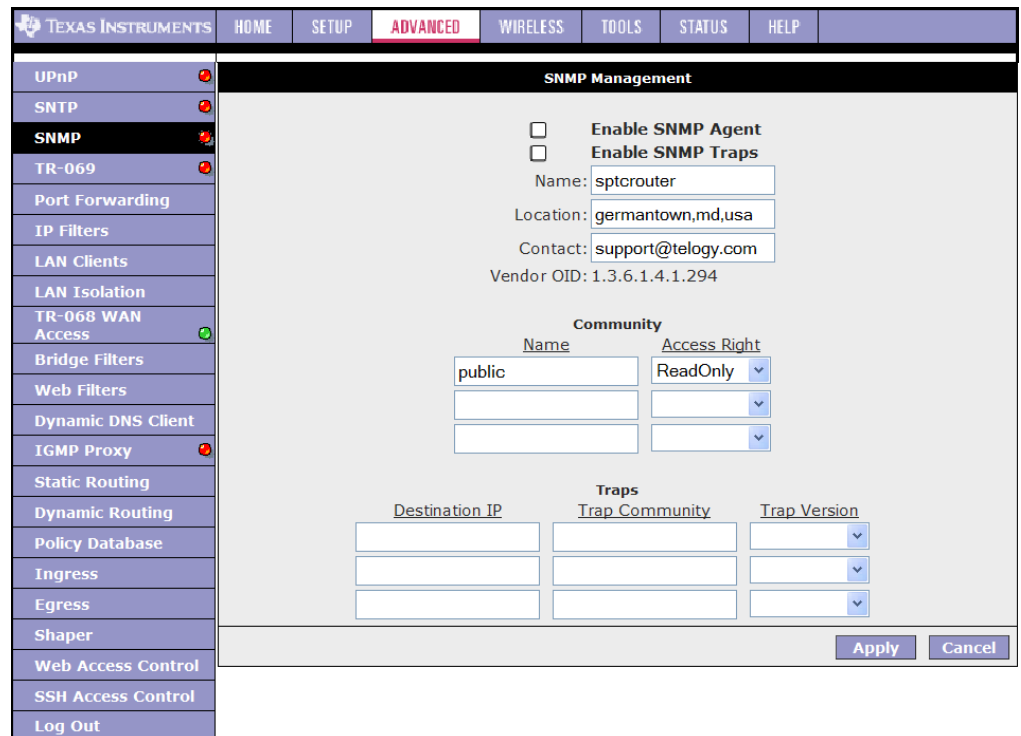


Figure 3-8 shows the default SNMP page.

Figure 3-8 SNMP Management



SNMP uses a Manager- Management information base (MIB)-Agent solution to fulfill network management needs. The manager is a separate station that can request data from an SNMP agent, which resides in each modem on the network. The agent uses the MIBs as dictionaries of manageable objects. The SNMP agent supports GET, SET, GETNEXT, and TRAP for four groups with MIB-II: System, Interface, IP, and ICMP.

The SNMP agents support three community names authentication. [Table 3-2](#) describes the **SNMP Management** page fields.

**Table 3-2 SNMP Field Descriptions**

Field	Definition/ Description
Enable SNMP Agent	The SNMP agent is enabled by default.
Enable SNMP Traps	SNMP traps are enabled to send by default.
Name	An administratively-assigned name for the RG.
Location	The physical location of the RG.
Contact	Contact person and/or contact information for the RG.
Vendor OID	Vendor object identifier. The vendor's authoritative identification of the network management subsystem contained in the entity. This value is allocated within the SMI enterprises subtree (1.3.6.1.4.1). For example, Texas Instruments was assigned the subtree 1.3.6.1.4.1.294.
Community	<p>SNMP defines a community to be a relationship between an SNMP agent and one or more SNMP managers. Once the clear-text community name corresponds to a community known to the receiving SNMP entity, the sending SNMP entity is considered to be authenticated as a member of that community and is granted different levels of access: <i>read-only</i> or <i>read-write</i>. The combination of community access mode and a MIB-managed project defines the community profile for each object. The community profile defines the operations that can be applied to the object. In the RG, a default community name of <i>public</i> with access mode of read-only is created in the configuration file. It allows a GET or a GETNEXT operation to all objects with access rights of READ-ONLY and READ-WRITE in the MIB.</p> <p>In the RG, up to three community names can be configured through the web page. The view_subtrees of SNMPv2c and user-based security model and view-based access control model of SNMPv3 will be supported in future SNMP agent development.</p>
Community Name	Name of community. SNMP supports up to 3 communities including the default community name of <i>public</i> .
Community Access Right	<p>Two options are offered:</p> <ul style="list-style-type: none"> <li>• ReadOnly: Allows a GET or a GETNEXT operation to all objects in the MIB.</li> <li>• ReadWrite: Allows ReadOnly access right to all objects and SET operation to objects defined as read-writable in the MIB.</li> </ul>

**Table 3-2 SNMP Field Descriptions**

Field	Definition/ Description
Trap	Trap is an event notification. There are four standard traps supported in the RG: <ul style="list-style-type: none"><li>• WarmStartTrap</li><li>• LinkUpTrap</li><li>• LinkDownTrap</li><li>• AuthenticationFailureTrap</li></ul>
Trap Destination IP	Destination IP address of the trap. Traps can be sent to three different destinations.
Trap Community	Community name of the trap.
Trap Version	Two trap versions/formats are supported: <ul style="list-style-type: none"><li>• SNMP v1</li><li>• SNMP v2c</li></ul>
<b>End of Table 3-2</b>	

## 3.6 TR-069

TR-069 is CPE Management Protocol from WAN side, intended for communication between a CPE and Auto-Configuration Server (ACS). The CPE WAN Management Protocol defines a mechanism that encompasses secure auto-configuration of a CPE, and also incorporates other CPE management functions into a common framework.

The CPE WAN Management Protocol is intended to support a variety of functionalities to manage a collection of CPE, including the following primary capabilities:

- Auto-configuration and dynamic service provisioning
- Software/firmware image management
- Status and performance monitoring
- Diagnostics

Figure 3-9 shows the default TR-069 page, which is accessed by clicking the TR-069 link on the **Advanced** page. The TR-069 page allows you to set up connection parameters and may not be seen by the end user.

**Figure 3-9 TR-069 Page**

TEXAS INSTRUMENTS	HOME	SETUP	ADVANCED	WIRELESS	TOOLS	STATUS	HELP
Voice	<b>TR-069</b>						
UPnP	TR-069 is enabled by default. Select a default WAN connection and set the ACS URL below.						
SNTP	ACS URL: <input type="text" value="http://192.168.1.2:9995"/> <input type="button" value="ACS Connect"/>						
<b>TR-069</b>	Periodic Inform Enabled: <input type="checkbox"/>						
Port Forwarding	Periodic Inform Interval: <input type="text" value="86400"/>						
IP Filters	<b>ACS Connection Request</b>						
LAN Clients	Username: <input type="text" value="00E0A6-111"/>						
LAN Isolation	Password: <input type="password" value="••••••••"/>						
TR-068 WAN Access	<input type="button" value="Apply"/> <input type="button" value="Cancel"/>						
Bridge Filters							
Web Filters							
Dynamic DNS Client							
IGMP Proxy							
Static Routing							
Policy Database							
Ingress							
Egress							
Shaper							
Web Access Control							
SSH Access Control							
Voice provision							
Log Out							

[Table 3-3](#) describes the **TR-069** page settings.

**Table 3-3 TR-069 Field Descriptions**

Field	Definition/ Description
ACS URL	URL of the auto configuration server (ACS) provided by the ISP.
Periodic Inform Enabled	Enable/disables the RG to connect to the ACS periodically. If you enable this feature, you should enter a value in the <b>Periodic Inform Interval</b> field.
Periodic Inform Interval	This field is enabled only when the <b>Periodic Inform Enabled</b> field is checked. It defines the amount of time (in seconds) between a successful connection with an ACS server and a new attempt to connect to an ACS server. A recommended value is <i>86400</i> seconds ( <i>1</i> day).
ACS Connect	By clicking the ACS Connect button, you manually connect the RG to the ACS.
ACS Connection Request: Username/Password	The username/password are used when the ACS wants to initiate a connection with the RG. The RG authenticates the ACS using the username/password. The username/password are provided by the ISP.
<b>End of Table 3-3</b>	

Use [Table 3-3](#) as a reference and follow [Procedure 3-3](#) to configure parameters related to TR-069.

**Procedure 3-3 Configure TR-069**

**Step – Action**

- 1 Leave the default URL in the **ACS URL** field.
- 2 Check **Periodic Inform Enabled** and enter a value in the **Periodic Inform Interval** field.  
  
or  
Click **ACS Connect** to manually connect to the ACS. Once a connection is established, the ACS can update all three fields: **ACS URL**, **Periodic Inform Enabled**, and **Periodic Inform Interval**.
- 3 To allow ACS to initiate a connection with your RG, you can enter the ACS Connection Request **Username** and **Password**.  
The RG uses these two fields to authenticate the ACS.
- 4 Click **Apply** to temporarily activate the settings.  
**Note**—The changes take effect when you click **Apply**; however, if the RG configuration is not saved, these changes will be lost upon RG reboot.
- 5 To make the change permanent, click **Tools** and select **System Commands**.
- 6 On the **System Commands** page ([Figure 5-2](#) on page 5-3), click **Save All**.

**End of Procedure 3-3**

## 3.7 Port Forwarding Page

The port forwarding (or virtual server) feature allows you to direct incoming traffic to specific LAN hosts based on a protocol port number and protocol. Using the **Port Forwarding** page, you can provide local services (for example, web hosting) for people on the Internet or play Internet games. Port forwarding is configurable per LAN group.

A database of predefined port forwarding rules allows you to apply one or more rules to one or more members of a defined LAN group. You can view the rules associated with a predefined category and add the available rules for a given category. You can also create, edit, or delete your own port forwarding rules.

**Figure 3-10 Port Forwarding Page**

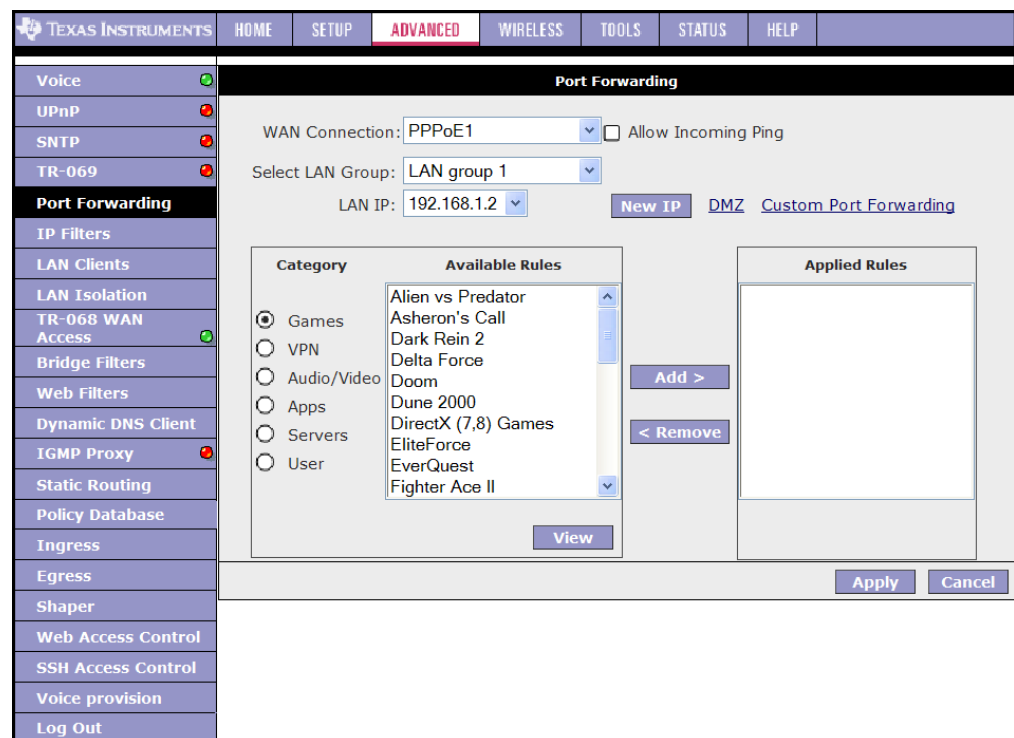


Table 3-4 describes the **Port Forwarding** page fields.

**Table 3-4 Port Forwarding Field Descriptions**

Field	Definition/ Description
WAN Connection	Select the WAN connection to which port forwarding is applied.
Select LAN Group	Select the LAN Group to which port forwarding is applied.
LAN IP	Select the IP address to host the service.
Allow Incoming Ping	Enabling incoming ping (ICMP) requests on the <b>Port Forwarding</b> page allows the RG to respond to a ping from the Internet.
DMZ	Demilitarized zone. More information on DMZ is available in 3.7.1 <a href="#">“DMZ Settings Page”</a> on page 3-20



**Table 3-4 Port Forwarding Field Descriptions**

Field	Definition/ Description
Custom Port Forwarding	This link takes you to the <b>Custom Port Forwarding</b> page. More information is available in 3.7.2 “ <a href="#">Custom Port Forwarding Page</a> ” on page 3-21.
Category	Custom and user-defined categories.
Available Rules	Predefined and user-defined IP filtering rules for each category.
Applied Rules	Lists the IP filtering rules you elect to apply for each given category.
<b>End of Table 3-4</b>	

You can use the pre-configured entry for a LAN segment following [Procedure 3-4](#).

#### **Procedure 3-4 Configure Port Forwarding**

##### **Step – Action**

- 1 On the **Port Forwarding Configuration** page, select **WAN Connection**, **LAN Group**, and **LAN IP**.

If the desired LAN IP is not available in the **LAN IP** drop-down menu, you can add it using the **LAN Client** page ([Figure 3-19](#) on page 3-28), which is accessed by clicking **New IP**.

- 2 Select the available rules for a given category and click **Add** to apply the rule for this category.

**Note**—You can click **View** to view the rule associated with a predefined filter on the **Rule Management** page ([Figure 3-11](#)).

**Figure 3-11 Port Forwarding - View An Existing Rule**

Protocol	Port Start	Port End	Port Map
TCP	47624	47624	47624
TCP	6073	6073	6073
TCP,UDP	2300	2400	2300

- If a rule is not in the list, you can create your own rule in the **User** category. Select **User** (Figure 3-12), then click **New**.

**Figure 3-12 Port Forwarding - User Category**

**Note**—The **New**, **View**, and **Delete** buttons become available only when the **User** category is selected. All the custom rules you create fall under the **User** Category.

- 4 The **Rule Management** page (Figure 3-13) populates for you to create new rules. Enter **Rule Name**, **Protocol**, **Port Start**, **Port End**, and **Port Map** fields, then click **Apply**.

**Figure 3-13 Rule Management**

The screenshot shows the Texas Instruments web interface. The top navigation bar includes 'HOME', 'SETUP', 'ADVANCED' (highlighted), 'WIRELESS', 'TOOLS', 'STATUS', and 'HELP'. A sidebar on the left lists various configuration categories: Voice, UPnP, SNTP, TR-069, Port Forwarding (highlighted), IP Filters, LAN Clients, LAN Isolation, TR-068 WAN Access, Bridge Filters, Web Filters, Dynamic DNS Client, IGMP Proxy, Static Routing, Policy Database, Ingress, Egress, Shaper, Web Access Control, SSH Access Control, Voice provision, and Log Out. The main content area is titled 'Rule Management' and contains the following fields: 'Rule Name:' (text input), 'Protocol:' (dropdown menu showing 'TCP'), 'Port Start:' (text input), 'Port End:' (text input), and 'Port Map:' (text input). Below these fields are 'Apply' and 'Cancel' buttons. At the bottom of the panel, there are links for 'Protocol', 'Port Start', 'Port End', and 'Port Map'.

The rules you create become available in the **User** category. You are able to view or delete the rules you create.

- 5 Continue to add rules as they apply from each category.
- 6 Click **Apply** when you finish to temporarily activate the settings.
 

**Note**—The changes take effect when you click **Apply**; however, if the RG configuration is not saved, these changes will be lost upon RG reboot.
- 7 To make the change permanent, click **Tools** and select **System Commands**.

- 8 On the **System Commands** page (Figure 5-2 on page 5-3), click **Save All**.

**End of Procedure 3-4**



**Note**—You can also use the **Custom Port Forwarding** link to add programs to the existing list, which is discussed in 3.7.2 “[Custom Port Forwarding Page](#)” on page 3-21.

### 3.7.1 DMZ Settings Page

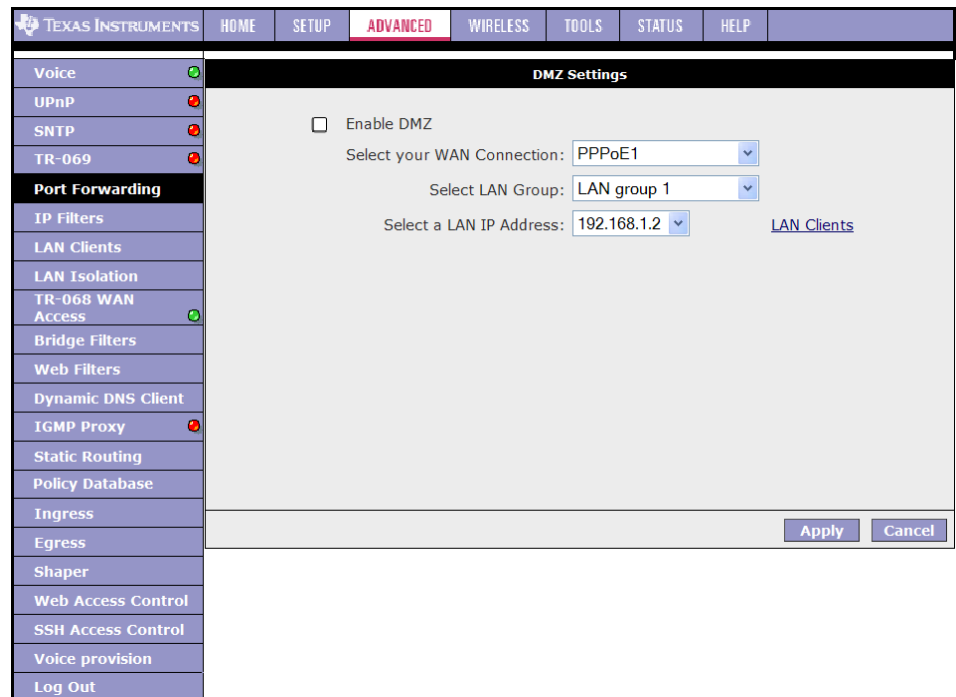
By setting a PC on your local network as demilitarized zone (DMZ), you can choose to forward all incoming packets that cannot be routed to a specific IP address to the PC with the DMZ IP address. This opens the access to the DMZ host from the Internet. This function is disabled by default. By enabling DMZ, you add an extra layer of security protection for hosts behind the firewall. Use the [Procedure 3-5](#) to enable it.

**Procedure 3-5 Enable DMZ**

**Step – Action**

- 1 On the **Port Forwarding** page (Figure 3-12), click the **DMZ** link.  
You are taken to the **DMZ Settings** page (Figure 3-14).

**Figure 3-14 Port Forwarding - DMZ Settings Page**



- 2 Check the **Enable DMZ** box.

- 3 Select the **WAN Connection, LAN Group, and LAN IP Address**.  
DMZ is configurable per LAN segment.
- 4 Click **Apply** when you finish to temporarily activate the settings.  
**Note**—You can access the **LAN Clients** page by clicking the **LAN Clients** link.  
**Note**—The changes take effect when you click **Apply**; however, if the RG configuration is not saved, these changes will be lost upon RG reboot.
- 5 To make the change permanent, click **Tools** and select **System Commands**.
- 6 On the **System Commands** page (Figure 5-2 on page 5-3), click **Save All**.

**End of Procedure 3-5**

Table 3-5 describes the **DMZ Settings** page fields.

**Table 3-5 DMZ Field Descriptions**

Field	Definition/ Description
Enable DMZ	Enables/disables the Demilitarized Zone feature. This field is unchecked (disabled) by default.
Select your WAN Connection	Select the WAN connection on which the DMZ feature is applied.
Select LAN Group	Select the LAN Group on which the DMZ feature is applied.
Select a LAN IP Address	Select the LAN IP address you are going to use as the DMZ host. This host is exposed to the Internet. Be aware that this feature may expose your local network to security risks.
LAN Clients	This link takes you to the <b>LAN Clients</b> page. More information on LAN Clients can be found in 3.9 “ <a href="#">LAN Clients Page</a> ” on page 3-28.
<b>End of Table 3-5</b>	

### 3.7.2 Custom Port Forwarding Page

The **Custom Port Forwarding** page (Figure 3-15) allows you to create up to 15 custom port forwarding entries to support specific services or applications, such as concurrent NAT/NAPT operation.

**Figure 3-15 Custom Port Forwarding Page**

The screenshot shows the 'Custom Port Forwarding' configuration page. On the left is a sidebar menu with items like Voice, UPnP, SNTP, TR-069, Port Forwarding (selected), IP Filters, LAN Clients, LAN Isolation, TR-068 WAN Access, Bridge Filters, Web Filters, Dynamic DNS Client, IGMP Proxy, Static Routing, Policy Database, Ingress, Egress, Shaper, Web Access Control, SSH Access Control, Voice provision, and Log Out. The main content area is titled 'Custom Port Forwarding' and includes the following fields:

- Connection: pppoe1 (dropdown)
- Enable:
- Application: (text input)
- Protocol: TCP (dropdown)
- Source IP Address: (text input)
- Source Netmask: (text input)
- Destination IP Address: (text input)
- Destination Netmask: 255.255.255.255
- Destination Port Start: (text input)
- Destination Port End: (text input)
- Destination Port Map: (text input)

At the bottom right of the main area are 'Apply' and 'Cancel' buttons. Below the main fields is a table header:

Enabled	Name	Source IP Mask	Destination IP Mask	Port Start Port End	Protocol	Edit	Delete
---------	------	----------------	---------------------	---------------------	----------	------	--------

Table 3-6 describes the Custom Port Forwarding page fields.

**Table 3-6 Custom Port Forwarding Field Descriptions**

Field	Definition/ Description
Connection	Select the WAN connection on which the Custom Port Forwarding rule is to be applied.
Enable	The <b>Enable</b> button is checked by default, meaning this rule is automatically applied when you click the <b>Apply</b> button.
Application	Name of the application for which your ports will be opened.
Protocol	There are three options available: <i>TCP</i> , <i>UDP</i> , and <i>TCP and UDP</i> .
Source IP Address	You can define the source IP address from which the incoming traffic is allowed. Enter <i>0.0.0.0</i> for all.
Source Netmask	Netmask of the source IP address. Enter <i>255.255.255.255</i> for all.
Destination IP Address	The LAN-side destination IP address for incoming traffic.
Destination Netmask	The LAN-side destination netmask for incoming traffic. The default value of this field is <i>255.255.255.255</i> .
Destination Port Start	The starting port number that is made open for this application.
Destination Port End	The ending port number that is made open for this application.

**Table 3-6 Custom Port Forwarding Field Descriptions**

Field	Definition/ Description
Destination Port Map	<p>Destination port mapped on the LAN (destination) side to which packets are forwarded. There are two types of port mapping:</p> <ul style="list-style-type: none"> <li>• One-to-one (one port mapped to one)</li> <li>• Multiple-to-one (multiple ports mapped to one port)</li> </ul> <div style="display: flex; justify-content: space-around; align-items: center;"> <div style="text-align: center;"> <p><b>Multiple-to-One</b></p> <p>WAN [ 500 ... 600 ]</p> <p>↓</p> <p>LAN 700</p> </div> <div style="text-align: center;"> <p><b>One-to-One</b></p> <p>[ 500 ... 600 ]</p> <p>↓ ... ↓</p> <p>[ 500 ... 600 ]</p> </div> </div>
<p>Note: Wildcard (*) entries are allowed for IP Address/Netmask and Port range fields.</p>	
<p><b>End of Table 3-6</b></p>	

## 3.8 IP Filters Page

The IP filtering feature allows you to block specific applications/services based on the IP address of a LAN device. You can use the **IP Filters** page (Figure 3-16) to block specific traffic (for example, block web access) or any traffic from a host on your local network.

A database of predefined IP filters allows you to apply one or more filtering rules to one or more members of a defined LAN group. You can view the rules associated with a predefined filter and add the available rules for a given category. You can also create, edit, or delete your own IP filter rules.

**Figure 3-16 IP Filters Page**

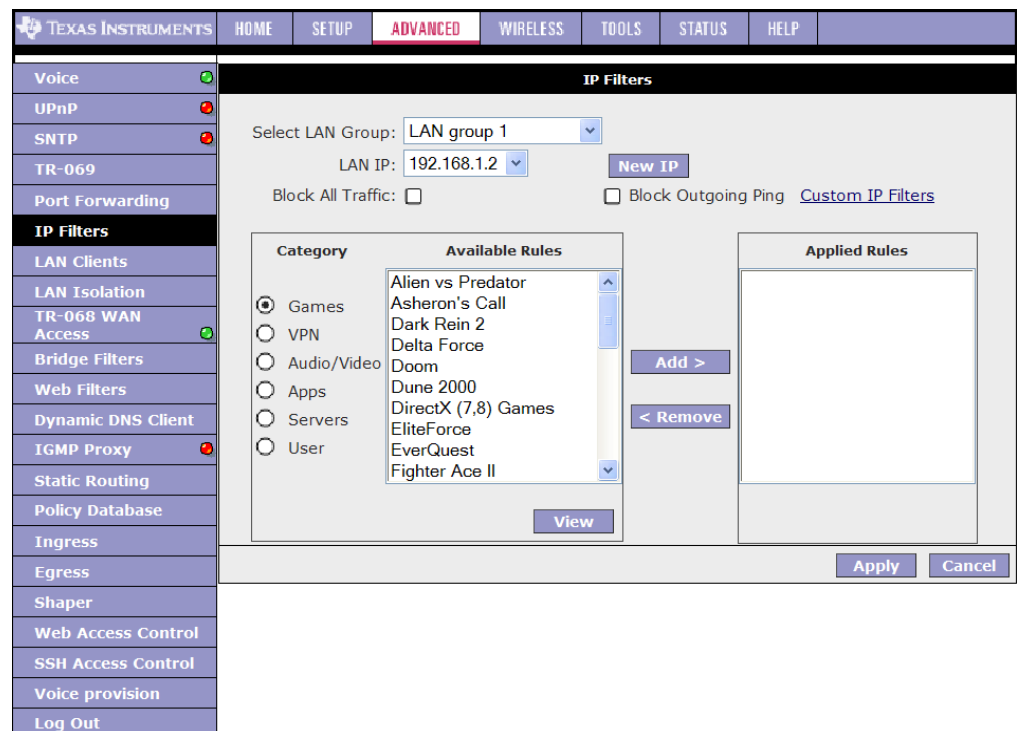


Table 3-7 describes the **IP Filters** page fields.

**Table 3-7 IP Filters Field Descriptions**

Field	Definition/ Description
Select LAN Group	Select the LAN group to which the IP filters feature will be applied.
LAN IP	Select the IP address in the given LAN group to which the IP Filters feature will be applied.
Block All Traffic	When checked, complete network access is blocked for the specific IP address.
Block Outgoing Ping	Blocking outgoing ping (ICMP) generated from a particular LAN IP can be used if your host has a virus that attempts a Ping-of-Death Denial of Service attack.



**Table 3-7 IP Filters Field Descriptions**

Field	Definition/ Description
Custom IP Filters	This link takes you to the <b>Custom IP Filters</b> page. More information is available in 3.8.1 “ <a href="#">Custom IP Filters Page</a> ” on page 3-26.
Available Rules	Predefined and user-defined IP filtering rules for each category.
Applied Rules	Lists the IP filtering rules you elect to apply for each given category.
<b>End of Table 3-7</b>	

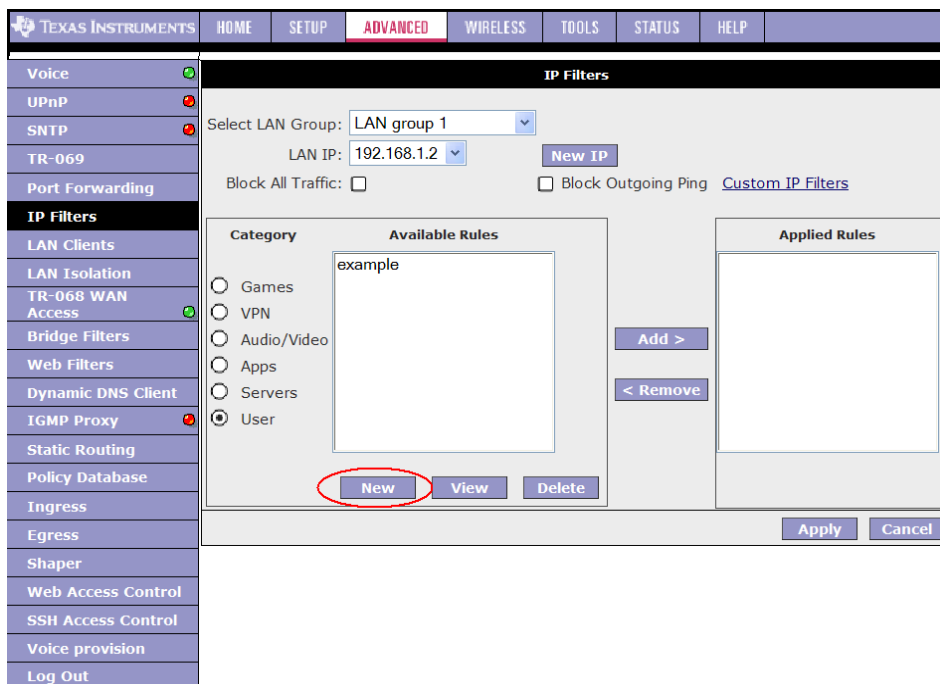
You can use the pre-configured entry for a LAN group using [Procedure 3-6](#).

**Procedure 3-6 Configure IP Filters**

**Step – Action**

- 1 On the **IP Filters** page ([Figure 3-16](#) on page 3-24), select **LAN Group** and **LAN IP**.  
  
If the desired LAN IP is not available in the **LAN IP** drop-down menu, you can add it using the **LAN Client** page ([Figure 3-19](#) on page 3-28), which is accessed by clicking **New IP**.
- 2 Select the available rules for a given category. Click **View** to view the rule associated with a predefined filter. Click **Add** to apply the rule for this category.
- 3 If a rule is not in the list, you can create your own rule in the **User** category. Select **User** ([Figure 3-17](#)), then click **New**.

**Figure 3-17 IP Filters - User Category**



**Note**—The **New**, **View**, and **Delete** buttons become available only when the **User** category is selected. All the custom rules you create fall under the **User** Category.

- 4 The **Rule Management** page (Figure 3-13 on page 3-19) populates for you to create new rules. Enter **Rule Name**, **Protocol**, **Port Start**, **Port End**, and **Port Map** fields, then click **Apply**.

The rules you create appear in the **Available Rules** box in the **User** category. You can view or delete the rules you create.

- 5 Continue to add rules as they apply from each category using the **Add** button.
- 6 Click **Apply** when you finish to temporarily activate the settings.

**Note**—The changes take effect when you click **Apply**; however, if the RG configuration is not saved, these changes will be lost upon RG reboot.

- 7 To make the change permanent, click **Tools** and select **System Commands**.
- 8 On the **System Commands** page (Figure 5-2 on page 5-3), click **Save All**.

**End of Procedure 3-6**

---



**Note**—You can also use the **Custom IP Filters** link to add programs to the existing list. This is discussed in the following section.

---

### 3.8.1 Custom IP Filters Page

The **Custom IP Filters** page (Figure 3-18) allows you to define up to 20 custom IP filtering entries to block specific services or applications based on:

- Source/destination IP address and netmask
- TCP port (ranges supported)
- Protocol
  - TCP
  - UDP
  - TCP and UDP
  - ICMP
  - Any

**Figure 3-18 Custom IP Filters**

Table 3-8 describes the Custom IP Filters page fields.

