



UTT Routers/Firewalls Advanced Configuration Guide

Version: ReOS V10

UTT Technologies Co., Ltd.

<http://www.uttglobal.com>

Copyright Notice

Copyright © 2000-2011 UTT Technologies Co., Ltd. All rights reserved.

Information in this document, including URL and other Internet Web site references, is subject to change without further notice.

Unless otherwise noted, the companies, organizations, people and events described in the examples of this document are fictitious, which have no relationship with any real company, organization, people and event.

Complying with all applicable copyright laws is the responsibility of the user. No part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or used for any commercial and profit purposes, without the express prior written permission of UTT Technologies Co., Ltd.

UTT Technologies Co., Ltd. has the patents, patent applications, trademarks, trademark applications, copyrights and other intellectual property rights that are mentioned in this document. You have no license to use these patents, trademarks, copyrights or other intellectual property rights, without the express prior written permission of UTT Technologies Co., Ltd.

艾泰[®] and UTT[®] are the registered trademarks of UTT Technologies Co., Ltd.

NE[®] is the registered trademark of UTT Technologies Co., Ltd.

Unless otherwise announced, the products, trademarks and patents of other companies, organizations or people mentioned herein are the properties of their respective owners.

Product Number (PN): 0900-0306-001

Document Number (DN): PR-PMMU-1104.56-PPR-EN-1.0A

FCC Warning

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

- (1) this device may not cause harmful interference, and
- (2) this device must accept any interference received, including interference that may cause undesired operation.

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

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.

If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

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

Table of Contents

About This Manual	1
0.1 Scope	1
0.2 Web UI Style	1
0.3 Documents Conventions	2
0.3.1 Detailed Description of List.....	2
0.3.1.1 Editable List.....	2
0.3.1.2 Read-only List.....	3
0.3.1.3 Sorting Function.....	4
0.3.2 Keyboard Operation.....	5
0.3.3 Other Conventions.....	5
0.3.3.1 Convention for a Page Path.....	5
0.3.3.2 Convention for Clicking a Button.....	5
0.3.3.3 Convention for Selecting an Option.....	5
0.4 Partial Factory Default Settings	6
0.5 Document Organization	6
Chapter 1 Product Overview	14
1.1 Key Features	14
1.2 Main Features	15
1.3 VPN Features	17
1.4 Physical Specification	18
1.5 Detailed Specifications Table	19
Chapter 2 Hardware Installation	23
2.1 Installation Requirements	23
2.2 Installation Procedure	23
2.3 Installation Procedure of UTT 2512	24
2.4 Installation Procedure of U2000	27
Chapter 3 Logging in to the Device	32
3.1 Configuring Your PC	32
3.2 Logging in to the Device	34
3.3 Shortcut Icons	35
Chapter 4 Quick Wizard	37

4.1	Running the Quick Wizard	37
4.2	LAN Settings	38
4.3	Choosing an Internet Connection Type	38
4.4	Internet Connection Settings	40
4.4.1	Notes on Internet Connection Settings.....	40
4.4.2	PPPoE Internet Connection Settings.....	40
4.4.3	Static IP Internet Connection Settings.....	42
4.4.4	DHCP Internet Connection Settings	44
4.5	Reviewing and Saving the Settings	44
4.6	Summary	45
Chapter 5	System Status	46
5.1	System Information	46
5.1.1	System Up Time	46
5.1.2	System Resource	47
5.1.3	System Version.....	48
5.1.4	Port Information	48
5.1.4.1	Port Status	48
5.1.4.2	Interface Rate Chart.....	49
5.2	NAT Statistics	51
5.3	DHCP Statistics	53
5.3.1	DHCP Pool Statistics List	53
5.3.2	DHCP Server Statistics List	55
5.3.3	DHCP Conflict Statistics List	56
5.3.4	DHCP Client Statistics List	57
5.3.5	DHCP Relay Statistics List	58
5.4	Interface Statistics	60
5.5	Routing Table	62
5.6	Session Monitor	65
5.6.1	Session Monitor Settings	65
5.6.2	NAT Session List	67
5.6.3	Examples	68
5.6.3.1	Searching Internet Activities of the LAN User with IP Address 192.168.16.68/24	68
5.6.3.2	Searching the LAN Users Accessing 200.200.200.251	69
5.6.3.3	Searching the LAN Users Using MSN	70
5.6.3.4	Searching Internet Activities of the LAN users Using WAN1 IP address.....	71
5.7	System Log	74

5.7.1	System Log Settings.....	74
5.7.2	Viewing System Logs	75
5.8	Web Log.....	78
5.8.1	Enable Web Log	78
5.8.2	View Web Logs.....	79
5.9	Application Traffic Statistics	80
5.9.1	Global Setup	80
5.9.2	Application Traffic Statistics List	80
5.9.3	User Traffic Statistics List	81
5.10	WAN Traffic Statistics	83
Chapter 6	Basic Setup	84
6.1	LAN Settings	84
6.2	WAN Settings	86
6.2.1	WAN List.....	86
6.2.1.1	Parameter Definitions	86
6.2.1.2	List Function	88
6.2.1.3	How to Dial and Hang up a PPPoE connection	89
6.2.1.4	How to Renew and Release a DHCP Connection	89
6.2.2	WAN Internet Connection Settings	91
6.2.2.1	PPPoE Internet Connection Settings	91
6.2.2.2	Static IP Internet Connection Settings	96
6.2.2.3	DHCP Internet Connection Settings.....	98
6.2.2.4	How to Delete the Internet Connection	99
6.2.2.5	Related Default Routes.....	100
6.3	Load Balancing.....	101
6.3.1	Introduction to Load Balancing and Failover	101
6.3.1.1	Internet Connection Detection Mechanism	101
6.3.1.2	Load Balancing Mode	102
6.3.1.3	Internet Connection Detection Method.....	103
6.3.2	The Operation Principle of Load Balancing	105
6.3.2.1	Allocating Traffic according to Connection Bandwidth	105
6.3.2.2	Two Load Balancing Policies	106
6.3.3	ID Binding	107
6.3.4	Load Balancing Global Settings	108
6.3.4.1	Global Settings - Full Load Balancing	108
6.3.4.2	Global Settings --Partial Load Balancing	109

6.3.5	Detection and Weight Settings	110
6.3.6	Load Balancing List	112
6.3.7	How to Configure Load Balancing	112
6.3.7.1	The Process of Configuring Load Balancing.....	112
6.3.7.2	The Configuration Steps of Connection Detection and Weight	113
6.3.7.3	The Configuration Steps of Load Balancing Global Settings	113
6.3.7.4	The Configuration Steps of ID Binding.....	114
6.3.8	Related Detection Route	114
6.4	DHCP & DNS	115
6.4.1	DHCP Server	115
6.4.2	DHCP Auto Binding	116
6.4.3	DNS Proxy	117
Chapter 7	Advanced Setup.....	119
7.1	Static Route.....	119
7.1.1	Static Route	119
7.1.1.1	Introduction to Static Route.....	119
7.1.1.2	System Reserved Static Routes	119
7.1.1.3	Static Route Settings	121
7.1.1.4	Static Route List.....	123
7.1.1.5	How to Add the Static Routes	123
7.1.2	Static Route Policy Database	125
7.1.2.1	Introduction to Static Route PDB	125
7.1.2.2	Static Route PDB Settings	127
7.1.2.3	How to Add the Static Route PDB Entries.....	128
7.1.2.4	How to Update a System Default Static Route PDB	129
7.2	Policy-Based Routing	131
7.2.1	Policy-Based Routing Settings	131
7.2.2	Enable Policy-Based Routing	133
7.2.3	Policy-Based Routing List.....	133
7.3	DNS Redirection	135
7.3.1	Introduction to DNS Redirection	135
7.3.2	Enable DNS Redirection.....	135
7.3.3	DNS Redirection List	136
7.3.4	DNS Redirection Settings.....	137
7.3.5	How to Configure DNS Redirection.....	138
7.4	Plug and Play	139

7.4.1	Introduction to Plug and Play.....	139
7.4.2	Enable Plug and Play	139
7.5	SNMP	140
7.6	SYSLOG.....	143
7.7	DDNS	145
7.7.1	Introduction to DDNS.....	145
7.7.2	DDNS Service Offered by iplink.com.cn.....	145
7.6.1.1	Apply for a DDNS Account from iplink.com.cn	145
7.7.2.1	DDNS Settings Related to ipink.com.cn.....	147
7.7.3	DDNS Service Offered by 3322.org	148
7.7.3.1	Apply for a DDNS Account from 3322.org.....	148
7.7.3.2	DDNS Settings Related to 3322.org	149
7.7.4	DDNS Verification	150
7.8	Advanced DHCP	152
7.8.1	Introduction to DHCP.....	152
7.8.1.1	Overview.....	152
7.8.1.2	DHCP Operation Process	152
7.8.1.3	DHCP Message types.....	154
7.8.2	Introduction to DHCP Feature of the Device	155
7.8.2.1	Introduction to DHCP Server	156
7.8.2.2	Introduction to DHCP Client.....	158
7.8.2.3	Introduction to DHCP Relay Agent.....	159
7.8.2.4	Introduction to Raw Option	160
7.8.3	DHCP Client	161
7.8.3.1	DHCP Client Settings.....	161
7.8.3.2	DHCP Client List.....	163
7.8.3.3	How to Configure DHCP Client.....	163
7.8.4	DHCP Server	164
7.8.4.1	DHCP Server Global Settings	164
7.8.4.2	DHCP Manual Binding List	165
7.8.4.3	DHCP Manual Binding Settings	166
7.8.4.4	How to Add the DHCP Manual Bindings.....	168
7.8.4.5	DHCP Address Pool List.....	168
7.8.4.6	DHCP Address Pool Settings.....	169
7.8.4.7	How to Add the DHCP Address Pools.....	172
7.8.5	DHCP Relay Agent	173

7.8.5.1	DHCP Relay Agent Settings	174
7.8.5.2	DHCP Relay Agent List.....	175
7.8.5.3	How to Configure DHCP Relay Agent.....	176
7.8.6	Raw Option	177
7.8.6.1	Raw Option Settings	177
7.8.6.2	Raw Option List	178
7.8.6.3	How to Add the DHCP Raw Options	179
7.8.7	Configuration Examples for DHCP	179
7.8.7.1	Configuration Example for the DHCP Server.....	179
7.8.7.2	Configuration Example for the DHCP Client	184
7.8.7.3	Configuration Example for the DHCP Relay Agent	186
7.8.7.4	Configuration Example for the Raw Option.....	187
7.8.7.5	Comprehensive Example for DHCP.....	188
7.9	Switch	196
7.9.1	Port Mirroring	196
7.9.1.1	Introduction to Port Mirroring	196
7.9.1.2	Port Mirroring Setup.....	196
7.9.2	Port-Based VLAN	197
7.9.2.1	Introduction to VLAN.....	197
7.9.2.2	Port-Based VLAN Setup	197
7.10	Miscellaneous	198
7.10.1	Miscellaneous	198
7.10.2	Scheduled Task	199
Chapter 8	NAT	201
8.1	Port Forwarding.....	201
8.1.1	Introduction to Port Forwarding	201
8.1.2	Port Forwarding Settings	202
8.1.3	Port Forwarding List	203
8.1.4	How to Add the Port Forwarding Rules	204
8.1.5	Configuration Examples for Port Forwarding	204
8.1.5.1	Example One	204
8.1.5.2	Example Two	205
8.1.5.3	Example Three.....	205
8.2	DMZ Host.....	207
8.2.1	Introduction to DMZ host	207
8.2.2	DMZ Host Settings.....	208

8.2.2.1	Global DMZ Host Settings	208
8.2.2.2	Interface DMZ Host Settings.....	208
8.2.3	The Priorities of Port Forwarding and DMZ Host	209
8.3	NAT Rule.....	210
8.3.1	Introduction to NAT	210
8.3.1.1	NAT Address Space Definitions	210
8.3.1.2	NAT Types	210
8.3.1.3	The Relations of Internet Connection, NAT Rule and Port Forwarding Rule.....	211
8.3.1.4	System Reserved NAT Rules.....	212
8.3.2	NAT and Multi-WAN Load Balancing.....	212
8.3.2.1	Overview.....	212
8.3.2.2	Assigning Preferential Channel according to Source IP.....	212
8.3.2.3	Allocating Traffic according to Connection Bandwidth	213
8.3.2.4	Two Load Balancing Policies	213
8.3.2.5	The Priorities of NAT Rules.....	214
8.3.3	NAT Rule Settings	215
8.3.3.1	EasyIP NAT Rule Settings	215
8.3.3.2	One2One NAT Rule Settings	216
8.3.3.3	Passthrough NAT Rule Settings.....	217
8.3.4	NAT Rule List.....	218
8.3.5	How to Add the NAT Rules	219
8.3.6	Configuration Examples for NAT Rule.....	220
8.3.6.1	An Example for Configuring EasyIP NAT Rule.....	220
8.3.6.2	An Example for Configuring One2One NAT Rule	221
8.3.6.3	An Example for Configuring Passthrough NAT Rule.....	223
8.4	UPnP	226
8.4.1	Enable UPnP	226
8.4.2	UPnP Port Forwarding List	227
Chapter 9	PPPoE Server.....	228
9.1	Introduction to PPPoE	228
9.1.1	PPPoE Stages	228
9.1.2	PPPoE Discovery Stage	228
9.1.3	PPP Session Stage	229
9.1.4	PPPoE Session Termination.....	230
9.2	PPPoE Server Settings	230
9.2.1	PPPoE Server Global Settings	230