**Table 3-8 Custom IP Filters Field Descriptions**

Field	Definition/ Description
Filter Name	Name of the IP filter rule you are creating.
Enable	The <b>Enable</b> button is checked by default, meaning this rule is automatically applied when you click <b>Apply</b> .
Source IP	The LAN-side source IP address assigned to outgoing traffic on which filtering is applied.
Source Netmask	Netmask of the source IP on your LAN side.
Destination IP	You can define the destination IP address to which your source IP will be banned access. Enter <i>0.0.0.0</i> for all.
Destination Netmask	Netmask of the destination IP. Enter <i>255.255.255.255</i> for all.
Port Stat	The starting port number that will be blocked for this application.
Port End	The ending port number that will be blocked for this application.
Protocol	There are five options available: <i>TCP, UDP, TCP and UDP, ICMP</i> , and <i>Any</i> .
<b>End of Table 3-8</b>	

## 3.9 LAN Clients Page

The LAN clients feature allows you to see all the hosts on the LAN segment. Each host is qualified to be either *dynamic* (host obtained a lease from this RG) or *static* (host has a manually-configured IP address).

You can add a *static* IP address (belonging to the RG's LAN subnet) using the **LAN Clients** page (Figure 3-19). Any existing static entry falling within the DHCP server's range can be deleted and the IP address is made available for future allocation.



**Note**—Dynamic clients show up in the list only when the DHCP server is running.

**Figure 3-19 LAN Clients**

The screenshot shows the 'LAN Clients' configuration page. The left sidebar contains a navigation menu with the following items: Voice, UPnP, SNTP, TR-069, Port Forwarding, IP Filters, LAN Clients (highlighted), LAN Isolation, TR-068 WAN Access, Bridge Filters, Web Filters, Dynamic DNS Client, IGMP Proxy, Static Routing, Policy Database, Ingress, Egress, Shaper, Web Access Control, SSH Access Control, Voice provision, and Log Out. The main content area is titled 'LAN Clients' and includes the instruction: 'To add a LAN Client, Enter IP Address and Hostname, then click Apply.' Below this instruction are three input fields: 'Select LAN Connection' (a dropdown menu with 'LAN group 1' selected), 'Enter IP Address', 'Hostname', and 'MAC Address'. At the bottom right of the form are 'Apply' and 'Cancel' buttons.

You can configure a LAN client using [Procedure 3-7](#).

### Procedure 3-7 Configure a LAN Client

#### Step – Action

- 1 On the **LAN Clients** page, select **LAN Connection**, and enter **IP Address**, **Hostname**, and **MAC Address**.
- 2 Click **Apply**.

The IP address is allocated and it shows up in the list of LAN clients as a *Dynamic* entry (Figure 3-20).

**Figure 3-20 LAN Clients with Dynamic Address**

The screenshot shows the 'LAN Clients' configuration page in the Texas Instruments web interface. The left sidebar contains a menu with options like Voice, UPnP, SNTP, TR-069, Port Forwarding, IP Filters, LAN Clients (selected), LAN Isolation, TR-068 WAN Access, Bridge Filters, Web Filters, Dynamic DNS Client, IGMP Proxy, Static Routing, Policy Database, Ingress, Egress, Shaper, Web Access Control, SSH Access Control, Voice provision, and Log Out. The main content area is titled 'LAN Clients' and includes instructions: 'To add a LAN Client, Enter IP Address and Hostname, then click Apply.' Below this, there are input fields for 'Select LAN Connection' (set to 'LAN group 1'), 'Enter IP Address', 'Hostname', and 'MAC Address'. A table titled 'Dynamic Addresses' is highlighted with a red box, containing one entry with a 'Reserve' checkbox, IP Address '192.168.1.2', Hostname 'GTD63C871', MAC '00:11:43:75:dc:42', and Type 'Dynamic'. 'Apply' and 'Cancel' buttons are at the bottom right.

- 3 You can convert the dynamic entry into a static entry by clicking **Reserve**, then **Apply**.

As shown in [Figure 3-21](#), the IP is now changed to a *Static* address. You can delete this entry by selecting **Delete**.

**Figure 3-21 LAN Clients with Static Address**

The screenshot shows the 'LAN Clients' configuration page, similar to Figure 3-20. The 'Dynamic Addresses' table is replaced by a 'Static Addresses' table, also highlighted with a red box. This table has a 'Delete' checkbox, IP Address '192.168.1.2', Hostname 'GTD63C871', MAC '00:11:43:75:dc:42', and Type 'Static'. The rest of the interface, including the sidebar and input fields, remains the same.

- 4 When you finish, click **Apply** to temporarily activate the settings.  
**Note**—The changes take effect when you click **Apply**; however, if the RG configuration is not saved, these changes will be lost upon RG reboot.
- 5 To make the change permanent, click **Tools** and select **System Commands**.
- 6 On the **System Commands** page (Figure 5-2 on page 5-3), click **Save All**.

**End of Procedure 3-7**

---



**Note**—The firewall rules that are applied to a *Dynamic* IP address will be removed after the release time expires.

---

Table 3-9 describes the **LAN Clients** page fields.

**Table 3-9 LAN Clients Field Descriptions**

Field	Definition/ Description
Select LAN Connection	Select the LAN connection to which the client is to be added.
Enter IP Address	Assign the dynamic IP address to the host here. This is a mandatory field.
Hostname	Hostname of the client. This is an optional field.
MAC Address	MAC address of the host. This is an optional field.
<b>End of Table 3-9</b>	

## 3.10 LAN Isolation Page

The **LAN Isolation** page (Figure 3-22) allows you to disable the flow of packets between up to five user-defined LAN groups (interfaces include WLAN, USB, Ethernet, SSID1, SID2, and SSID3). This allows you to secure information in private portions of the LAN (such as a hot spot deployment) from other publicly accessible LAN segments.

**Figure 3-22 LAN Isolation**

TEXAS INSTRUMENTS	HOME	SETUP	ADVANCED	WIRELESS	TOOLS	STATUS	HELP
Voice	LAN Isolation						
UPnP	To block traffic from one LAN to another LAN, check the Disable check box.						
SNTP	<input type="checkbox"/> Disable traffic between LAN group 1 and LAN group 2						
TR-069							
Port Forwarding							
IP Filters							
LAN Clients							
<b>LAN Isolation</b>							
TR-068 WAN Access							
Bridge Filters							
Web Filters							
Dynamic DNS Client							
IGMP Proxy							
Static Routing							
Policy Database							
Ingress							
Egress							
Shaper							
Web Access Control							
SSH Access Control							
Voice provision							
Log Out							

Use [Procedure 3-8](#) to configure LAN isolation.

### Procedure 3-8 Configure LAN Isolation

#### Step – Action

- 1 Check the LAN group combinations that define which traffic will be blocked.
- 2 Click **Apply** to temporarily activate the settings.
 

**Note**—The changes take effect when you click **Apply**; however, if the RG configuration is not saved, these changes will be lost upon RG reboot.
- 3 To make the change permanent, click **Tools** and select **System Commands**.
- 4 On the **System Commands** page (Figure 5-2 on page 5-3), click **Save All**.

#### End of Procedure 3-8

### 3.11 TR-068 WAN Access

The TR-068 WAN Access page (Figure 3-23) enables you to give temporary permission to someone (such as technical support staff) to be able to access your RG from the WAN side. From the moment the account is enabled, the user is expected to log in within 20 active minutes, otherwise the account expires. Once the user has logged in, if the session remains inactive for more than 20 minutes, the user will be logged out and the account expires.

**Figure 3-23 TR-068 WAN Access Page**

Table 3-10 describes the TR-068 WAN Access page settings.

**Table 3-10 TR-068 WAN Access Field Descriptions**

Field	Definition/ Description
WAN Update	Check this field to give the account read and write access.
WAN Access	Check this field to give the account read-only access.
User Name	User name of the WAN access account.
Password	Password of the WAN access account.
Port	Enter the port number to be opened for the temporary WAN access.
<b>End of Table 3-10</b>	

To create a temporary user account for a remote access to your RG, use Table 3-10 as a reference and follow Procedure 3-9.



---

**Procedure 3-9 Create Temporary User Account (WAN-Side)**

---

**Step – Action**

- 1** Check **WAN Update** to enable write privilege of the RG.
- 2** Check **WAN Access** to enable read privilege of the RG.
- 3** Enter a user name and password in the **User Name** and **Password** fields.
- 4** Enter a port number in the **Port** field (for example, 51003).
- 5** Click **Apply** to temporarily activate the temporary user account.

**Note**—This is a temporary account and cannot be saved to the flash. It expires upon RG reboot.

- 6** To access your RG remotely, from the remote PC, enter the following in the URL:

*http(s)://10.10.10.5:51003*

Syntax: *http(s)://WAN IP of RG:Port Number*

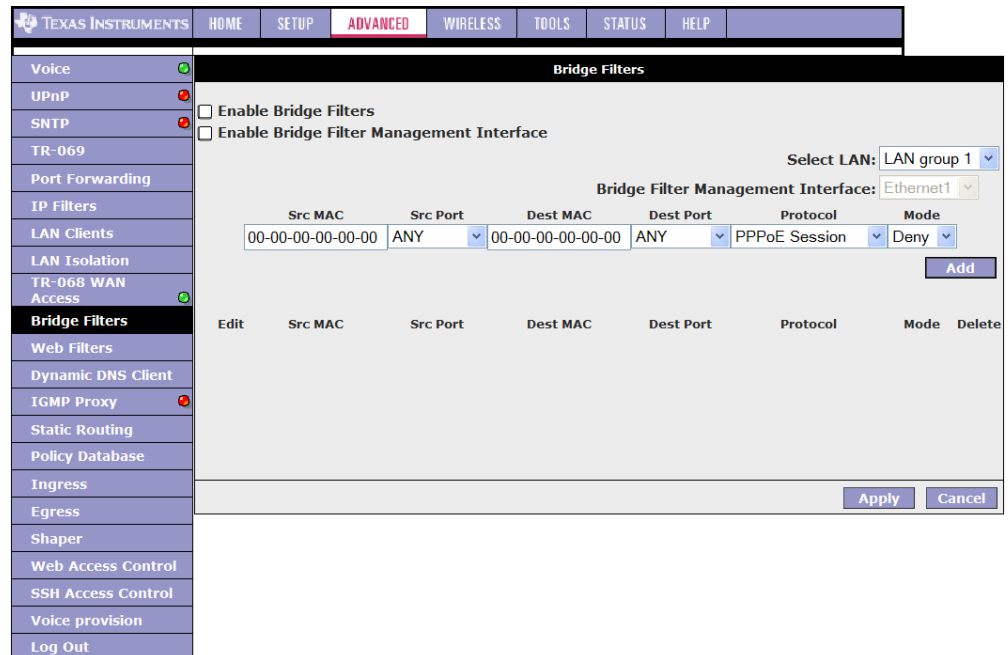
**End of Procedure 3-9**

---

## 3.12 Bridge Filters Page

The bridge filtering mechanism provides a way for you to define rules to allow or deny frames through the bridge based on source MAC address, destination MAC address, frame type, and physical ports. When bridge filtering is enabled, each frame is examined against every defined filter rule in sequence. When a match is found, the appropriate filtering action (allow or deny) is performed. Note that the bridge filter only examines frames from interfaces that are part of the bridge itself. Up to 20 filter rules are supported with bridge filtering.

**Figure 3-24 Bridge Filters Page**



The **Bridge Filters** page (Figure 3-24) allows you to enable, add, edit, or delete the filter rules.

Use [Procedure 3-10](#) to enable and configure bridge filters.

### Procedure 3-10 Configure Bridge Filters

#### Step – Action

- 1 Check **Enable Bridge Filters**.
- 2 To add a rule, enter the source MAC address, destination MAC address, and frame type with desired filtering type, then click **Add**.

**Note**—You can also edit a rule that you created using the **Edit** checkbox. You can delete a rule using **Delete**.

- 3 Click **Apply** to temporarily activate the settings.  
**Note**—The changes take effect when you click **Apply**; however, if the RG configuration is not saved, these changes will be lost upon RG reboot.
- 4 To make the change permanent, click **Tools** and select **System Commands**.
- 5 On the **System Commands** page (Figure 5-2 on page 5-3), click **Save All**.

**End of Procedure 3-10**

**Note**—There are four hidden filter rules within the bridge filter table. These rules are entered to ensure you do not "lock" yourself out of the RG on a particular port. The rules pertain to the combination of source/destination MAC addresses, source/destination ports, and protocols.

Table 3-11 describes the **Bridge Filters** page fields.

**Table 3-11 Bridge Filters Field Descriptions**

Field	Definition/ Description
Enable Bridge Filters	Enables/disables bridge filtering. It can be set/unset during any <i>add</i> , <i>edit</i> , or <i>delete</i> operation. It can also be set/unset independently by clicking <b>Apply</b> .
Enable Bridge Filter Management Interface	When checked, it enables the Bridge Filter Management Interface field. This ensures that you do not get locked out of the RG on the interface of the LAN group specified in the next two fields.
Select LAN	Select your LAN group to enable the Bridge Filter Management Interface feature.
Bridge Filter Management Interface	Select the interface of the LAN group to have the Bridge Filter Management Interface feature enabled. Depending on the LAN group that is selected, the interface selections are <i>Ethernet</i> , <i>USB</i> , and/or <i>WLAN</i> .
SRC MAC	The source MAC address. It must be in a <i>xx-xx-xx-xx-xx-xx</i> format, with <i>00-00-00-00-00-00</i> as <i>don't care</i> . Blanks can be used in the MAC address space and are also considered as <i>don't care</i> .
SRC Port	Source port. You can choose from <i>Any</i> , <i>Ethernet</i> , <i>USB</i> , <i>WLAN</i> , or <i>WAN Bridge Connection Port</i> for the particular bridge. If any of the selections are not available, please check your DSL connection.
Dest MAC	The destination MAC address.
Dest Port	Destination port. You can choose from <i>Any</i> , <i>Ethernet</i> , <i>USB</i> , and <i>WLAN</i> .
Protocol	You can choose from the following options: <i>PPPoE Session</i> , <i>PPPoE Discovery</i> , <i>IPX - Ethernet II</i> , <i>RARP</i> , <i>IPv6</i> , <i>IPv4</i> , and <i>Any</i> .
Mode	There are two filtering modes: <i>Deny</i> and <i>Allow</i> .
<b>End of Table 3-11</b>	

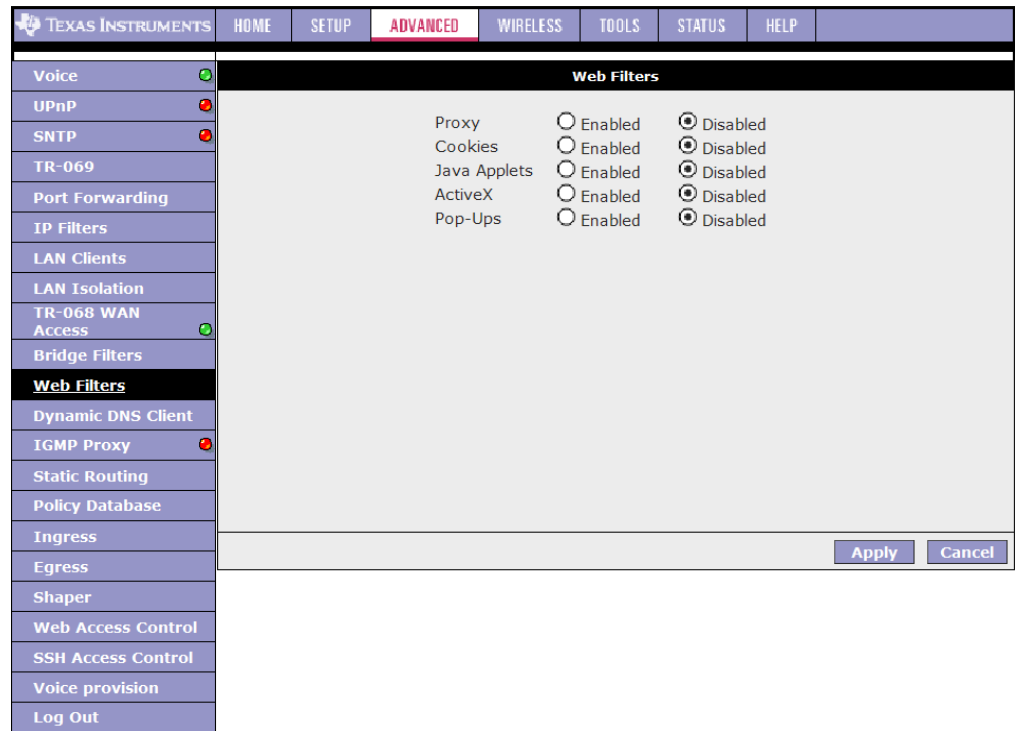
### 3.13 Web Filters Page

The **Web Filters** page (Figure 3-25) allows you to manage the type of web content that passes through your RG.



**Note**—This feature is not present on some RG platforms due to runtime memory limitations.

**Figure 3-25 Web Filters Page**



The following web filters are disabled by default:

- Proxy server
- Cookies
- Java applets
- ActiveX controls
- Pop-ups

To enable a web filter, check **Enabled** next to the filter name, then click **Apply**.

## 3.14 Dynamic DNS Client

Each time your RG connects to the Internet, your ISP assigns a different IP address to your RG. In order for you or other users to access your RG from the WAN-side, you need to manually track the IP that is currently used. The Dynamic DNS feature allows you to register your RG with a DNS server and access your RG each time using the same host name. The **Dynamic DNS Client** page (Figure 3-26) allows you to enable/disable the Dynamic DNS feature.

**Figure 3-26 Dynamic DNS Client**

Navigation Menu	Dynamic DNS Client Configuration
TEXAS INSTRUMENTS	Dynamic DNS Client
HOME	Connection: PPPoE1
SETUP	DDNS Server: DynDNS
ADVANCED	DDNS Client: <input type="checkbox"/>
WIRELESS	User Name: <input type="text"/>
TOOLS	Password: <input type="text"/>
STATUS	Domain Name: <input type="text"/>
HELP	Buttons: Apply, Cancel
Voice (green)	
UPnP (red)	
SNTP (red)	
TR-069	
Port Forwarding	
IP Filters	
LAN Clients	
LAN Isolation	
TR-068 WAN Access (green)	
Bridge Filters	
Web Filters	
<b>Dynamic DNS Client</b>	
IGMP Proxy (red)	
Static Routing	
Policy Database	
Ingress	
Egress	
Shaper	
Web Access Control	
SSH Access Control	
Voice provision	
Log Out	

Use Table 3-12 as a reference and follow Procedure 3-11 to enable Dynamic DNS feature on your RG.

### Procedure 3-11 Enable Dynamic DNS

#### Step – Action

- On the **Dynamic DNS Client** page, configure the following fields:
  - Connection
  - DDNS Server
  - DDNS Client
  - User Name
  - Password
  - Domain Name

- 2 Click **Apply** to temporarily activate the settings.

**Note**—The changes take effect when you click **Apply**; however, if the RG configuration is not saved, these changes will be lost upon RG reboot.

- 3 To make the change permanent, click **Tools** and select **System Commands**. On the **System Commands** page (Figure 5-2 on page 5-3), click **Save All**.

**End of Procedure 3-11**

Table 3-12 describes the **Dynamic DNS Client** page fields.

**Table 3-12 Dynamic DNS Client Field Descriptions**

Field	Definition/ Description
Connection	This field defaults to your RG's WAN connection over which your RG will be accessed.
DDNS Server	This is where you select the server from different DDNS service providers. A charge may occur depends on the service you select.
DDNS Client	Enables/disables the DDNS client feature for the WAN connection. This field is disabled by default.
User Name	User name assigned by the DDNS service provider.
Password	Password assigned by the DDNS service provider.
Domain Name	Domain name to be registered with the DDNS server.
<b>End of Table 3-12</b>	

## 3.15 IGMP Proxy Page

Multicasting is a form of limited broadcast. UDP is used to send datagrams to all hosts that belong to what is called a **Host Group**. A host group is a set of one or more hosts identified by a single IP destination address. The following statements apply to host groups:

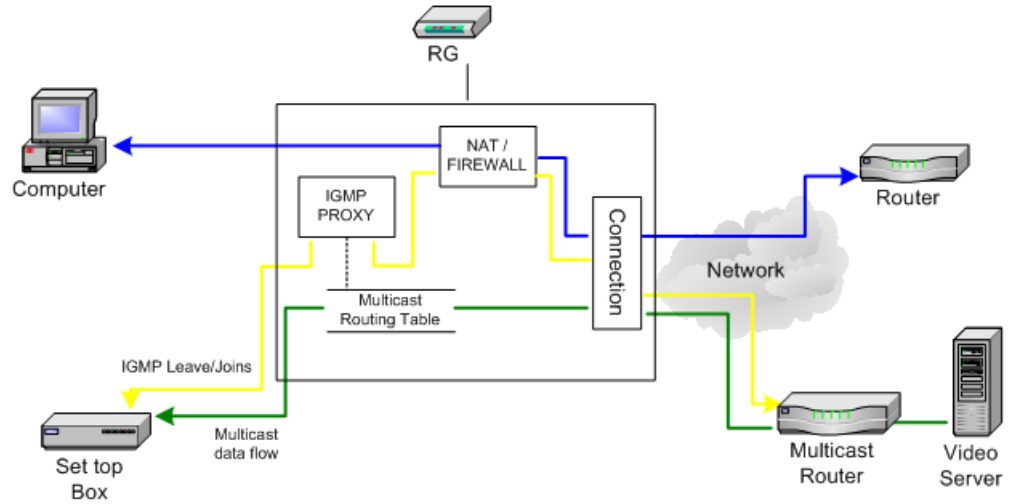
- Anyone can join or leave a host group at will.
- There are no restrictions on a host's location.
- There are no restrictions on the number of members that may belong to a host group.
- A host may belong to multiple host groups.
- Non-group members may send UDP datagrams to the host group.

Multicasting is useful when the same data needs to be sent to more than one device. For instance, if one device is responsible for acquiring data that many other devices need, then multicasting is a natural fit. Note that using multicasting as opposed to sending the same data to individual devices uses less network bandwidth. The multicast feature also enables you to receive multicast video streams from multicast servers.

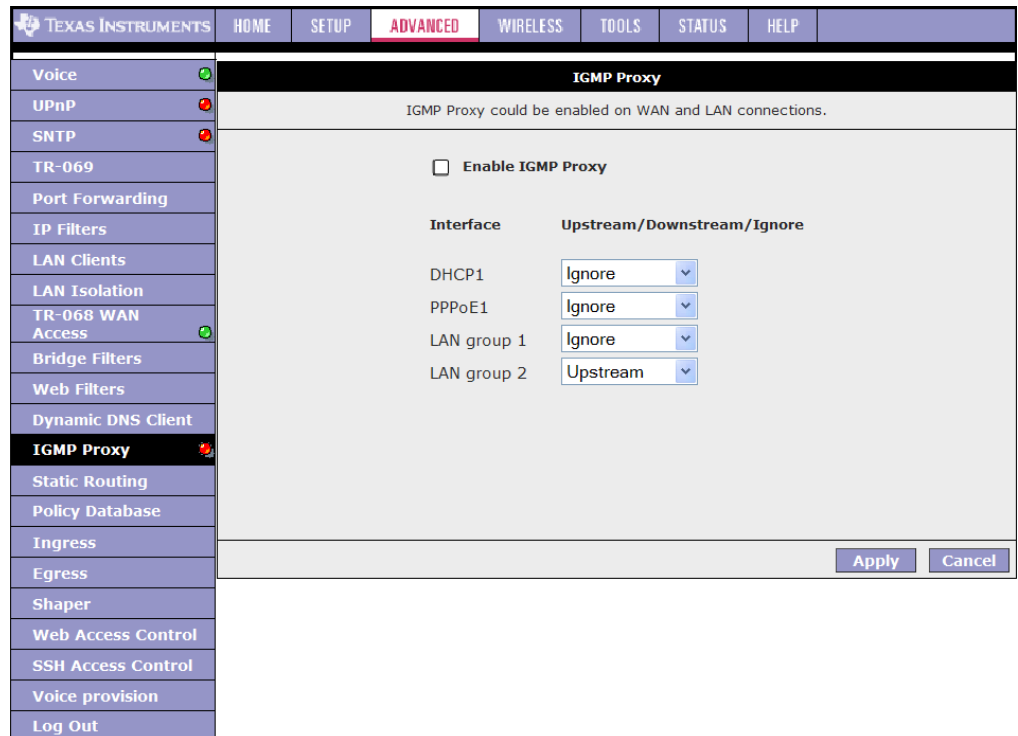
IP hosts use Internet group management protocol (IGMP) to report their multicast group memberships to neighboring routers. Similarly, multicast routers use IGMP to discover which of their hosts belong to multicast groups. Your RG supports IGMP proxy that handles IGMP messages. When enabled, your RG acts as a proxy for a LAN host making requests to join and leave multicast groups, or a multicast router sending multicast packets to multicast groups on the WAN side. This application needs to be run when NAT is enabled. As can be seen in [Figure 3-27](#), the IGMP proxy intercepts the Join and Leave commands for Version 1 and 2 IGMP messages. On a Join, the proxy sets up a multicast route for the interface and PC requesting the video content. It

then forwards the Join to the upstream multicast router. The Multicast IP traffic will then be forwarded to the requesting device. Multicast traffic does not pass through the Firewall or NAT. On a leave, the Proxy removes the route and then forwards the leave to the upstream Multicast router.

**Figure 3-27 IGMP Proxy Data Flow**



**Figure 3-28 IGMP Proxy Page**





The **IGMP Proxy** page (Figure 3-28) allows you to enable multicast on available WAN and LAN connections. You can configure the WAN or LAN interface as one of the following:

- **Upstream:** The interface that IGMP requests from hosts are sent to the multicast router.
- **Downstream:** The interface data from the multicast router are sent to hosts in the multicast group database.
- **Ignore:** No IGMP request nor data multicast are forwarded.

You can perform one of the two options:

1. Configure one or more WAN interface as the upstream interface.
2. Configure one or more LAN interface as the upstream interface.

Each option is discussed in more details as follows.

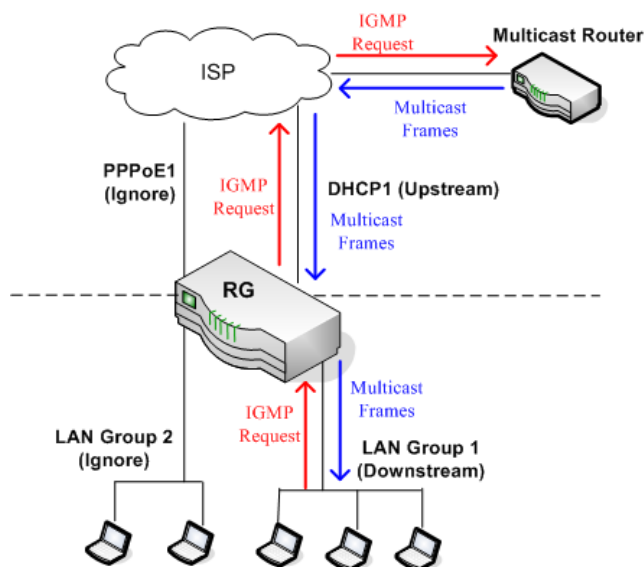
### 3.15.1 Configure a WAN Interface as the Upstream IGMP Proxy:

This applies when the multicast server is on the network. Hosts on your LAN side can send IGMP requests through the WAN interface. And the WAN will pass multicast packets from the multicast server to the hosts on the LAN side.

In Figure 3-29 shown below, the WAN interface DHCP1 is enabled as the upstream IGMP interface, which forwards IGMP requests from LAN group 1 to the multicast router on the network and forwards multicast frames from the multicast router to hosts on the downstream interface (LAN group 1). No IGMP request nor data multicast are forwarded to PPPoE1 or LAN Group 2.

**Figure 3-29 Enable IGMP Proxy: WAN = Upstream**

Enable IGMP Proxy: WAN = Upstream



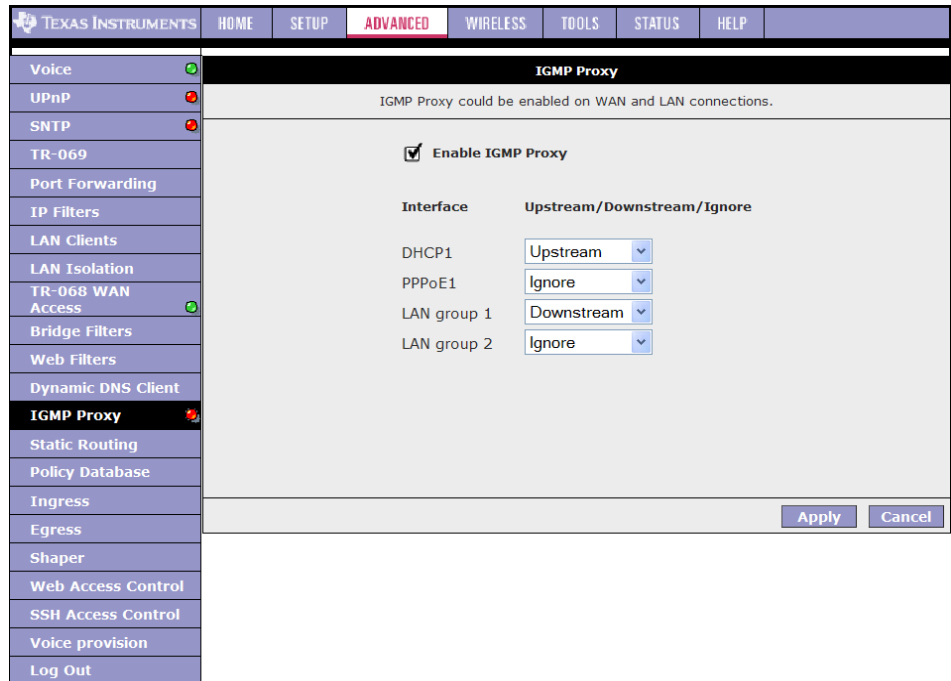
Use [Procedure 3-12](#) to configure a WAN connection as the upstream interface.

### Procedure 3-12 Enable IGMP Proxy - Configure WAN as Upstream Interface

#### Step – Action

- 1 Check **Enable IGMP Proxy**.
- 2 Configure the following WAN/LAN interfaces:
  - DHCP1: Upstream
  - PPPoE1: Ignore
  - LAN group 1: Downstream
  - LAN group 2: Ignore

**Figure 3-30 IGMP Proxy Page (WAN = Upstream)**



- 3 Click **Apply** to temporarily activate the settings.

**Note**—The changes take effect when you click **Apply**; however, if the RG configuration is not saved, these changes will be lost upon RG reboot.

- 4 To make the change permanent, click **Tools** and select **System Commands**. On the **System Commands** page ([Figure 5-2](#) on page 5-3), click **Save All**.

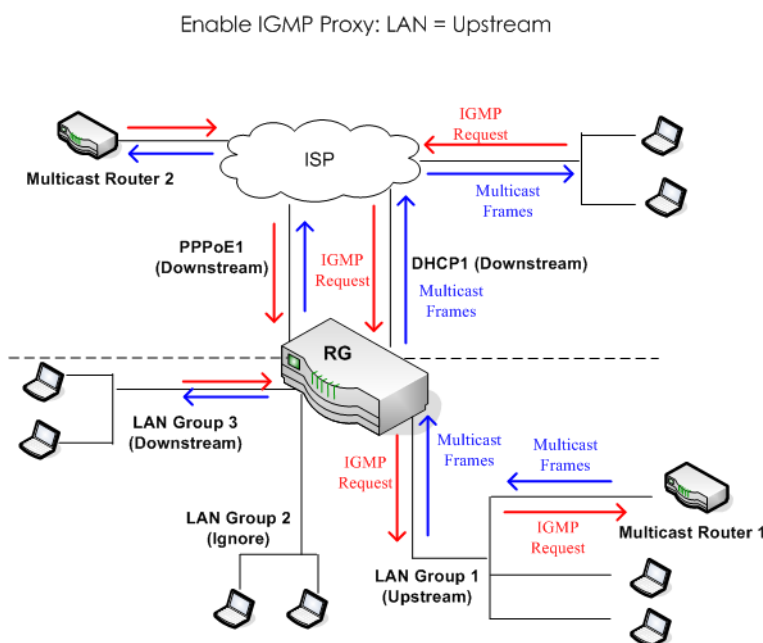
**End of Procedure 3-12**

### 3.15.2 Configure a LAN interface as the Upstream Interface.

This applies when the multicast server is on the LAN side. Hosts on the network can send IGMP requests from the WAN side through the LAN interface. And the LAN interface, acting as the upstream interface, forwards data multicast from the LAN-side multicast server to hosts on the network.