9.2.2	Internet Access Control	231
9.3	PPPoE Account	233
9.3.1	PPPoE Account Settings	233
9.3.2	PPPoE Account List.....	236
9.3.3	Import Accounts.....	237
9.3.4	PPPoE Account Billing.....	238
9.3.4.1	Introduction to PPPoE Account Billing Mechanism	238
9.3.4.2	PPPoE Account Billing By Date	239
9.3.4.3	PPPoE Account Billing By Hour.....	239
9.3.4.4	PPPoE Account Billing By Traffic	240
9.4	PPPoE IP/MAC Binding.....	241
9.4.1	PPPoE IP/MAC Binding Settings.....	241
9.4.2	PPPoE IP/MAC Binding List.....	242
9.5	PPPoE Status.....	244
9.6	Configuration Example for PPPoE Server	246
9.7	PPPoE Account Expiration Notice.....	250
9.7.1	PPPoE Account Expiration Notice by Date	251
9.7.2	PPPoE Account Expiration Notice by Hours	253
9.7.3	PPPoE Account Expiration Notice by Traffic	255
Chapter 10	QoS.....	257
10.1	Introduction to Bandwidth Management.....	257
10.1.1	Why We Need Bandwidth Management.....	257
10.1.2	Token Bucket Algorithm	258
10.1.3	Implementation of Bandwidth Management	259
10.2	Rate Limit Global Settings.....	260
10.3	Rate Limit Rule	261
10.3.1	Rate Limit Rule Settings	261
10.3.2	Rate Limit Rule List	264
10.3.3	The Execution Order of Rate Limit Rules	265
10.4	P2P Rate Limit	266
10.5	Application QoS.....	268
10.6	Configuration Examples for QoS.....	269
10.6.1	Example One	269
10.6.2	Example Two	272
Chapter 11	Restriction	277

11.1	User Admin	277
11.1.1	User Status List	277
11.1.2	Personal Rate Limit	279
11.1.3	Personal Internet Behavior Management	279
11.2	Internet Behavior Management	281
11.2.1	Internet Behavior Management Policy Settings	282
11.2.2	Internet Behavior Management Policy List.....	286
11.3	Policy Database	288
11.3.1	Introduction to Policy Database	288
11.3.2	Policy Database List	289
11.3.3	Policy Database Version Check	290
11.3.4	Import Policy Database	291
11.4	QQ Whitelist	292
11.4.1	Enable QQ Whitelist	292
11.4.2	QQ Whitelist Settings	292
11.4.3	QQ Whitelist.....	293
11.5	Configuration Example for Internet Behavior Management	294
11.6	Notice	300
11.6.1	Introduction to Notice.....	300
11.6.2	Notice Settings.....	300
11.6.2.1	One-Time Notice Settings.....	300
11.6.2.2	Daily Notice Settings.....	303
11.7	Web Authentication	304
11.7.1	Enable Web Authentication	304
11.7.2	Web Authentication User Account Settings	305
11.7.3	Web Authentication User Account List.....	305
11.7.4	How to Use Web Authentication	306
Chapter 12	Security	308
12.1	Attack Defense	308
12.1.1	Internal Attack Defense	308
12.1.2	External Attack Defense	311
12.2	IP/MAC Binding	313
12.2.1	Introduction to IP/MAC Binding	313
12.2.1.1	IP/MAC Overview	313
12.2.1.2	The Operation Principle of IP/MAC Binding	313
12.2.2	IP/MAC Binding Settings	317

12.2.3 IP/MAC Binding Global Setup	318
12.2.4 IP/MAC Binding List.....	319
12.2.5 How to Add the IP/MAC Bindings	319
12.2.6 Internet Whitelist and Blacklist.....	320
12.2.6.1 Introduction to Internet Whitelist and Blacklist Based on IP/MAC Binding	320
12.2.6.2 How to Configure an Internet Whitelist.....	321
12.2.6.3 How to Configure Internet Blacklist.....	322
12.3 Firewall	324
12.3.1 Introduction to Access Control.....	324
12.3.1.1 The Purpose of Access Control Feature	324
12.3.1.2 The Operation Principle of Access Control	324
12.3.1.3 The Action of an Access Control Rule.....	325
12.3.1.4 The Execution Order of Access Control Rules	325
12.3.1.5 Address Group and Service Group.....	326
12.3.1.6 System Default Access Control Rules.....	326
12.3.2 Access Control Rule Settings	327
12.3.3 Enable Access Control	330
12.3.4 Access Control List.....	330
12.3.5 Configuration Examples for Access Control	331
12.3.5.1 Example One	331
12.3.5.2 Example Two	336
12.4 Domain Filtering	342
12.4.1 Domain Filtering Settings	342
12.4.2 Domain Blocking Notice	343
12.5 NAT Session Limit	345
12.5.1 NAT Session Limit Rule Settings.....	346
12.5.2 NAT Session Limit Rule List	347
12.6 Address Group	349
12.6.1 Introduction to Address Group.....	349
12.6.2 Address Group Settings	350
12.6.3 Address Group List.....	351
12.6.4 How to Add the Address Groups	352
12.6.5 How to Edit an Address Group	352
12.7 Service Group	354
12.7.1 Introduction to Service Group.....	354
12.7.2 Service Group Settings.....	355

12.7.3 Service Group List	357
12.7.4 How to Add the Service Groups	357
12.7.5 How to Edit an Service Group	358
12.8 Schedule.....	359
12.8.1 Introduction to Schedule	359
12.8.2 Schedule Settings.....	360
12.8.3 Schedule List	361
12.8.4 How to Add the Schedules	362
12.8.5 Configuration Example for Schedule	363
Chapter 13 System	365
13.1 Administrator	365
13.1.1 Administrator Settings	365
13.1.2 Administrator List.....	366
13.1.3 How to Add the Administrator Accounts	367
13.2 System Time	368
13.3 Firmware Upgrade.....	370
13.3.1 Save Firmware.....	370
13.3.2 Firmware Upgrade.....	371
13.4 Configuration	372
13.4.1 Backup Configuration	372
13.4.2 Restore Configuration.....	372
13.4.3 Restore Defaults	373
13.5 Remote Admin	374
13.6 WEB Server	376
13.7 Restart	378
Appendix A How to configure your PC.....	380
Appendix B FAQ	383
1. How to connect the Device to the Internet using PPPoE.....	383
2. How to connect the Device to the Internet using Static IP.....	386
3. How to connect the Device to the Internet using DHCP.....	387
4. How to reset the Device to factory default settings.....	389
4-1 Case One: Remember the administrator password	389
4-2 Case Two: Forget the administrator password	394
5. How to use CLI Rescue Mode	400
6. IP/MAC Binding and Access Control.....	407

7. How to find out who uses the most bandwidth?	411
8. How to troubleshoot faults caused by worm viruses or hacker attacks on the Device?	412
9. How to enable WAN ping respond?.....	416
Appendix C Common IP Protocols	417
Appendix D Common Service Ports	418
Appendix E Figure Index	422
Appendix F Table Index.....	430

About This Manual

Note

For best use of our product, it is strongly recommended that you update Windows Internet Explorer browser to version 6.0 or higher.

0.1 Scope

This guide describes the characteristics and features of the UTT Series Security Firewalls, which are based on ReOS V10 firmware platform. It mainly describes how to configure and manage the Device via Web UI. Please make sure that your Device's firmware version accords with ReOS V10. As the product or firmware version upgrades, or other reasons, this guide will be updated aperiodically.


In addition, as the product specifications of each model are different, you had better contact the UTT customer engineer to ask for help on the product specifications.


Note

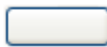
The **Device** (The first letter is uppercase.) mentioned in this guide stands for the NE high-performance gateway.

0.2 Web UI Style

The Web UI style complies with the browser standard, which is as follows:

 **Radio Button:** It allows you to choose only one of a predefined set of options.

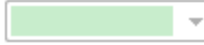
 **Check Box:** It allows you to choose one or more options.

 **Button:** It allows you to click to perform an action.

 **Text Box:** It allows you to enter text information.



List Box: It allows you to select one or more items from a list contained within a static, multiple line text box.



Drop-down List: It allows you to choose one item from a list. When a drop-down list is inactive, it displays a single item. When activated, it drops down a list of items, from which you may select one.

0.3 Documents Conventions

0.3.1 Detailed Description of List

The Web UI contains two kinds of lists: editable list and read-only list. The following examples will describe them respectively.

0.3.1.1 Editable List

An editable list allows you to add, view, modify and delete the entries. Let's take the **IP/MAC Binding List** (see Figure 0-1) as an example to explain it.

ID	Description	IP Address	MAC Address	Allow Internet Access	Edit
<input type="checkbox"/> 2	test1	192.168.16.12	0022aa112233	<input checked="" type="checkbox"/>	Edit
<input type="checkbox"/> 3	test2	192.168.16.22	0022aa334455	<input checked="" type="checkbox"/>	Edit

Figure 0-1 IP/MAC Binding List

2/500 : Configured number / maximum number, the example means there are two

configured IP/MAC bindings and the maximum number of bindings supported by the Device is 500.

Lines/Page: : This drop-down list allows you to select the number of entries displayed per page. In this example, the available options are 10, 30 and 50, and the default value is 10.

First : Click it to jump to the first page.

Prev : Click it to jump to the previous page.

Next : Click it to jump to the next page.

Last : Click it to jump to the last page.

: Click it to add a new entry to the list. Here it will jump to the **Security > IP/MAC Binding > IP/MAC Binding Settings** page, then you can add a new IP/MAC binding.

Search: : Enter the text string you want to search for in this text box, then press **<Enter>** key to display all the matched entries. What's more, you can do the search within the displayed results. If you want to display all the entries, you only need clear the text box and then press **<Enter>** key.

Note that the matching rule is substring matching, that is, it will search for and display those entries that contain the specified text string.

[Edit](#) : Click it to go to the corresponding setup page.

Select All : Click it (add the check mark) to select all the entries in the current page. Click it again (remove the check mark) to unselect all the entries in the current page.

: To delete one or more entries, select the leftmost check boxes of them at first, and then select **Delete** from the drop-down list, lastly click **OK** to delete the selected entries. To delete all the entries in the list, select **Delete All** from the drop-down list at first, and then click **OK**.

0.3.1.2 Read-only List

A read-only list is used to display the system status information that is not editable. Let's take the **NAT Statistics** list (see Figure 0-2) as an example to explain the functions.

third time to sort them in descending order, and so forth. After sorted, the list will be displayed from the first page.

0.3.2 Keyboard Operation


<>: It is used to represent the name of a key on the keyboard. For example, <Enter> key represents the Enter key on the keyboard.

0.3.3 Other Conventions

0.3.3.1 Convention for a Page Path

First Level Menu Name > Second Level Menu Name (bold font) means the menu path to open a page. E.g., **System > Time** means that in the Web UI, click the first level menu **System** firstly, and then click the second level menu **Time** to open the corresponding page.

0.3.3.2 Convention for Clicking a Button

Click the **XXX** button (**XXX** is the name of the button, bold font) means performing a corresponding action. E.g., click the **Delete** button means performing a deleting action, the **Delete** button is showed as .

0.3.3.3 Convention for Selecting an Option

Select the **XXX** option (**XXX** is the name of the option, bold font) means selecting the corresponding function. E.g., select the **Enable DNS Proxy** check box means enabling the DNS proxy feature (see Figure 0-3).

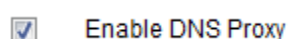


Figure 0-3 Enable DNS Proxy

0.4 Partial Factory Default Settings

1. The default administrator user name is **Default** (case sensitive) with a blank password.
2. The following table provides the factory default settings of the interfaces.

Interface	IP Address	Subnet Mask
LAN	192.168.16.1	255.255.255.0
WAN1	192.168.17.1	255.255.255.0
WAN2/DMZ	192.168.18.1	255.255.255.0

Table 0-1 Factory Default Settings of Interfaces

0.5 Document Organization

This manual mainly describes the settings and applications of the UTT products, which is organized as follows:

Chapter		Contents
1	Product Overview	The functions and features of the Device.
2	Hardware Installation	How to install the Device.
3	Login to the Device	How to Login to the Device, including: <ul style="list-style-type: none"> • Configure Your PC: How to install and configure TCP/IP properties on your PC. • Login to the Device: How to login to the Device; introduction to

		<p>the web page of the Device.</p> <ul style="list-style-type: none"> • Shortcut Icons: Introduction to the shortcut Icons in the web page of the Device.
4	Quick Setup	<p>How to configure the basic parameters to quickly connect the Device to the Internet, including:</p> <ul style="list-style-type: none"> • LAN Settings: How to configure the IP address and subnet mask of the LAN interface. • WAN Settings: How to configure the Internet connection on each WAN interface one by one. The Device provides three types of connections: PPPoE, Static IP and DHCP. <p>Note that the number of WAN interfaces depends on the specific product model.</p>
5	System Status	<p>How to view the system statistics and status information, including:</p> <ul style="list-style-type: none"> • System Information: It displays system up time, system resource usage information, system version, port status, and interface rate chart. • NAT Statistics: It displays the NAT session details of each LAN host. • DHCP Statistics: It displays the statistics of the DHCP address pool, DHCP server, DHCP conflict, DHCP client and DHCP relay agent. • Interface Statistics: It displays traffic statistics of each physical interface. • Route Statistics: It displays the routing table. • Session Monitor: How to monitor the Internet activities of the LAN users by the NAT session list. It allows you to filter and display sessions by certain criteria, such as source IP address, destination IP address/domain name, destination port, NAT translated IP

		<p>address/domain name, and so on.</p> <ul style="list-style-type: none"> ● System Log: It displays the system logs; it also allows you to select the types of logs that you want the Device to store and display. ● Application Traffic Statistics: It displays the traffic statistics of some special applications per Internet connection; it also displays each application traffic statistics per LAN user. ● WAN Traffic Statistics: It displays traffic and rate related information of each Internet connection.
<p>6</p>	<p>Basic Setup</p>	<p>How to configure the basic features of the Device, including:</p> <ul style="list-style-type: none"> ● Quick Wizard: How to configure the basic parameters to quickly connect the Device to the Internet. ● LAN Settings: How to configure the parameters of the LAN interface, e.g., IP address, subnet mask, IP address2, proxy ARP, MAC address. ● WAN Settings: How to configure the Internet connection on each WAN interface, and how to view the related configuration and status information. ● Load Balancing: How to configure the load balancing feature, which includes: detection and weight settings, global settings, ID binding; how to view load balancing list. Note that only after you have configured more than one Internet connections, the second level menu Load Balancing will be displayed. ● DHCP & DNS: How to configure DHCP server, DHCP auto binding, and DNS proxy.
<p>7</p>	<p>Advanced Setup</p>	<p>How to configure the advanced features of the Device, including:</p> <ul style="list-style-type: none"> ● Static Route: How to configure static routes and static route PDBs.