In [Figure 3-31](#) shown below, there is a multicast router on the LAN side and LAN Group 1 interface is enabled as the upstream IGMP proxy. IGMP requests from the network are forwarded to LAN group 1 and multicast frames from multicast router 1 are forwarded to hosts on the LAN side (LAN group 3) and on the WAN side (DHCP1 and PPPoE1). No IGMP request nor data multicast are forwarded to LAN Group 2.

**Figure 3-31 Enable IGMP Proxy: LAN = Upstream**



Use [Procedure 3-13](#) to configure your LAN group 1 as the upstream interface.

#### **Procedure 3-13 Enable IGMP Proxy - Configure a LAN Group as Upstream Interface**

##### **Step – Action**

- 1 Check **Enable IGMP Multicast**.
- 2 Configure the following WAN/LAN interfaces:
  - DHCP1: Downstream
  - PPPoE1: Downstream
  - LAN group 1: Upstream
  - LAN group 2: Ignore

- LAN group 3: Downstream

**Figure 3-32 IGMP Proxy Page (LAN = Upstream)**

- 3 Click **Apply** to temporarily activate the settings.

**Note**—The changes take effect when you click **Apply**; however, if the RG configuration is not saved, these changes will be lost upon RG reboot.

- 4 To make the change permanent, click **Tools** and select **System Commands**. On the **System Commands** page (Figure 5-2 on page 5-3), click **Save All**.

**End of Procedure 3-13**



**Note**—At least one WAN interface should be configured in order to enable the IGMP proxy.

Table 3-13 describes the **IGMP Proxy** page fields.

**Table 3-13 IGMP Proxy Field Descriptions**

Field	Definition/ Description
Enable IGMP Proxy	Enables/disables IGMP multicast feature of the RG.
Connections	There are three types of configuration for each WAN/LAN connection: <ul style="list-style-type: none"> <li>• Upstream</li> <li>• Downstream</li> <li>• Ignore</li> </ul>

**End of Table 3-13**

### 3.16 Static Routing Page

The **Static Routing** page (Figure 3-33) enables you to define routes for specific subnets on the WAN/LAN side. The RG allows you to manually program the RG's routing table. Up to 16 static routes can be added.

**Figure 3-33 Static Routing Page (Default)**

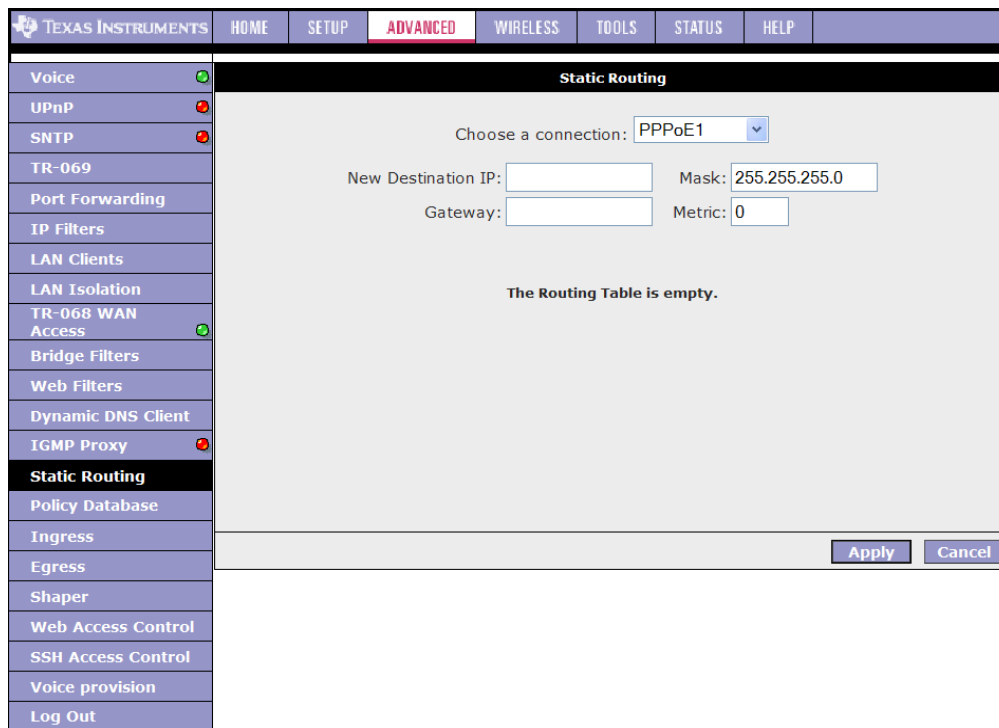


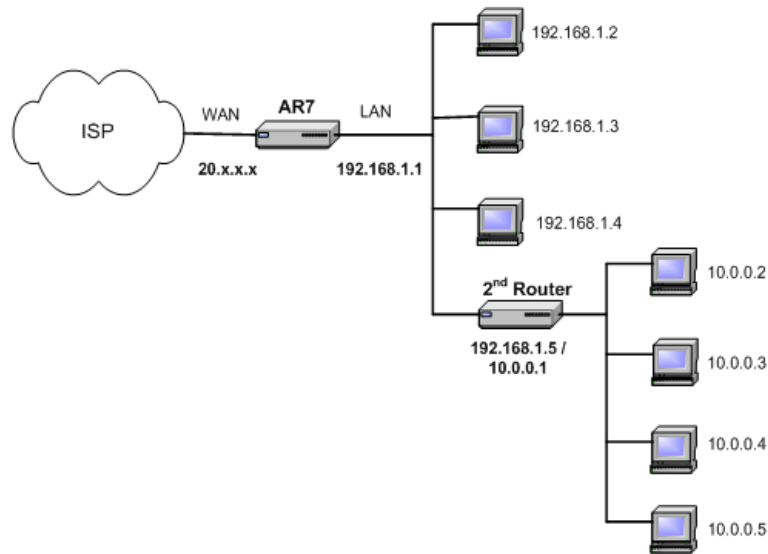
Table 3-14 describes the **Static Routing** page fields.

**Table 3-14 Static Routing Field Descriptions**

Field	Definition/ Description
Select a Connection	Select the LAN group or WAN connection to which a static routing subnet is to be applied.
New Destination IP	The network IP address of the subnet. (You can also enter the IP address of each individual station in the subnet).
Mask	The network mask of the destination subnet.
Gateway	The IP address of the next hop through which traffic will flow towards the destination subnet.
Metric	Defines the number of hops the between network nodes that data packets travel. The default value is 0, which means that the subnet is directly one hop away on the local LAN network.
<b>End of Table 3-14</b>	

Suppose you have a network like the one shown in [Figure 3-34](#). In your LAN, you have an RG (192.168.1.1) and three stations connected to it (192.168.1.x). A subnet is added to your LAN group by adding a second router (192.168.1.5/10.0.0.1) with four stations (10.0.0.x) connected to it. The four stations in the subnet cannot receive packets unless they are added to the routing table of your RG. You can add each individual station to the routing table using the **Static Routing** page, or more easily, you can add the whole subnet in one entry. [Procedure 3-14](#) explains how to add the subnet to the RG routing table.

**Figure 3-34 Static Routing - LAN with Subnet**



### Procedure 3-14 Configure Static Routing

#### Step – Action

- 1 From the **Choose a connection** drop-down menu, select your LAN connection *LAN Group 1*.
- 2 Enter or leave the default entry for the following parameters:
  - **New Destination IP:** *10.0.0.0* (the network IP address of the subnet)
  - **Mask:** *255.255.255.0* (the subnet mask)
  - **Gateway:** *192.168.1.5* (the LAN-side IP address of the second router, through which the stations in the subnet access the network)
  - **Metric:** *0*

You are telling the RG that a new subnet with an IP of *10.0.0.0* and a netmask of *255.255.255.0* has been added and can access the RG via station *192.168.1.5*. The metric is *0* since the subnet is one level down on the LAN.

- 3 Click **Apply** to temporarily activate the settings.

You have added the subnet to the routing table (Figure 3-35). The four stations in the subnet can receive packets from the WAN.

**Figure 3-35 Static Routing (with One Entry)**

Connection	Destination IP	Mask	Gateway	Metric	Delete
LAN group 1	10.0.0.0	255.255.255.0	192.168.1.5	0	<input type="checkbox"/>

**Note**—You can add up to 16 entries. You can also delete any entry using the **Delete** checkbox.

- 4 Click **Apply** again when you finish making all the changes.

**Note**—The changes take effect when you click **Apply**; however, if the RG configuration is not saved, these changes will be lost upon RG reboot.

- 5 To make the change permanent, click **Tools** and select **System Commands**.
- 6 On the **System Commands** page (Figure 5-2 on page 5-3), click **Save All**.

**End of Procedure 3-14**

### 3.17 Dynamic Routing Page

The **Dynamic Routing** page is only available on the AR7WRD platform and not available on the AR7VW platform in this release.

The dynamic routing feature enables the RG to dynamically define routes for WAN and LAN subnets. Dynamic routing uses routing information protocol (RIP) for exchanging routing information with other routers in the network. It is supported across both WAN and LAN interfaces. Any RIP-enabled router sends out automatic update packets containing its own routing table on a periodic basis (every 30 secs). Similarly, it accepts such periodic updates from other routers and adds, deletes, or modifies routes in its own routing table accordingly. The router is also expected to receive requests for its routing table and respond accordingly. Use the **Dynamic Routing** page (Figure 3-36) to define dynamic routing routes for the available interfaces.

**Figure 3-36 Dynamic Routing Page**





Table 3-15 describes the **Dynamic Routing** page fields.

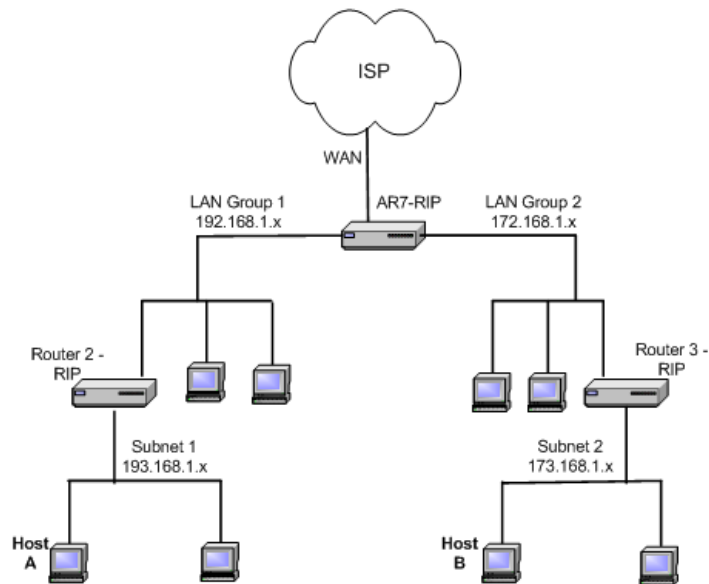
**Table 3-15 Dynamic Routing Field Descriptions**

Field	Definition/ Description
Enable RIP	Enables/disables RIP.
Protocol	The following three RIP versions are available: <ul style="list-style-type: none"> <li>• RIP v1 (UDP protocol)</li> <li>• RIP v2 (multicast protocol)</li> <li>• RIP v1 compatible (UDP protocol with multicast format)</li> </ul> <p>Note: Routers using RIP v1 or RIP v1-compatible protocol can talk to each other, but not to routers using RIP v2 protocol.</p>
Enable Password	This is an optional field. RIP version v2 compatibility allows you to provide simple plain-text password-based authentication to RIP packets. This field is disabled if RIP v1 protocol is selected.
Password	The password can be up to 16 characters long.
Direction	Normally when RIP is enabled on a router, it dynamically learns/provides routes on all its configured interfaces. This parameter allows you to select the interfaces on which RIP is expected to learn and distribute routing information. This feature allows you to control how and which routes get distributed through the network. For example, by selecting <i>In only</i> mode, routes to private LAN networks are prevented from being sent over to the WAN-side router. The following four direction options are available: <ul style="list-style-type: none"> <li>• <b>Both:</b> Receive updates on the interface and also send its routing table to other routers connected to that interface.</li> <li>• <b>In:</b> Receive routing updates from other routers connected to that interface but do <b>NOT</b> send routing updates on that interface.</li> <li>• <b>Out:</b> Send routing updates but do <b>NOT</b> receive updates on this interface from the other routers connected to that interface.</li> <li>• <b>None:</b> Ignore this interface and do not send or receive routing updates through this interface.</li> </ul>
<b>End of Table 3-15</b>	

To demonstrate the use of the dynamic routing feature, consider an expanded version of the network used in the static routing example in 3.16 “[Static Routing Page](#)” on page 3-45. As shown in [Figure 3-37](#), you have a network with two LAN connections (192.168.1.x and 172.168.1.x), and each has a router and a subnet. How can host A in subnet 1 (193.168.1.x) talk to host B in subnet 2 (173.168.1.x)? You have two options:

- As previously demonstrated in [Procedure 3-14](#), using the static routing feature, you can add both subnets to the routing table using the **Static Routing** page (two separate entries).
- You can enable dynamic routing on all routers without having to manually enter the individual routes. Keep in mind that you need to enable all routers on this network and they should use the same protocol to be able to communicate with each other. [Procedure 3-15](#) shows you how to enable and configure the dynamic routing feature on your RG.

**Figure 3-37 Dynamic Routing - LAN with Subnets**



**Procedure 3-15 Configure Dynamic Routing**

**Step – Action**

- 1 Check **Enable RIP**.
- 2 Select the RIP Protocol **RIP v2** for training purpose.  
The **Enable Password** field is enabled.  
**Note**—The same RIP protocol should be used to enable dynamic routing on all routers on the network.
- 3 Check **Enable Password** and enter a password.  
This is an optional field for additional security.
- 4 For LAN group 1 and LAN group 2, leave *Both* checked in the **Direction** field.
- 5 Click **Apply** to temporarily activate the settings.  
Notice you did not need to enter the subnet IP, mask, or gateway when using the dynamic routing feature. The RGs can receive and transmit routing information and add it to their own routing tables.  
You also need to enable dynamic routing on routers 2 and 3.
- 6 Click **Apply** again when you finish making all the changes.  
**Note**—The changes take effect when you click **Apply**; however, if the RG configuration is not saved, these changes will be lost upon RG reboot.
- 7 To make the change permanent, click **Tools** and select **System Commands**.

---

**8** On the **System Commands** page ([Figure 5-2](#) on page 5-3), click **Save All**.

**End of Procedure 3-15**

---

## 3.18 QoS

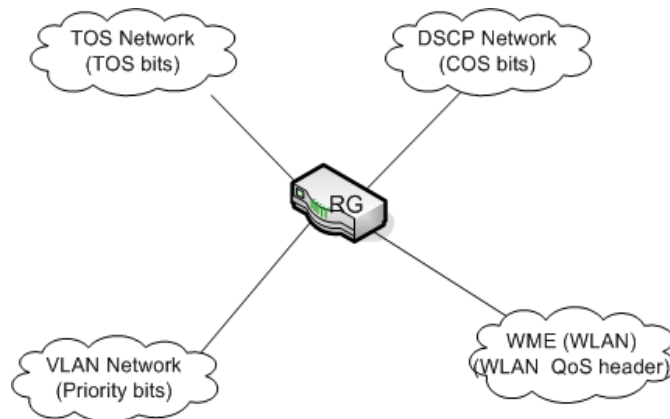
Quality of service (QoS) is an important feature for this release. The QoS framework allows network administrators to configure the routers to meet the real time requirements for voice and video.

**QoS challenges in multiple networks:**

As shown in [Figure 3-38](#), 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.

**Figure 3-38 QoS Network**



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 are 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:

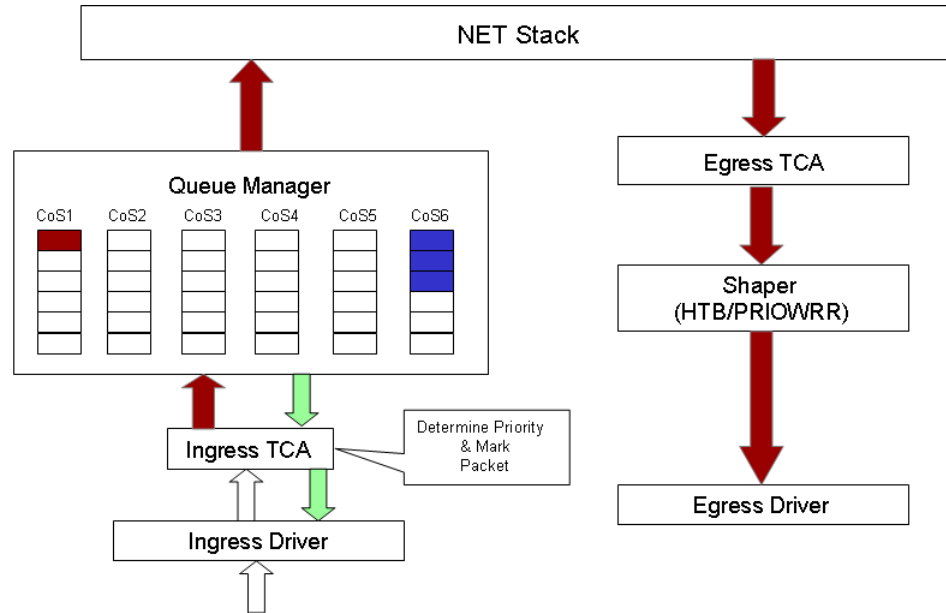
- Ingress: Packets arriving into the RG from a WAN/LAN interface.
- Egress: Packets sent from the RG to a WAN/LAN interface.
- Trusted mode: Honors the domain mapping (ToS byte, WME, WLAN user priority).
- Untrusted mode: Does not honor domain mapping. This is the default QoS setting.
- Traffic Conditioning 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

**QoS Flow Diagram**

Figure 3-39 is a diagram that shows the QoS packet flow.

**Figure 3-39 QoS Flow Diagram**



**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. For more information, visit 3.18.1 [“Ingress”](#) on page 3-55.
- **Egress page:** The **Egress** page allows you to translate CoS of an outgoing packet to a domain mapping. For more information, visit 3.18.2 [“Egress”](#) on page 3-66.
- **Shaper page:** The **Shaper** page allows you to define rules and assign bandwidth for the CoS types. This page is applicable only to the Egress interface. For more information, visit 3.18.4 [“Shaper”](#) on page 3-69.
- **Policy Database page:** Policy Routing (PR) rules apply when you configure QoS for multiple WAN connection. The **Policy Database** page also enables you to classify packets on the basis of various fields in the packet. For information on how to configure PR, visit 3.19 [“Policy Database”](#) on page 3-74. For information on QoS Ingress Payload Database configuration, visit [“Ingress Payload Database Configuration”](#) on page 3-61.



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

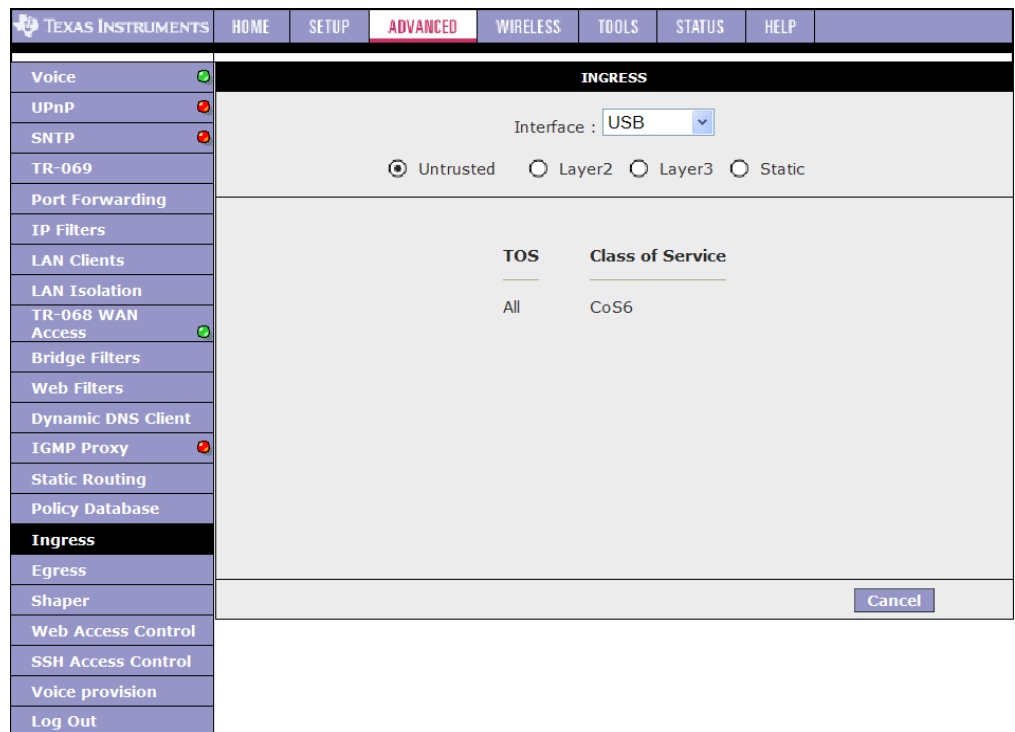
### 3.18.1 Ingress

The **Ingress** page (Figure 3-40) enables you to configure QoS for packets as soon as they come into the RG. This page is accessed by selecting **Ingress** on the **Advanced** main page. The domain mappings are converted to CoS (the common language) so that the priority marking is carried over. There are four modes that are discussed below:

#### Ingress Untrusted Mode

Untrusted is the default **Ingress** page setting for all interfaces. In this mode, no domain mapping is honoured in the RG. All packets are treated as CoS6 (best effort) as shown in Figure 3-40.

**Figure 3-40 Ingress Page - Untrusted**



## Ingress Layer 2 Configuration

**Layer 2** page (([Figure 3-41](#)) enables you to map an incoming packet with VLAN priority to CoS. This feature is only configurable on the WAN interfaces as VLAN is only supported on the WAN side in the current software release.

**Figure 3-41 Ingress Page - Layer 2**

[Table 3-16](#) describes the **Ingress Layer 2 Configuration** page settings.

**Table 3-16 Ingress - Layer 2 Page Descriptions**

Field	Definition/ Description
Interface	Select the WAN interface here to configure the CoS for incoming traffic. Only WAN interface can be selected as VLAN is currently supported only on the WAN side.
Class of Service	The selections are (in the order of descending priority): CoS1, CoS2, CoS3, CoS4, CoS5, and CoS6.
User Priority	The selections are 0, 1, 2, 3, 4, 5, 6, 7.
<b>End of Table 3-16</b>	

Use [Table 3-16](#) as a reference and follow [Procedure 3-16](#) to configure Ingress Layer 2 QoS settings.

### Procedure 3-16 Ingress Layer 2 Priority Bits to CoS Configuration

#### Step – Action

- 1 From **Interface** drop-down box, select *PPPoE1*.

You are configuring QoS on this WAN interface.



- 2 Select *CoS1* in **Class of Service** and **5** in **Priority Bits**.  
Any packets with priority marking **5** is mapped to *CoS1*, the highest priority that is normally given to the voice packets.
- 3 Click **Apply** to temporarily activate the settings.
- 4 Select *CoS2* in the **Class of Service** field and **1** in the **Priority Bits** field.  
Any packets that have a priority bits of **1** is mapped to *CoS2*, which is the second highest priority. This is given to the high priority packets such as video.
- 5 Click **Apply** to temporarily activate the settings.  
**Note**—The changes take effect when you click **Apply**; however, if the RG configuration is not saved, these changes will be lost upon RG reboot.
- 6 Repeat step 2-5 to add more rules to PPPoE1.  
Up to eight rules can be configured for each interface.  
**Note**—Any priority bits that have not been mapped to a CoS default to *CoS6*, the lowest priority.
- 7 Repeat step 1-6 to create rules to another WAN interface.  
**Note**—Any WAN interface that is not configured has the default *Untrusted* mode.
- 8 To make the change permanent, click **Tools** and select **System Commands**. On the **System Commands** page (Figure 5-2 on page 5-3), click **Save All**.

---

**End of Procedure 3-16**

---

### Ingress Layer 3 Configuration

The Layer 3 page (Figure 3-42) allows you to map ToS bits of incoming packets from the IP network to CoS for each WAN/LAN interface.

**Figure 3-42 Ingress Page - Layer 3**

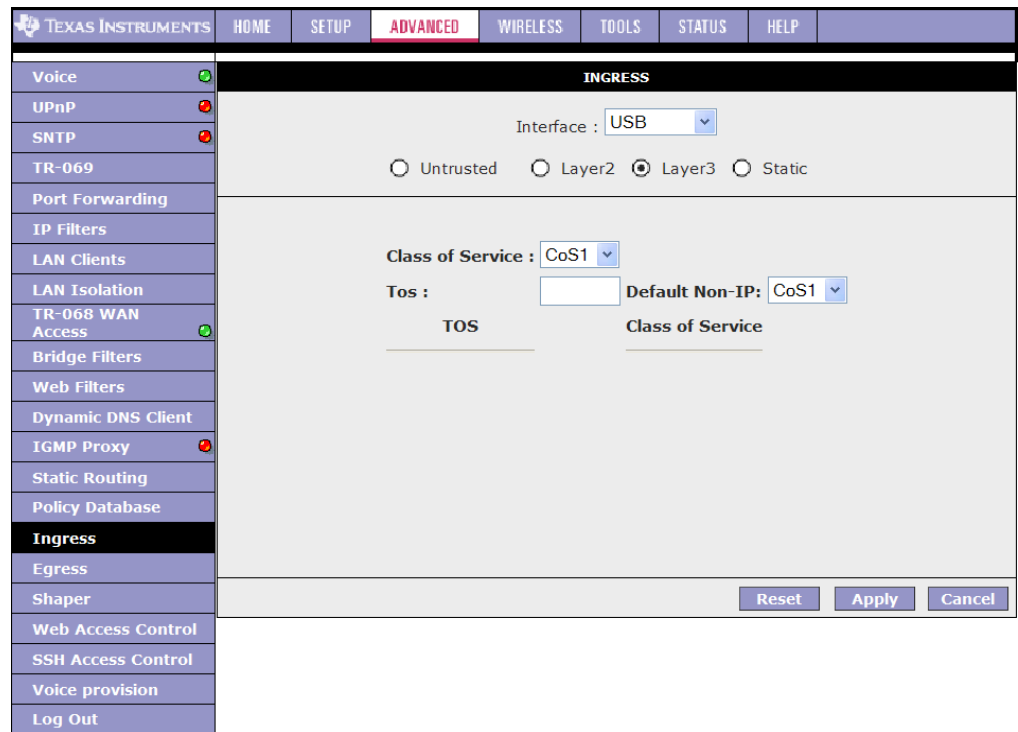


Table 3-17 describes the **Ingress - Layer 3 Configuration** page settings.

**Table 3-17 Ingress - Layer 3 Page Descriptions**

Field	Definition/ Description
Interface	For both WAN and LAN interfaces, you can configure QoS for layer 3 (IP) data traffic.
Class of Service	This CoS field allows you to map incoming layer 3 WAN/LAN packets to one of the following CoS (in the order of descending priority): CoS1, CoS2, CoS3, CoS4, CoS5, and CoS6.
Tos	The type of service field takes values from 0 to 255.
Default Non IP	A static CoS can be assigned to all layer 3 incoming packets (per interface) that do not have an IP header, such as PPP control packets and ARP packets. The default is CoS1 (recommended).
<b>End of Table 3-17</b>	

Use Table 3-17 as a reference and follow Procedure 3-17 to configure Ingress Layer 3 QoS settings.

**Procedure 3-17 Ingress Layer 3 ToS to CoS Configuration**

**Step – Action**

- 1 From **Interface** drop-down box, select *LAN Group 1*.  
You are configuring QoS on this interface.

- 2** Select *CoS1* in **Class of Service** and enter 22 in **Type of Service (ToS)**.  
Any incoming packet from LAN Group 1 (layer 3) with a ToS of 22 is mapped to *CoS1*, the highest priority, which is normally given to the voice packets.
- 3** Leave the default value *CoS1* in **Default Non-IP**.  
Any incoming packet from LAN Group 1 without an IP is mapped to *CoS1*, the highest priority.
- 4** Click **Apply** to temporarily activate the settings.  
**Note**—The changes take effect when you click **Apply**; however, if the RG configuration is not saved, these changes will be lost upon RG reboot.
- 5** Repeat step 2-4 to add more rules to LAN Group 1.  
Up to 255 rules can be configured for each interface.  
**Note**—Any ToS that have not been mapped to a CoS is treated as *CoS6*, the lowest priority.
- 6** Repeat step 1-5 to create rules to another WAN/LAN interface.  
**Note**—Any WAN/LAN interface that is not configured has the default *Untrusted* mode.
- 7** To make the change permanent, click **Tools** and select **System Commands**.  
On the **System Commands** page (Figure 5-2 on page 5-3), click **Save All**.

---

**End of Procedure 3-17**

---

## Ingress Static Configuration

The **Ingress - Static** page (Figure 3-43) enables you to configure a static CoS for all packets received on a WAN or LAN interface.

**Figure 3-43 Ingress Page - Static**

The screenshot shows the 'Ingress Static Configuration' page. The navigation menu on the left includes: Voice, UPnP, SNTP, TR-069, Port Forwarding, IP Filters, LAN Clients, LAN Isolation, TR-068 WAN Access, Bridge Filters, Web Filters, Dynamic DNS Client, IGMP Proxy, Static Routing, Policy Database, **Ingress**, Egress, Shaper, Web Access Control, SSH Access Control, Voice provision, and Log Out. The main content area is titled 'INGRESS' and contains the following settings:

- Interface: USB (dropdown menu)
- Mode:  Untrusted,  Layer2,  Layer3,  Static
- Class of Service: CoS1 (dropdown menu)

At the bottom right of the main content area are three buttons: Reset, Apply, and Cancel.

To configure, follow [Procedure 3-18](#) to configure Ingress static QoS settings.

### Procedure 3-18 Ingress Static Configuration

#### Step – Action

- 1 At the **Interface** drop-down box, select *Ethernet*.  
You are configuring QoS on this interface only. Any WAN/LAN interface that is not configured has the default *Untrusted* mode.
- 2 Select *CoS1* in **Class of Service**.  
All incoming traffic from the Ethernet interface receives CoS1, the highest priority.
- 3 Click **Apply** to temporarily activate the settings.

**Note**—The changes take effect when you click **Apply**; however, if the RG configuration is not saved, these changes will be lost upon RG reboot.

- To make the change permanent, click **Tools** and select **System Commands**. On the **System Commands** page (Figure 5-2 on page 5-3), click **Save All**.

#### End of Procedure 3-18

## Ingress Payload Database Configuration

The **Policy Database Configuration** page (Figure 3-44) is accessed by selecting **Policy Database** on the **Advanced** home page. This page enables you to configure QoS payload database and policy routing. The QoS payload database configuration will be discussed here. The policy routing configuration will be discussed in 3.19 “**Policy Database**” on page 3-74.

**Figure 3-44 Policy Database Page - Ingress Payload Database Configuration**

The screenshot displays the 'Policy Database Configuration' page. On the left is a navigation menu with 'Policy Database' selected. The main content area is titled 'Policy Database Configuration' and contains the following fields:

- Ingress Interface: LAN group 1 (dropdown)
- Destination Interface: PPPoE1 (dropdown)
- DiffServ Code Point: [ ]
- Class of Service: CoS1 (dropdown)
- Source IP: [ ]
- Destination IP: [ ]
- Mask: [ ]
- Mask: [ ]
- Protocol: TCP (dropdown) tcp (text)
- Source Port Start: [ ]
- Source Port End: [ ]
- Destination Port Start: [ ]
- Destination Port End: [ ]
- Source MAC: [ ]
- Local Routing Mark: [ ]

A red box highlights the fields from Source IP to Source MAC, labeled 'QoS related fields'. Below the form is a table with the following columns: Ingress Interface, DSCP, Source IP, Destination IP, Source Port Start, Destination Port Start, Protocol, Local Mark, and Delete. The table is currently empty. At the bottom right are 'Apply' and 'Cancel' buttons.

QoS can be configured in the **Ingress** and **Egress** pages on a per interface basis. The **Policy Database** page enables you to classify packets on the basis of various fields in the packet.