		<ul style="list-style-type: none"> ● PBR: How to configure PBR (Policy-Based Routing) based on source and destination addresses, protocols, ports, schedules, and other criteria. ● DNS Redirection: How to configure DNS redirection feature which is used to redirect domain names directly to the specified IP addresses. ● SNMP: How to configure SNMP (Simple Network Management Protocol). ● DDNS: How to apply for DDNS account service and configure DDNS (Dynamic Domain Name System). ● DHCP: How to configure DHCP client, server, relay agent and raw option. ● Switch: How to configure switch features, such as VLAN, port mirroring and so on. ● Miscellaneous: How to configure miscellaneous, such as scheduled task.
<p>8</p>	<p>NAT</p>	<p>How to configure NAT features, including:</p> <ul style="list-style-type: none"> ● Port Forwarding: How to configure and view port forwarding rules. ● DMZ Host: How to configure the global DMZ host and interface DMZ hosts. ● NAT Rule: How to configure and view NAT rules. The Device provides three types of NAT: One2One, EasyIP and Passthrough; and you can create more than one NAT rule for each type of NAT when you obtain multiple public IP addresses. ● UPnP: How to enable UPnP and view the port forwarding rules established using UPnP.

<p>9</p>	<p>PPPoE Server</p>	<p>How to configure PPPoE server feature, including:</p> <ul style="list-style-type: none"> • Global Settings: How to configure PPPoE server global parameters, e.g., enable PPPoE server; and IP addresses, gateway IP address and DNS servers IP addresses that will be assigned to the PPPoE dial-in users. • PPPoE Account: How to configure PPPoE accounts. It provides rate limit based on the account, account/MAC binding and account/IP binding features; also, it allows you to import multiple accounts at a time. • PPPoE IP/MAC Binding: How to use IP/MAC binding feature to assign static IP addresses to the PPPoE dial-in users. • PPPoE Status: How to view the status and usage information of each online PPPoE dial-in user.
<p>10</p>	<p>QoS</p>	<p>How to configure QoS features, including:</p> <ul style="list-style-type: none"> • Global Settings: How to enable or disable rate limit, how to configure the capacity, i.e., the maximum number of network devices that can be connected to the Device at the same time. • Rate Limit Rule: How to configure flexible rate limit rules based on address group, service group and schedule to improve bandwidth utilization. • P2P Rate Limit: How to limit the maximum upload and download rate of the P2P traffic for the LAN users. • Application QoS: How to configure preferential forwarding for some predefined special applications traffic.
<p>11</p>	<p>Restriction</p>	<p>How to configure restriction features, including:</p> <ul style="list-style-type: none"> • User Admin: How to view the current status information of LAN users, and configure personal settings for each user individually, including rate limit and Internet behavior management settings.

		<ul style="list-style-type: none"> • Internet Behavior Management: How to control and manage the Internet behaviors of the LAN users to improve bandwidth utilization and network security. • Policy Database: How to view the policy databases related information; and how to upload or update policy databases. • QQ Whitelist: How to configure QQ whitelist feature. The LAN users still can use the QQ numbers in the QQ whitelist to login to QQ even if you have blocked them from using QQ by Internet behavior management policies. • Notice: How to configure notice feature. The Device can push the notice message to the specified LAN users; and there are two types of notices: one-time notice and daily notice.
<p>12</p>	<p>Security</p>	<p>How to configure security features, including:</p> <ul style="list-style-type: none"> • Attack Defense: How to configure the internal and external attack defense features to enhance network security. • IP/MAC Binding: How to configure IP/MAC address pair bindings to prevent IP address spoofing. By utilizing IP/MAC binding feature, you can flexibly configure an Internet whitelist or blacklist for the LAN users. • Firewall: How to configure firewall access control rules which are applied on the LAN interface. • Domain Filtering: How to configure domain filtering feature. You can only block certain specified domain names or only allow certain specified domain names. • NAT Session Limit: How to configure NAT session limit rules to limit the maximum number of concurrent NAT sessions, TCP sessions, UDP sessions, and ICMP sessions based on LAN hosts. And you can limit different maximum sessions for different LAN hosts. • Address Group: How to configure address groups. You can

		<p>divide some discontinuous IP addresses into an address group, and then reference the address group in an access control rule or rate limit rule.</p> <ul style="list-style-type: none"> • Service Group: How to configure service groups. It provides five types of services including general service, URL, Keyword, DNS and MAC address. It allows you to add multiple services into a service group, and then reference the service group in an access control rule or rate limit rule. • Schedule: How to configure schedules. The schedules can be applied to various time-related features, e.g., dial schedule, rate limit rule, access control rule, etc.
13	System Admin	<p>How to manage the Device, including:</p> <ul style="list-style-type: none"> • Administrator: How to configure the administrator account. It provides three privilege groups: admin, read and execute. • System Time: How to configure the system date and time manually or automatically. • Firmware upgrade: How to backup, download and upgrade firmware. • Configuration: How to backup and restore the system configuration, and reset the Device to the factory default settings. • Remote Admin: How to enable HTTP remote management feature to remotely configure and manage the Device via Internet. • Web server: How to configure the Web server. • Restart: How to restart the Device in the Web UI.
14	Appendix	<p>Provides six appendixes, including:</p> <ul style="list-style-type: none"> • Appendix A How to configure your PC: How to install and

		<p>configure TCP/IP properties for Windows 95 and Windows 98.</p> <ul style="list-style-type: none"> • Appendix B FAQ: Frequent questions and answers. • Appendix C Common IP Protocols: Provides the list of common IP protocol numbers and names. • Appendix D Common Service Ports: Provides the list of common service port numbers and names. • Appendix E Figure Index: Provides a figure index directory. • Appendix F Table Index: Provides a table index directory.
--	--	--

Table 0-2 Document Organization

Chapter 1 Product Overview

Thanks for choosing UTT products from UTT Technologies Co., Ltd.

This chapter describes the functions and features of the UTT products in brief.

1.1 Key Features

- Provides multiple Internet connection types: PPPoE, Static IP and DHCP
- Provides real-time monitoring and management of the LAN traffic and users via Web UI
- Provides multiple WAN ports that support intelligent load balancing and auto backup
- Supports ID binding for some applications, such as online banking, QQ, etc
- Supports intelligent bandwidth management based on token bucket algorithm
- Supports Internet behavior management for the LAN users, such as block QQ, MSN and BT download applications
- Defense against DoS/DDoS attacks
- Supports IP packet filtering based on IP address, protocol and TCP/UDP port
- Supports URL and keyword filtering
- Supports MAC address filtering
- Supports DNS request filtering
- Supports address group and service group setup
- Supports advanced firewall function based on address group and service group
- Supports strong DHCP features: DHCP Server, DHCP Relay Agent and DHCP Client
- Supports PPPoE Server feature
- Supports UPnP (universal plug and play)
- Supports express forwarding
- Supports rate limit of the LAN hosts based on schedules
- Supports port-based VLAN
- Supports port mirroring

1.2 Main Features

1. LAN Interface

- Multiple-port Switch: Provides an integrated multiple-port 10/100Mbps, each port supports auto MDI/MDI-X.
- DHCP Server: It can act as a DHCP server to dynamically assign IP addresses and other TCP/IP configuration parameters (such as gateway IP address, DNS and WINS server IP addresses) to the LAN hosts.
- Multiple Subnets: It can be assigned multiple IP addresses to connect multiple subnets.
- Routing Protocols: It supports static routing and dynamic routing protocols including RIP I and RIP II.
- Port-based VLAN: A VLAN (Virtual Local Area Network) is a group of devices that form a logical LAN segment, that is, a broadcast domain. The members on the same VLAN can communicate with each other. The traffic will not disturb among different VLANs. Note that only some models support this feature.
- Port Mirroring: It allows an administrator to monitor network traffic. It copies the traffic from specified ports to another port where the traffic can be monitored. Then the administrator can perform traffic monitoring, performance analysis and fault diagnosis. Note that only some models support this feature.

2. WAN Interface

- Multiple WAN Interfaces: It provides multiple 10/100Mbps WAN interfaces that support auto MDI/MDI-X.
- DSL and Cable Modem Supported: UTT products have passed the compatibility testing with many DSL and cable modems provided by popular manufacturers.
- PPPoE: Each WAN interface can act as a PPPoE (PPP over Ethernet) client to connect to the ISP's PPPoE server.
- Internet Connection Sharing: The LAN users can share multiple Internet connections to access the Internet using NAT (Network Address Translation).
- Load Balancing and Failover: Provides multiple WAN interfaces that support intelligent load balancing and automatic failover.
- Supports ID Binding for Some Applications, such as online banking, QQ, etc.

3. IP/MAC Binding and Access Control

- Supports IP and MAC address pairs binding

- Supports management and control of multiple Internet services
- Supports Internet harmful websites filtering
- Supports IP packet filtering based on IP address, protocol and TCP/UDP port
- Supports Web content filtering based on URL and keyword
- Supports DNS request filtering
- Supports MAC address filtering

4. IP QoS

- Supports intelligent bandwidth management based on token bucket algorithm. It can limit the upload and download rates for each LAN host. Also it provides flexible bandwidth management function to effectively control network transmission rate and improve bandwidth utilization.
- Supports rate limiting for the P2P applications traffic. Limiting P2P traffic can effectively solve the network problems which are caused by the abuse of P2P software.
- Supports preferential forwarding for some predefined special applications traffic, that is, these applications traffic aren't restricted by the rate limit rules, so that you can run these applications more smoothly and faster.

5. Configuration and Management

- Easy Configuration: It provides the Web UI and CLI to facilitate configuration and management.
- Remote Admin: It allows a network administrator to manage the Device remotely from any host on the LAN or WAN.
- Device Restart: It allows you to restart the Device via the Web UI for ease of use.

6. Advanced Features

- DMZ Host: Supports multiple DMZ hosts. The DMZ (Demilitarized Zone) host feature allows one local host to be exposed to the Internet, so the users can easily access it via the Internet.
- Port Forwarding: You can create multiple port forwarding rules to allow the Internet users to access the services offered by the local servers.
- Advanced DHCP: All the physical interfaces support DHCP client, DHCP server and DHCP relay agent. When acting as a DHCP server, the Device supports multiple address pools, also provides flexible and sufficient IP address allocation policy. If you use the DHCP server and DHCP relay agent together, it can fully meet the various user requirements.

- **Special Application Supported:** Supports the use of some special Internet applications, such as the Tencent QQ, online games, Video software, Audio software, and so on.
- **DDNS:** Supports Dynamic Domain Name System (DDNS) service.
- **PPPoE Server:** Supports rich PPPoE server features, which includes PPPoE account and MAC address binding, PPPoE account and IP address binding, and PPPoE IP and MAC address pair binding feature.
- **Express Forwarding:** It supports express forwarding to greatly improve system performance.
- **Notice Feature:** The Device can pop up the notice messages to the LAN users.

7. Security Features

- **Configuration File:** You can configure and modify the administrator password to prevent those unauthorized users from modifying the settings of the Device; and you can back up the configuration file to prevent accidental loss of settings.
- **Access Control:** The administrator can restrict some LAN users from accessing the Internet or some Internet services.
- **Real-time Monitoring:** Supports real-time monitoring and management of the LAN traffic and users, to promptly detect network problems and abnormal users.
- **Firewall Protection:** The Device can monitor all the traffic from the Internet, block all the illegal requests to the LAN servers, block IP address and port scanning by hacker software, to prevent malicious attacks from the Internet, such as DoS/DDoS attacks. It also allows you to set up an Internet blacklist and whitelist. Furthermore, it supports advanced firewall function based on address group and service group.
- **Internet Behavior Management:** You can allow or block the specified LAN users from using popular IM (e.g., QQ, MSN) and P2P applications (e.g., BitComet, BitSpirit, Thunder Search), downloading the files with the extension .exe, .dll, .vbs, .com, .bat or .sys over HTTP, playing online games, accessing stock and game websites, submitting input in the webpage, using HTTP proxy, and so on.

1.3 VPN Features

The UTT products provide full VPN features including IPSec VPN, L2TP and PPTP VPN; and it allows you to use them at the same time. The detailed features are as follows:

1. Supports VPN tunnels using dynamic IP addresses
2. Supports site-to-site VPN
3. Supports remote access VPN (mobile user-to-site)

4. Supports L2TP server and client
5. Supports PPTP server and client
6. The main features of IPSec are as follows:
 - AutoIKE based on preshared key
 - Manual key tunnel
 - ESP and AH protocols
 - DES, 3DES and AES 128/192/256 encryption algorithms
 - MD5 and SHA-1 hash algorithms
 - Diffie-Hellman group 1, 2 and 5
 - Main mode and aggressive mode
 - DPD (dead peer detection) and Anti-Replay
 - Hub-spoke and mesh connections
 - IPSec NAT traversal

**Note**

For detailed information about how to configure VPN features, please refer to the related VPN configuration manual.

1.4 Physical Specification

1. Conforms to IEEE 802.3 Ethernet and IEEE 802.3u Fast Ethernet standards
2. Supports TCP/IP, PPPoE, DHCP, ICMP, NAT, Static Route, RIP/II, SNMP (MIB II), etc.
3. Each physical port supports auto-negotiation for the speed and duplex mode
4. Each physical port supports auto-MDIX
5. Provides system and port LEDs
6. Operating Environment:
 - Temperature: 32°F to 104°F (0°C to 40°C)
 - Relative Humidity: 10% to 90%, Non-condensing
 - Height: 0m to 4000m

1.5 Detailed Specifications Table

The UTT products include multiple models. The features and specifications of each model are different. The following table lists detailed specifications for each model.

Model Feature	UTT 2512	U2000
Number of LAN Ports	4	4
Number of WAN Interfaces	1	2
LAN Interface Speed	10/100M	10/100M
WAN Interface Speed	10/100M	10/100M
Internet Connection Setup	✓	✓
Load Balancing and failover	✗	✓
DHCP and DNS	✓	✓
DDNS	✓	✓
NAT	✓	✓
Static Route	✓	✓
Policy-based Routing	✓	✓
IP/MAC binding	✓	✓
DNS Redirection	✓	✓
Advanced DHCP	✓	✓
UPnP	✓	✓

Plug and Play	✓	✓
Express Forwarding	✓	✓
VLAN	✓	✓
Port Mirroring	✓	✓
Administrator Setup	✓	✓
System Time Setup	✓	✓
Firmware Upgrade	✓	✓
Backup & Restore Configuration	✓	✓
SNMP	✓	✓
SYSLOG	✓	✓
Remote Admin	✓	✓
PPPoE Server	✓	✓
PPPoE IP/MAC Binding	✓	✓
Account Billing of PPPoE Server	✓	✓
PPPoE Account Expiration Notice	✓	✓
PPPoE Session Status	✓	✓
User Statistics	✓	✓
NAT Statistics	✓	✓
DHCP Statistics	✓	✓

Interface Statistics	✓	✓
Route Table	✓	✓
System Information	✓	✓
System Log	✓	✓
Intelligent Bandwidth Management	✓	✓
Web Log	✓	✓
P2P Traffic Rate Limiting	✓	✓
Application QoS	✓	✓
Application Traffic Statistics	✓	✓
WAN Traffic Statistics	✓	✓
Notice Feature	✓	✓
Domain Name Filtering	✓	✓
Domain Name Blocking Notice	✓	✓
Access Control List	✓	✓
Address Group	✓	✓
Service Group	✓	✓
Schedule	✓	✓
Internal and External Attack Defense	✓	✓
Internet Behavior Management	✓	✓

Policy Database	✓	✓
ARP Spoofing Defense	✓	✓
NAT Session Limit	✓	✓
Web Authentication	✓	✓
VPN (PPTP/L2TP/IPSec)	✓	✓

Table 1-1 Detailed Specifications

Chapter 2 Hardware Installation

This chapter describes how to install the UTT products, which include UTT 2512, U2000.

2.1 Installation Requirements

1. A standard 10/100M or 10/100/1000M Ethernet network.
2. Each LAN PC needs an Ethernet card that works well.
3. TCP/IP should be installed on each PC properly.
4. You should have a DSL modem, cable modem or fiber optic modem.
5. If you will use a PPPoE Internet connection to access the Internet, you should have a login name and password provided by your ISP.

2.2 Installation Procedure

Please make sure that the Device is powered off before installing it. The installation procedures of UTT products are very similar, which include the following steps in general.

- Step 1** Select a proper location to install the Device. You can install the Device in a 19-inch standard rack; or on a level surface such as a desktop or shelf if you don't have a 19-inch standard rack.
- Step 2** Connect the Device to the LAN, that is, connect the PC or switch on your LAN to a LAN port of the Device.
- Step 3** Connect the Device to the WAN, that is, connect your DSL, cable or fiber optic modem to a WAN port of the Device.
- Step 4** Power on the Device. Note: Before powering on the Device, make sure that the power supply and connectivity are normal, and the power outlet is grounded properly.
- Step 5** Check the LEDs on the front panel of the Device to see whether the Device is working well or not.

The following sections describe the installation procedure, network connection diagram, and LEDs status of each model respectively.

2.3 Installation Procedure of UTT 2512

1. Selecting the Proper Location

Before installing the UTT 2512, you should make sure that it is powered off, and then select a proper location to install the UTT 2512. The UTT 2512 is designed as a desktop device, you can install it on a level surface such as a desktop or shelf.

Note

Please ensure that the desktop or shelf is stable and the power outlet is grounded properly, and do not place heavy objects on the UTT 2512.

2. Connecting the UTT 2512 to the LAN

See Figure 2-1, connect a standard network cable from a PC or switch to a LAN port of the UTT 2512. The UTT 2512 will automatically adapt to any Ethernet device which is operating at 10Mbps or 100Mbps.

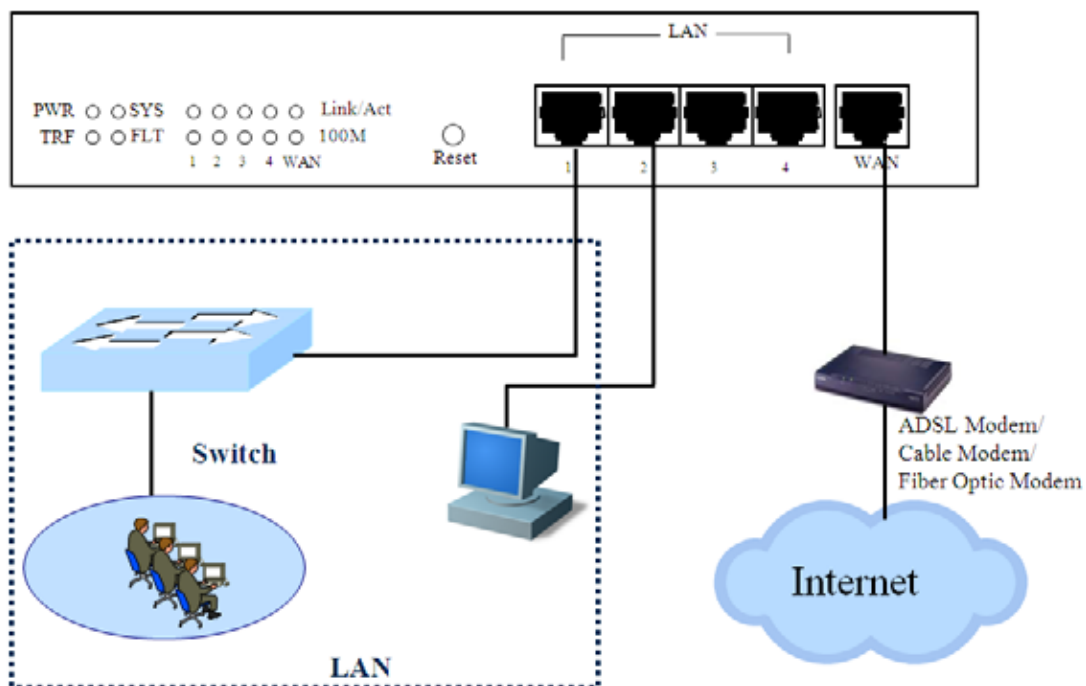


Figure 2-1 Connecting the UTT 2512 to the LAN and Internet

3. Connecting the UTT 2512 to the Internet

Connect the network cable provided by the manufacturer from the DSL, cable or fiber optic modem to a WAN port of the UTT 2512, see Figure 2-1. If you don't have a network

cable provided by the manufacturer, please use a standard network cable.

4. Powering On the UTT 2512

Connect the supplied power cord to the power connector on the back panel of the UTT 2512, and then plug the other end of the power cord to a grounded power outlet, lastly turn on the power switch on the back of the UTT 2512.

 **Note**

To prevent the UTT 2512 from working abnormally or being damaged, make sure that the power supply and connectivity are normal, and the power outlet is grounded properly before powering on the UTT 2512.

5. Checking the LEDs

The LEDs are located on the front panel of the UTT 2512, see Figure 2-2. We divide the LEDs into two groups:

- The first group includes four system LEDs on the left two columns, which indicate power status, operational status and failures of the UTT 2512, see Table 2-1 for detailed description.
- The second group includes the ten port LEDs on the right five columns, which indicate the status of each port, see Table 2-2 for detailed description. Each port has two LEDs, LEDs 1 through 4 are corresponding to LAN1 through LAN4 respectively, and LED WAN is corresponding to WAN.

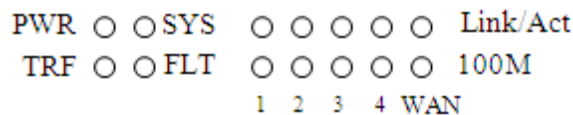


Figure 2-2 LEDs on the UTT 2512

LEDs	Status During Startup	Status During Operating
SYS	One second after powering up, the LED flashes fast for one second, and then extinguishes for two seconds, lastly flashes twice per second.	The LED flashes twice per second when the system is operating properly, and it will flash slower if the system is under heavy load. The LED will extinguish or light steady if a fault occurred in the Device.
PWR	The LED lights during startup.	The LED lights steady when the power is being supplied to the Device.

TRF	The LED lights during startup.	The LED flashes when the Device is sending or receiving data. The LED will extinguish if there is no network traffic on the Device.
FLT	The LED lights during startup.	The LED extinguishes when the Device is operating properly. The LED will flash if a fault occurred in the Device. And the Device will restart automatically after a certain number of flashes.

Table 2-1 Description of the System LEDs on the UTT 2512

LEDs	Status During Startup	Status During Operating
Link/Act	All the Link/Act LEDs flash firstly, and then they extinguish.	The LED lights steady when a link between the corresponding port and another device is detected. The LED flashes when the corresponding port is sending or receiving data.
100Mbps	After the Link/Act LEDs extinguished, all the 100Mbps LEDs flash firstly, and then extinguish.	The LED lights steady when another device is connected to the corresponding port; and a 100Mbps link is established between them.

Table 2-2 Description of the Port LEDs on the UTT 2512

6. Reset Button

If you forget the administrator password, you can use the Reset button to reset the Device to factory default settings. The operation is as follows: While the Device is powered on, use a pin or paper clip to press and hold the Reset button for more than 5 seconds, and then release the button. After that, the Device will restart with factory default settings.

 **Note**

This operation will clear all the custom settings on the Device. If you remember the administrator account, it is strongly recommended that you go to **System > Configuration** page to backup the current configuration firstly, and then reset the Device to factory default settings.

2.4 Installation Procedure of U2000

1. Selecting the Proper Location

Before installing the U2000, you should make sure that it is powered off, and then select a proper location to install the U2000. As the U2000 is designed according to the 11-inch standard rack, you can install it in a standard rack. Also you can install it on a level surface such as a desktop or shelf.

1) Installing the U2000 in a 11-inch Rack

See Figure 2-3, to install the U2000 in a 11-inch rack, firstly attach the rack-mount brackets to the sides of the U2000 (one on each side) with the supplied screws and secure them tightly, and then position the U2000 into the rack and use the supplied screws to secure it in the rack.

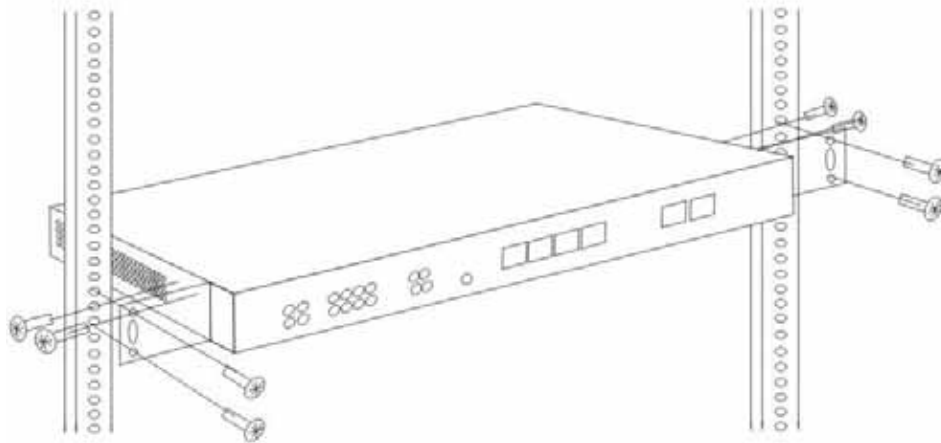


Figure 2-3 Install the U2000 in a Rack

2) Installing the U2000 on a desktop or shelf

If you don't have a 11-inch standard rack, you may directly place the U2000 on a sturdy, flat surface (such as a desktop or shelf) with a power outlet nearby.

Note

Please ensure that the desktop or shelf is stable and the power outlet is grounded properly, and do not place heavy objects on the U2000.

2. Connecting the U2000 to the LAN

See Figure 2-4, connect a standard network cable from a PC or switch to a LAN port of the U2000. The U2000 will automatically adapt to any Ethernet device which is operating at

10Mbps or 100Mbps.

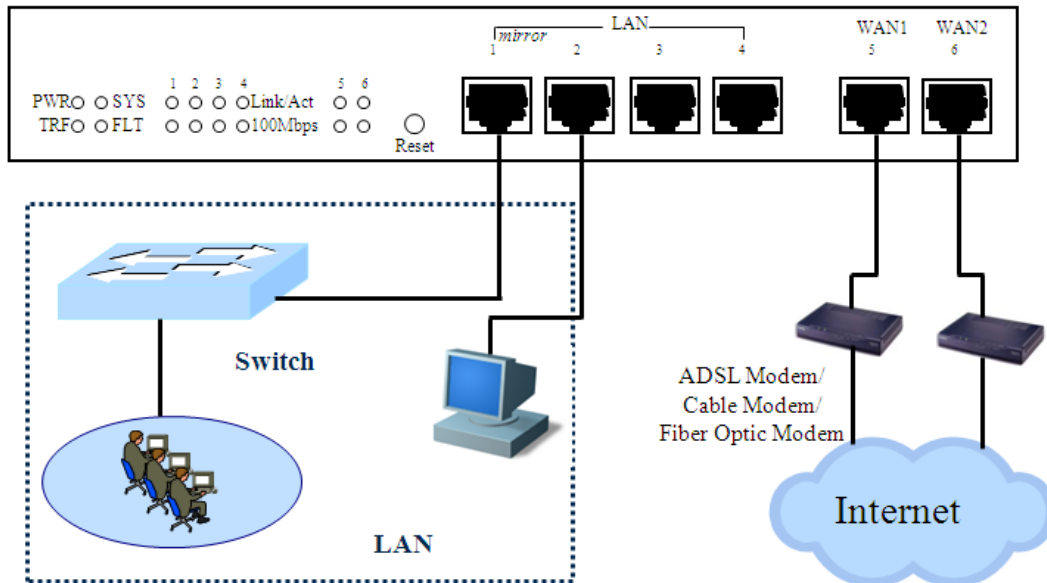


Figure 2-4 Connecting the U2000 to the LAN and Internet

3. Connecting the U2000 to the Internet

Connect the network cable provided by the manufacturer from the DSL, cable or fiber optic modem to a WAN port of the U2000, see Figure 2-4. If you don't have a network cable provided by the manufacturer, please use a standard network cable.