The following fields, as shown in Figure 3-44, can be configured for QoS:

- CoS
- Source IP address/mask
- Destination IP address/mask
- Protocol
- Source port start

- Source port end
- Destination port start
- Destination port end
- Source Mac address

You can configure any or all field as needed. [Table 3-18](#) describes the QoS-related fields on the **Policy Database Configuration** page.

**Table 3-18 Policy Database Page QoS-related Field Descriptions**

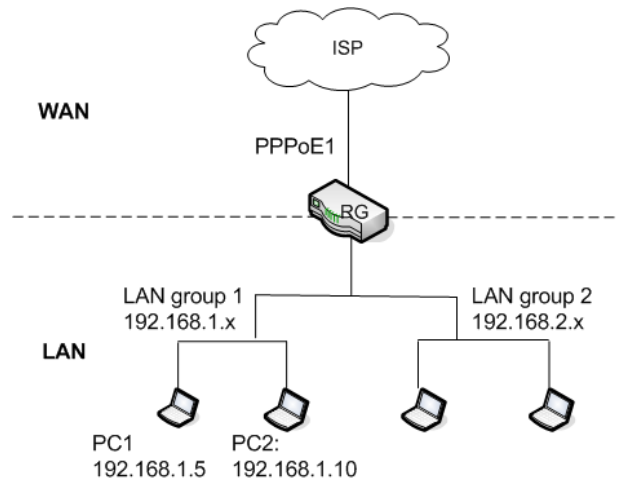
Field	Definition/ Description
Ingress Interface	This field is applicable for policy routing configuration only and will be discussed in 3.19 “Policy Database” on page 3-74.
Destination Interface	This field is applicable for policy routing configuration only and will be discussed in 3.19 “Policy Database” on page 3-74.
DiffServ Code Point	This field is applicable for policy routing configuration only and will be discussed in 3.19 “Policy Database” on page 3-74.
Class of Service	The selections are (in the order of priority): CoS1, CoS2, CoS3, CoS4, CoS5, CoS6, and N/A.
Source IP	The IP address of the traffic source.
Mask	The source IP netmask. This field is required if the source IP has been entered.
Destination IP	The IP address of the traffic destination.
Mask	The netmask of the destination. This field is required if the destination IP has been entered.
Protocol	The selections are <i>TCP</i> , <i>UDP</i> , <i>ICMP</i> , <i>Specify</i> , and <i>none</i> . If you choose <i>Specify</i> , you need to enter the protocol number in the box next to the <b>Protocol</b> field.  This field cannot be configured alone, additional fields like <b>IP</b> and/or <b>Source MAC</b> should be configured.  This field is also required if the source port or destination port has been entered.
Source Port Start	The starting port of the source protocol. You cannot configure this field without entering the protocol first.
Source Port End	The ending port of the source protocol. You cannot configure this field without entering the protocol first.
Destination Port Start	The starting port of the destination protocol. You cannot configure this field without entering the protocol first.
Destination Port End	The ending port of the destination protocol. You cannot configure this field without entering the protocol first.
Source MAC	The MAC address of the traffic source.
Local Routing Mark	This field is applicable for policy routing configuration only and will be discussed in 3.19 “Policy Database” on page 3-74.
Note: Wildcard (*) entries are allowed for IP Address/Netmask and Port range fields.	
<b>End of Table 3-18</b>	

**Example** Using [Table 3-18](#) as a reference, let’s configure QoS using the **Policy Database Configuration** page. In [Figure 3-45](#), your RG has the following configuration:

- WAN connection: PPPoE1 (default gateway).
- Two LAN groups: LAN group 1 and LAN group 2
- Two PCs in LAN group 1. You use PC 1 (192.168.1.5) to download movie and PC 2 (192.168.1.10) to surf the internet.

**Goal:** You want to give priority to PC 1 traffic over PC 2 traffic.

**Figure 3-45 Ingress Payload Database Configuration Example 1**



Follow [Procedure 3-19](#) to configure the QoS rule. Use [Table 3-18](#) on page 3-63 as a reference.

**Procedure 3-19 Configure Ingress Payload Database**

**Step – Action**

- 1 In the **Ingress** field, select *not applicable*.  
The field is applicable for policy routing only.
- 2 In the **Destination Interface** field, select *not applicable*.  
The field is applicable for policy routing only.
- 3 In the **Class of Service** field, leave the default *CoS1*.
- 4 In the **Destination IP** field, enter *192.168.1.5*.
- 5 In the **Destination IP Mask** field, enter *255.255.255.255*.
- 6 In the **Protocol** field, leave the default selection *TCP*.
- 7 Click **Apply** to temporarily activate the settings on the page.  
The rule is generated at the bottom of the page ([Figure 3-46](#)).



**Figure 3-46 Ingress Payload Database Rule 1**

**Policy Database Configuration**

Ingress Interface : LAN group 1      Destination Interface : PPPoE1  
 DiffServ Code Point :      Class of Service : CoS1

Source IP :      Destination IP :  
 Mask :      Mask :

Protocol : TCP [tcp]  
 Source Port Start :      Source Port End :  
 Destination Port Start :      Destination Port End :

Source MAC :  
 Local Routing Mark :

Ingress Interface	DSCP	Source IP	Destination IP	Source Port Start	Destination Port Start	Protocol	Local Mark	Delete
			192.168.1.5			tcp		<input type="checkbox"/>
	CoS1	255.255.255.255						

Apply    Cancel

**Note**—The changes take effect when you click **Apply**; however, if the RG configuration is not saved, these changes will be lost upon RG reboot.

- 8 To make the change permanent, click **Tools** and select **System Commands**. On the **System Commands** page (Figure 5-2 on page 5-3), click **Save All**.

#### End of Procedure 3-19

### WLAN Ingress Support

WLAN Ingress is supported; however, it is hard-coded and is not configurable on the **Ingress** pages. More information is available at 3.18.3 “[WLAN QoS Support](#)” on page 3-69.

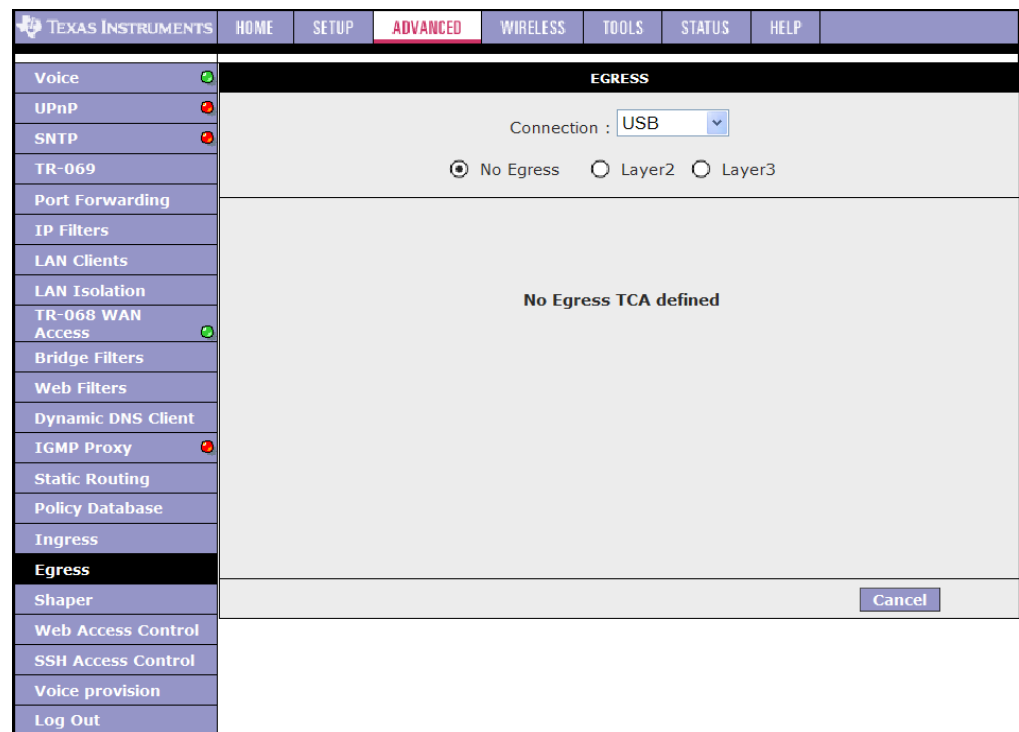
### 3.18.2 Egress

For packets going out of the RG, the marking (CoS) need to be translated to the mappings understood by the network domains. The reverse CoS and domain mapping is configured using the **Egress** page (Figure 3-47). This page is accessed by selecting **Egress** on the **Advanced** main page.

#### No Egress Mode

The default **Egress** page setting for all interfaces is *No Egress*. In this mode, the domain mappings of the packets are untouched.

**Figure 3-47 Egress Page - No Egress**



#### Egress Layer 2 Configuration

The **Egress Layer 2** page (Figure 3-48) enables you to map the CoS of an outgoing packet to user priority bits, which is honoured by the VLAN network. Again, this feature is only configurable on the WAN interfaces as VLAN is only supported on the WAN side in the current release.

**Figure 3-48 Egress Page - Layer2**

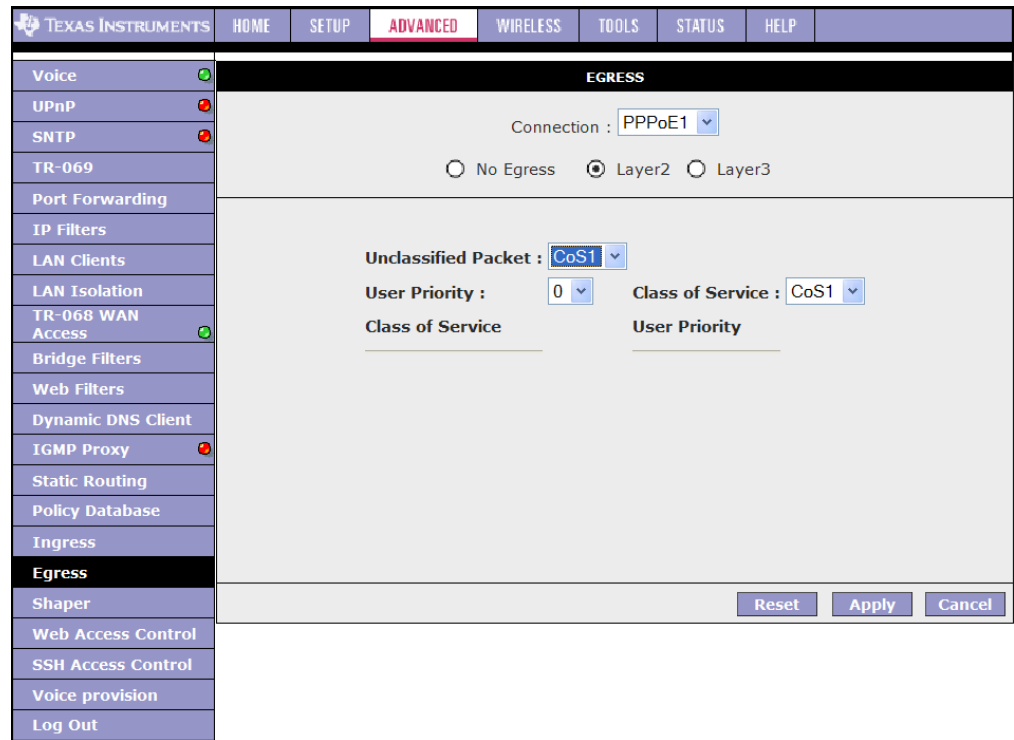


Table 3-19 describes the Egress Layer 2 Configuration page settings.

**Table 3-19 Egress - Layer 2 Page Descriptions**

Field	Definition/ Description
Interface	Select the WAN interface to configure the QoS for outgoing packets. LAN interface can not be selected as VLAN is currently supported on the WAN side only.
Unclassified Packet	Some locally generated packets might not have been classified and thus do not have a CoS value, such as PPP control packet and ARP packet. You can define the CoS for all unclassified outgoing packets on layer 2 using this field, which will then pick up the user priority bits based on the mapping rules you create. The selections are (in the order of descending priority): CoS1, CoS2, CoS3, CoS4, CoS5, and CoS6. The default value is CoS1 (recommended).
User Priority	The selections are 0, 1, 2, 3, 4, 5, 6, 7.
Class of Service	The selections are (in the order of descending priority): CoS1, CoS2, CoS3, CoS4, CoS5, and CoS6.
<b>End of Table 3-19</b>	

## Egress Layer 3 Configuration

The **Egress Layer 3** page (Figure 3-49) enables you to map CoS to ToS so that the priority marking of outgoing packets can be carried over to the IP network.

**Figure 3-49 Egress Page - Layer 3**

Table 3-20 describes the **Egress - Layer 3 Configuration** page settings.

**Table 3-20 Egress - Layer 3 Page Descriptions**

Field	Definition/ Description
Interface	Select the WAN/LAN interface here to configure the QoS for outgoing traffic to the IP network.
Default Non-IP	Locally generated packets (such as ARP packets) do not have a CoS marking. You can define the CoS for all unclassified outgoing packets on layer 3 using this field. The selections are (in the order of descending priority): CoS1, CoS2, CoS3, CoS4, CoS5, and CoS6. The default value is CoS1 (recommended).
Translated ToS	The Type of Service field takes values from 1 to 255. The selections are 0, 1, 2, 3, 4, 5, 6, 7.
Class of Service	The selections are (in the order of descending priority): CoS1, CoS2, CoS3, CoS4, CoS5, and CoS6.
<b>End of Table 3-20</b>	

### WLAN Egress Support

WLAN Egress is supported; however, it is hard-coded and is not configurable on the **Egress** pages. More information is available in the [WLAN QoS Support](#) section that follows.

### 3.18.3 WLAN QoS Support

The WLAN QoS is supported; however, it is hard-coded and is not configurable on the **Ingress** and **Egress** pages.

[Table 3-20](#) describes the **WLAN QoS** settings.

**Table 3-21 WLAN QoS Settings**

User Priority	Class of Service	WME Priority	DSCP Map
0 (Best-Effort)	CoS5	0	0 (0x0)
1 (Background)	CoS6	1	8 (0x20)
2 (Background)	CoS6	2	16 (0x40)
3 (Best-Effort)	CoS5	3	24 (0x60)
4 (Video)	CoS2	4	32 (0x80)
5 (Video)	CoS2	5	40 (0xA0)
6 (Voice)	CoS1	6	48 (0xC0)
7 (Voice)	CoS1	7	56 (0xE0)
<b>End of Table 3-21</b>			

There is no shaper support on WLAN interface.

### 3.18.4 Shaper

The **Shaper Configuration** page ([Figure 3-50](#)) is accessed by selecting **Shaper** on the **Advanced** main page. Three shaper algorithms are supported:

- HTB
- Low Latency Queue Discipline
- PRIOWRR



**Note**—Egress TCA is required if shaper is configured for that interface.

**Figure 3-50 Shaper Page**

The screenshot shows the 'Shaper Configuration' page. On the left is a sidebar with navigation items: Voice, UPnP, SNTP, TR-069, Port Forwarding, IP Filters, LAN Clients, LAN Isolation, TR-068 WAN Access, Bridge Filters, Web Filters, Dynamic DNS Client, IGMP Proxy, Static Routing, Policy Database, Ingress, Egress, Shaper (highlighted), Web Access Control, SSH Access Control, Voice provision, and Log Out. The main area has a title bar 'Shaper Configuration' and a navigation bar with 'HOME', 'SETUP', 'ADVANCED', 'WIRELESS', 'TOOLS', 'STATUS', and 'HELP'. The configuration options include:
 

- Interface: USB (dropdown menu)
- HTB Queue Discipline:  Max Rate: [input field]
- Low Latency Queue Discipline:
- CoS1: [input] Kbits, CoS2: [input] Kbits
- CoS3: [input] Kbits, CoS4: [input] Kbits
- CoS5: [input] Kbits, CoS6: [input] Kbits
- PRIOWRR:
- CoS2: [input]%, CoS3: [input]%, CoS4: [input]%, CoS5: [input]%, CoS6: [input]%

 At the bottom right are 'Reset', 'Apply', and 'Cancel' buttons.

Table 3-22 describes the **Shaper Configuration** page settings.

**Table 3-22 Shaper Configuration Descriptions**

Field	Definition/ Description
Interface	The selections are WAN/LAN interfaces except WLAN, which does not support Shaper feature. This field needs to be selected before shaper configuration.
Max Rate	This field is applicable for the HTB Queue Discipline and Low Latency Queue Discipline, both are rate-based shaping algorithms.
HTB Queue Discipline	The hierarchical token bucket queue discipline is a rate-based shaping algorithm. This algorithm rate shapes the traffic of a class over a specific interface. All CoSx traffic is assigned a specific rate to which data will be shaped to. For example: If CoS1 is configured to 100Kbps then even if 300Kbps of CoS1 data is being transmitted to the interface only 100Kbps will be sent out.
Low Latency Queue Discipline	This is similar to the above algorithm except that CoS1 is not rate limited. So in the example above CoS1 data is not rate limited to 100Kbps but instead all 300Kbps is transmitted. The side effect is that a misconfigured stream can potentially take all bandwidth.
PRIOWRR	This is a priority based weighted round robin algorithm operating on CoS2-CoS6. CoS1 queues have the highest priority and are not controlled by the WRR algorithm.
<b>End of Table 3-22</b>	

Of the three shaping algorithms available on the **Shaper Configuration** page, only one can be enabled at a time. An example of each configuration is given as follows.

**Example 1: HTB Queue Discipline Enabled**

In the example below, **HTB Queue Discipline** is enabled. The PPPoE1 connection has a total of 300 kbits of bandwidth, of which 100 kbits is given to CoS1 and another 100 kbits is given to CoS2. When there is no CoS1 or CoS2 packets, CoS6 packets have the whole 300 kbits of bandwidth.

**Figure 3-51 Shaper Page - HTD Queue Discipline Enabled**

The screenshot shows the 'Shaper Configuration' page in a web interface. On the left is a navigation menu with items like 'Voice', 'UPnP', 'SNTP', 'TR-069', 'Port Forwarding', 'IP Filters', 'LAN Clients', 'LAN Isolation', 'TR-068 WAN Access', 'Bridge Filters', 'Web Filters', 'Dynamic DNS Client', 'IGMP Proxy', 'Static Routing', 'Policy Database', 'Ingress', 'Egress', 'Shaper', 'Web Access Control', 'SSH Access Control', 'Voice provision', and 'Log Out'. The 'Shaper' menu item is highlighted. The main content area is titled 'Shaper Configuration' and includes a dropdown menu for 'Interface' set to 'PPPoE1'. Below this, there are three sections: 'HTB Queue Discipline' (checked), 'Low Latency Queue Discipline' (unchecked), and 'PRIOWRR' (unchecked). The 'HTB Queue Discipline' section has a 'Max Rate' field set to '300'. Below it are six 'CoS' (Class of Service) settings: CoS1 (100 Kbits), CoS2 (100 Kbits), CoS3 (0 Kbits), CoS4 (0 Kbits), CoS5 (0 Kbits), and CoS6 (300 Kbits). The 'PRIOWRR' section has percentage fields for CoS2 through CoS6, all of which are empty. At the bottom right of the configuration area are 'Reset', 'Apply', and 'Cancel' buttons.

### Example 2: Low Latency Queue Discipline Enabled

In this second example (Figure 3-52), **Low Latency Queue Discipline** is enabled. CoS1 is not rate controlled (hence the field is disabled). CoS2 takes 100 kbits when there is no CoS1 packets. CoS6 has 300 kbits when there is no CoS1 or CoS2 packets. This is similar to the **HTB** queue discipline as they are both rate-based algorithm, except that CoS1 is handled differently.

Figure 3-52 Shaper Page - Low Latency Queue Discipline Enabled

The screenshot shows the 'Shaper Configuration' page in the Texas Instruments web interface. The page is titled 'Shaper Configuration' and is located under the 'ADVANCED' tab. The interface includes a navigation menu on the left with options like Voice, UPnP, SNTP, TR-069, Port Forwarding, IP Filters, LAN Clients, LAN Isolation, TR-068 WAN Access, Bridge Filters, Web Filters, Dynamic DNS Client, IGMP Proxy, Static Routing, Policy Database, Ingress, Egress, Shaper, Web Access Control, SSH Access Control, Voice provision, and Log Out. The main configuration area is for the 'Interface: PPPoE1'. It features three sections: 'HTB Queue Discipline' (disabled), 'Low Latency Queue Discipline' (enabled), and 'PRIOWRR' (disabled). The 'Low Latency Queue Discipline' section has input fields for CoS1 through CoS6. CoS1 is disabled (indicated by a red circle around the field), CoS2 is set to 100 Kbits, CoS3 is 0 Kbits, CoS4 is 0 Kbits, CoS5 is 0 Kbits, and CoS6 is 300 Kbits. The 'HTB Queue Discipline' section has a 'Max Rate' field set to 300. The 'PRIOWRR' section has percentage fields for CoS2 through CoS6, all of which are empty. At the bottom right, there are 'Reset', 'Apply', and 'Cancel' buttons.



### Example 3: PRIOWRR Enabled

In this third example, **PRIOWRR** is enabled. Since PRIOWRR operates only on the number of packets being transmitted, the max rate field has been disabled. Only percentage can be assigned to the CoS2 - CoS6. CoS1 is not rate controlled (hence the field is not displayed). When there is no CoS1 packets, CoS2, CoS3, CoS4 each has 10 percent, and CoS6 has 70 percent. This is similarly to the **Low Latency Queue** discipline, except that one is packet-based, and the other is rate-based.

**Figure 3-53 Shaper Page - PRIOWRR Enabled**

The screenshot shows the 'Shaper Configuration' page in the Texas Instruments web interface. The left sidebar contains a navigation menu with items like Voice, UPnP, SNTP, TR-069, Port Forwarding, IP Filters, LAN Clients, LAN Isolation, TR-068 WAN Access, Bridge Filters, Web Filters, Dynamic DNS Client, IGMP Proxy, Static Routing, Policy Database, Ingress, Egress, Shaper, Web Access Control, SSH Access Control, Voice provision, and Log Out. The main content area is titled 'Shaper Configuration' and includes the following settings:

- Interface: PPPoE1
- HTB Queue Discipline Max Rate: [ ]
- Low Latency Queue Discipline
- CoS1: [ ] Kbits
- CoS2: [ ] Kbits
- CoS3: [ ] Kbits
- CoS4: [ ] Kbits
- CoS5: [ ] Kbits
- CoS6: [ ] Kbits
- PRIOWRR
- CoS2: 10 %
- CoS3: 10 %
- CoS4: 10 %
- CoS5: [ ] %
- CoS6: 70 %

Buttons for 'Reset', 'Apply', and 'Cancel' are located at the bottom right of the configuration area.

## 3.19 Policy Database

The **Policy Database Configuration** page (Figure 3-54) is accessed by selecting **Policy Database** on the **Advanced** home page. This page enables you to configure policy routing and QoS. The policy routing configuration is discussed as follows. The QoS configuration is discussed in “[Ingress Payload Database Configuration](#)” on page 3-61.

**Figure 3-54 Policy Database Configuration Page**

The screenshot shows the 'Policy Database Configuration' page. The top navigation bar includes 'TEXAS INSTRUMENTS', 'HOME', 'SETUP', 'ADVANCED', 'WIRELESS', 'TOOLS', 'STATUS', and 'HELP'. The left sidebar contains a menu with items like 'Voice', 'UPnP', 'SNTP', 'TR-069', 'Port Forwarding', 'IP Filters', 'LAN Clients', 'LAN Isolation', 'TR-068 WAN Access', 'Bridge Filters', 'Web Filters', 'Dynamic DNS Client', 'IGMP Proxy', 'Static Routing', 'Policy Database', 'Ingress', 'Egress', 'Shaper', 'Web Access Control', 'SSH Access Control', 'Voice provision', and 'Log Out'. The main content area is titled 'Policy Database Configuration' and contains the following fields:

- Ingress Interface: LAN group 1 (dropdown)
- Destination Interface: PPPoE1 (dropdown)
- DiffServ Code Point: (text input)
- Class of Service: CoS1 (dropdown)
- Source IP: (text input)
- Destination IP: (text input)
- Mask: (text input)
- Mask: (text input)
- Protocol: TCP (dropdown) tcp (text input)
- Source Port Start: (text input)
- Source Port End: (text input)
- Destination Port Start: (text input)
- Destination Port End: (text input)
- Source MAC: (text input)
- Local Routing Mark: (text input)

At the bottom, there is a table with columns: Ingress Interface, DSCP, Source IP, Destination IP, Source Port Start, Destination Port Start, Protocol, Local Mark, Delete. Below the table are 'Apply' and 'Cancel' buttons.

Table 3-23 describes the **Policy Database Configuration** page settings.

**Table 3-23 Policy Database Configuration Field Descriptions**

Field	Definition/ Description
Ingress Interface	The incoming traffic interface for a Policy Routing rule. Selections include <i>LAN interfaces</i> , <i>WAN interfaces</i> , <i>Locally generated (traffic)</i> , and <i>not applicable</i> . Examples of Locally generated traffic are: voice packets, packets generated by applications such as DNS, DHCP, etc.
Destination Interface	The outgoing traffic interfaces for a Policy Routing rule. Selections include <i>LAN Interfaces</i> and <i>WAN interfaces</i> .
DiffServ Code Point	The diffServ code point (DSCP) field value ranges from 1 to 255. This field cannot be configured alone, additional fields like <b>IP</b> , <b>Source MAC</b> , and/or <b>Ingress Interface</b> should be configured.
Class of Service	This field is applicable for Ingress Payload Database configuration only and is discussed in “ <a href="#">Ingress Payload Database Configuration</a> ” on page 3-61.
Source IP	The IP address of the traffic source.

**Table 3-23 Policy Database Configuration Field Descriptions**

Field	Definition/ Description
Mask	The source IP netmask. This field is required if the source IP has been entered.
Destination IP	The IP address of the traffic destination.
Mask	The netmask of the destination. This field is required if the destination IP has been entered.
Protocol	<p>The selections are <i>TCP</i>, <i>UDP</i>, <i>ICMP</i>, <i>Specify</i>, and <i>none</i>. If you choose <i>Specify</i>, you need to enter the protocol number in the box next to the <b>Protocol</b> field.</p> <p>This field cannot be configured alone, additional fields like <b>IP</b>, <b>Source MAC</b>, and/or <b>Ingress Interface</b> should be configured.</p> <p>This field is also required if the source port or destination port has been entered.</p>
Source Port Start	The starting port number of the source protocol. You cannot configure this field without entering the protocol first.
Source Port End	The ending port number of the source protocol. You cannot configure this field without entering the protocol first.
Destination Port Start	The starting port number of the destination protocol port. You cannot configure this field without entering the protocol first.
Destination Port End	The ending port number of the destination protocol. You cannot configure this field without entering the protocol first.
Source MAC	The MAC address of the traffic source.
Local Routing Mark	<p>This field is enabled only when <i>Locally Generated</i> is selected in the <b>Ingress Interface</b> field. The mark for DNS traffic generated by different applications are described below:</p> <ul style="list-style-type: none"> <li>• Dynamic DNS: 0xE1</li> <li>• Dynamic Proxy: 0xE2</li> <li>• Web Server: 0xE3</li> <li>• MSNTP: 0xE4</li> <li>• DHCP Server: 0xE5</li> <li>• IPtables Utility: 0xE6</li> <li>• PPP Daemon: 0xE7</li> <li>• IP Route: 0xE8</li> <li>• ATM Library: 0xE9</li> <li>• NET Tools: 0xEA</li> <li>• RIP: 0xEB</li> <li>• RIP v2: 0xEC</li> <li>• UPNP: 0xEE</li> <li>• Busybox Utility: 0xEF</li> <li>• Configuration Manager: 0xF0</li> <li>• DropBear Utility: 0xF1</li> <li>• Voice: 0</li> </ul>
Note: Wildcard (*) entries are allowed for IP Address/Netmask and Port range fields	
<b>End of Table 3-23</b>	

Currently routing algorithms make decision based on destination address, i.e., only Destination IP address and subnet mask is supported. The **Policy Routing** page enables you to route packets on the basis of various fields in the packet. The following fields can be configured for Policy Routing:

- Destination IP address/mask
- Source IP address/mask
- Source MAC address
- Protocol (TCP, UDP, ICMP, etc)
- Source port
- Destination port
- Incoming interface
- DSCP

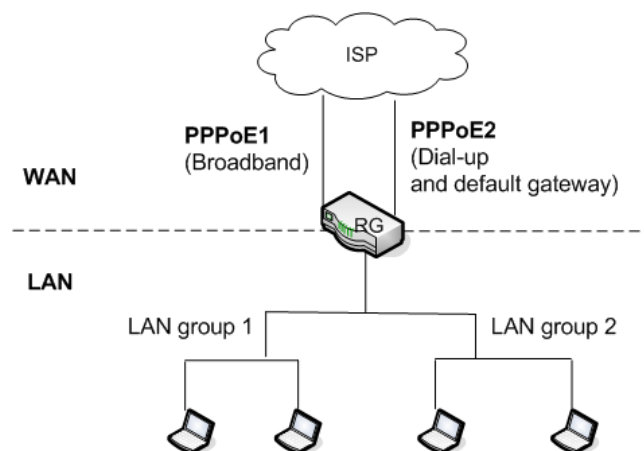
#### Example 1: Traffic Segregation

In the first example, we will use the **Policy Routing Configuration** page to configure traffic segregation. In [Figure 3-55](#), your RG has the following configuration:

- Two WAN connection: PPPoE1 (broadband connection) and PPPoE2 (dial-up and default gateway).
- Two LAN groups: LAN group 1 and LAN group 2
- Two computers in LAN group 1
- Two computers in LAN group 2

**Goal:** You want to reserve PPPoE1 for use by LAN group 1 computers only.

**Figure 3-55 Policy Routing Configuration Example 1**



Use [Table 3-23](#) on page 3-74 as a reference and follow [Procedure 3-20](#) to configure the PR rule.

---

**Procedure 3-20 Create PR rule**

---

**Step – Action**

- 1** In the **Ingress** field, select *LAN Group 1*.
- 2** In the **Destination Interface** field, select *PPPoE1*.
- 3** In the **Class of Service** field, select *N/A*.
- 4** In the **Protocol** field, leave the default selection *None*.  
This is to select all protocols.
- 5** Click **Apply to** temporarily activate the settings on the page.  
The first rule is created. Voice traffic from *LAN group 1* will go out on *PPPoE1*.
- 6** In the **Ingress** field, select *PPPoE1*.
- 7** In the **Destination Interface** field, select *LAN Group 1*.
- 8** In the **Class of Service** field, select *N/A*.
- 9** In the **Protocol** field, leave the default selection *None*.  
This is to select all protocols.
- 10** Click **Apply to** temporarily activate the settings on the page.  
Packets arriving into *LAN group 1* will come from *PPPoE1*. The rule is generated at the bottom of the page ([Figure 3-56](#)).

**Figure 3-56 Policy Database Rule 1**

Ingress Interface	DSCP	Source IP	Destination IP	Source Port	Protocol	Local Mark	Delete
br0	PPPoE						<input type="checkbox"/>
PPPoE	br0						<input type="checkbox"/>

**Note**—The changes take effect when you click **Apply**; however, if the RG configuration is not saved, these changes will be lost upon RG reboot.

- To make the change permanent, click **Tools** and select **System Commands**. On the **System Commands** page (Figure 5-2 on page 5-3), click **Save All**.

**End of Procedure 3-20**

**Example 2: Handling Voice Traffic**

In the second example, you will learn how to handle voice traffic in policy routing.

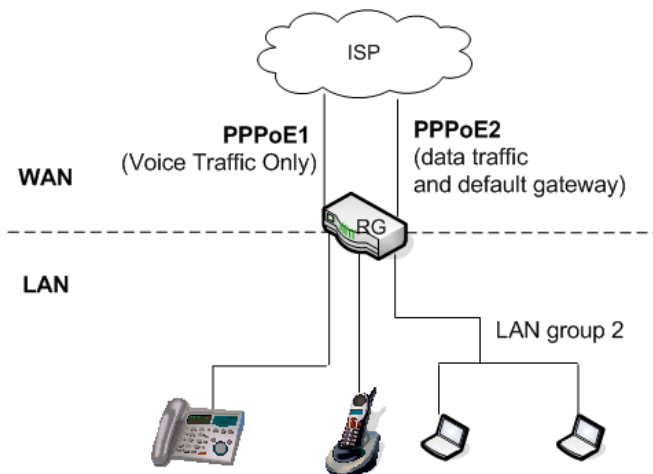
In Figure 3-55, your RG has the following configuration:

- Two WAN connection: PPPoE1 (broadband connection) and PPPoE2 (data traffic and default gateway).
- LAN side: LAN group 2 with two computers connected
- Two phones plugged into the phone ports

**Goal:** You want to route the locally-generated voice traffic to PPPoE1.

**What you should do:** You should enable voice on the **Voice** setup page (“**Voice Page**” on page 3-4). By default, voice is enable on the first WAN connection that is created. Make sure PPPoE1 is enabled and Policy routing rules are automatically added. No configuration is required on the **Policy Database** page.