4. Powering On the U2000

Connect the supplied power cord to the power connector on the back panel of the U2000, and then plug the other end of the power cord to a grounded power outlet, lastly turn on the power switch on the back of the U2000.

Note

To prevent the U2000 from working abnormally or being damaged, make sure that the power supply and connectivity are normal, and the power outlet is grounded properly before powering on the U2000.

5. Checking the LEDs

The LEDs are located on the front panel of the U2000, see Figure 2-5. We divide the LEDs into two groups:

- The first group includes four system LEDs on the left two columns, which indicate

power status, operational status and failures of the U2000, see Table 2-3 for detailed description.

- The second group includes the twelve port LEDs on the right six columns, which indicate the status of each port, see Table 2-4 for detailed description. Each port has two LEDs, LEDs 1 through 4 are corresponding to LAN1 through LAN4 respectively, and LEDs 5 through 6 are corresponding to WAN1 through WAN2 respectively.

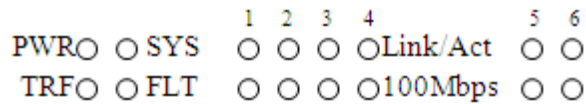


Figure 2-5 LEDs on the U2000

LEDs	Status During Startup	Status During Operating
SYS	One second after powering up, the LED flashes fast for one second, and then extinguishes for two seconds, lastly flashes twice per second.	The LED flashes twice per second when the system is operating properly, and it will flash slower if the system is under heavy load. The LED will extinguish or light steady if a fault occurred in the Device.
PWR	The LED lights during startup.	The LED lights steady when the power is being supplied to the Device.
TRF	The LED lights during startup.	The LED flashes when the Device is sending or receiving data. The LED will extinguish if there is no network traffic on the Device.
FLT	The LED lights during startup.	The LED extinguishes when the Device is operating properly. The LED will flash if a fault occurred in the Device. And the Device will restart automatically after a certain number of flashes.

Table 2-3 Description of the System LEDs on the U2000

LEDs	Status During Startup	Status During Operating
Link/Act	All the Link/Act LEDs flash firstly, and then they extinguish.	The LED lights steady when a link between the corresponding port and another device is detected. The LED flashes when the corresponding port is sending or receiving data.
100Mbps	After the Link/Act LEDs extinguished, all the 100Mbps LEDs flash firstly, and then extinguish.	The LED lights steady when another device is connected to the corresponding port; and a 100Mbps link is established between them.

Table 2-4 Description of the Port LEDs on the U2000

6. Reset Button

If you forget the administrator password, you can use the Reset button to reset the Device to factory default settings. The operation is as follows: While the Device is powered on, use a pin or paper clip to press and hold the Reset button for more than 5 seconds, and then release the button. After that, the Device will restart with factory default settings.



Note

This operation will clear all the custom settings on the Device. If you remember the administrator account, it is strongly recommended that you go to **System > Configuration** page to backup the current configuration firstly, and then reset the Device to factory default settings.

Chapter 3 Logging in to the Device

This chapter describes how to properly configure TCP/IP properties on the PC that you use to administer the Device, how to login to the Device, and how to use shortcut icons to fast link to the corresponding pages of UTT's website for the products information and services.

3.1 Configuring Your PC

Before configuring the Device via Web UI, you need properly install and configure TCP/IP properties on the PC that you use to administer the Device. The configuration steps are as follows:

- Step 1** Connect the PC to a LAN port of the Device.
- Step 2** Install TCP/IP protocol components on your PC. If it has been installed, please ignore it.
- Step 3** Configure TCP/IP parameters on your PC: If the Device's LAN interface is using the default IP address **192.168.16.1/24**, you should set the PC's IP address to an IP address in the range of 192.168.16.2 through 192.168.16.254 that is not already being used by another LAN device, set its subnet mask to 255.255.255.0, set its default gateway to 192.168.16.1, and set its DNS server to an available IP address provided by your ISP.
- Step 4** To verify the network connection between your PC and the Device, you can use the ping command at the MS-DOS command prompt on the PC: **Ping 192.168.16.1**
- If the displayed page is similar to the screenshot below, the connection between your PC and the Device has been established.

```
C:\>ping 192.168.16.1

Pinging 192.168.16.1 with 32 bytes of data:

Reply from 192.168.16.1: bytes=32 time<1ms TTL=255
Reply from 192.168.16.1: bytes=32 time<1ms TTL=255
Reply from 192.168.16.1: bytes=32 time<1ms TTL=255
Reply from 192.168.16.1: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.16.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

- If the displayed page is similar to the screenshot below, it means that your PC has not connected to the Device.

```
C:\>ping 192.168.16.1

Pinging 192.168.16.1 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.16.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

If failed to connect, please do the check according to the following steps:

1. Is the physical link between your PC and the Device connected properly?

The Link/Act LED corresponding to the Device's LAN port and the LED on your PC's adapter should light.

2. Is the TCP/IP configuration for your PC correct?

If the Device's LAN interface is using the default IP address **192.168.16.1/24**, your PC's IP address should be an IP address in the range of 192.168.16.2 through 192.168.16.254 that is not already being used by another LAN device, and its default gateway should be 192.168.16.1.

3.2 Logging in to the Device

No matter what operating system is installed on the PC, such as, MS Windows, Macintosh, UNIX, or Linux, and so on, you can configure the Device through the Web browser (for example, Internet Explorer).

Once your PC is properly configured, please do the following to login to the Device: Open a Web browser, enter the Device's LAN IP address in the address bar (by default, the address is **192.168.16.1**, see Figure 3-1), and then press **<Enter>** key.

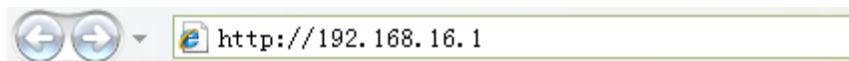


Figure 3-1 Entering IP address in the Address Bar

A login screen prompts you for your user name and password. When you first login to the Device, you should use the default administrator account: Enter **Default** (case sensitive) in the **User name** field, and leave the **Password** field blank (see Figure 3-2), lastly click **OK**.



Figure 3-2 Login Screen

Once you have entered correct user name and password, the **Status > System Info** page will appear (see Figure 3-3).



Figure 3-3 Homepage - System Info Page

In the Device’s Web page, the system model and version are displayed at the top right corner, some shortcut icons are displayed at the top, and a toolbar is displayed below the shortcut icons.

It allows you to click **Add to Toolbar** to add a shortcut menu for the current page to the toolbar. The shortcut menus are arranged from left to right in chronological order of creation, and by default the Device provides the shortcut menu of **Quick Wizard** displayed on the most left of the toolbar.

If you have not configured any Internet connection yet, please click the **Quick Wizard** hyperlink to configure the basic parameters to quickly connect the Device to the Internet. Refer to **Chapter 4 Quick Wizard** for detailed operation.

3.3 Shortcut Icons

The eight shortcut icons are displayed at the top of the Web page, which include **Product**, **Firmware**, **Datasheet**, **Register**, **Contact**, **Forum**, **Feedback** and **UTT**, see Figure 3-4. These shortcut icons are used for fast link to the corresponding pages on the website of UTT Technologies Co., Ltd., see Table 3-1 for detailed description.



Figure 3-4 Shortcut Icons

Icons	Description
Product	Click it to link to the products page of the UTT's website to find more products.
Firmware	Click it to link to the download page of the UTT's website to download the latest firmware.
Datasheet	Click it to link to the download page of the UTT's website to download the product data, such as product manual, datasheet, etc.
Register	Click it to link to the UTT Forums registry page of the UTT's website to register an account to post messages on the UTT Forums.
Contact	Click it to link to the contact us page of the UTT's website to view contact information.
Forum	Click it to link to the forum homepage of the UTT's website to participate in product discussions.
Feedback	Click it to link to send us your feedback by E-mail.
UTT	Click it to link to the homepage of the UTT's website.

Table 3-1 Detailed Description of Shortcut Icons

Chapter 4 Quick Wizard

This chapter describes the **Basic > Quick Wizard** page. The **Quick Wizard** allows you to configure the basic parameters to quickly connect the Device to the Internet.

Before using **Quick Wizard**, you need properly install and configure TCP/IP properties on the LAN PCs. Refer to **section 3.1 Configure Your PC** for detailed operation.

4.1 Running the Quick Wizard

Click the **Quick Wizard** hyperlink at the top of the Web page or click **Basic > Quick Wizard** to run the **Quick Wizard**. The **Quick Wizard** will guide you to configure the most basic features of the Device, such as Internet connection settings. Even if unfamiliar with our product, you still can finish the settings via instruction easily.

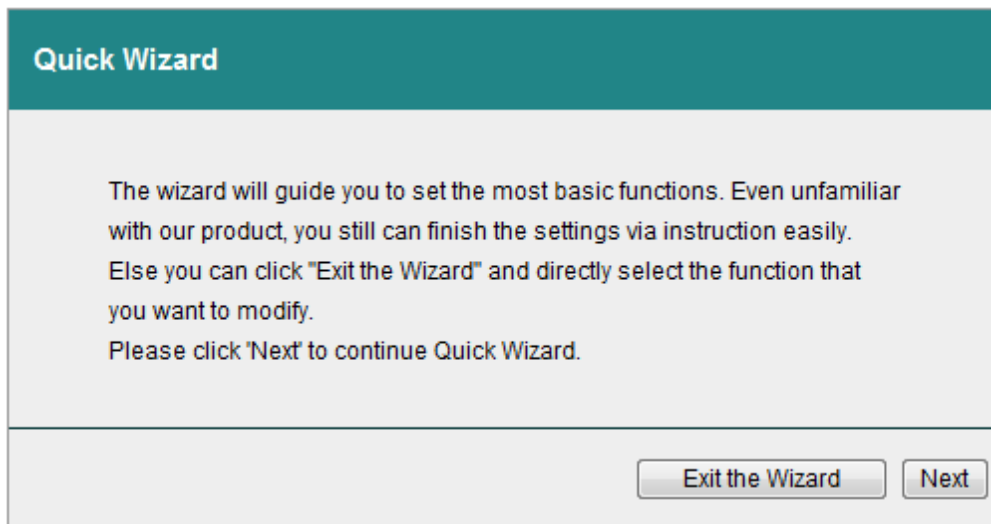
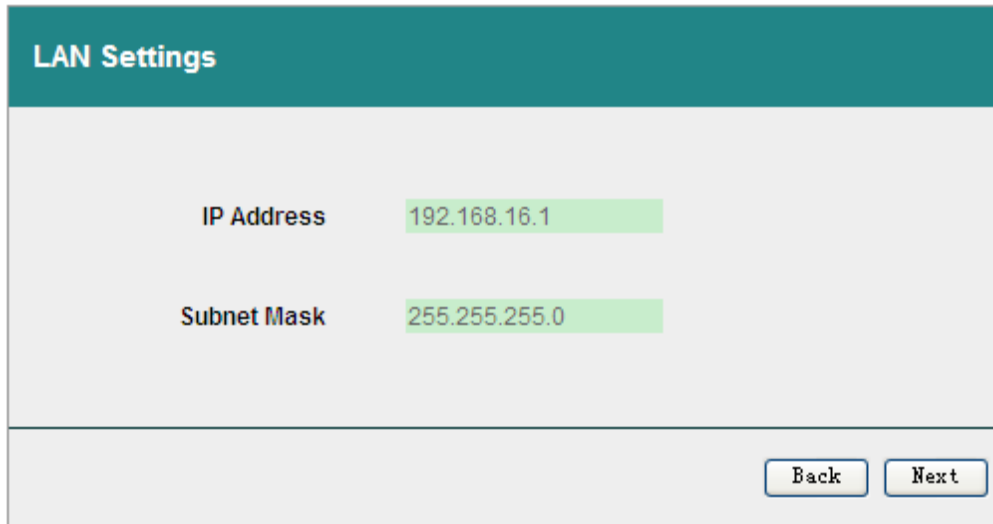


Figure 4-1 Running the Quick Wizard

- **Exit the Wizard:** Click it to exit the **Quick Wizard**.
- **Next:** Click it to go to the next page of the **Quick Wizard** to set the IP address and subnet mask of the LAN interface.