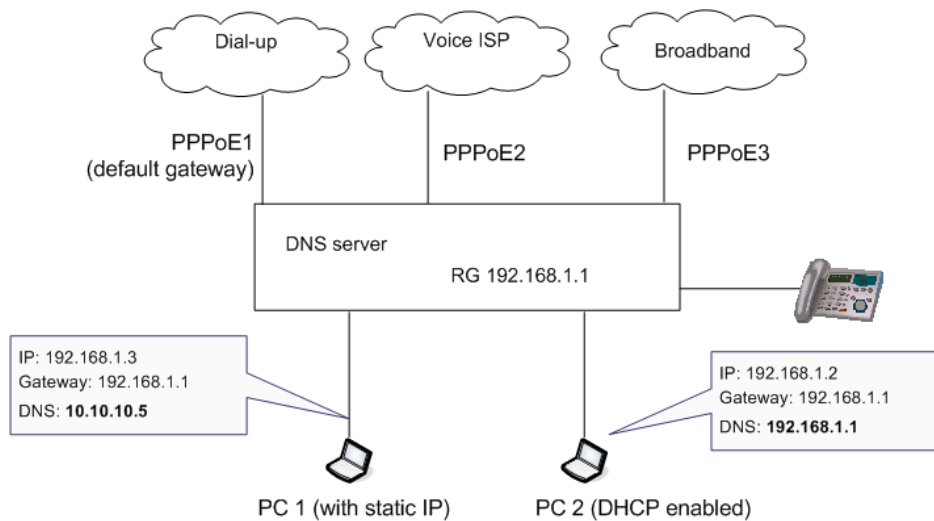
**Figure 3-57 Policy Routing Configuration Example 2**



**Example 3: Handling DNS Packets**

In example 3 (Figure 3-58), you will learn how to handle DNS packets. The policy routing configuration for all four types of DNS packets are discussed below.

**Figure 3-58 Policy Routing Configuration Example 3**



1. DNS packets generated by voice application

The following settings should be configured:

- **Ingress interface:** *Locally generated*
  - **Destination interface:** *PPPoE2*
  - **Protocol:** *UDP*
  - **Destination port start:** *53 (DNS port)*
  - **Destination port end:** *53 (DNS port)*
  - **Local marker:** *0*
- DNS packets generated by applications such as DDNS

The following settings should be configured:

- **Ingress interface:** *Locally generated*
  - **Destination interface:** *PPPoE3*
  - **Protocol:** *UDP*
  - **Destination port start:** *53 (DNS port)*
  - **Destination port end:** *53 (DNS port)*
  - **Local marker:** *225 (0xE1)*
- DNS requests from DHCP clients (when the RG is the DHCP/DNS server)

The following settings should be configured:

- **Ingress interface:** *Locally generated*
  - **Destination interface:** *PPPoE3*
  - **Protocol:** *UDP*
  - **Destination port start:** *53 (DNS port)*
  - **Destination port end:** *53 (DNS port)*
  - **Local marker:** *226 (0xE2)*
- DNS requests from the LAN side (When there is a external DHCP/DNS server)
- **Ingress interface:** *LAN Group 1 or N/A (not Locally generated)*
  - **Source IP address:** *192.168.1.3*
  - **Mask:** *255.255.255.255*
  - **Protocol:** *UDP*
  - **Destination port start:** *53 (DNS port)*
  - **Destination port end:** *53 (DNS port)*



## 3.20 Web Access Control Page

The **Web Access Control** page (Figure 3-59) allows you to access the RG remotely via the web from the WAN side.

**Figure 3-59 Web Access Control Page**

If you want to access your RG at home from a remote location such as your office, use [Table 3-24](#) on page 3-82 as a reference and configure your WAN IP address using [Procedure 3-21](#).

### Procedure 3-21 Enable Web Access Control (WAN-Side)

#### Step – Action

- 1 On your LAN-side PC, access the **Web Access Control** page.
- 2 Check **Enable** to enable the Web Access Control feature.
- 3 In the **Choose a Connection** field, leave the default WAN connection selected.
- 4 In the **Remote Host IP** field, enter the IP address of the PC on the WAN-side (for example, *10.10.10.1*). This is the PC you will use to access your RG remotely.
- 5 In the **Remote Netmask** field, enter the IP netmask of the WAN-side PC for remote access.
- 6 Enter a port number in the **Redirect Port** field (for example, 8080).

- 7 Click **Apply to** temporarily activate the settings on the page.  
This WAN address is added to the **IP Access List**. This allows you to access you RG at home from a WAN IP (10.10.10.1) via Web.  
**Note**—The changes take effect when you click **Apply**; however, if the RG configuration is not saved, these changes will be lost upon RG reboot.
- 8 To make the change permanent, click **Tools** and select **System Commands**. On the **System Commands** page (Figure 5-2 on page 5-3), click **Save All**.
- 9 To access your RG from the remote IP (10.10.10.1), enter the following in the URL:  
**Syntax:** *http(s)://WAN IP of RG:Port Number*  
**Example:** *http(s)://10.10.10.5:80*  
**Note**—The WAN-side IP address of the RG can be obtained from the **Status => Connection Status** page (Figure 6-6 on page 6-6).
- 10 Log in as *Admin/Admin*, *user/user*, or *router/router*.

**End of Procedure 3-21**

Table 3-24 describes the **Web Access Control** page settings:

**Table 3-24 Web Access Control Field Descriptions**

Field	Definition/ Description
Enable	Enables/disables the remote web access feature.
Choose a connection	Select the WAN connect over which the remote web access feature is enabled.
Remote Host IP	Enter the IP address of the remote host.
Remote Netmask	Enter the netmask of the remote host.
Redirect Port	You can enter a port number in this field that is different from the well-known IP port number 80. The port number that you enter will be viewed externally and mapped to port 80 internally in the RG.
<b>End of Table 3-24</b>	

## 3.21 SSH Access Control Page

The **SSH Access Control** page (Figure 3-60) allows you to access the RG remotely via SSH from the WAN side. You need a SSH client such as Tera term (v.31).

**Figure 3-60 SSH Access Control Page**

The screenshot shows the 'SSH Access Control' configuration page. On the left is a vertical navigation menu with items like Voice, UPnP, SNTP, TR-069, Port Forwarding, IP Filters, LAN Clients, LAN Isolation, TR-068 WAN Access, Bridge Filters, Web Filters, Dynamic DNS Client, IGMP Proxy, Static Routing, Policy Database, Ingress, Egress, Shaper, Web Access Control, **SSH Access Control**, Voice provision, and Log Out. The main area contains the following settings:

- Enable:
- Choose a connection: PPPoE1 (dropdown menu)
- Remote Host IP: 0.0.0.0
- Remote Netmask: 255.255.255.255

At the bottom right of the main area are 'Apply' and 'Cancel' buttons.

If you want to access your RG at home from a remote location such as your office via SSH, use Table 3-25 on page 3-84 as a reference and configure your WAN IP address using Procedure 3-22.

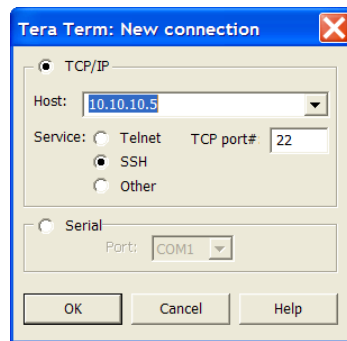
### Procedure 3-22 Enable SSH Access Control (WAN-Side)

#### Step – Action

- 1 On your LAN-side PC, access the **SSH Access Control** page.
- 2 Check **Enable** to enable the SSH Access Control feature.
- 3 In the **Choose a Connection** field, leave the default WAN connection selected.
- 4 In the **Remote Host IP** field, enter the IP address of the PC on the WAN-side (for example, *10.10.10.1*). This is the PC you will use to access your RG remotely.
- 5 In the **Remote Netmask** field, enter the IP netmask of the WAN-side PC for remote access.
- 6 Enter a port number in the **Redirect Port** field (for example, *8080*).

- 7 Click **Apply** to temporarily activate the settings on the page.  
This WAN IP address is added to the **IP Access List**. This allows you to access your RG at home from a WAN IP (10.10.10.1) via the Web.  
**Note**—The changes take effect when you click **Apply**; however, if the RG configuration is not saved, these changes will be lost upon RG reboot.
- 8 To make the change permanent, click **Tools** and select **System Commands**. On the **System Commands** page (Figure 5-2 on page 5-3), click **Save All**.
- 9 To access your RG from the remote IP (10.10.10.1), open a SSH client such as Tera term (v.3.1). Select **New Connection** under **File** and configure the following:
  - **TCP/IP:** check to enable TCP/IP
  - **Host:** Enter the RG’s WAN-side IP address, for example, 10.10.10.5
  - **Service:** Select **SSH**

**Figure 61 Create New SSH Connection Using Tera term**



**Note**—The WAN-side IP address of the RG can be obtained from the **Status => Connection Status** page (Figure 6-6 on page 6-6).

- 10 Click **OK**. At the prompts, enter your login and password, such as *Admin/Admin*.

**End of Procedure 3-22**

Table 3-25 describes the **SSH Access Control** page settings:

**Table 3-25 SSH Access Control Field Descriptions**

Field	Definition/ Description
Enable	Enables/disables the remote SSH access feature.
Choose a connection	Select the WAN connection over which the remote SSH access feature is enabled.

**Table 3-25 SSH Access Control Field Descriptions**

Field	Definition/ Description
Remote Host IP	Enter the IP address of the remote PC you will use to access the RG.
Remote Netmask	Enter the netmask of the remote PC you will use to access the RG.
<b>End of Table 3-25</b>	

## 3.22 Voice Provision

Figure 3-62 shows the default **Voice Provision** page. The **Voice Provisioning** page (Figure 3-62) allows you to define voice DNS servers, view provisioning status, and access the voice parameters configuration page.

**Figure 3-62 Voice Provision Page**

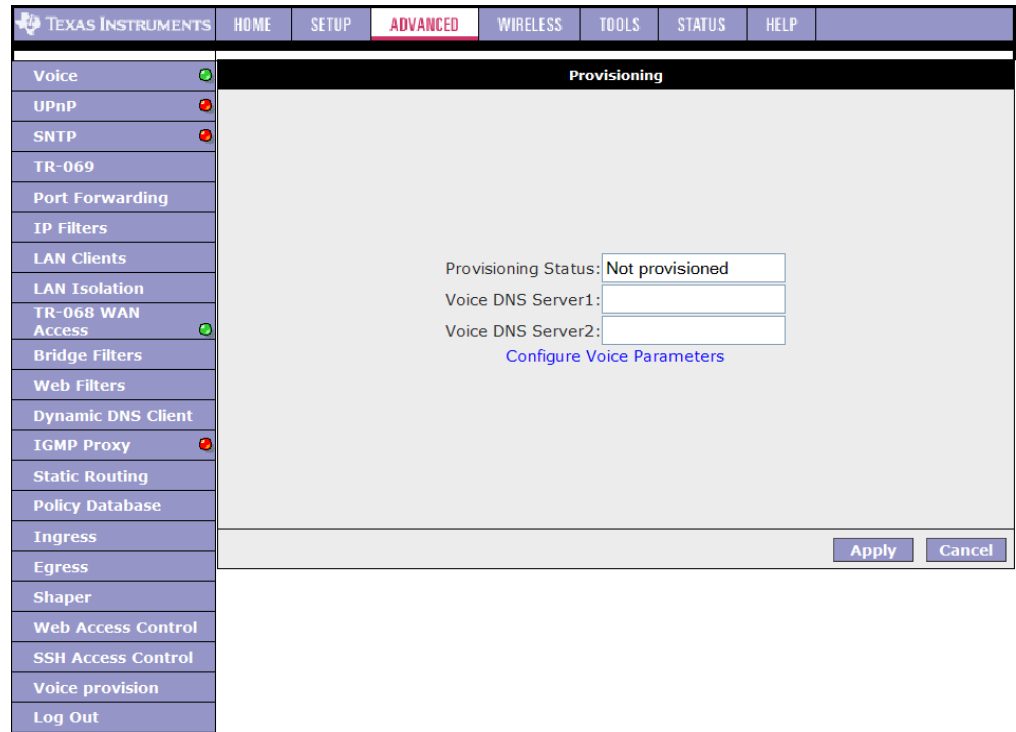


Table 3-26 describes the **Voice Provision** page settings:

**Table 3-26 Voice Provision Field Descriptions**

Field	Definition/ Description
Provisioning Status	Provides the provisioning status: <i>Provisioned</i> or <i>Not provisioned</i> . This is a view-only field.
Voice DNS Server 1	The IP address of the primary voice DNS server provided by the voice service provider.
Voice DNS Server 2	The IP address of the secondary voice DNS server provided by the voice service provider.
<b>End of Table 3-26</b>	

### 3.22.1 Voice Parameters Page

The **Voice Parameters** page can be accessed by clicking the **Configure Voice Parameters** link on the **Provisioning** page (Figure 3-63 is for the SIP build and Figure 3-64 is for the MGCP build). This page enables ODM/OEMs to configure voice parameters for phone port 1. Since port 2 is also supported, ODM/OEMs have the option to add a voice parameters page for port 2. The Voice Parameters pages should not be seen by the end user.



**Note**—More information about voice configuration parameters can be found in the *XML Provisioning Developer Guide*.

**Figure 3-63 Voice Parameters Page (SIP Build)**

TEXAS INSTRUMENTS		HOME	SETUP	ADVANCED	WIRELESS	TOOLS	STATUS	HELP
Voice	<input checked="" type="checkbox"/>							
UPnP	<input checked="" type="checkbox"/>							
SNTP	<input checked="" type="checkbox"/>							
TR-069								
Port Forwarding								
IP Filters								
LAN Clients								
LAN Isolation								
TR-068 WAN Access	<input checked="" type="checkbox"/>							
Bridge Filters								
Web Filters								
Dynamic DNS Client								
IGMP Proxy	<input checked="" type="checkbox"/>							
Static Routing								
Policy Database								
Ingress								
Egress								
Shaper								
Web Access Control								
SSH Access Control								
Voice provision								
Log Out								

Voice Parameters	
<b>Port 1 Configuration</b>	
DIGIT_MAP: xxxxx	PREF_CODING_PROFILE: 0
CID_NAME: LINE-0	CID_NUMBER: 1000
PROXY_FQDN:	PROXY_PORT: 5060
REG_FQDN:	REG_PORT: 5060
AUTH_USER_NAME:	AUTH_USER_PASSWD:
RING_ID: 1	
MWI_STATE <input type="checkbox"/>	NWAY_CONF <input type="checkbox"/>
CW_DEFAULT <input checked="" type="checkbox"/>	CID_EMERGENCY <input type="checkbox"/>
CID_DEFAULT <input checked="" type="checkbox"/>	ACBLOCK_DEFAULT <input type="checkbox"/>
TONE_PLAY <input checked="" type="checkbox"/>	REG_RINGING <input type="checkbox"/>
MSG_DISPLAY <input type="checkbox"/>	EMERGENCY_CALL <input checked="" type="checkbox"/>
CALL_RETURN <input type="checkbox"/>	REPEAT_DIAL <input checked="" type="checkbox"/>
DO_NOT_DISTURB <input type="checkbox"/>	NET_REG_CHECK <input type="checkbox"/>
ANON_CALL_BLOCK <input type="checkbox"/>	CALLER_ID <input checked="" type="checkbox"/>
CALL_WAITING <input checked="" type="checkbox"/>	MWI <input checked="" type="checkbox"/>
CONFERENCING <input checked="" type="checkbox"/>	CALL_TRANSFER <input checked="" type="checkbox"/>
CALL_FORWARD <input type="checkbox"/>	
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

**Figure 3-64 Voice Parameters Page (MGCP Build)**

TEXAS INSTRUMENTS	HOME	SETUP	ADVANCED	WIRELESS	TOOLS	STATUS	HELP
Voice	<b>Voice Parameters</b>						
UPnP							
SNTP							
TR-069							
Port Forwarding							
IP Filters							
LAN Clients							
LAN Isolation							
TR-068 WAN Access							
Bridge Filters							
Web Filters							
Dynamic DNS Client							
IGMP Proxy							
Static Routing							
Policy Database							
Ingress							
Egress							
Shaper							
Web Access Control							
SSH Access Control							
Voice provision							
Log Out							

Voice Parameters	
<b>Port 1 Configuration</b>	
DIGIT_MAP:	<input type="text"/>
PREF_CODING_PROFILE:	<input type="text" value="0"/>
CID_NAME:	<input type="text" value="LINE-0"/>
CID_NUMBER:	<input type="text" value="1000"/>
CALL_AGENT:	<input type="text"/>
<b>MGCP Configuration</b>	
DEFAULT_CA_PORT:	<input type="text" value="2727"/>
RGW_NAME:	<input type="text" value="mta-100.telogy.com"/>



## Wireless LAN (WLAN)

---

---

---

The **wireless local area networks (WLAN)** tab allows you to perform WLAN interface configuration functions.

This chapter discusses:

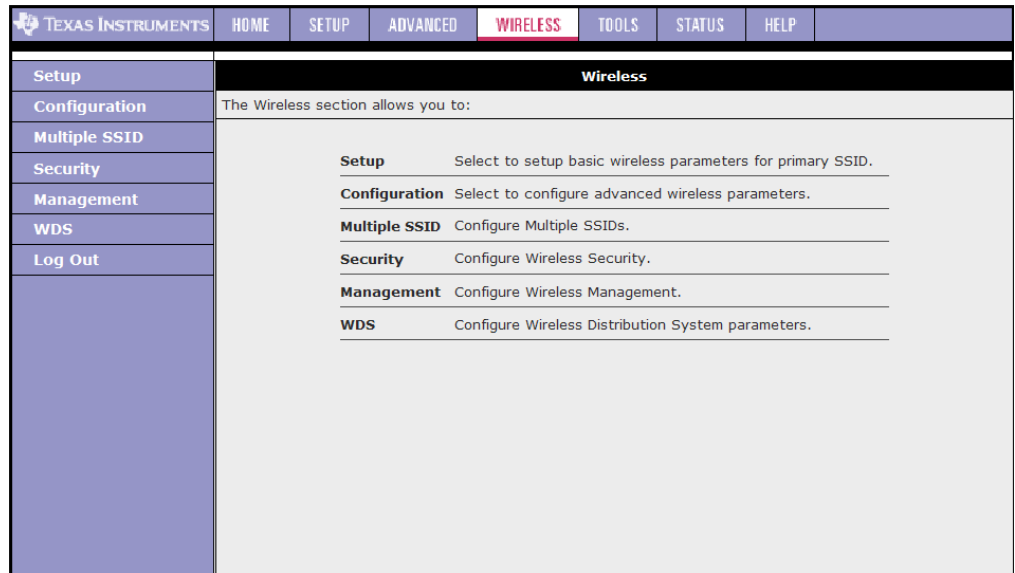
- ["Wireless Main Page"](#) on page 4-2
- ["Wireless Setup Page"](#) on page 4-3
- ["Wireless Configuration Page"](#) on page 4-7
- ["Multiple SSID"](#) on page 4-9
- ["Wireless Security Page"](#) on page 4-11
- ["Wireless Management"](#) on page 4-16
- ["WDS"](#) on page 4-18
- ["Wireless Statistics Page"](#) on page 4-20
- ["Hidden Pages"](#) on page 4-21

## 4.1 Wireless Main Page

Figure 4-1 shows the **Wireless** main page, which 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

**Figure 4-1 Wireless Main**



## 4.2 Wireless Setup Page

Figure 4-2 shows the default **Wireless Setup** page, which is accessed by clicking the **Setup** link. This page provides basic access point (AP) parameter settings.

**Figure 4-2 Wireless Setup Page**

Table 4-1 describes the **Wireless Setup** page fields.

**Table 4-1 Wireless Setup Field Descriptions**

Field	Definition/Definition
Enable AP	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 <i>TI-AR7VW</i> 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.

**Table 4-1 Wireless Setup Field Descriptions**

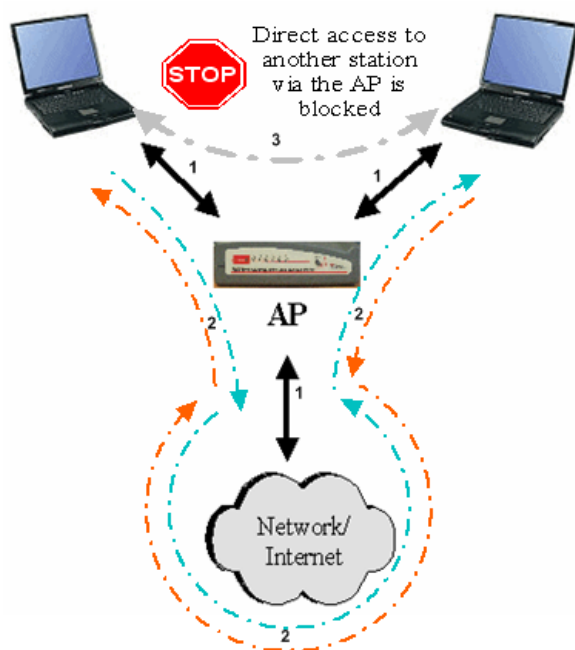
Field	Definition/Definition
802.11 Mode	You can select from the following modes: <ul style="list-style-type: none"> <li>• <b>Mixed mode:</b> Both 802.11b and g modes are supported. The legacy supported rates information element (SR IE) contains the 802.11b legacy supported rates and the additional OFDM supported rates. Extended SR IE contains the extended supported rates, if present. Beacon &amp; Probe Response Frames are sent in b rate.</li> <li>• <b>11b only Mode:</b> The legacy SR IE contains only the 802.11b legacy supported rates. The extended SR IE is not present.</li> <li>• <b>11b+ Mode:</b> Similar to the 802.11b-only mode except that 22Mbps PBCC rate/modulation is included, which is TI proprietary.</li> <li>• <b>11g only Mode:</b> The legacy SR IE contains only the OFDM additional supported rates. The extended SR IE contains the extended supported rates, if present.</li> </ul>
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 in 4.2.1 “ <a href="#">User Isolation</a> ” on page 4-4.
QoS Support	Refer to 3.18.3 “ <a href="#">WLAN QoS Support</a> ” on page 3-69 for more information.
<b>End of Table 4-1</b>	

### 4.2.1 User Isolation

When user isolation is enabled, wireless users will not be able to directly access other wireless users. Access can be controlled by the AP.

[Figure 4-3](#) illustrates the three states of enabling the user isolation feature:

1. AP disabled basic service set (BSS) bridging: Before user isolation is enabled, the stations can exchange data via the AP. This is disabled when user isolation is enabled.
2. All data is sent to WAN.
3. Enable/disable flag: No station has direct access to other stations as a result of user isolation.

**Figure 4-3 User Isolation**

### 4.2.2 Save Your Changes

Follow [Procedure 4-1](#) to save changes you have made on the **Wireless Setup** page.



**CAUTION**—Any changes you make to the WLAN page do NOT get saved automatically. Clicking **Apply** on the individual page is not sufficient for the changes you made to take effect. For changes you made to any WLAN page to take effect, you must perform the steps in [Procedure 4-1](#).

#### Procedure 4-1 Save Your Changes

##### Step – Action

- 1 Click **Apply**.
- 2 Click **Restart Access Point** at the bottom of the page, which takes you to the **System Commands** page.

**Note**—An alternative way to access the **System Commands** page is to select **Tools** (at the top of the page), then click the **System Commands** link.

- 3 On the **System Commands** page, click **Save All**.

This temporarily saves all the changes you have made. You will still need to restart the access point for any changes to take effect.

---

**4** Click **Restart Access Point** for changes to the WLAN settings to take effect.

**End of Procedure 4-1**

---

## 4.3 Wireless Configuration Page

You can access the **Wireless Configuration** page (Figure 4-4) by clicking the **Configuration** link. This page provides the advanced wireless network parameter settings.

**Figure 4-4 Wireless Configuration Page**

The screenshot shows the 'Wireless Configuration' page with the following fields:

- Beacon Period: 100 msec
- DTIM Period: 3
- RTS Threshold: 2347
- Frag Threshold: 2346
- Power Level: Full
- Multi Domain Capability (highlighted):
  - Country String: US
  - Band B/G
  - Current Reg. Domain: FCC
  - Private Reg. Domain: 0

Note: you must [Restart Access Point](#) for Wireless changes to take effect.



**Note**—The highlighted area relates to the multi domain capability function, which cannot be configured on this page. It is configured on a hidden page (Figure 4-15). For more information on the wireless hidden pages, refer to the *AP-DK Web-based Configuration Utility User's Guide*.

Table 4-2 describes the **Wireless Configuration** page fields.

**Table 4-2 Configuration Field Descriptions**

Field	Definition/Definition
Beacon Period	The time interval between beacon frame transmissions, which ranges from 0 - 65535 msec. The default value of this field is 100 msec.
DTIM period	Delivery traffic identification map period: The number of beacon frame transmissions before frames that are targeted for stations operating in low-power mode, will be transmitted. The default value of this field is 3.
RTS threshold	Request to send threshold: The number of bytes in a Mac protocol data unit (MPDU) below which an RTS/CTS handshake will not be performed. The default value is 2347; however, when 4x is enabled on the setup page, the RTS threshold value changes to 4096.
Fragmentation Threshold	The minimum length of a frame that will be fragmented. The default value is 2346; however, when 4x is enabled on the <b>Setup</b> page, the fragmentation threshold value changes to 4096.
Power Level	The Tx output power percentage compared to the maximum Tx power: full, 75%, 50%, 25%, and 6%.

**Table 4-2 Configuration Field Descriptions**

Field	Definition/Definition
Multi Domain Capability	This feature can only be configured on a hidden page (Figure 4-15) 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 hidden page (Figure 4-15) 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 hidden page (Figure 4-15) 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 hidden page (Figure 4-15) by the OEM/ODM. It is not recommended that the end users configure this feature.
<b>End of Table 4-2</b>	

For information on how to save the settings you have changed, refer to [Procedure 4-1](#) on page 4-5.



## 4.4 Multiple SSID

You can access the **Multiple SSID** page (Figure 4-5) by clicking the **Multiple SSID** link. The **Enable SSID** field allows you to create multiple SSIDs for the AP. The Multiple SSID feature supports up to four SSIDs (one primary and three secondary).

**Figure 4-5** Configure Multiple SSID (Default)

The screenshot shows the 'Configure Multiple SSID' page. The top navigation bar includes 'TEXAS INSTRUMENTS', 'HOME', 'SETUP', 'ADVANCED', 'WIRELESS', 'TOOLS', 'STATUS', and 'HELP'. The left sidebar lists 'Setup', 'Configuration', 'Multiple SSID', 'Security', 'Management', 'WDS', and 'Log Out'. The main content area is titled 'Configure Multiple SSID' and contains the following elements:

- Enable Multiple SSID
- Secondary SSID:
- Hide this SSID:
- 

At the bottom of the page, there is a note: 'Note: you must Restart Access Point for Wireless changes to take effect.' and two buttons: 'Apply' and 'Cancel'.

Follow [Procedure 4-2](#) to configure multiple SSIDs.

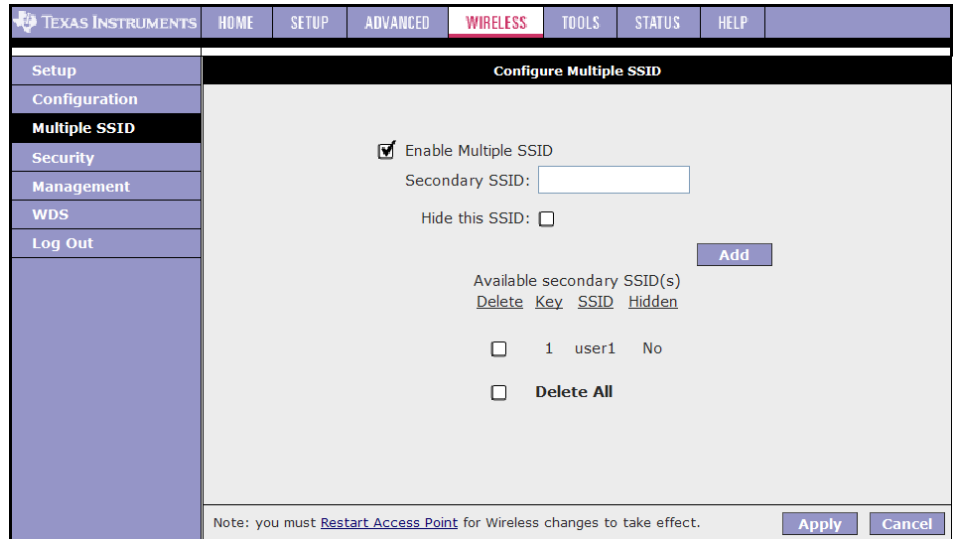
### Procedure 4-2 Configure Multiple SSIDs

#### Step – Action

- 1 Check **Enable Multiple SSID**.
- 2 Enter a value in the **Secondary SSID** field, for example, *user1*.  
**Note**—The SSID field takes up to 32 alpha-numeric characters.
- 3 You can enable the **Hide this SSID** field or leave it disabled.
- 4 Click **Add**.

The SSID appears as shown in [Figure 4-6](#).

**Figure 4-6 Configure Multiple SSID (New)**



5 You can repeat step 2 - 4 to add more SSIDs.

**Note**—Up to 3 secondary SSIDs are supported (in addition to the primary SSID).

6 To delete an SSID, check the SSID, then click **Delete** in the pop-up window. To delete all SSIDs, check **Delete All**.

**Note**—When the last secondary SSID is deleted, WLAN QoS is disabled and the VLAN ID of the primary SSID is changed to the default 0.

7 To save your settings, refer to Procedure 4-1 “Save Your Changes” on page 4-5.

**End of Procedure 4-2**

Table 4-3 describes the **Configure Multiple SSID** page fields.

**Table 4-3 Configure Multiple SSID Field Descriptions**

Field	Definition/Definition
Enable Multiple SSID	Enables/disables multiple SSID.
Secondary SSID	The secondary SSID of the AP, is up to 32 characters and is unique from the primary SSID.
Hide this 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.
<b>End of Table 4-3</b>	

## 4.5 Wireless Security Page

Figure 4-7 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 stations with WPA capability to connect the AP.
- WPA2: Enable stations with WPA2 capability to connect the AP. This option is available under the WPA option.

**Figure 4-7 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*.

### 4.5.1 Wireless Security - WEP

WEP is a security protocol for WLAN. WEP provides security by encrypting the data that is sent over the WLAN.

The RG supports three levels of WEP encryption:

- 64-bit encryption
- 128-bit encryption
- 256-bit 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. [Figure 4-8](#) shows the default setting of the **WEP Wireless Security** page.

**Figure 4-8 Wireless Security Page- WEP**

The screenshot shows the 'Wireless Security' configuration page for WEP. The page has a navigation menu on the left with 'Security' selected. The main content area is titled 'Wireless Security' and includes a dropdown for 'Select an SSID and its security level' set to 'TI-AR7VW'. Below this are radio buttons for 'None', 'WEP' (selected), '802.1x', and 'WPA'. There is a checkbox for 'Enable WEP Wireless Security' which is unchecked. The 'Authentication Type' is set to 'Open'. Under 'Encryption Key', there are four radio buttons, all of which are selected. To the right, under 'Cipher', there are four dropdown menus, all set to '64 bits'. A note at the bottom states: 'Note: you must Restart Access Point for Wireless changes to take effect.' There are 'Apply' and 'Cancel' buttons at the bottom right.

WEP is disabled by default. Follow [Procedure 4-3](#) to enable WEP on your AP.

#### **Procedure 4-3 Enable WEP**

##### **Step – Action**

- 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, refer to Procedure 4-1 [“Save Your Changes”](#) on page 4-5.

**End of Procedure 4-3**

Table 4-4 describes the **Wireless Security - WEP** page settings.

**Table 4-4 WEP Field Descriptions**

Field	Definition/ Description
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 <i>Legacy</i> . When the security configuration is set to <i>802.1x</i> or <i>WPA</i> , the authentication algorithm is always open. This field is enabled when the WEP security field is checked. There are three options: <ul style="list-style-type: none"> <li>• <b>Open</b> (default): In open-system authentication, the access point accepts any station without verifying its identify.</li> <li>• <b>Shared</b>: Shared-key authentication requires a shared key (WEP encryption key) be distributed to the stations before attempting authentication.</li> <li>• <b>Both</b>: If both is selected, the access point will perform shared-key authentication, then open-system authentication.</li> </ul>
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 <i>64 bits</i> , <i>128 bits</i> , and <i>256 bits</i> . The WEP cipher that is used when the security configuration is set to <i>WEP</i> . This field is not used when the security configuration is set to <i>802.1x</i> and <i>WPA</i> .
<b>End of Table 4-4</b>	

## 4.5.2 Wireless Security - 802.1x

802.1x is a security protocol for WLAN. It is a port-based network access control that keeps the network port disconnected until authentication is completed. 802.1x is based on extensible authentication protocol (EAP). EAP messages from the authenticator to the authentication server typically use the remote authentication dial-in user service (RADIUS) protocol. [Figure 4-9](#) shows the default setting of the **Wireless Security - 802.1x** page.

**Figure 4-9 Wireless Security - 802.1x**

Table 4-5 describes the **Wireless Security - 802.1x** page settings.

**Table 4-5 802.1 Field Descriptions**

Field	Definition/ Description
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.
Server IP Address	The IP address of the RADIUS server. Used for authentication.
Port	The protocol port of the RADIUS server.
Secret	The secret that the AP shares with the RADIUS server. You can enter up to 63 alpha-numeric characters in this field.
Group Key Interval	The group key interval that is used to distribute the group key to 802.1x and WPA stations. The default value of this field is 3600 secs.
<b>End of Table 4-5</b>	

### 4.5.3 Wireless Security - WPA

WPA is a security protocol for WLAN. WPA uses a sophisticated key hierarchy that generates new encryption keys each time a mobile device establishes itself with an AP. Protocols including 802.1X, EAP, and RADIUS are used for strong authentication. Like WEP, keys can still be entered manually (pre-shared keys); however, using a RADIUS authentication server provides automatic key generation and enterprise-wide authentication. WPA uses temporal key integrity protocol (TKIP) for data encryption. WPA2, also known as 802.11i, uses advanced encryption standard counter mode CBC-MAC protocol (AES-CCMP) for data encryption.

Figure 4-10 shows the default setting of the **Wireless Security - WPA** page.

**Figure 4-10 Wireless Security - WPA**

Table 4-6 describes the **Wireless Security - WPA** page settings.

**Table 4-6 WPA Field Descriptions**

Field	Definition/ Description
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.
WPA	Enables stations that support WPA v.1 to connect to the AP.
WPA2	Enables stations that support WPA v.2 to connect to the AP.
AnyWPA	Enables stations that support WPA v.1 and WPA v.2 to connect to the AP.
Enable WPA2 Pre-authentication	Enables/disables WPA2 pre-authentication. This field is activated only when <b>WPA2</b> or <b>AnyWPA</b> is enabled.
Group Key Interval	This value is measured in seconds.
Radius Server	When selected, the WPA stations authenticate with the RADIUS server using extensible authentication protocol - transport layer security (EAP-TLS) over 802.1x.
IP Address	IP address of the RADIUS server.
Port	The protocol port of the RADIUS server.
Secret	The secret that the AP shares with the RADIUS server. You can enter up to 64 alpha-numeric characters in this field.
Pre-shared Key	When selected, the WPA stations do not authenticate with the RADIUS server using EAP-TLS. Instead they share a pre-shared secret with the AP (ASCII format).
PSK String	Pre-shared key string. The PSK string needs to be entered in the first-time configuration of each station. You can enter 8 - 63 alpha-numeric characters in this field.
<b>End of Table 4-6</b>	

## 4.6 Wireless Management

The wireless management function gives another level of security to your AP. It allows you to create an allowed access list or a banned access list (not both) and view a list of stations associated with your access point.

### 4.6.1 Access List

By clicking **Management** from the left-hand navigation list, you are taken to the default **Access List** page (Figure 4-11).

**Figure 4-11 Wireless Management - Access List**

The screenshot shows the 'Wireless Management' interface. The top navigation bar includes 'TEXAS INSTRUMENTS', 'HOME', 'SETUP', 'ADVANCED', 'WIRELESS' (highlighted), 'TOOLS', 'STATUS', and 'HELP'. The left sidebar contains 'Setup', 'Configuration', 'Multiple SSID', 'Security', 'Management' (highlighted), 'WDS', and 'Log Out'. The main content area is titled 'Wireless Management' and features a dropdown menu for 'Select an SSID' with 'TI-AR7VW' selected. Below this are two buttons: 'Access List' (highlighted) and 'Associated Stations'. Under the 'Access List' section, there is a checkbox for 'Enable Access List' which is unchecked. Below the checkbox are two radio buttons: 'Allow' (selected) and 'Ban'. At the bottom of this section is a 'Mac Address' input field and an 'Add' button. At the very bottom of the page, there is a note: 'Note: you must Restart Access Point for Wireless changes to take effect.' and 'Apply' and 'Cancel' buttons.

You can create an **Allowed** or **Banned** access list for each SSID from the **Access List** page using Procedure 4-4.

#### Procedure 4-4 Create an Access List

##### Step – Action

- 1 Select a **SSID** from the drop down list.
- 2 Check **Enable Access List**.
- 3 Select **Allow** to create an allowed access list or **Ban** to create a banned list.  
**Note**—You can create only one (allowed or banned) access list for each SSID. Only the same type of access list (allowed or banned) can be created for all SSIDs.
- 4 Enter a MAC address of an allowed or banned station, then click **Add**.  
This station appears in your allowed or banned access list.
- 5 Repeat this step for each station you want to add to your access list.



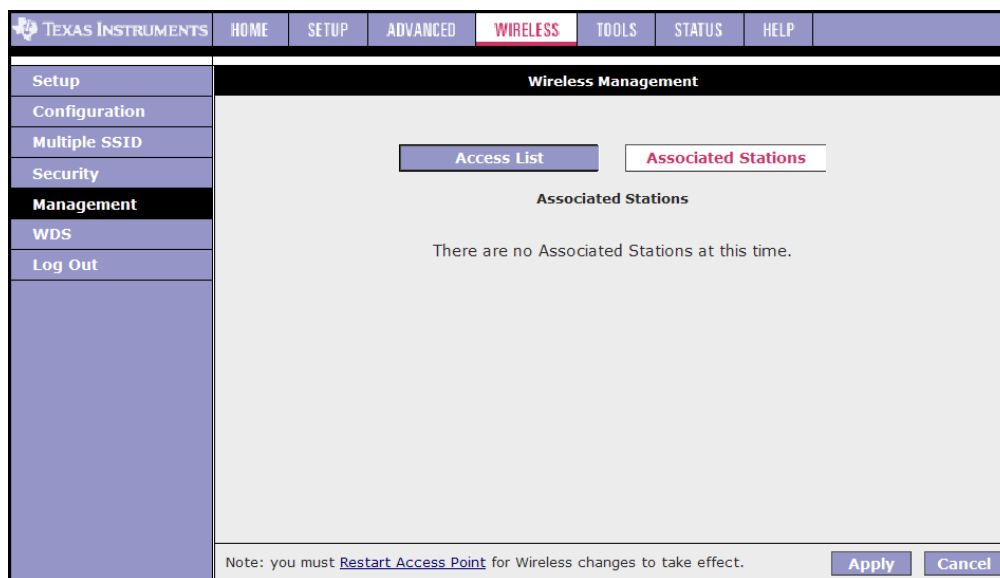
- To save your settings, refer to Procedure 4-1 “[Save Your Changes](#)” on page 4-5.

**End of Procedure 4-4**

## 4.6.2 Associated Stations

By clicking **Associated Stations** on the **Wireless Management** page, you are taken to the **Associated Stations** page (Figure 4-12). This page allows you to see a list of all stations associated with the access point. You can ban any stations on the list by clicking **Ban Station** next to the MAC Address. If the **Allowed Access** list is enabled, this station will be deleted from the **Allowed Access** List. If the **Banned Access** list is enabled, this station will be added to the **Banned Access** List. To save your settings, refer to Procedure 4-1 “[Save Your Changes](#)” on page 4-5.

**Figure 4-12 Wireless Management - Associated Stations**



## 4.7 WDS

Wireless distribution system (WDS) is a system that interconnects BSS to build a premise wide network. WDS network allows users of mobile equipment to roam and stay connected to the available network resources. You can configure your RG/AP as WDS mode using the WDS page (Figure 4-13).

**Figure 4-13 WDS**

The screenshot shows the 'Wireless Distribution System' configuration page. The left sidebar contains navigation options: Setup, Configuration, Multiple SSID, Security, Management, **WDS**, and Log Out. The main content area is titled 'Wireless Distribution System' and contains the following settings:

- WDS Mode: **Disabled** (dropdown menu)
- WDS Name: **WDS\_TI** (text input)
- Activate as Root:
- WDS Privacy:  Secret:
- Auto Channel Selection:
- Auto Configuration:

Below these settings is a table for 'Bridging Direction' with columns for 'Enable' and 'MAC address':

Bridging Direction	Enable	MAC address
Uplink:	<input type="checkbox"/>	<input type="text"/>
Downlink 1:	<input type="checkbox"/>	<input type="text"/>
Downlink 2:	<input type="checkbox"/>	<input type="text"/>
Downlink 3:	<input type="checkbox"/>	<input type="text"/>
Downlink 4:	<input type="checkbox"/>	<input type="text"/>

At the bottom, a note reads: 'Note: you must [Restart Access Point](#) for Wireless changes to take effect.' There are 'Apply' and 'Cancel' buttons.

Table 4-7 describes the WDS page settings.

**Table 4-7 WDS Field Descriptions**

Field	Definition/ Description
WDS Mode	<p>The following WDS modes are available:</p> <ul style="list-style-type: none"> <li>• <b>Bridge:</b> In Bridge mode, the AP basic service set (BSS) service is enabled.</li> <li>• <b>Repeater:</b> In Repeater mode, the AP BSS is disabled when connection to the upper layer AP is established.</li> <li>• <b>Crude:</b> In Crude mode, the AP BSS service is always enabled; however, the links between APs are configured statically and are not maintained.</li> <li>• <b>Disabled (Default):</b> WDS inactive.</li> </ul> <p>In Both Bridge and Repeater modes, WDS uses management protocol to establish and maintain links between APs.</p>
WDS Name	The WDS name is used to identify WDS network. The field takes up to eight characters. Two or more WDS networks may exist in the same area.
Activate as Root	This field must be checked for the root device in WDS hierarchy. Only one WDS root device may exist in WDS network. This field is not applicable for Crude mode.

**Table 4-7 WDS Field Descriptions**

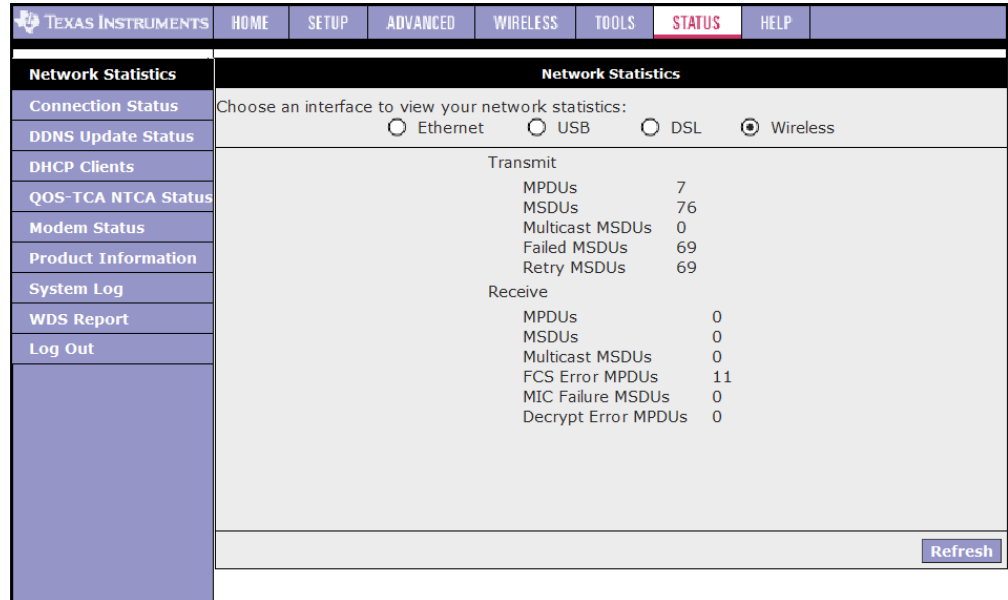
Field	Definition/ Description
WDS Privacy	Checking this field commands WDS manager to use a secured connection between APs in the WDS network. Security settings must be the same in all APs in the WDS network.  Note: WDS privacy is not supported in Crude mode.
Secret	The 32-character alpha-numeric privacy key.
Auto Channel Selection	Auto channel selection is not supported in the current version.
Auto Configuration	Auto configuration is not supported in the current version.
Uplink Connection Check Box	The BSS ID of the upper device in the WDS hierarchy. This uplink cannot be configured if Root is enabled.
Downlink Connection Check Boxes	The BSS ID of the lower device in the WDS hierarchy connected to this AP. Up to four downlinks can be configured.
<b>End of Table 4-7</b>	

To learn more about WDS report, visit 6.10 [“WDS Report”](#) on page 6-14.

## 4.8 Wireless Statistics Page

The **Network Statistics - Wireless** page (Figure 4-14) allows you to check on the wireless statistics of your RG.

**Figure 4-14 Network Statistics Page - Wireless**



Use [Procedure 4-5](#) to access the **Network Statistics - Wireless** page.

### Procedure 4-5 Wireless Statistics

#### Step – Action

- 1 Click **Status** at the top of the page.
- 2 Select **Network Statistics** from the left-hand column.
- 3 Click **Wireless**.

For your information, here is a description of the acronyms used in this page:

- **MPDU**: MAC protocol data unit
- **MSDU**: MAC service data unit
- **FCS**: Frame check sequence

**End of Procedure 4-5**

## 4.9 Hidden Pages

There are four WLAN hidden pages:

- Wireless Production 1
- Wireless Channel Range
- Wireless Production 2
- Wireless Advanced



**Note**—The hidden pages are to be used by ODMs/OEMs for development and debugging purposes only. Do **NOT** distribute this section to the end user.

### 4.9.1 Wireless Production 1

The **Wireless Production 1** hidden page (Figure 4-15) allows you to configure country string, domain, and so on. You can access this page by replacing the pagename in the URL with “pagename=wireless\_production1” or by typing in the following address:

[http://192.168.1.1/cgi-bin/webcm?getpage=..%2Fhtml%2Fdefs%2Fstyle5/menus%2Fmenu.html&var:style=style5&var:main=menu&var:pagename=wireless\\_production1&var:pagetitle=Home&var:menu=wireless&var:menutitle=Wireless](http://192.168.1.1/cgi-bin/webcm?getpage=..%2Fhtml%2Fdefs%2Fstyle5/menus%2Fmenu.html&var:style=style5&var:main=menu&var:pagename=wireless_production1&var:pagetitle=Home&var:menu=wireless&var:menutitle=Wireless)

Figure 4-15 Wireless Hidden 1

<p>Setup</p> <p>Configuration</p> <p>Multiple SSID</p> <p>Security</p> <p>Management</p> <p>WDS</p> <p>Log Out</p>	<p><b>Wireless Production 1</b></p> <p>4X Concatenate: <input type="checkbox"/></p> <p>4X Packet Bursting: <input type="checkbox"/></p> <p>4X Mixed: <input type="checkbox"/></p> <p>4X Feature Set: <input type="button" value="Version 1"/></p> <p>Power Constraint: <input type="text" value="0"/> (-50 to 50 dBm)</p> <p>Multi Domain Capability: <input type="checkbox"/> Country String: <input type="text" value="US"/></p> <p>Band B/G</p> <p>Current Reg. Domain: <input type="button" value="FCC"/></p> <p>Private Reg. Domain: <input type="text" value="0"/></p> <p>Note: you must <a href="#">Restart Access Point</a> for Wireless changes to take effect.</p> <p><input type="button" value="Apply"/> <input type="button" value="Cancel"/></p>
--	--

Table 4-8 describes the **Wireless Production 1** page settings.

**Table 4-8 Wireless Production 1 Field Descriptions**

Field	Definition/ Description
4X Concatenate	4x is a TI proprietary feature that is designed to improve throughput. 4X Concatenate, when enabled along with the 4X Packet Bursting field, enables the 4X feature.
4X Packet Bursting	4x is a TI proprietary feature that is designed to improve throughput. 4X Packet Bursting, when enabled along with the 4X Concatenate field, enables the 4X feature.
4X Mixed	Enables/disables 4x with CCK (Complementary Code Key).
4X Feature Set	Two options are provided: <i>version 0</i> and <i>version 1</i> .
Power Constraint	The power constraint to the Tx power in dBm. The range is -50 to 50 dBm.
Multi Domain Capability	Enables/disables multi domain capability (802.11d). This field is disabled by default.
Country String	The first two characters of the country string specifies the country name. The third character is defined as <i>I</i> for indoor, <i>O</i> for outdoor, and <i>none</i> for any.
Current Reg. Domain	The current regulatory domain options are: <i>FCC</i> , <i>IC</i> , <i>ETSI</i> , <i>Spain</i> , <i>France</i> , <i>MKK</i> , and <i>MKK1</i> .
Private Reg. Domain	This field defines a private regulatory domain. This domain is an addition to the standard domains that already reside in the AP. The range is 1-8 for band a, and 1-4 for band b/g.
<b>End of Table 4-8</b>	

### 4.9.2 Wireless Channel Range

The **Wireless Channel Range** hidden page (Figure 4-16) allows you to configure the wireless channel range. You can access this page by replacing the pagename in the URL with “*pagename=wireless\_chl\_range*” or by typing in the following address:

[http://192.168.1.1/cgi-bin/webcm?getpage=..%2Fhtml%2Fdefs%2Fstyle5/menus%2Fmenu.html&var:style=style5&var:main=menu&var:pagename=wireless\\_chl\\_range&var:pagetitle=Home&var:menu=wireless&var:menutitle=Wireless](http://192.168.1.1/cgi-bin/webcm?getpage=..%2Fhtml%2Fdefs%2Fstyle5/menus%2Fmenu.html&var:style=style5&var:main=menu&var:pagename=wireless_chl_range&var:pagetitle=Home&var:menu=wireless&var:menutitle=Wireless)

**Figure 4-16 Wireless Channel Range**

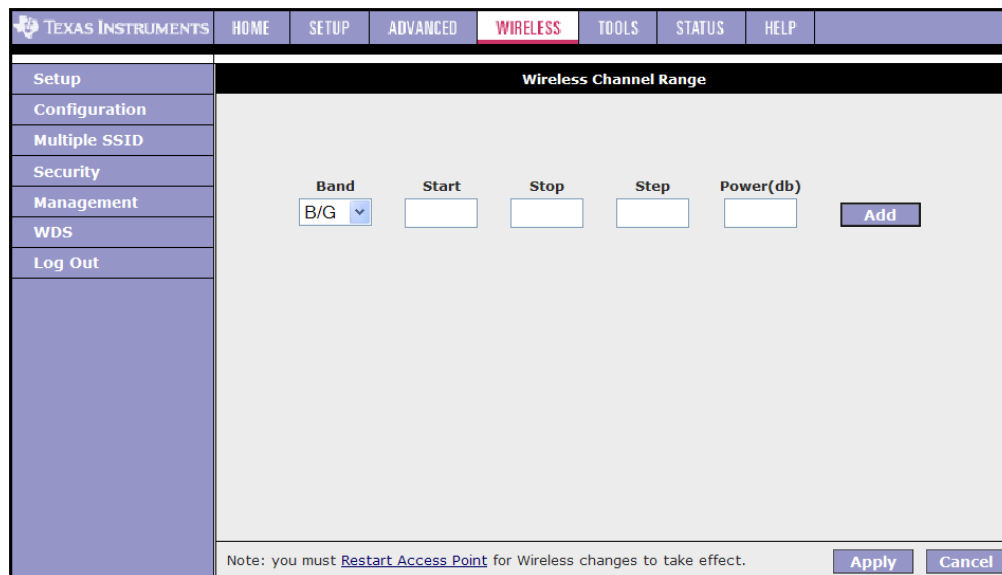


Table 4-9 describes the **Wireless Channel Range** page settings.

**Table 4-9 Wireless Channel Range Field Descriptions**

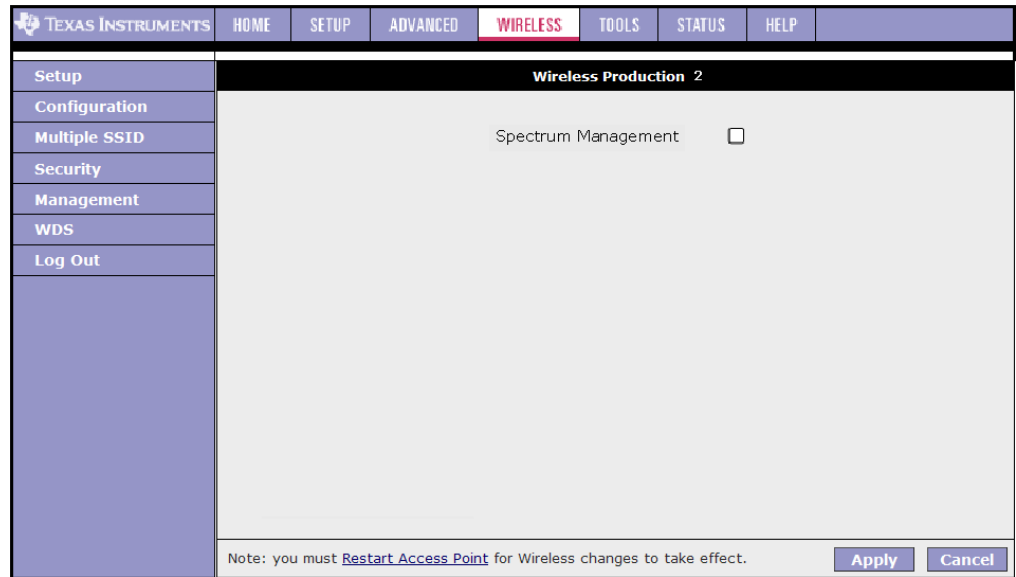
Field	Definition/ Description
Band	The default value is <i>B/G</i> .
Start	The <b>Start</b> and <b>Stop</b> fields define the range of the channels. Enter the starting channel in this field.
Stop	The <b>Start</b> and <b>Stop</b> fields define the range of the channels. Enter the ending channel in this field.
Step	This defines how the channel value increments in the channel range. For example, if the channel range is 1-8 and the step value is 1, the channels defined are: 1, 2, 3, 4, 5, 6, 7, 8, 9.
Power (db)	The transmit power limit in dBm. The range is -50 to 50 dBm.
<b>End of Table 4-9</b>	

### 4.9.3 Wireless Production 2

The **Wireless Production 2** hidden page (Figure 4-17) enables/disables spectrum management. The Spectrum Management (IEEE 802.11h) defines spectrum management for 802.11a (only) to ensure that concurrent deployment of the technology inter-operates and effectively shares the bandwidth of the spectrum. You can access the **Wireless Production 2** page by replacing the pagename in the URL with “*pagename=wireless\_production2*” or by typing in the following address:

[http://192.168.1.1/cgi-bin/webcm?getpage=..%2Fhtml%2Fdefs%2Fstyle5/menus%2Fmenu.html&var:style=style5&var:main=menu&var:pagename=wireless\\_production2&var:pagetitle=Home&var:menu=wireless&var:menutitle=Wireless](http://192.168.1.1/cgi-bin/webcm?getpage=..%2Fhtml%2Fdefs%2Fstyle5/menus%2Fmenu.html&var:style=style5&var:main=menu&var:pagename=wireless_production2&var:pagetitle=Home&var:menu=wireless&var:menutitle=Wireless)

**Figure 4-17 Wireless Production 2**



#### 4.9.4 Wireless Advanced

The **Wireless Advanced** hidden page (Figure 4-18) allows advanced configuration of the wireless connection. You can access this page by replacing the pagename in the URL with “*pagename=wireless\_advanced*” or by typing in the following address:

[http://192.168.1.1/cgi-bin/webcm?getpage=..%2Fhtml%2Fdefs%2Fstyle5/menus%2Fmenu.html&var:style=style5&var:main=menu&var:pagename=wireless\\_advanced&var:pagetitle=Home&var:menu=wireless&var:menutitle=Wireless](http://192.168.1.1/cgi-bin/webcm?getpage=..%2Fhtml%2Fdefs%2Fstyle5/menus%2Fmenu.html&var:style=style5&var:main=menu&var:pagename=wireless_advanced&var:pagetitle=Home&var:menu=wireless&var:menutitle=Wireless)



Figure 4-18 Wireless Advanced

TEXAS INSTRUMENTS HOME SETUP ADVANCED **WIRELESS** TOOLS STATUS HELP

Setup  
Configuration  
Multiple SSID  
Security  
Management  
WDS  
Log Out

**Wireless Advanced**

Select Band: Band B/G

Preamble Algo  
 Always Long  Always Short  Local STAs

Time Slot Algo  
 Always Off  Always On  Local STAs  Enhanced Dynamic

PBCC Algo  
 Always Off  Always On  Local STAs  Dynamic  Enhanced Dynamic

ERP Mode  
 Always Off  Always On  Local STAs  Dynamic  Enhanced Dynamic

ERP Type  
 RTS CTS  CTS To Self

ERP TI:  Rate Adaption Algorithm:

Additional 802.11g AP Legacy rates  
6M  9M  12M  18M  24M  36M  48M  54M

Additional 802.11g AP Extended rates  
6M  9M  12M  18M  24M  36M  48M  54M

CwMin Mode:  Usage Time:  msec

Long Retry Limit:  Short Retry Limit:

Tx Lifetime Limit:  Rx Lifetime Limit:

Energy Detect:  Radio Calibration:  Radio Calibration Interval:  sec

Rate Fallback:

Apply Cancel

Table 4-10 describes the **Wireless Advanced** page fields.

**Table 4-10 Wireless Advanced Field Descriptions**

Field	Definition/ Description
Preamble Algo	The preamble algorithm mode, which can be one of the following: <ul style="list-style-type: none"> <li>• <b>Always Long:</b> Transmission uses long preamble, the Barker bit in the effective radiated power (ERP) IE is set, and the short preamble (SP) bit in the Capability field is cleared.</li> <li>• <b>Always Short:</b> Transmission uses short preamble, the Barker bit in the ERP IE is cleared, and the SP bit in the Capability field is set.</li> <li>• <b>Local STAs (default):</b> The SP setting depends on the SP capability of the AP's associated stations. If all associated stations support the SP, then the AP clears the Barker bit in the ERP ISE and uses short preamble. If one or more associated stations do not support the SP, then the AP sets the Barker bit in the ERP IE and uses long preamble.</li> </ul>
Time Slot Algo	The short slot time algorithm mode, which can be one of the following: <ul style="list-style-type: none"> <li>• <b>Always Off:</b> The SST bit in the capability field is cleared and the TNETW1x30 or 1350/A works with a 20µs slot time.</li> <li>• <b>Always On:</b> The SST bit in the Capability field is set and the TNETW1x30 or 1350/A works with a 9µs slot time.</li> <li>• <b>Local STAs (default):</b> The SST setting depends on the SST capability of the AP's associated stations. If all associated stations support the SST, then the AP sets the SST bit in the Capability field and the TNETW1x30 or 1350/A uses a 9µs slot time. If one or more associated stations do not support the SST, then the AP clears the SST bit and the TNETW1x30 or 1350/A uses a 20µs slot time.</li> <li>• <b>Enhanced Dynamic:</b> Similar to the Dynamic mode with the following extension: If associated stations with no SST capability do not transmit for a period of time, the SST bit in the Capability field is set and the TNETW1x30 or 1350/A uses a 9µs slot time.</li> </ul>
PBCC Algo	The packet binary convolution coding (PBCC) algorithm mode, which can be one of the following: <ul style="list-style-type: none"> <li>• <b>Always Off:</b> The PBCC bit in the Capability field is cleared.</li> <li>• <b>Always On:</b> The PBCC bit in the Capability field is set.</li> <li>• <b>Local STAs:</b> The PBCC setting depends on the PBCC capability of the AP's associated stations. If all associated stations support PBCC, then the AP sets the PBCC bit in the Capability field. If one or more associated stations do not support PBCC, then the AP clears the PBCC bit in the Capability field.</li> <li>• <b>Dynamic:</b> Similar to Local STAs mode with the following extension: The PBCC capability setting is dependent on received beacon frames from overlapping BSSs. If beacons with no PBCC capability are received, the PBCC capability is cleared. The algorithm is rechecked in intervals that equal the longest beacon interval.</li> <li>• <b>Enhanced Dynamic (default):</b> Similar to dynamic mode with the following extension: If associated stations with no PBCC capability do not transmit for a period of time, the PBCC bit in the Capability field is set.</li> </ul>

**Table 4-10 Wireless Advanced Field Descriptions**

Field	Definition/ Description
ERP Mode	<p>The Extended rate phy protection mode, which can be one of the following:</p> <ul style="list-style-type: none"> <li>• <b>Always Off:</b> MPDUs transmitted at one of the OFDM rates do not use protection. The Use_Protection bit is always cleared. The NonERP_Present bit is set if as least one non-ERP STA is associated with the AP; otherwise, it is cleared.</li> <li>• <b>Always On:</b> MPDUs transmitted at one of the OFDM rates are protected according to the prototype command setting. The Use_Protection bit is always set. The NonERP_Present bit is set if at least one one-ERP STA is associated with the AP; otherwise, it is cleared.</li> <li>• <b>Local STAs:</b> The protection mode setting depends on the ERP capability of the AP's associated stations. If all associated stations support ERP, then the AP clears the Use_Protection bit. If one or more associated stations do not support ERP, then the AP sets the Use_Protection bit in the Capability field.</li> <li>• <b>Dynamic (default):</b> Protection is enabled or disabled using the following triggers: <ul style="list-style-type: none"> <li>- Non-ERP STAs association or disassociation.</li> <li>- Starting or stopping the reception of beacons with the NonERP_Present bit set from an overlapping BSS.</li> </ul> </li> <li>• <b>Enhanced Dynamic:</b> Similar to Dynamic mode with the following extension: When there is no interference by an overlapping BSS, the AP acts as follows: <ul style="list-style-type: none"> <li>- On MPDU reception from a non-ERP STA, the AP updates the FrameFromNonERPstaion timestamp.</li> <li>- Before MPDU transmission, the AP checks the difference between the time elapsed from the last timestamp update. If the difference is below a configurable threshold (set by the dynalgotimeout command), the AP protects its FOFDM transmission. If the difference is above the threshold, there is no need for protection.</li> <li>- On beacon reception with the NonERP_Preset bit set from an overlapping BSS (that is, interference exists), the Enhanced Dynamic and Dynamic modes are the same.</li> </ul> </li> </ul>
ERP Type	<p>The following two options are available:</p> <ul style="list-style-type: none"> <li>• <b>RTS/CTS:</b> A CCK RTS/CTS handshake will precede the OFDM transmission.</li> <li>• <b>CTS to Self (default):</b> A CCK CTS frame will precede the OFDM transmission.</li> </ul>
ERP TI	<p>Enables/disables ERP TI proprietary:</p> <ul style="list-style-type: none"> <li>• Short CCK frame with a preamble that indicates a duration that protects the OFDM frame that follows.</li> <li>• Used only by TI APs and STAs that announce this capability during association frame exchange.</li> <li>• Used by AP only for MPDUs transmitted to TI STAs, OFDM transmission to other STAs will be protected by CTS to Self frames.</li> <li>• Legacy RTS/CTS frame exchange is checked first and only in case the MPDU length is below the threshold, the protection mechanism is used.</li> </ul> <p>This field is disabled by default.</p>

**Table 4-10 Wireless Advanced Field Descriptions**

Field	Definition/ Description
Rate Adaption Algorithm	Enables/disables the rate adaption algorithm, which is the ability of the access point to change the bit rate depending on the network conditions. This field is enabled by default.
Additional 802.11g AP Legacy rates	The additional OFDM rates in the legacy supported rates IE (information element). The options are: <ul style="list-style-type: none"> <li>• <b>Y</b>: Rate supported</li> <li>• <b>N</b> (default): Rate not supported</li> <li>• <b>B</b>: Basic rate supported</li> </ul>
Additional 802.11g AP Extended rates	The OFDM rates in the extended supported rates IE. The options are: <ul style="list-style-type: none"> <li>• <b>Y</b> (default): Rate supported</li> <li>• <b>N</b>: Rate not supported</li> <li>• <b>B</b>: Basic rate supported</li> </ul>
CwMin Mode	The following contention window minimum modes are available: <ul style="list-style-type: none"> <li>• <b>0</b>: CwMin=31, the CW min. is set to the range 1-31.</li> <li>• <b>1</b>: CwMin=15, the CW min. is set to the range 1-15.</li> <li>• <b>2</b> (default): CWMin dot11mode dependent. The CW min. is dot11mode command dependent:                             <ul style="list-style-type: none"> <li>- For dot11mode settings 802.11b only and 802.11b+, CW Min. is set to the range 1-31.</li> <li>- For dot11mode settings 802.11g only and 802.11a only and Mixed, CW Min. is set to the range 1-15.</li> </ul> </li> </ul> If the 4x feature is enabled, CW Min. is set to the range 1-15.
Usage Time	Sets initial time slice for b/g band and a band. The default value of this field is 20.
Long Retry Limit	A retry limit is the number of times a station attempts to retransmit a frame before discarding it. The long retry limit applies to frames longer than the RTS threshold. The default value of this field is 4 (out of 1-255)
Short Retry Limit	A retry limit is the number of times a station attempts to retransmit a frame before discarding it. The short retry limit applies to frames shorter than the RTS threshold. The default value of this field is 7 (out of 1-255).
Tx Lifetime Limit	In addition to the associated retry count, fragments are given a maximum lifetime by the MAC. When the fragment is transmitted, the transmit lifetime counter is started. When the transmit lifetime limit is reached, the frame is discarded and no attempt is made to transmit any remaining fragments. The default value of this field is 512.
Rx Lifetime Limit	In addition to the associated retry count, fragments are given a maximum lifetime by the MAC. When the fragment is received, the receive lifetime counter is started. When the receive lifetime limit is reached, the frame is discarded and no attempt is made to receive any remaining fragments. The default value of this field is 512.
Energy Detect	Enables/disables energy detection mechanism. This field is enabled by default.
Radio Calibration	Sets the radio calibration algorithm. The default value of this field is 1.