4.2 LAN Settings



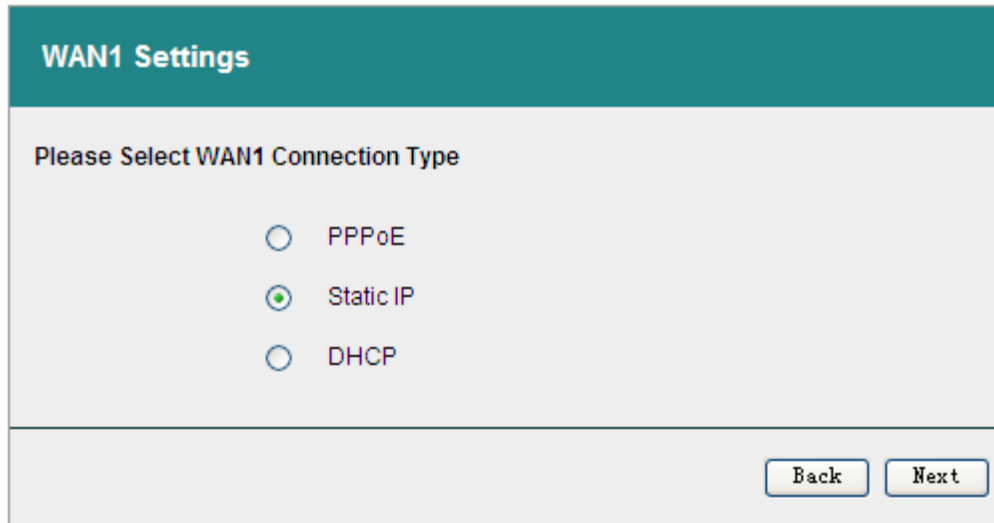
LAN Settings	
IP Address	192.168.16.1
Subnet Mask	255.255.255.0
<input type="button" value="Back"/> <input type="button" value="Next"/>	

Figure 4-2 LAN Settings

- ✧ **IP Address:** It specifies the IP address of the LAN interface. The default value is 192.168.16.1.
- ✧ **Subnet Mask:** It specifies the subnet mask that defines the range of the LAN. The default value is 255.255.255.0
- **Back:** Click it to go back to the previous page of the **Quick Wizard**.
- **Next:** Click it to go to the next page of the **Quick Wizard** to choose the Internet connection type.

4.3 Choosing an Internet Connection Type

The Device provides three Internet connection types including PPPoE, Static IP and DHCP, see Figure 4-3. Please select a connection type from the radio buttons, which is provided by your Internet Service Provider (ISP).



WAN1 Settings

Please Select WAN1 Connection Type

PPPoE

Static IP

DHCP

Back Next

Figure 4-3 Choosing an Internet Connection Type

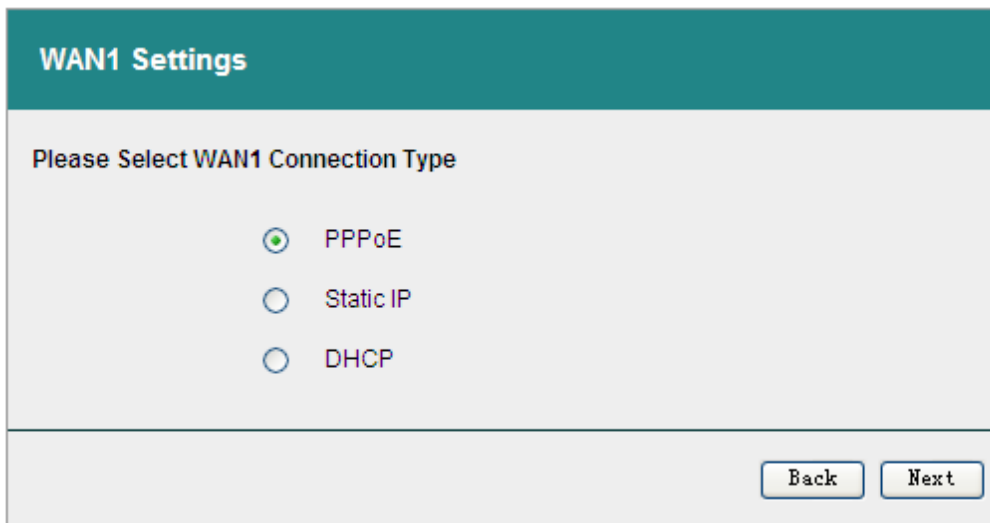
- ✧ **PPPoE:** Some DSL-based ISPs use PPPoE to establish Internet connections for end-users. If you use a DSL line, check with your ISP to see if they use PPPoE, and then select the **PPPoE** radio button.
- ✧ **Static IP:** If you are required to use a static IP address, select the **Static IP** radio button.
- ✧ **DHCP:** If your ISP will dynamically assigns an IP address to the Device, select the **DHCP** radio button. Most cable modem subscribers use this connection type.
- **Back:** Click it to go back to the previous page of the **Quick Wizard**.
- Select the **PPPoE** radio button, and then click the **Next** button to go to the next page of the **Quick Wizard** to configure a PPPoE Internet connection on the WAN1 interface.
- Select the **Static IP** radio button, and then click the **Next** button to go to the next page of the **Quick Wizard** to configure a static IP Internet connection on the WAN1 interface.
- Select the **DHCP** radio button, and then click the **Next** button to go to the next page of the **Quick Wizard** to configure a DHCP Internet connection on the WAN1 interface.

4.4 Internet Connection Settings

4.4.1 Notes on Internet Connection Settings

1. If you have changed the LAN IP address and saved the change, you should use the new IP address to re-login to the Device. And each LAN host's default gateway should be changed to this new IP address to access the Device and Internet normally.
2. After you have finished configuring the Internet connection on the WAN1 interface, you also can continue to configure the Internet connection on the WAN2, WAN3 and WAN4 interface in turn. Note that the number of WAN interfaces depends on the specific product model.
3. After you have finished configuring one or more Internet connections, you had better click the **Review Your Configuration** button in the **Quick Wizard's** confirmation page to review the settings that you have made in the **Quick Wizard** firstly, and then modify any of them if desired, lastly click the **Finish** button to save the settings to make them take effect.

4.4.2 PPPoE Internet Connection Settings



WAN1 Settings

Please Select WAN1 Connection Type

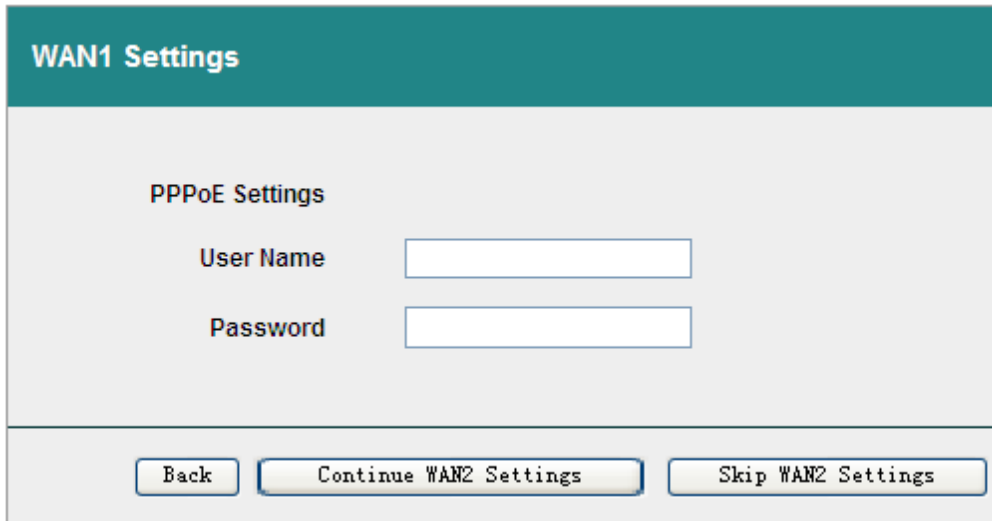
PPPoE

Static IP

DHCP

Figure 4-4 Choose PPPoE as the Connection Type

In the page of choosing an Internet connection type (see Figure 4-4), select the **PPPoE** radio button, and then click the **Next** button to go to the PPPoE Internet connection settings page, see Figure 4-5.



The screenshot shows a web interface titled "WAN1 Settings". Under the heading "PPPoE Settings", there are two input fields: "User Name" and "Password". At the bottom of the form, there are three buttons: "Back", "Continue WAN2 Settings", and "Skip WAN2 Settings".

Figure 4-5 PPPoE Internet Connection Settings

- ✧ **User Name** and **Password**: They specify the PPPoE login user name and password provided by your ISP.
- **Back**: Click it to go back to the previous page of the **Quick Wizard**.
- **Continue WAN2 Settings**: Click it to continue to configure the Internet connection on the WAN2 interface if needed.
- **Skip WAN2 Settings**: Click it to go to the confirmation page at the end of the **Quick Wizard** if you don't want to configure another Internet connection in the **Quick Wizard**.

4.4.3 Static IP Internet Connection Settings

The screenshot shows a web interface titled "WAN1 Settings". Below the title, it says "Please Select WAN1 Connection Type". There are three radio button options: "PPPoE", "Static IP" (which is selected with a green dot), and "DHCP". At the bottom right, there are two buttons: "Back" and "Next".

Figure 4-6 Choosing Static IP as the Connection Type

In the page of choosing an Internet connection type (see Figure 4-6), select the **Static IP** radio button, and then click the **Next** button to go to the static IP Internet connection settings page, see Figure 4-7.

The screenshot shows the "WAN1 Settings" page with the "Static IP Settings" section. It contains five fields with their respective values: IP Address (192.168.1.55), Subnet Mask (255.255.255.0), Default Gateway (192.168.1.99), Primary DNS Server (200.200.200.251), and Secondary DNS Server (0.0.0.0). At the bottom, there are three buttons: "Back", "Continue WAN2 Settings", and "Skip WAN2 Settings".

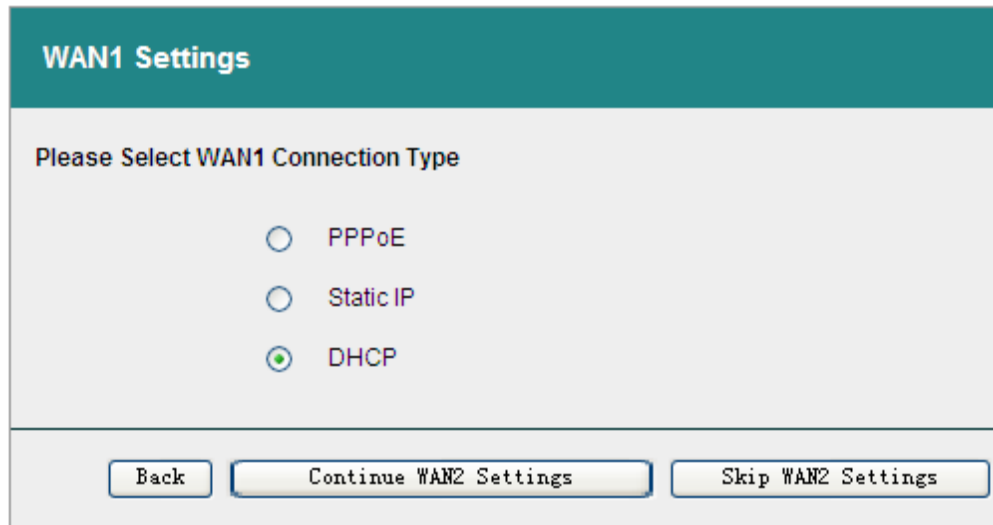
Figure 4-7 Static IP Internet Connection Settings

- ✧ **IP Address:** It specifies the IP address of the WAN interface, which is provided by your ISP.
- ✧ **Subnet Mask:** It specifies the subnet mask of the WAN interface, which is provided by your ISP.
- ✧ **Default Gateway:** It specifies the IP address of the default gateway, which is provided by your ISP.
- ✧ **Primary DNS Server:** It specifies the IP address of your ISP's primary DNS server.
- ✧ **Secondary DNS Server:** It specifies the IP address of your ISP's secondary DNS server. If it is available, you may set it. Else, please leave it 0.0.0.0.
- **Back:** Click it to go back to the previous page of the **Quick Wizard**.
- **Continue WAN2 Settings:** Click it to continue to configure the Internet connection on the WAN2 interface if needed.
- **Skip WAN2 Settings:** Click it to go to the confirmation page at the end of the **Quick Wizard** if you don't want to configure another Internet connection in the **Quick Wizard**.

**Note**

The WAN IP address and default gateway IP address should be on the same subnet. If they are not, please modify the **Subnet Mask** to make them be on the same subnet. If you don't have the subnet related knowledge, please ask a professional or UTT customer engineer for help.

4.4.4 DHCP Internet Connection Settings



The screenshot shows a web interface titled "WAN1 Settings". Below the title, it says "Please Select WAN1 Connection Type". There are three radio button options: "PPPoE", "Static IP", and "DHCP". The "DHCP" option is selected, indicated by a green dot in the center of the radio button. At the bottom of the form, there are three buttons: "Back", "Continue WAN2 Settings", and "Skip WAN2 Settings".

Figure 4-8 Choosing DHCP as the Connection Type

In the page of choosing an Internet connection type (see Figure 4-8), select the **DHCP** radio button, and then directly click the **Continue WAN2 Settings** button to continue to configure the Internet connection on the WAN2 interface if needed, or click the **Skip WAN2 Settings** button to the confirmation page at the end of the **Quick Wizard** if you don't want to configure another Internet connection in the **Quick Wizard**.

4.5 Reviewing and Saving the Settings

After you have finished configuring one or more Internet connections, you had better click the **Review Your Configuration** button in the **Quick Wizard**'s confirmation page to review the settings that you have made in the **Quick Wizard** firstly, and then modify any of them if desired, lastly click the **Finish** button to save the settings to make them take effect.

 **Note**

Do not forget to click the **Finish** button to save the settings you have made in the **Quick Wizard**, else the related settings will be discarded.

Configuration completed

Click "Finish" to finish setting, then you can surf online!
If you need modify the configuration, please click "Back".
In order to protect your network security, please go to **Security - Attack Defense**.

LAN Settings

IP Address:	192.168.16.1
Subnet Mask:	255.255.255.0

WAN1 Settings

Static IP

IP Address:	200.200.202.56
Subnet Mask:	255.255.255.0
Default Gateway:	200.200.202.254
Primary DNS Server:	200.200.200.251
Secondary DNS Server:	202.106.46.151

Figure 4-9 Viewing and Saving the Settings Made in the Quick Wizard

4.6 Summary

Once clicked the **Finish** button in the confirmation page, you have completed the configuration of the most basic features through the **Quick Wizard**. If you cannot access the Internet through the Device yet, please check whether all the settings that you have made in the **Quick Wizard** are correct. Also, you can go to the **Basic > WAN** page to view the Internet connection(s) status, view and modify the related configuration parameters.

Chapter 5 System Status

This chapter describes the system status related pages, which provide a lot of operating status information and statistics of the Device. By viewing them, the network administrator can easily analyze the system status and monitor the activities on the Device.

When NAT is enabled, the Device provides a set of powerful monitoring functions, which is divided into two categories: One is classification statistics, which can help the administrator find the problems that occurred in the network. The other is real-time monitoring, which can help the administrator analyze the occurring problem to find out in which host it happens, what the problem is, and the impact on other hosts.

The management of the Device operating status is divided into two levels:

- **Physical status:** The status and statistics for each physical interface, which includes operating status, ingress and egress traffic statistics, routing table, and so on.
- **NAT status:** The status and statistics for every LAN user (i.e., LAN host), which includes upload and download packets statistics, upload and download rate, total NAT sessions, and so on.

5.1 System Information

In the **Status > System Info** page, you may view some system information, which include system up time, system resource usage status, system version, port status, and interface rate chart.

5.1.1 System Up Time

System Up Time

System Time: 2010-12-21 9:59:9

System Up Time: 0 Day, 15 Hours, 12 Minutes, 25 Seconds

Figure 5-1 System Up Time

- ✧ **System Time:** It displays the system current date (YYYY-MM-DD) and time (HH:MM:SS).

- ✧ **System Up Time:** It displays the elapsed time (in days, hours, minutes and seconds) since the Device was last started.

5.1.2 System Resource

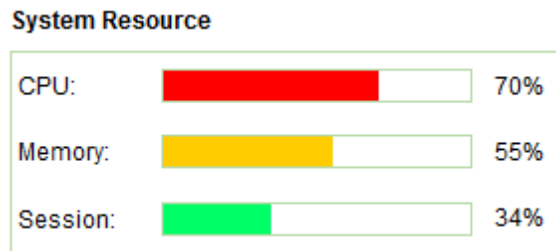


Figure 5-2 System Resource Usage Information

- ✧ **CPU:** The real-time CPU usage information, which is displayed as a status bar and percentage.
- ✧ **Memory:** The real-time memory usage information, which is displayed as a status bar and percentage.
- ✧ **Session:** The ratio of current active NAT sessions to the maximum sessions that the Device supports, which is displayed as a status bar and percentage.



Note

1. The color of the status bar indicates the usage percentage for each resource.
 - When the percentage is below 1%, the bar is blank.
 - When the percentage is between 1% and 50% (below 50%), the color is green.
 - When the percentage is between 50% and 70% (below 70%), the color is yellow.
 - When the percentage is equal to or above 70%, the color is red.
2. The above resources usage information indicates the load of the Device. If the usage percentages are all relatively low, it means that the Device still has the ability to process more tasks. If they are all very high, it means that the Device is nearly under the full load. In this case, the network delays may occur if the Device processes new

tasks.

5.1.3 System Version

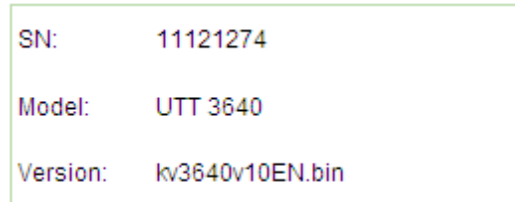


Figure 5-3 System Version

- ✧ **SN:** It displays the internal serial number of the Device, which may be different from the SN found on the label at the bottom of the Device.
- ✧ **Model:** It displays the product model of the Device.
- ✧ **Version:** It displays the version of ReOS firmware running on the Device.

5.1.4 Port Information

5.1.4.1 Port Status

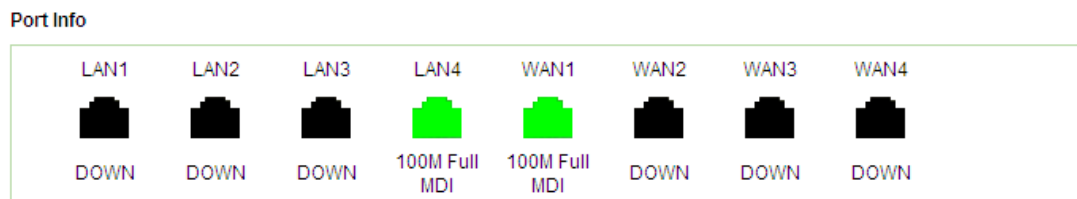


Figure 5-4 Port Status

The port status figure indicates whether each physical port of the Device is active (Up) or inactive (Down). If a port is down, it is shaded black. Else it is shaded green, and its speed, duplex and MDI or MDI-X status are displayed. See Figure 5-4, the LAN4 and WAN1 ports are active.

5.1.4.2 Interface Rate Chart

The interface rate chart dynamically displays the real-time RX/TX rate, average RX/TX rate, maximum RX/TX rate and total RX/TX traffic of each physical interface. If you want to view the rate chart of an interface, click the corresponding interface name hyperlink.

In the interface rate chart, the abscissa (x-axis) shows the time axis, and the ordinate (y-axis) shows the real-time RX/TX rate axis. Furthermore, you can adjust some parameters of the chart if needed, such as the time interval during which the real-time rates are calculated and displayed, and the displayed colors. Note: The rate chart can only show the rate and traffic information in the last ten minutes. Each time you open this page, the rate chart starts anew.



Figure 5-5 Interface Rate Chart

- ✧ **RX:** It indicates the real-time RX rate of the physical interface, which is calculated every two seconds. For the LAN interface, RX means uploading; for the WAN interface, it means downloading.
- ✧ **TX:** It indicates the real-time TX rate of the physical interface, which is calculated every two seconds. For the LAN interface, TX means downloading; for the WAN interface, it means uploading.
- ✧ **Avg:** It indicates the average RX or TX rate of the physical interface since last opened the current page.
- ✧ **Peak:** It indicates the maximum RX or TX rate of the physical interface since last

opened the current page.

- ✧ **Total:** It indicates the total RX or TX traffic of the physical interface since last opened the current page.
- **LAN/WANx:** It allows you to click the interface name hyperlink to view the rate chart of the selected interface. Therein, x (value: 1, 2, 3, 4) indicates the corresponding WAN interface, and the number of WAN interfaces depends on the specific product model. For example, click the **WAN1** hyperlink to view the rate chart of the WAN1 interface.



Note

If the SVG Viewer isn't installed on your PC, the rate chart cannot be displayed properly. To view the rate chart, click the **(Please install svgviewer if the page cannot display properly.)** hyperlink to download and install the SVG Viewer.

5.2 NAT Statistics

Through the **NAT Statistics** list in the **Status > NAT Stats** page, you can view the NAT session details for each LAN user (host).

ID	Description	IP Address	Active Sessions	Overflow	Rx Packets	Tx Packets	Tx Broadcast Packets	Total Sessions
1		10.0.0.1	0	0	0	547	0	177
2		192.168.16.1	0	0	0	1	0	1
3		10.0.0.2	0	0	0	1061	0	277
4		10.0.0.3	1	0	23	24	1	1
5		200.200.202.54	0	0	0	31	0	2
6		192.168.16.55	0	0	0	2	0	2
7		192.168.16.68	60	0	42026	45598	0	553
8		200.200.202.95	0	0	0	31	0	2
9		200.200.202.132	3	0	2636	4899	0	30
10		192.168.1.1	0	0	0	15	0	2
11		192.168.0.1	0	0	0	29	0	2
12		58.26.245.9	0	0	0	154	0	51
13		58.26.245.10	0	0	0	642	0	219
14		58.26.245.11	0	0	0	309	0	105
15		58.26.245.23	0	0	0	111	0	43

Figure 5-6 NAT Statistics List

- ✧ **ID:** It is used to identify each entry in the list.
- ✧ **Description:** If the LAN user is an IP/MAC binding user, it displays the description of the user; else it is blank.
- ✧ **IP Address:** It displays the IP address of the LAN host.
- ✧ **Active Sessions:** It displays the number of NAT sessions that are being used by the LAN host now.
- ✧ **Overflow:** It displays the cumulative count of the LAN host's overflowing requests due to the maximum sessions limit. The maximum sessions can be configured in the **Security > NAT Session Limit** page.
- ✧ **Rx Packets:** It displays the number of packets downloaded by the LAN host through NAT function.

- ✧ **Tx Packets:** It displays the number of packets uploaded by the LAN host through NAT function.
- ✧ **Tx Broadcast Packets:** It displays the number of broadcast and multicast packets transmitted from the LAN host to the Device.
- ✧ **Total Sessions:** It displays the total number of NAT sessions of the LAN host, which include those sessions that aren't being used now.
- **Clear:** Click it to clear the NAT statistics in the list, which include **Overflow**, **Rx Packets**, **Tx Packets**, **Tx Broadcast Packets** and **Total Sessions**.
- **Refresh:** Click it to view the latest information in the list.

**Note**

1. The NAT session limit feature can help the Device prevent some types of network attacks. If a user's **Total Sessions** has reached the maximum value (configured in the **Security > NAT Session Limit** page), any further request for creating a new session will be discarded, and the **Overflow** will be updated synchronously. In this case, the administrator can find potential DDoS attacks by viewing the logs in the **Status > System Log** page.
2. The most **Rx Packets** means the corresponding user has downloaded the most packets from the Internet.
3. The most **Tx Packets** means the corresponding user has uploaded the most packets to the Internet.
4. The most **Active Sessions** means the corresponding user is the most active now.
5. If the **Overflow** is larger than 100, or the **Tx Packets** is far larger than the **Rx Packets**, this host is suspicious of using port scanner software now.
6. If the **Tx Packets** is very large, but the **Rx Packets** is very small or zero, this host is suspicious of performing a DoS/DDoS attack.

5.3 DHCP Statistics

This section describes the **Status > DHCP Stats** page, including the **DHCP Pool Statistics** list, **DHCP Server Statistics** list, **DHCP Conflict Statistics** list, **DHCP Client Statistics** list and **DHCP Relay Statistics** list.

5.3.1 DHCP Pool Statistics List

The **DHCP Pool Statistics** list displays the usage information of each DHCP address pool, including IP address and subnet mask, associated MAC address, lease left, DHCP address pool name, status of IP address, and so on.

It allows you to manually bind one or more dynamic IP addresses to the corresponding MAC addresses. The steps are as follows: Click the leftmost check boxes of the entries you want to bind, and then click the **Bind** button to bind the selected IP and MAC address pairs. Then you may go to the **Advanced > DHCP > DHCP Server** or **Security > IP/MAC Binding** page to view or modify them.

ID	IP Address	Subnet Mask	MAC Address	Lease Left	Pool Name	Status	Type	Client ID	Relay Agent ID
<input type="checkbox"/>	200.200.202.102	255.255.255.0	0022a90de509	0:01:00:32	132	Assigned	Dynamic		
<input type="checkbox"/>	200.200.202.101	255.255.255.0	002185c5f8ce	0:01:00:30	132	Conflicted	Dynamic		

Figure 5-7 DHCP Pool Statistics List

- ✧ **ID:** It is used to identify each entry in the list.
- ✧ **IP Address:** It displays the IP address of the DHCP client.
- ✧ **Subnet Mask:** It displays the subnet mask of the DHCP client.
- ✧ **MAC Address:** It displays the MAC address of the DHCP client.
- ✧ **Lease Left:** It displays the time remaining until the current IP address lease expires,

shown as DD: HH: MM: SS.

- ✧ **Pool Name:** It displays name of the DHCP address pool.
- ✧ **Status:** It displays the status of the IP address. The possible values are **Detecting**, **Assigned**, and **Conflicted**.
 - **Detecting:** It indicates that the DHCP server is detecting whether the IP address is already in use or not.
 - **Assigned:** It indicates that the DHCP server has assigned the IP address to the client.
 - **Conflicted:** It indicates that the DHCP server has detected a conflict for the IP address, i.e., there is another host on the network using the same IP address.
- ✧ **Type:** It displays the manner in which the IP address was assigned to the DHCP client. The possible values are **Static** and **Dynamic**.
 - **Static:** It indicates that the IP address was assigned manually through DHCP manual binding.
 - **Dynamic:** It indicates that the IP address was assigned dynamically from a DHCP address pool by the DHCP sever.
- ✧ **Client ID:** It displays the client identifier of the DHCP client.
- ✧ **Relay Agent ID:** It displays the relay agent ID of the DHCP client.
- **Bind:** If you want to manually bind one or more dynamic IP addresses to the corresponding MAC addresses, select the leftmost check boxes of them, and then click the **Bind** button. Then you may go to the **Advanced > DHCP > DHCP Server** or **Security > IP/MAC Binding** page or to view and modify those IP/MAC bindings.
- **Refresh:** Click it to view the latest information in the list.
- **Display IP/MAC Binding:** Click it to go to the **Security > IP/MAC Binding** page to view or configure IP/MAC bindings for the LAN hosts.



Note

In the **DHCP Pool Statistics** list, only the dynamic IP addresses can be bound manually, but the static IP addresses cannot be bound again.

5.3.2 DHCP Server Statistics List

The **DHCP Server Statistics** list displays the DHCP server statistics, which includes the number of each type of DHCP message and the number of assigned IP addresses. The statistics is counted and displayed per physical interface.