**Table 4-10 Wireless Advanced Field Descriptions**

Field	Definition/ Description
Radio Calibration Interval	Sets the radio calibration interval in seconds. The default value of this field is 65535.
Rate Fallback	Sets rate fallback retry limit value. The default value of this field is 0.
<b>End of Table 4-10</b>	



# Tools

---

---

---

The **Tools** chapter discusses:

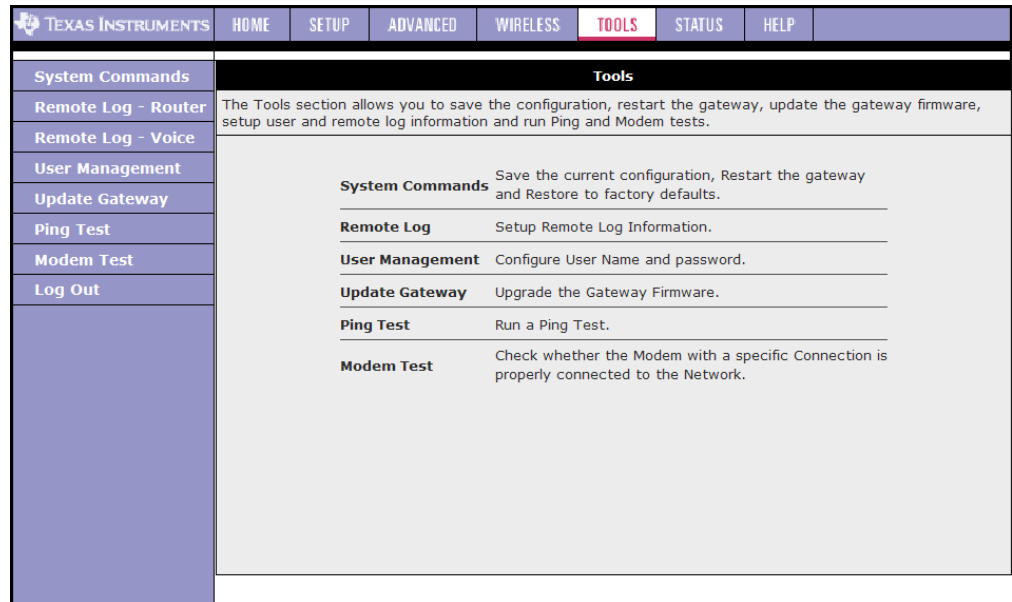
- ["Tools Main Page"](#) on page 5-2
- ["System Commands Page"](#) on page 5-3
- ["Remote Log - Router Page"](#) on page 5-4
- ["Remote Log - Voice Page"](#) on page 5-6
- ["User Management Page"](#) on page 5-7
- ["Update Gateway Page"](#) on page 5-8
- ["Ping Test Page"](#) on page 5-11
- ["Modem Test Page"](#) on page 5-13

## 5.1 Tools Main Page

Figure 5-1 shows the **Tools** main page, which is accessed by clicking **Tools** at the top of the page. This page provides access to the following tools pages:

- System Commands
- Remote Log - Router
- Remote Log - Voice
- User Management
- Update Gateway
- Ping Test
- Modem Test

**Figure 5-1 Tools Main Page**

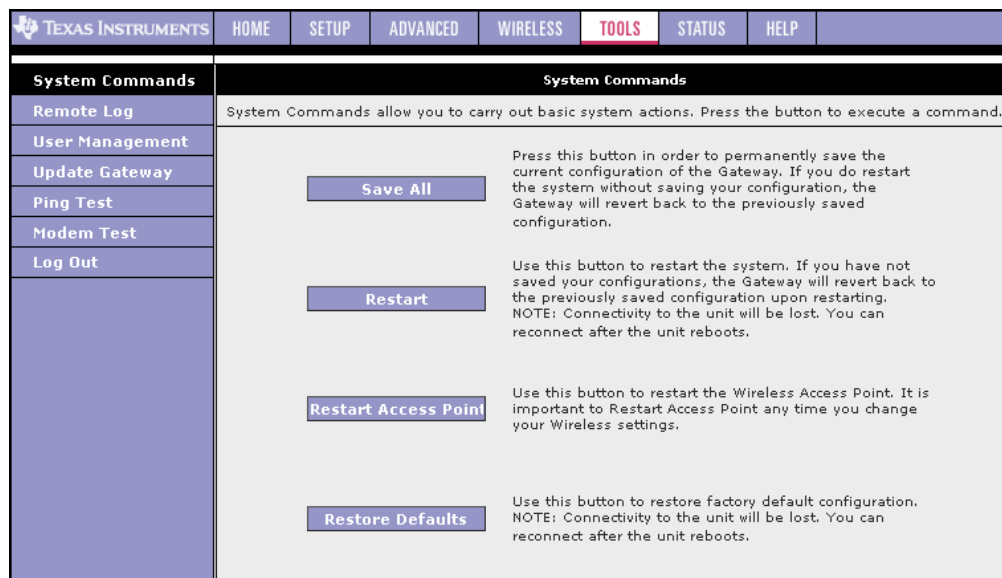




## 5.2 System Commands Page

Figure 5-2 shows the default System Commands page. Figure 5-3 shows the default System Commands page. This page is accessed by clicking the System Commands link at the left of the Tools page.

**Figure 5-2 System Commands Page (Admin and user)**



**Figure 5-3 System Commands Page (router)**

Table 5-1 describes the System Commands page options.

**Table 5-1 System Commands Field Descriptions**

Field	Definition/Definition
Save All	This button allows you to permanently save the current configuration of the RG. If you restart the system without saving your configuration, the RG reverts to the previously saved configuration.
Restart	This button allows you to restart the system. If you have not saved your configurations, the RG reverts to the previously saved configuration upon re-starting.  Note: Connectivity to the unit will be lost. You can reconnect after the unit reboots.
Restart Access Point	This button allows you to restart the wireless AP. It is important to restart the AP any time you change your wireless settings.
Restore Defaults	Use this button to restore the factory default configuration.  Note: Connectivity to the unit will be lost. You can reconnect after the unit reboots.
<b>End of Table 5-1</b>	

## 5.3 Remote Log - Router Page

Figure 5-4 shows the default **Remote Log** page, which is accessed by clicking the **Remote Log** link at the left of the **Tools** page. The remote log feature is used in conjunction with the PC tool (software provided with your RG). For PPPoE and PPPoA connections, you can select **Debug** in the **Log Level** field if you want to log the connection information. This is helpful when trying to debug connection problems. The remote log feature allows you to forwards all logged information to one (or more) remote syslog server. The type of information forwarded to the remote server depends upon the Log level. Each log message is assigned a severity level, which indicates how seriously the triggering event affects RG functions. When you configure logging, you must specify a severity level. Log messages that are rated at that level or higher are sent to the syslog server and can be viewed using the syslog server application, which can be downloaded from the web or comes with a linux machine. To view the log information on the web, refer to 6.9 “[System Log Page](#)” on page 6-13.

Figure 5-4 Remote Log Page

The screenshot shows the 'Remote Log - Router Settings' page. At the top, there is a navigation bar with tabs: TEXAS INSTRUMENTS, HOME, SETUP, ADVANCED, WIRELESS, TOOLS (highlighted), STATUS, and HELP. On the left side, there is a vertical menu with the following items: System Commands, Remote Log - Router (highlighted), Remote Log - Voice, User Management, Update Gateway, Ping Test, Modem Test, and Log Out. The main content area is titled 'Remote Log - Router Settings' and contains the following configuration options: a 'Log Level' section with a dropdown menu currently set to 'Notice'; an 'Add an IP Address:' section with a text input field and an 'Add' button; and a 'Select a logging destination:' section with a dropdown menu currently set to 'None' and a 'Delete' button. At the bottom right of the main content area, there are 'Apply' and 'Cancel' buttons.

Use [Table 5-2](#) as a reference and follow [Procedure 5-1](#) to configure remote log settings.

### Procedure 5-1 Configure Remote Log Settings

#### Step – Action

- 1 Select you desired **Log Level** from the drop-down list.

**Note**—When you select a log level, all log information within this severity level and levels above (meaning, more severe levels) are sent to the remote station.

- 2 Enter the **IP Address** of the remote station (for example, the syslog server) that the log information is to be sent to, and click **Add**.

This station is added to the drop-down list of the **Select a Logging Destination** field.

- 3 Select the **Logging Destination**.

You can edit the logging destination list using the **Add** and **Delete** buttons.

- 4 Click **Apply**.

#### End of Procedure 5-1

Table 5-2 describes the **Remote Log** page options.

**Table 5-2 Remote Log - Router Page Field Descriptions**

Field	Definition/Definition
Log Level	<p>There are eight log levels listed below in order of severity:</p> <ul style="list-style-type: none"> <li>• <b>Panic:</b> System panic or other condition that causes the RG to stop functioning.</li> <li>• <b>Alert:</b> Conditions that require immediate correction, such as a corrupted system database.</li> <li>• <b>Critical:</b> Critical conditions, such as hard drive errors.</li> <li>• <b>Error:</b> Error conditions that generally have less serious consequences than errors in the emergency, alert, and critical levels.</li> <li>• <b>Warning:</b> Conditions that warrant monitoring.</li> <li>• <b>Notice:</b> Conditions that are not errors but might warrant special handling.</li> <li>• <b>Info:</b> Events or non-error conditions of interest.</li> <li>• <b>Debug:</b> Software debugging message. Specify the level only when so directed by a technical support representative.</li> </ul> <p>The default log level is <i>Notice</i>.</p> <p>Note: When you select a log level, all log information within this severity level and levels above (meaning, more severe levels) will be sent to the remote host.</p>
Add an IP Address	<p>You should enter the IP address of the remote host to which you want the log information be forwarded. You can add more than more IP address, and any IP address you add here appears in the drop-down list of the next field: <b>Select a logging destination</b>.</p>
Select a Logging Destination	<p>You can select a destination IP address from the drop-down list. This defines where the log information will be sent. You can customize the destination list using the <b>Add</b> and <b>Delete</b> buttons.</p>
<b>End of Table 5-2</b>	

## 5.4 Remote Log - Voice Page

Figure 5-5 shows the default **Remote Log - Voice Settings** page, which can be accessed by clicking the **Remote Log - Voice** link at the left of the **Tools** page.

**Figure 5-5 Remote Log - Voice Settings Page**

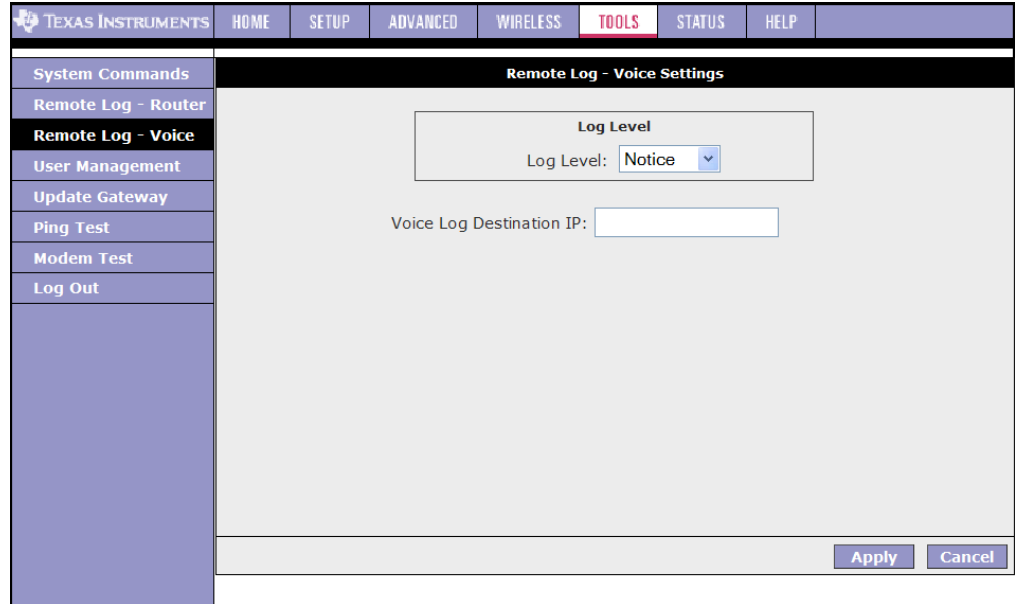


Table 5-2 describes the **Remote Log** page options.

**Table 5-3 Remote Log - Voice Page Field Descriptions**

Field	Definition/Definition
Log Level	<p>There are eight log levels listed below in order of severity:</p> <ul style="list-style-type: none"> <li>• Panic</li> <li>• Alert:</li> <li>• Critical</li> <li>• Error</li> <li>• Warning</li> <li>• Notice</li> <li>• Info</li> <li>• Debug</li> </ul> <p>The default log level is <i>Notice</i>.</p>
Add an IP Address	<p>You should enter the IP address of the remote host to which you want the log information be forwarded. You can add more than more IP address, and any IP address you add here appears in the drop-down list of the next field: <b>Select a logging destination</b>.</p>
Select a Logging Destination	<p>You can select a destination IP address from the drop-down list. This defines where the log information will be sent. You can customize the destination list using the <b>Add</b> and <b>Delete</b> buttons.</p>
<b>End of Table 5-3</b>	

## 5.5 User Management Page

Figure 5-6 shows the **User Management** page, which is accessed by clicking **User Management** at the left of the **Tools** page. This page allows you to change your login name and password.

**Figure 5-6 User Management Page**

Table 5-4 describes the **User Management** page options.

**Table 5-4 User Management Field Descriptions**

Field	Definition/Definition
User Name	<i>Admin</i> is your default user name. You can enter your new user name here.
Password	<i>Admin</i> is your default password. You can enter your new password here.  Note: If you forget your password, you can press and hold the reset to factory default button for 10 seconds (or more). The RG will reset to its factory default configuration and all custom configuration will be lost.
Confirmed Password	Enter your new password here again to confirm.
Idle Timeout	The default is 30 minutes. You will need to log back onto the RG after your session has been inactive for 30 minutes. You can change the timeout here.
<b>End of Table 5-4</b>	

## 5.6 Update Gateway Page

Figure 5-7 shows the **Update Gateway** page, which is accessed by clicking the **Update Gateway** link at the left of the **Tools** page. This page allows you to update the RG's firmware, voice provision file, and/or configurations files.

**Figure 5-7 Update Gateway Page**

TEXAS INSTRUMENTS	HOME	SETUP	ADVANCED	WIRELESS	<b>TOOLS</b>	STATUS	HELP
System Commands	<b>Update Gateway</b>						
Remote Log - Router	To update your gateway firmware, choose an updated firmware image or configuration file in "Select a File", and then click the Update Gateway button. Additionally, you may download your configuration file from the system by clicking Get Configuration.						
Remote Log - Voice							
User Management							
<b>Update Gateway</b>	Select a File: <input type="text"/> <input type="button" value="Browse..."/>						
Ping Test	(Max file size 3.5 MB)						
Modem Test	Firmware Image can be the combined single image with or without digital signature.						
Log Out	<input type="button" value="Update Gateway"/>						
	The system will be restarted automatically, after the Filesystem image is successfully updated. You will need to reconnect again to configure your setup.						
	<input type="button" value="Get Configuration"/>						
	The system will give the configuration file only if it was earlier saved by pressing "SaveAll" in System Command Menu.						
	Status: None						

Use [Procedure 5-2](#) to upload configuration files and firmware for your RG.

### Procedure 5-2 Update Gateway Firmware

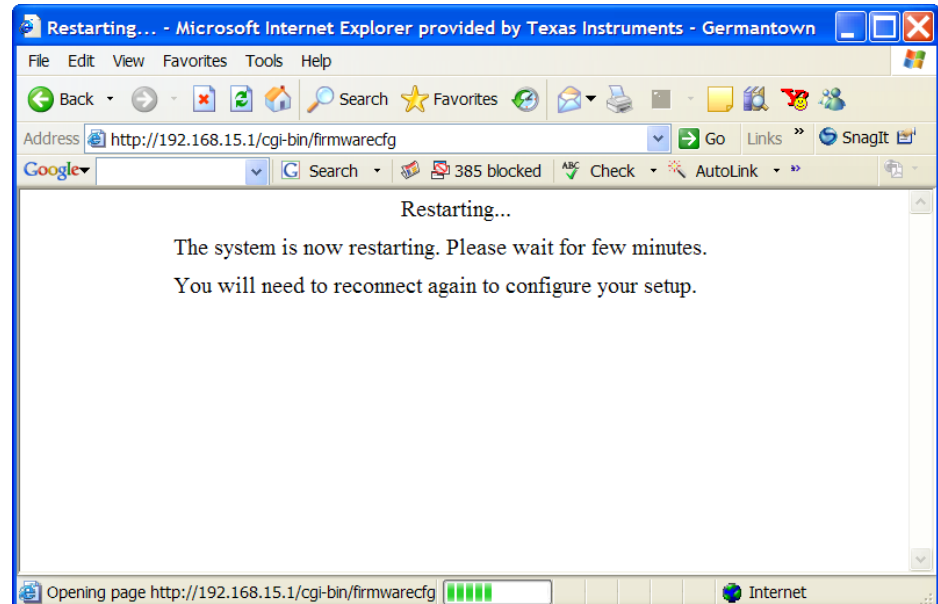
#### Step – Action

- 1 Upload firmware:** Click **Browse** and select the firmware image to upload.
  - For RG NSP version 3.5 and before, you need to upload two files: kernel and filesystem.
  - For RG NSP version 3.5.1 onwards, the two files are combined into one single image and you only need to upload this one file. The file name should look something like this: *nsp.ar7vw.firmware.upgrade.img*. The file for web upload should have "upgrade" in the name. The file without "upgrade" in the name is for upload using the serial connection.

**Note**—The file size should not exceed what is specified for the platform on this page.

- 2 Click Update Gateway.**

The status of the uploading appears at the bottom of the page. When the upload is finished, the RG reboots and you are prompted to log in again.

**Figure 5-8 Update Gateway - Restarting Page**

**Note**—If you are loading multiple files, it is recommended that you upload the firmware image at last as the system reboots after loading firmware image.

- 3 At the login prompt, enter your **Username** and **Password** to log back in.
- 4 If you want to make sure the firmware is properly upgraded, go to **Status /Product Information** and check on the Gateway version information on the **Product Information** page (Chapter 6 “[Product Information Page](#)” on page 6-12).
- 5 **Upload configuration file:** You can use the same procedure to update the configuration file (*config.bin*).
- 6 **Upload voice provisioning file.** Local provisioning is supported in this release. You can also use the same procedure to update the voice provisioning file (e.g., *nsp370\_voice\_sip.xml*).
  - This feature is only available for RG NSP version 3.7.0 onwards.
  - The profile should start with `<provision>` (`<pro` is the magic number that is used to identify the file).
  - The profile should contain the `<reconfig/>` option.
  - The body of the profile should resemble with what is in the default configuration file. The values can be changed as needed. An example is given below:

```
<provision>
  <options>
    <reconfig/>
  </options>
  <settings>
<VOICE_CONFIG>
```

```
...  
</VOICE_CONFIG>  
</settings>  
</provision>
```

- For more information on Voice Provisioning, go to 3.22 [“Voice Provision”](#) on page 3-86.
- 7 You can download to your hard drive a copy of the configuration file (*config.bin*) that has been saved to the RG flash. To do so, click **Get Configuration** and follow the prompt.
  - 8 You can also upload a saved configuration file (*config.bin*) back to the RG. To do so, click **Browse** and select the file, then click **Update Gateway**.
- Note**—For easy viewing and modification, you can decompress the *config.bin* file into a *config.xml* file using the **mkconfig** utility in the build environment. You will need to convert it back to the *config.bin* file format (using the **mkconfig** utility) for uploading.



## 5.7 Ping Test Page

Once you have your RG configured, it is a good idea to make sure you can ping the network. [Figure 5-7](#) shows the default **Ping Test** page, which is accessed by clicking the **Ping Test** link from the left of the **Tools** page. If you can ping an IP on the WAN side successfully, you should be able to surf the Internet.

**Figure 5-9 Ping Test Page**

Use [Figure 5-9](#) as a reference and follow [Procedure 5-3](#) to perform a ping test.

### Procedure 5-3 Perform a Ping Test

#### Step – Action

- 1 Click **Ping Test** from the **Tools** menu to access the **Ping Test** page.
- 2 Change or leave the default settings of the following fields:
  - Enter the IP Address to Ping
  - Packet Size
  - Number of Echo Requests
- 3 Click **Test**.

The ping results are displayed in the box on the page. If the ping test was successful, it means that the TCP/IP protocol is up and running. If the Ping test failed, you should restart the RG.

#### End of Procedure 5-3

Table 5-5 describes the **Ping Test** page options.

**Table 5-5 Ping Test Field Descriptions**

Field	Definition/Definition
Enter IP Address to Ping	Enter the WAN-side IP address that you want to ping. The default is set to the default IP address of your RG (192.168.1.1).
Packet Size	You can define the packet size of the ping test. The default is 64 bytes.
Number of Echo Requests	You can define how many times the IP address will be pinged. The default is 3 times.
<b>End of Table 5-5</b>	

## 5.8 Modem Test Page

The **Modem Test** page is used to check the connectivity to the WAN. This test may take a few seconds to complete. Before running this test, make sure you have at least one WAN connection configured and have a valid DSL link. If the DSL link is not connected, the test will fail. Also make sure the DSLAM supports this feature. Not all DSLAMs have F4 and F5 support. F4/F5 cells are used for operation, administration, and maintenance (OAM) on ATM level. They are used for two main purposes:

- Fault management (detection and notification)
- Loopback testing and link integrity

The ATM OAM is divided into several levels:

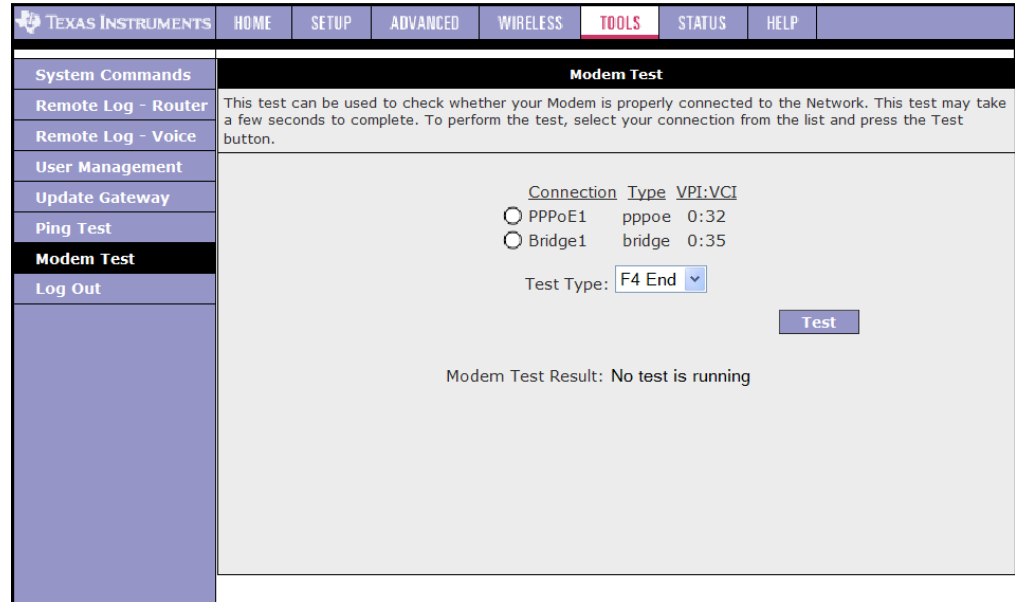
- F4: VP level. OAM information flows between network elements (NEs) used within virtual paths to report an unavailable path or a virtual path (VP) that cannot be guaranteed. Segment flows are processed, as well as end-to-end flows that terminate in the management processor.
- F5: VC level. OAM information flows between network elements (NEs) used within virtual connections to report degraded virtual channel (VC) performance such as late arriving cells, lost cells, and cell insertion problems. Segment flows are processed, as well as end-to-end flows that terminate in the management processor.

Both F4 and F5 flows can be configured as one of the test types:

- Segment: This test verifies that ATM continuity exists between the virtual channel link segment from the RG to the DSL provider network (typically this is a DSLAM at the DSL provider site).
- End-to-End: This test verifies ATM connectivity of the virtual channel link with the ATM endpoint, such as a remote broadband access router located at the DSL provider or ISP site.

Figure 5-10 shows the **Modem Test** page with two WAN connections (PPPoE1 and Bridge1) pre-configured. The **Modem Test** page is accessed by clicking the **Modem Test** link at the left of the **Tools** page.

**Figure 5-10 Modem Test Page**



Use Figure 5-10 as a reference and follow Procedure 5-4 to perform a connectivity test.

**Procedure 5-4 Perform a Connectivity Test**

**Step – Action**

- 1 Click **Modem Test** at the **Tools** main page to access the **Modem Test** page.
- 2 Select the **Connection** you want to test and the **Test Type**.
- 3 Click **Test**.

The modem test results are displayed on the page.

**End of Procedure 5-4**

Table 5-6 describes the **Modem Test** page options.

**Table 5-6 Modem Test Field Descriptions**

Field	Definition/Definition
Connection	Select the WAN connection on which you want to run the modem test.  Note: You will not be able to perform a modem test without any WAN connections configured.
Type	The type of the WAN connection.

**Table 5-6 Modem Test Field Descriptions**

Field	Definition/Definition
VPI/VCI	Virtual path identifier/virtual channel identifier.
Test Type	There are four test types: <ul style="list-style-type: none"><li>• <b>F4 End:</b> F4 end to end.</li><li>• <b>F4 Seg:</b> F4 segment.</li><li>• <b>F5 End:</b> F5 end to end.</li><li>• <b>F5 Seg:</b> F5 segment.</li></ul>
<b>End of Table 5-6</b>	

## 5.9 Hidden Pages

There are two hidden pages in the **Tools** tab:

- Gateway System Information
- Remote Log Settings



**Note**—The hidden pages are to be used by ODMs/OEMs for development and debugging purposes only. Do NOT distribute this section to the end user.

### 5.9.1 Gateway System Information Page

You can access the **Gateway System Information** page (Figure 5-11) by replacing the pagename in the URL with “*pagename=dump\_debug*” or by typing in the following address:

```
http://192.168.1.1/cgi-bin/webcm?getpage=..%2Fhtml%2Fdefs%2Fstyle5/  
menus%2Fmenu.html&var:style=style5&var:main=menu&var:pagename  
=dump_debug&var:pagetitle=Home&var:menu=tools&var:menutitle=T  
ools
```

Note that *192.168.1.1* represents the default management address of the RG and it may be different depending on the configuration.

This page allows you to view the outputs of the following Linux commands on the GUI:

```
ps (processes running on the unit)  
route -n (routing table)  
arp -a (arp table)  
iptables -t nat -L -vn (NAT rules)  
iptables -t filter -L -vn (Firewall FILTER table rules)
```

In Figure 5-11, the command outputs are broken down by the commands for your easy viewing.

Figure 5-11 Gateway System Information Page

**Gateway System Information**

```

PID Uid VmSize Stat Command
1 root 1288 S init
2 root S [keventd]
3 root S [ksoftirqd_CPU0]
4 root S [kswapd]
5 root S [bdflush]
6 root S [kupdated]
7 root S [mtdblockd]
30 root 2840 S /usr/bin/cm_pc
32 root 1288 S init
33 root 1204 S /usr/sbin/tlhttpd -d /usr/www -u root -p 80 -c /cgi-b
34 root 3588 S /usr/bin/cm_logic -m /dev/tidfg -c /etc/config.xml
55 root 608 S /usr/bin/cm_klogd /dev/klog
56 root 700 S /sbin/dproxy -c /etc/resolv.conf -d
64 root 1668 S /usr/sbin/snmpd
65 root 1292 S /bin/sh -c /etc/voice_start
69 root 1292 S /bin/sh -c /etc/voice_start
173 root 6428 S /usr/sbin/ggsip
182 root 684 S /usr/sbin/udhcpd /var/tmp/udhcpd.conf
222 root 1736 R webcm
223 root 1204 S /usr/sbin/tlhttpd -d /usr/www -u root -p 80 -c /cgi-b
225 root 1288 R /bin/ps aux

```

Kernel IP routing table

```

Destination Gateway Genmask Flags Metric Ref Use Iface
192.168.1.0 0.0.0.0 255.255.255.0 U 0 0 0 br0
239.0.0.0 0.0.0.0 255.0.0.0 U 1 0 0 br0

```

Address HWtype HWaddress Flags Mask Iface

```

192.168.1.2 ether 00:10:60:24:92:27 C br0
Chain PREROUTING (policy ACCEPT 1255 packets, 130K bytes)
pkts bytes target prot opt in out source destination
Chain POSTROUTING (policy ACCEPT 4 packets, 254 bytes)
pkts bytes target prot opt in out source destination
Chain OUTPUT (policy ACCEPT 4 packets, 254 bytes)
pkts bytes target prot opt in out source destination
Chain INPUT (policy ACCEPT 3716 packets, 257K bytes)
pkts bytes target prot opt in out source destination
91 7237 CFG tcp -- * * 192.168.1.2 0.0.0.0/0 tcp dpt:80 Records Packet's Source Interface
Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target prot opt in out source destination
Chain OUTPUT (policy ACCEPT 1643 packets, 371K bytes)
pkts bytes target prot opt in out source destination

```

**Refresh**

## 5.9.2 Remote Log Settings Page

The **Remote Log Settings** page (Figure 5-12) is accessed by replacing the pagename in the URL with “pagename=rlog\_debug” or typing in the following address:

```

http://192.168.1.1/cgi-bin/webcm?getpage=..%2Fhtml%2Fdefs%2Fstyle5%2
Fmenus%2Fmenu.html&var:style=style5&var:main=menu&var:menu=tools&
var:menutitle=Tools&var:pagename=rlog_debug&var:pagetitle=Remote%2
0Log

```

This page provides similar function as the **Remote Log** page (Figure 5-4 on page 5-4); however, it gives you more customizing options. The configuration manager is logically broken down into different components for the purpose of logging. This page allows you to define log level by the following components/modules:

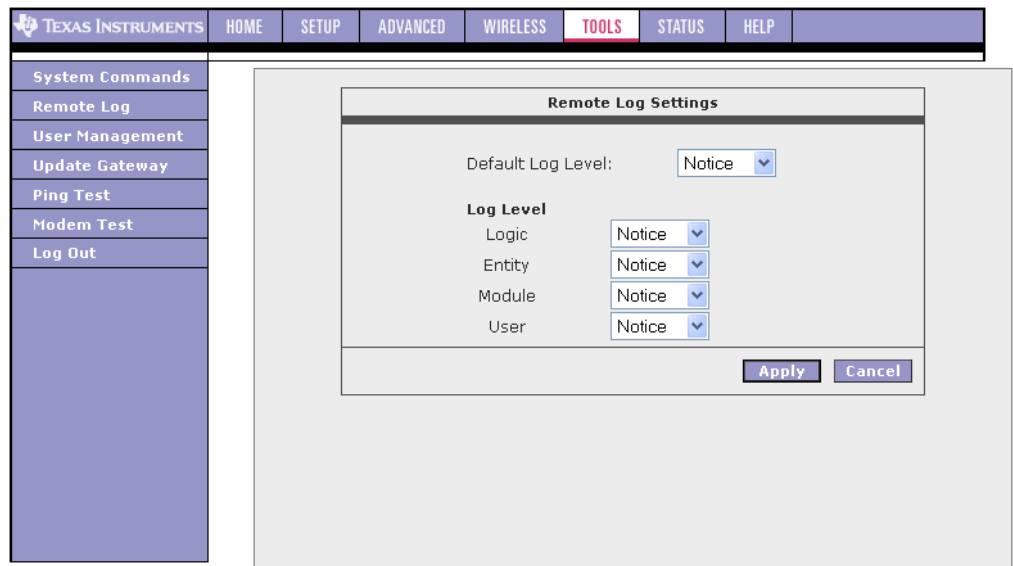
- **Default Log Level:** By selecting a severity level in this field, the same selection is made (not populated) for all the following four fields: Logic, Entry, Module, and User. You can modify the severity level in each individual field and it overrides selection in the default log level field.
- **Logic:** This field allows you to define log severity level for the configuration manager core logic facility.

- **Entity:** This field allows you to define log severity level for the entity facility.
- **Module:** This field allows you to define log severity level for the module facility.
- **User:** By selecting this field, all logical entities can print messages visible to the user via the status system log page.

The facility is used to specify what type of program or component is logging the message. This enables the configuration to specify that messages from different facilities will be handled differently.

Note, there are seven log levels for each field (in the order of the serverity): **Panic, Alert, Critical, Error, Warning, Notice, Information, and Debug.** For a further description of each log level, go to [Table 5-2](#) on page 5-5. When you select one severity level, the log information for this severity level and up (meaning more severe) are generated. Keep in mind the log level selections in the drop-down menu may not appear in the same order as in the table.

**Figure 5-12 Remote Log Settings Page**





# Status

---

---

---

The **Status** chapter discusses:

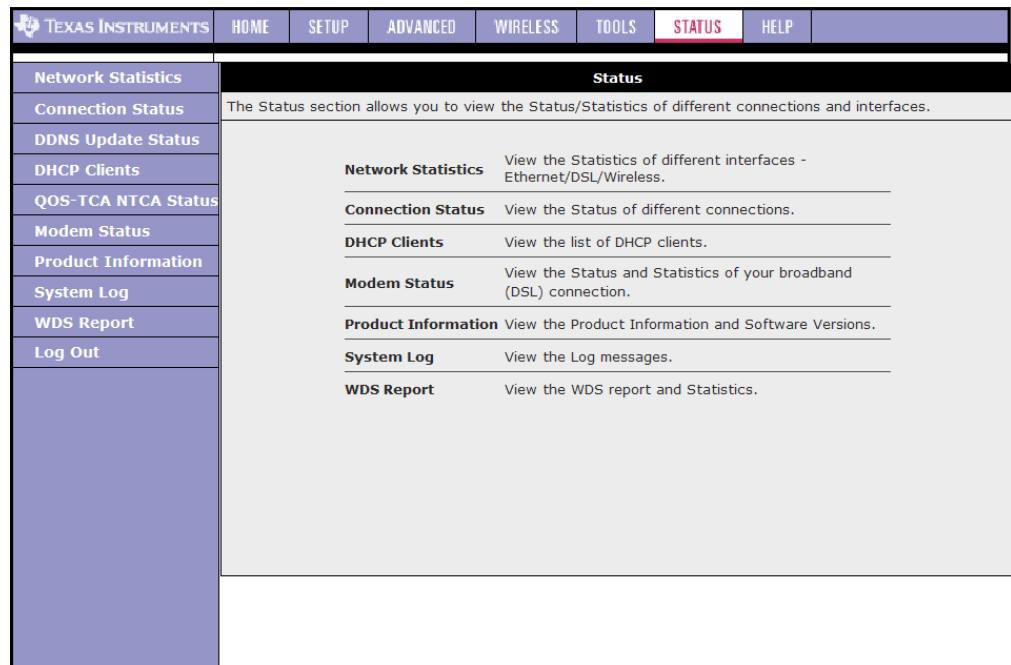
- ["Status Main Page"](#) on page 6-2
- ["Network Statistics Page"](#) on page 6-3
- ["Connection Status Page"](#) on page 6-6
- ["DDNS Update Status"](#) on page 6-7
- ["DHCP Clients Page"](#) on page 6-9
- ["QoS - TCA NTCA Status Page"](#) on page 6-10
- ["Modem Status Page"](#) on page 6-11
- ["Product Information Page"](#) on page 6-12
- ["System Log Page"](#) on page 6-13
- ["WDS Report"](#) on page 6-14

## 6.1 Status Main Page

Figure 6-1 shows the **Status** main page, which is accessed by clicking the **Status** tab from the top of the page. This page provides access to the following status pages:

- Network Statistics
- Connection Status
- DDNS Update Status
- DHCP Clients
- Modem Status
- Product Information
- System Log

**Figure 6-1** Status Main Page



## 6.2 Network Statistics Page

You can access the **Network Statistics** page by clicking the **Network Statistics** link from the **Status** main page. Click to view the statistics of the following four interfaces:

- Ethernet (Figure 6-2)
- USB (Figure 6-3)
- DSL (Figure 6-4)
- Wireless (Figure 4-14 on page 4-20)

**Figure 6-2 Network Statistics Page - Ethernet**

The screenshot shows the 'Network Statistics' page for the Ethernet interface. The page has a navigation bar at the top with tabs: TEXAS INSTRUMENTS, HOME, SETUP, ADVANCED, WIRELESS, TOOLS, STATUS (highlighted), and HELP. On the left is a sidebar menu with items: Network Statistics, Connection Status, DDNS Update Status, DHCP Clients, QOS-TCA NTCA Status, Modem Status, Product Information, System Log, WDS Report, and Log Out. The main content area is titled 'Network Statistics' and contains a sub-header 'Choose an interface to view your network statistics:' with radio buttons for Ethernet (selected), USB, DSL, and Wireless. Below this, statistics are listed under 'Transmit' and 'Receive' categories.

Transmit	
Good Tx Frames	5229
Good Tx Broadcast Frames	4
Good Tx Multicast Frames	0
Tx Total Bytes	3133206
Collisions	0
Error Frames	0
Carrier Sense Errors	0

Receive	
Good Rx Frames	6072
Good Rx Broadcast Frames	468
Good Rx Multicast Frames	8
Rx Total Bytes	559185
CRC Errors	0
Undersized Frames	0
Overruns	0

Refresh

**Figure 6-3 Network Statistics Page - USB**

TEXAS INSTRUMENTS   HOME   SETUP   ADVANCED   WIRELESS   TOOLS   <b>STATUS</b>   HELP	
<b>Network Statistics</b>	<b>Network Statistics</b>
Connection Status	Choose an interface to view your network statistics:
DDNS Update Status	<input type="radio"/> Ethernet <input checked="" type="radio"/> USB <input type="radio"/> DSL <input type="radio"/> Wireless
DHCP Clients	Transmit
QOS-TCA NTCA Status	Good Tx Frames 0
Modem Status	Good Tx Broadcast Frames 0
Product Information	Good Tx Multicast Frames 0
System Log	Tx Total Bytes 0
WDS Report	Receive
Log Out	Good Rx Frames 0
	Good Rx Broadcast Frames 0
	Good Rx Multicast Frames 0
	Rx Total Bytes 0
	<a href="#">Refresh</a>

**Figure 6-4 Network Statistics Page - DSL**

TEXAS INSTRUMENTS   HOME   SETUP   ADVANCED   WIRELESS   TOOLS   <b>STATUS</b>   HELP	
<b>Network Statistics</b>	<b>Network Statistics</b>
Connection Status	Choose an interface to view your network statistics:
DDNS Update Status	<input type="radio"/> Ethernet <input type="radio"/> USB <input checked="" type="radio"/> DSL <input type="radio"/> Wireless
DHCP Clients	Transmit
QOS-TCA NTCA Status	Tx PDUs 0
Modem Status	Tx Total Bytes 0
Product Information	Tx Total Error Counts 0
System Log	Receive
WDS Report	Rx PDUs 0
Log Out	Rx Total Bytes 0
	Rx Total Error Counts 0
	<a href="#">Refresh</a>

**Figure 6-5 Network Statistics Page - WLAN**

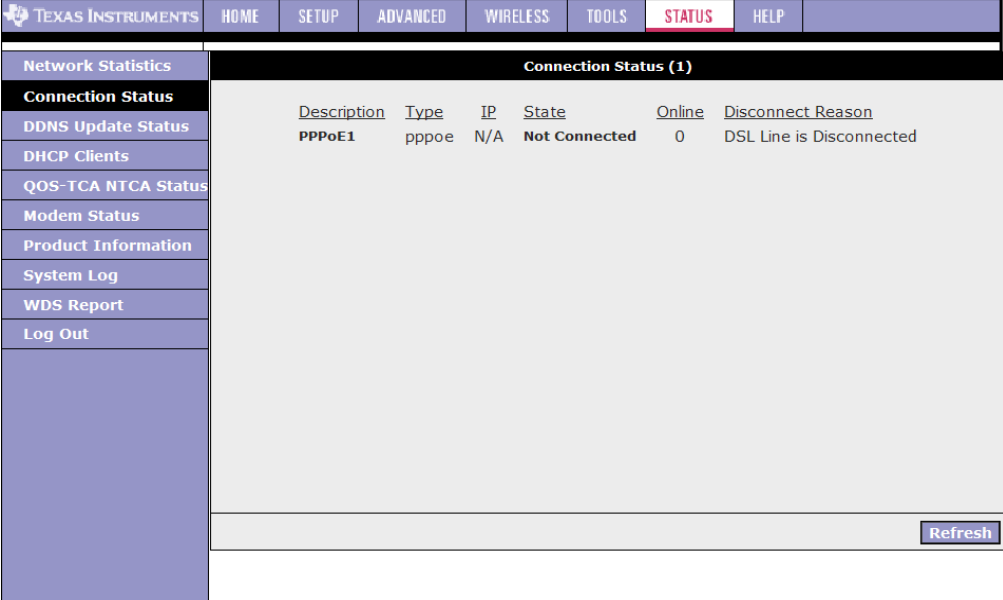
The screenshot displays the 'Network Statistics' page for a WLAN interface. The navigation bar at the top includes 'TEXAS INSTRUMENTS', 'HOME', 'SETUP', 'ADVANCED', 'WIRELESS', 'TOOLS', 'STATUS' (highlighted), and 'HELP'. The left sidebar contains the following menu items: 'Network Statistics', 'Connection Status', 'DDNS Update Status', 'DHCP Clients', 'QOS-TCA NTCA Status', 'Modem Status', 'Product Information', 'System Log', 'WDS Report', and 'Log Out'. The main content area is titled 'Network Statistics' and prompts the user to 'Choose an interface to view your network statistics:'. Four radio buttons are provided: 'Ethernet', 'USB', 'DSL', and 'Wireless' (which is selected). Below this, the statistics are divided into 'Transmit' and 'Receive' sections. The 'Transmit' section shows: MPDUs (7), MSDUs (76), Multicast MSDUs (0), Failed MSDUs (69), and Retry MSDUs (69). The 'Receive' section shows: MPDUs (0), MSDUs (0), Multicast MSDUs (0), FCS Error MPDUs (11), MIC Failure MSDUs (0), and Decrypt Error MPDUs (0). A 'Refresh' button is located at the bottom right of the statistics area.

Network Statistics	
Choose an interface to view your network statistics:	
<input type="radio"/> Ethernet <input type="radio"/> USB <input type="radio"/> DSL <input checked="" type="radio"/> Wireless	
Transmit	
MPDUs	7
MSDUs	76
Multicast MSDUs	0
Failed MSDUs	69
Retry MSDUs	69
Receive	
MPDUs	0
MSDUs	0
Multicast MSDUs	0
FCS Error MPDUs	11
MIC Failure MSDUs	0
Decrypt Error MPDUs	0

## 6.3 Connection Status Page

You can view the status of different connections from the **Connection Status** page (Figure 6-6). To access, click the **Connection Status** link from the **Status** main page.

**Figure 6-6 Connection Status Page**



The screenshot shows a web interface with a navigation menu at the top and a sidebar on the left. The main content area displays the 'Connection Status (1)' page. A table lists connection details for 'PPPoE1', which is currently 'Not Connected'. A 'Refresh' button is located at the bottom right of the table area.

Connection Status (1)						
Description	Type	IP	State	Online	Disconnect Reason	
PPPoE1	pppoe	N/A	Not Connected	0	DSL Line is Disconnected	

## 6.4 DDNS Update Status

You can view the DDNS update status of your WAN connection from the **DDNS Status** page (Figure 6-8). To access, click the **DDNS Update Status** link from the **Status** main page.

**Figure 6-7 DDNS Status Page (DDNS Client Disabled)**

The screenshot shows the DDNS Update Status page. The top navigation bar includes links for TEXAS INSTRUMENTS, HOME, SETUP, ADVANCED, WIRELESS, TOOLS, STATUS (highlighted), and HELP. A left sidebar contains a menu with the following items: Network Statistics, Connection Status, DDNS Update Status (highlighted), DHCP Clients, QOS-TCA NTCA Status, Modem Status, Product Information, System Log, WDS Report, and Log Out. The main content area is titled "DDNS Update Status" and displays the following information: "Connection: PPPoE1" (with a dropdown arrow), "DDNS Server: DynDNS" (with a dropdown arrow), and "DDNS Client is disabled". A "Refresh" button is located at the bottom right of the main content area.

As you can see from this page, the DDNS client is disabled by default for your RG. To enable the DDNS client feature, refer to [Procedure 3-11](#). When DDNS client is enabled, the DDNS client updates every time the RG gets a new IP address. The **DDNS Status** page (Figure 6-8) provides you the DDNS update status of your RG.

**Figure 6-8 DDNS Status Page (DDNS Client Enabled)**

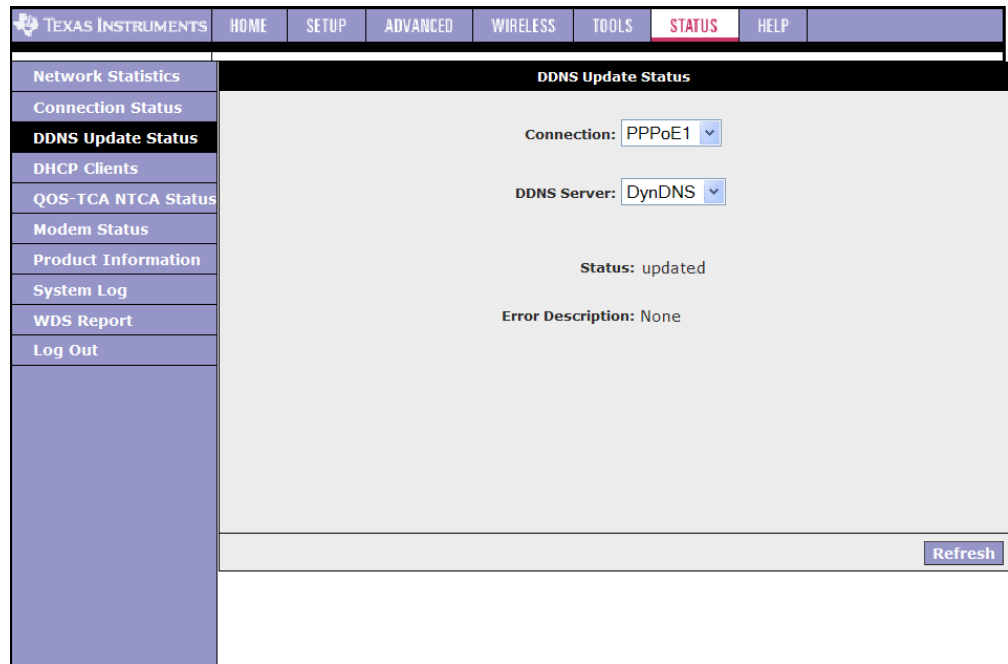


Table 6-1 describes the DDNS Status page fields.

**Table 6-1 DDNS Status Field Descriptions**

Field	Definition/ Description
Connection	This field defaults to your RG's WAN connection over which your RG will be accessed.
DDNS Server	This is where you select the server from different DDNS service providers. Only <b>DynDNS</b> and <b>TZO</b> are supported by your RG at this time.
Status	The status could be one of the following: <ul style="list-style-type: none"> <li>• Updated: The IP address of the client has been changed and an update has been sent to the DDNS server.</li> <li>• No change: The IP address of the client has not been changed.</li> <li>• Error: There is an error with the DDNS update.</li> </ul>
Error Description	If the DDNS update status is <i>Error</i> , this field gives a description of the error.
<b>End of Table 6-1</b>	



## 6.5 DHCP Clients Page

If you have enabled the DHCP server, you can view a list of the DHCP clients from the **DHCP Clients** page (Figure 6-9). From the **Status** main page, click the **DHCP Clients** link, select the **LAN Group**, and the following information of the DHCP LAN clients is displayed:

- MAC Address
- IP Address
- Host Name
- Lease Time

Figure 6-9 DHCP Clients Page

DHCP Clients (1)				
Select LAN: LAN group 1				
MAC Address	IP Address	Host Name	Lease Time	
00:11:43:75:dc:42	192.168.1.5	GTD63C871	0 days 0:51:26	

## 6.6 QoS - TCA NTCA Status Page

The QoS TCA NTCA Status page (Figure 6-10) is accessed by clicking the QoS-TCA NTCA Status link from the Status main page.

Figure 6-10 QoS TCA NTCA Status Page

The screenshot shows a web interface for Texas Instruments. At the top, there is a navigation bar with tabs: TEXAS INSTRUMENTS, HOME, SETUP, ADVANCED, WIRELESS, TOOLS, STATUS (highlighted), and HELP. On the left side, there is a vertical sidebar menu with the following items: Network Statistics, Connection Status, DDNS Update Status, DHCP Clients, QoS-TCA NTCA Status (highlighted), Modem Status, Product Information, System Log, WDS Report, and Log Out. The main content area is titled "QOS-TCA NTCA STATUS" and contains the following information:

- QOS FrameWork** : Enabled
- Scheduling Algorithm** : Strict Round-Robin
- NQM Received Statistics**
  - Cos1 Pkts received : 0
  - Cos2 Pkts received : 0
  - Cos3 Pkts received : 0
  - Cos4 Pkts received : 0
  - Cos5 Pkts received : 0
  - Cos6 Pkts received : 38355
- NQM Dropped Statistics**
  - Cos1 Pkts received : 0
  - Cos2 Pkts received : 0
  - Cos3 Pkts received : 0
  - Cos4 Pkts received : 0
  - Cos5 Pkts received : 0
  - Cos6 Pkts received : 0
- NQM Congestion Control**
  - Cos1 Queue : Empty
  - Cos2 Queue : Empty
  - Cos3 Queue : Empty
  - Cos4 Queue : Empty
  - Cos5 Queue : Empty
  - Cos6 Queue : Empty
- Translation Statistics**
  - Packets Remarked : 1544
  - Packets Unchanged : 0
  - Non-Ip Packets Marked : 14
  - Unclassified Ip Packets Marked : 4
  - Unclassified Non-Ip Packets Marked : 6
  - Unclassified Layer2 Packets : 0
- Congestion State : Not Congested
- Classification Statistics**
  - Classification Errors : 0
  - UnClassified Packets : 14 Fragmented Packets = 0

## 6.7 Modem Status Page

The **Modem Status** page (Figure 6-11) is accessed by clicking the **Modem Status** link from the **Status** main page.

**Figure 6-11 Modem Status**

Modem Status	
Modem Status	
Connection Status	Disconnected
Us Rate (Kbps)	0
Ds Rate (Kbps)	0
US Margin	0
DS Margin	0
Trained Modulation	NO_MODE
LOS Errors	0
DS Line Attenuation	0
US Line Attenuation	0
Peak Cell Rate	0 cells per sec
CRC Rx Fast	0
CRC Tx Fast	0
CRC Rx Interleaved	0
CRC Tx Interleaved	0
Path Mode	Fast Path
DSL Statistics	
Near End F4 Loop Back Count	0
Near End F5 Loop Back Count	0

## 6.8 Product Information Page

You can display the hardware and software information for your RG by clicking the **Product Information** link on the **Status** main page. [Figure 6-12](#) shows the product information.

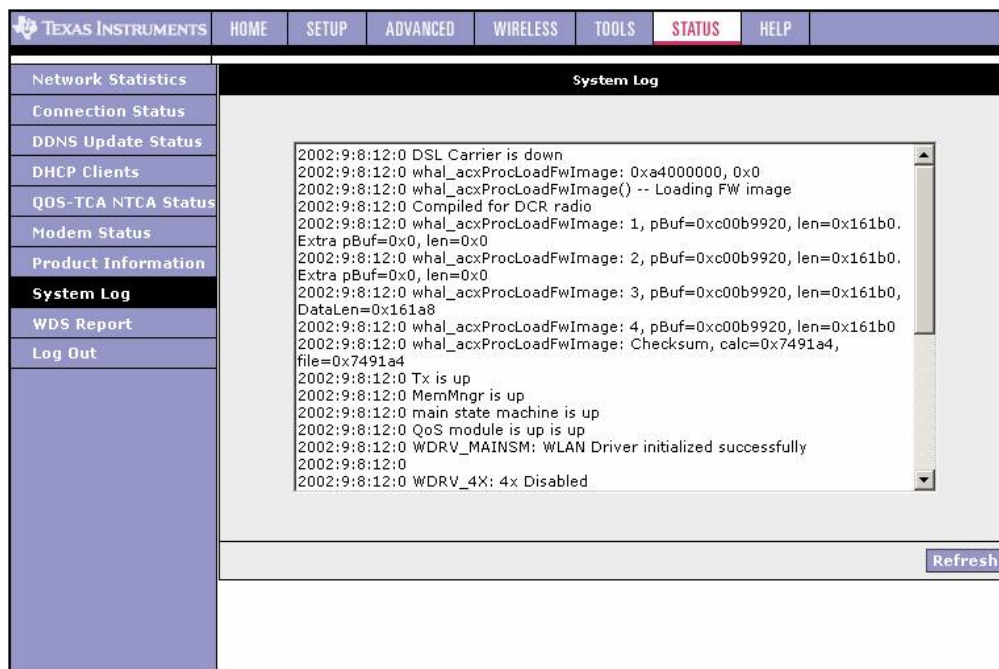
**Figure 6-12 Product Information Page**

TEXAS INSTRUMENTS		HOME	SETUP	ADVANCED	WIRELESS	TOOLS	STATUS	HELP	
Network Statistics	<b>Product Information</b>								
Connection Status	<b>Product Information</b>								
DDNS Update Status	Model Number	AR7WRD							
DHCP Clients	HW Revision	Unknown							
QOS-TCA NTCA Status	Serial Number	none							
Modem Status	USB PID	0x6060							
<b>Product Information</b>	USB VID	0x0451							
System Log	Ethernet MAC	02:03:04:05:06:07							
WDS Report	DSL Default MAC	01:02:03:04:05:06							
Log Out	DSL MAC0	10:11:12:13:14:15							
	DSL MAC1	11:12:13:14:15:16							
	DSL MAC2	13:14:15:16:15:17							
	USB MAC	00:E0:A6:66:41:EB							
	USB Host MAC	00:E0:A6:66:41:E1							
	AP MAC0	00:50:f1:12:12:10							
	<b>Software Versions</b>								
	Gateway	3.7.1							
	ATM Driver	5.02.01.02							
	DSL HAL	5.02.02.00							
	DSL Datapump	5.02.02.01 Annex A							
	SAR HAL	01.07.2b							
	PDSP Firmware	0.52							
	Wireless Firmware	3.4.0.41							
	Wireless APDK	6.4.4.27							
	Boot Loader	1.3.7.15							

## 6.9 System Log Page

You can display the system log for your RG by clicking the **System Log** link from the **Status** main page. The **System Log** page (Figure 6-13) allows you to view all logged information. Depending upon the severity level, the logged information generates log reports to a remote host (if remote logging is enabled). The system log maintained by the NSP is stored in RAM at run-time. It is a circular file with a maximum size that will overwrite itself (up to 32 logs can be displayed on this page). System log messages are not kept between reboots of the RG.

**Figure 6-13 System Log Page**

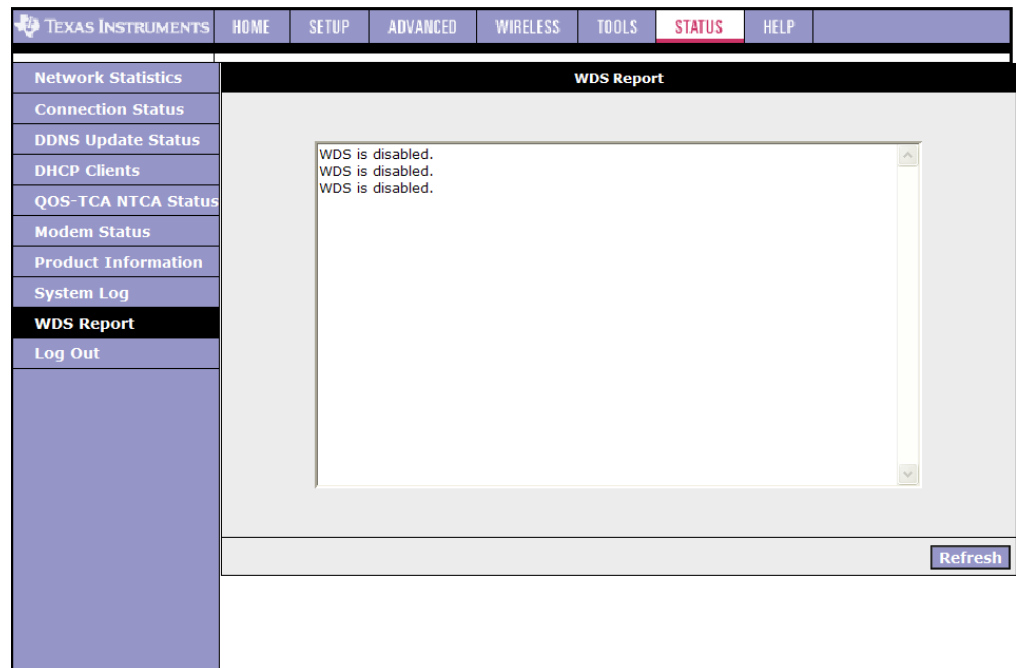


## 6.10 WDS Report

You can view the WDS report for your RG (AP) by clicking the **WDS Report** link from the **Status** main page. The **WDS Report** page (Figure 6-14) allows you to view the following WDS-related wireless activities:

- WDS configuration and states
- WDS management statistics
- WDS database

**Figure 6-14 WDS Report**



# Acronyms

---

---

---

<b>Term</b>	<b>Meaning</b>
<b>ACS</b>	auto configuration server
<b>AES - CCMP</b>	advanced encryption standard - counter mode CBC-MAC protocol
<b>AF</b>	assured forwarding
<b>ALG</b>	application level gateway
<b>AP</b>	access point
<b>BE</b>	best effort
<b>BSS</b>	basic service set
<b>CBR</b>	constant bit rate
<b>CCK</b>	complementary code key
<b>CDVT</b>	cell delay variation tolerance
<b>CID</b>	caller ID
<b>CLI</b>	common language infrastructure
<b>CLIP</b>	classical IP over ATM
<b>CoS</b>	class of service
<b>CTS</b>	clear to send
<b>DDNS</b>	Dynamic DNS, see DNS
<b>DHCP</b>	dynamic host configuration protocol
<b>DMZ</b>	demilitarized zone
<b>DDNS</b>	dynamic DNS, see DNS
<b>DNS</b>	domain name server
<b>DSL</b>	digital subscriber line
<b>DST</b>	daylight saving time
<b>DTIM</b>	delivery traffic identification map
<b>EAP-TLS</b>	extensible authentication protocol - transport layer security
<b>EF</b>	expedited forwarding

<b>Term</b>	<b>Meaning</b>
<b>ERP</b>	extended rate phy
<b>FCS</b>	frame check sequence
<b>FTP</b>	file transfer protocol
<b>GDMT</b>	G discrete multi-tone
<b>HTB</b>	hierachical token bucket
<b>ICMP</b>	Internet control message protocol
<b>IDEA</b>	international data encryption algorithm
<b>IEEE</b>	institute of electrical and electronics engineers
<b>IGD</b>	Internet gateway device
<b>IGMP</b>	Internet group management protocol
<b>IP</b>	Internet protocol
<b>LAN</b>	local area network
<b>LED</b>	light emitting diode
<b>LLC</b>	logical link control
<b>MAC</b>	medium access control
<b>MBS</b>	maximum burst size
<b>MIB</b>	management information base
<b>MMODE</b>	multi-mode
<b>MPDU</b>	Mac protocol data unit
<b>MSDU</b>	MAC service data unit
<b>MTA</b>	media terminal adapter
<b>MTU</b>	maximum transmit unit
<b>NAPT</b>	network address port translation
<b>NAT</b>	network address translation
<b>NIC</b>	network interface card
<b>NSP</b>	network support package
<b>OFDM</b>	orthogonal frequency division multiplexing
<b>PBCC</b>	packet binary convolution coding
<b>PCR</b>	peak cell rate
<b>PPP</b>	point-to-point
<b>PPPoA</b>	PPP over ATM, see PPP
<b>PPPoE</b>	PPP over ethernet, see PPP
<b>PR</b>	policy routing
<b>PRIOWRR</b>	priority based weighted round robin
<b>PSK</b>	pre-shared key
<b>PVC</b>	permanent virtual circuit
<b>QoS</b>	quality of service



---

<b>Term</b>	<b>Meaning</b>
<b>RADIUS</b>	remote authentication dial-in user service
<b>RC4</b>	rivest cipher 4
<b>RG</b>	residential gateway
<b>RIP</b>	routing information protocol
<b>RTS</b>	request to send
<b>SCR</b>	sustained cell rate
<b>SNMP</b>	simple network management protocol
<b>SNTP</b>	simple network timing protocol
<b>SPI</b>	stateful packet inspection
<b>SS IE</b>	supported rates information element
<b>SSH</b>	secure shell
<b>SSID</b>	service set identifier
<b>TCA</b>	traffic conditioning agreement
<b>TCP</b>	transmission control protocol
<b>TFTP</b>	trivial file transfer protocol
<b>TKIP</b>	temporal key integrity protocol
<b>ToS</b>	type of service
<b>UDP</b>	user datagram protocol
<b>UPnP</b>	universal plug and play
<b>USB</b>	universal serial bus
<b>VBR</b>	variable bit rate
<b>VC</b>	virtual circuit
<b>VCI</b>	virtual channel identifier
<b>Vendor OID</b>	vendor object identifier.
<b>VLAN</b>	virtual LAN, see LAN
<b>VPI</b>	virtual path identifier
<b>WAN</b>	wide area network connection
<b>WDS</b>	Wireless distribution system
<b>WEP</b>	wired equivalent privacy
<b>WLAN</b>	wireless LAN, see LAN
<b>WPA</b>	Wi-Fi protected access
<b>WRR</b>	weighted round robin