DHCP Server Statistics												
Interface	Discover	Offer	Request	Ack	Release	Decline	Nak	Conflict	Inform	Unknown	Client	
LAN1	1	1	4	1	0	0	0	0	0	0	1	
WAN1	83	1	1	1	0	0	0	1	0	0	84	
WAN2(DMZ)	0	0	0	0	0	0	0	0	0	0	0	
WAN3	0	0	0	0	0	0	0	0	0	0	0	
WAN4	0	0	0	0	0	0	0	0	0	0	0	

Figure 5-8 DHCP Server Statistics List

- ✧ **Interface:** The physical interface on which the DHCP server is applied.
- ✧ **Discover:** During the statistics interval, the number of DHCPDISCOVER messages that were received by the DHCP server.
- ✧ **Offer:** During the statistics interval, the number of DHCPOFFER messages that were sent by the DHCP server.
- ✧ **Request:** During the statistics interval, the number of DHCPREQUEST messages that were received by the DHCP server.
- ✧ **Ack:** During the statistics interval, the number of DHCPACK messages that were sent by the DHCP server.
- ✧ **Release:** During the statistics interval, the number of DHCPRELEASE messages that were received by the DHCP server.
- ✧ **Decline:** During the statistics interval, the number of DHCPDECLINE messages that were received by the DHCP server.
- ✧ **Nak:** During the statistics interval, the number of DHCPNAK messages that were sent by the DHCP server.
- ✧ **Conflict:** During the statistics interval, the number of address conflicts that were detected by the DHCP server.

- ✧ **Inform:** During the statistics interval, the number of DHCPINFORM messages that were received by the DHCP server.
- ✧ **Unknown:** During the statistics interval, the number of unknown packets.
- ✧ **Client:** During the statistics interval, the number of IP addresses that were assigned by the DHCP server.
- **Clear:** Click it to clear the DHCP server statistics in the list.
- **Refresh:** Click it to view the latest information in the list.



Note

The statistics interval is the elapsed time since the last clear action.

5.3.3 DHCP Conflict Statistics List

The **DHCP Conflict Statistics** list displays information related to the address conflicts found by the DHCP server, which include the conflicted IP address, MAC address, the detection method and detection time for each address conflict in the list.

DHCP Pool Statistics DHCP Server Statistics DHCP Conflict Statistics DHCP Client Statistics DHCP Relay Statistics						
1/1	Lines Page: 10	First	Prev	Next	Last	Search: <input type="text"/>
IP Address	MAC Address	Detection Method		Detection Time		
200.200.202.101	002185c5f5ce	ARP		1990-01-01 00:00:10		

Figure 5-9 DHCP Conflict Statistics List

- ✧ **IP Address:** It displays the conflicted IP address.
- ✧ **MAC Address:** It displays the MAC address of the LAN host where the IP address conflict occurred.
- ✧ **Detection Method:** It displays how the IP address conflict was detected. It may be

ARP or ICMP.

- ✧ **Detection Time:** It displays the date (YYYY-MM-DD) and time (HH:MM:SS) when the IP address conflict was detected.
- **Refresh:** Click it to view the latest information in the list.

5.3.4 DHCP Client Statistics List

The **DHCP Client Statistics** list displays the DHCP client statistics, which mainly includes the number of each type of DHCP message. The statistics is counted and displayed per physical interface.

DHCP Client Statistics										
Interface	Discover	Offer	Request	Ack	Release	Decline	Nak	Conflict	Inform	Unknown
LAN	0	0	0	0	0	0	0	0	0	0
WAN1	0	0	0	0	0	0	0	0	0	0
WAN2(DMZ)	2	1	1	1	0	0	0	0	0	0
WAN3	4	0	0	0	0	0	0	0	0	0
WAN4	2	15	1	1	0	0	0	0	0	0

Figure 5-10 DHCP Client Statistics List

- ✧ **Interface:** The physical interface on which the DHCP client is applied.
- ✧ **Discover:** During the statistics interval, the number of DHCPDISCOVER messages that were sent by the DHCP client.
- ✧ **Offer:** During the statistics interval, the number of DHCPOFFER messages that were received by the DHCP client.
- ✧ **Request:** During the statistics interval, the number of DHCPREQUEST messages that were sent by the DHCP client.
- ✧ **Ack:** During the statistics interval, the number of DHCPACK messages that were received by the DHCP client.
- ✧ **Release:** During the statistics interval, the number of DHCPRELEASE messages that were sent by the DHCP client.

- ✧ **Decline:** During the statistics interval, the number of DHCPDECLINE messages that were sent by the DHCP client.
- ✧ **Nak:** During the statistics interval, the number of DHCPNAK messages that were received by the DHCP client.
- ✧ **Conflict:** During the statistics interval, the number of address conflicts that were found by the DHCP server when trying to assign an address to the DHCP client.
- ✧ **Inform:** During the statistics interval, the number of DHCPINFORM messages that were sent by the DHCP client.
- ✧ **Unknown:** During the statistics interval, the number of unknown packets.
- **Clear:** Click it to clear the DHCP client statistics in the list.
- **Refresh:** Click it to view the latest information in the list.



Note

The statistics interval is the elapsed time since the last clear action.

5.3.5 DHCP Relay Statistics List

The **DHCP Relay Statistics** list displays the DHCP relay agent statistics, which includes the number of various types of DHCP messages. The statistics is counted and displayed per physical interface.

Interface	Discover	Offer	Request	Ack	Release	Decline	Nak	Inform	Nadd	Nreplace	Drop
LAN	0	0	3	0	0	0	0	0	0	0	0
WAN1	0	0	0	0	0	0	0	0	0	0	0
WAN2(DMZ)	11	0	0	0	0	0	0	0	0	0	0
WAN3	0	0	0	0	0	0	0	0	0	0	0
WAN4	0	0	0	0	0	0	0	0	0	0	0

Clear Refresh

Figure 5-11 DHCP Relay Statistics List

- ✧ **Interface:** The physical interface on which the DHCP relay agent is applied.

- ✧ **Discover:** During the statistics interval, the number of DHCPDISCOVER messages that were relayed by the DHCP relay agent.
- ✧ **Offer:** During the statistics interval, the number of DHCPOFFER messages that were relayed by the DHCP relay agent.
- ✧ **Request:** During the statistics interval, the number of DHCPREQUEST messages that were relayed by the DHCP relay agent.
- ✧ **Ack:** During the statistics interval, the number of DHCPACK messages that were relayed by the DHCP relay agent.
- ✧ **Release:** During the statistics interval, the number of DHCPRELEASE messages that were relayed by the DHCP relay agent.
- ✧ **Decline:** During the statistics interval, the number of DHCPDECLINE messages that were relayed by the DHCP relay agent.
- ✧ **Nak:** During the statistics interval, the number of DHCPNAK messages that were relayed by the DHCP relay agent.
- ✧ **Inform:** During the statistics interval, the number of DHCPINFORM messages that were relayed by the DHCP relay agent.
- ✧ **Nadd:** During the statistics interval, the number of DHCP messages to which relay information wasn't added because of the maximum packet size limit.
- ✧ **Nreplace:** During the statistics interval, the number of DHCP messages in which relay information wasn't replaced because of the maximum packet size limit.
- ✧ **Drop:** During the statistics interval, the number of DHCP messages that were dropped by the DHCP relay agent.
- **Clear:** Click it to clear the DHCP client statistics in the list.
- **Refresh:** Click it to view the latest information in the list.

**Note**

The statistics interval is the elapsed time since the last clear action.

5.4 Interface Statistics

The **Interface Statistics** list displays the traffic statistics of each physical interface, including the number of bytes, unicast packets, and non-unicast (i.e., multicast and broadcast) packets.

ID	Interface/Direction	Total Bytes	Unicast	Non-unicast
0	LAN1/In	1273108	7688	183
0	LAN1/Out	7728514	9660	0
1	WAN1/In	11556437	6992	70800
1	WAN1/Out	626019	6504	0
2	WAN2(DMZ)/In	13034	100	13
2	WAN2(DMZ)/Out	10158	126	0
3	WAN3/In	0	0	0
3	WAN3/Out	0	0	0
4	WAN4/In	0	0	0
4	WAN4/Out	0	0	0

Figure 5-12 Interface Statistics List

- ✧ **ID:** It is used to identify each interface of the Device.
- ✧ **Interface/Direction:** It displays the physical interface and the traffic direction.
 - **In:** The packets are received by the interface.
 - **Out:** The packets are transmitted by the interface.
- ✧ **Total Bytes:** During the statistics interval, the number of bytes that were received or transmitted by the interface.
- ✧ **Unicast:** During the statistics interval, the number of unicast packets that were received or transmitted by the interface.
- ✧ **Non-unicast:** During the statistics interval, the number of broadcast and multicast packets that were received or transmitted by the interface.
- **Clear:** Click it to clear the interfaces statistics in the list.
- **Refresh:** Click it to view the latest information in the list.



Note

1. The statistics interval is the elapsed time since the last clear action.

2. The following characteristics indicate that the Device is in normal operation:
 - The number of packets received by the WAN interface(s) is close to those transmitted by the LAN interface.

 - The number of bytes received by the WAN interface(s) is close to those transmitted by the LAN interface.

 - The number of packets transmitted by the WAN interface(s) is close to those received by the LAN interface.

 - The number of bytes transmitted by the WAN interface(s) is close to those received by the LAN interface.

 - The total network traffic is steady without sharp wave.

5.5 Routing Table

This section describes how to view and use the **Routing Table** in the **Status > Route Stats** page.

A router (or gateway) is a device that forwards data packets along networks. One of the basic functions of the router is the ability to select an optimal transmission path for each received packet, and forward the packet to the destination site effectively. The router uses the routing table, which lists the routes to particular network destinations, to accomplish this function. The routing table can be built and updated manually by the system administrator, or dynamically by the router with minimal or no manual intervention.

Routing Table

21/21 Lines/Page: 20 First Prev Next Last Search:

Destination IP/Mask	Gateway IP	Interface	Flag	Priority	Metric	Use	Age
0.0.0.0	200.200.202.254	ie1	lugaofF	60	1	179	54
0.0.0.0	-	ptpdial0	*luga	120	7	0	54
127.0.0.0/8	-	bhole0	cup	20	0	0	56
127.0.0.1/32	-	local	cuhp	20	0	0	56
127.0.0.2/32	-	reject0	cuhp	20	0	0	56
127.0.0.3/32	-	bhole0	cuhp	20	0	0	56
192.168.16.0/24	-	ie0	cuu	20	0	23	56
192.168.16.1/32	-	local	cuhp	20	0	10	56
192.168.16.0/24	-	ie2	cuu	20	0	2	56
192.168.16.1/32	-	local	cuhp	20	0	0	56
200.200.202.0/24	-	ie1	cuafF	20	0	210	54
200.200.202.134/32	-	local	cuhp	20	0	300	54
224.0.0.0/4	-	mcast	cup	20	0	0	56
224.0.0.1/32	-	local	cuhp	20	0	0	56
224.0.0.2/32	-	local	cuhp	20	0	0	56
224.0.0.5/32	-	bhole0	cuhp	20	0	0	56
224.0.0.6/32	-	bhole0	cuhp	20	0	0	56
224.0.0.8/32	-	local	cuhp	20	0	0	56
224.0.0.18/32	-	bhole0	cuhp	20	0	0	56
239.255.255.250/32	-	local	cuhp	20	0	0	56

Display Route Settings Refresh

Figure 5-13 Routing Table

- ✧ **Destination IP/Mask:** It indicates the destination network ID. The **Destination IP** indicates the IP address of the destination network or destination host; and the **Mask** indicates the subnet mask associated with the destination network. For example, **192.168.18.0/24** means that the destination network IP address is **192.168.18.0**, and subnet mask is **255.255.255.0**.
- ✧ **Gateway IP:** It displays the IP address of the next hop gateway or router to which to

forward the packets.

- ✧ **Interface:** It displays the outbound interface through which the packets are forwarded to the next hop gateway or router.
 - **ie0:** LAN interface; **ie1:** WAN1 interface; **ie2:** WAN2 interface;
 - **ptpdial0:** Virtual interface waiting for dialing;
 - **ptpx:** Virtual interface x (value: 1, 2, 3...);
 - **bhole0:** Internal interface, the Device will discard any packet forwarded to this interface;
 - **local:** Internal soft-route interface, the packets are forwarded to the Device itself;
 - **reject:** Internal interface, the Device will discard any packet forwarded to this interface and respond an ICMP unreachable packet;
 - **loopback:** Indicates the loopback network with network ID 127.0.0.0/8;
 - **mcast:** Virtual interface, multicast packets will be forwarded to it.
- ✧ **Flag:** *-Hidden, o-OSPF, i-ICMP, l-Local, r-RIP, n-SNMP, c-Connected, s-Static, R-Remote, g-Gateway, h-Host, p-Private, u-Up, t-Temp, M-Multiple, N-NAT, F-Float, a-Append,?-Unknown.
 - ***-Hidden:** The route is inactive as it is backup, or the corresponding Internet connection is inactive.
 - **N-NAT:** NAT is enabled on the route, and the LAN hosts are sharing the corresponding Internet connection to access the Internet.
 - **F-Float:** The priority related parameters of the route has been configured, and it is floating now. Whether to enable it or not is determined by the corresponding Internet connection's working status.
- ✧ **Priority:** It indicates the priority of the route. If there are multiple routes to the same destination with different priorities, the Device will choose the route with the highest priority to forward the packets. The smaller the value, the higher the priority.
- ✧ **Metric:** It indicates the cost of using the route, which is typically the number of hops to the destination. If there are multiple routes with same priority to the same

destination, the Device will choose the route with the lowest metric to forward the packets.

- ✧ **Use:** It indicates count of lookups for the route.
- ✧ **Age:** It indicates the elapsed time (in seconds) since the route was created in the routing table.
- **Refresh:** Click it to view the latest information in the list.
- **Display Route Settings:** Click it to go to the **Advanced > Static Route > Static Route List** page to view the configured static routes settings.

Taking Figure 5-13 as an example, the following describes the different types of routes:

- ✧ **0.0.0.0/0:** It indicates a default static route. The Device uses a default route if no other route matches the destination address included in a packet. The default route forwards the packet to a default gateway, whose IP address is configured manually or assigned dynamically by a PPPoE or DHCP server.
- ✧ **127.0.0.0/8:** It indicates a loopback route. The Class A network 127.0.0.0 is defined as the loopback network. Addresses from that network are assigned to interfaces that process data within the local system. These loopback interfaces do not access a physical network. Once received a packet which matches the route, the Device will send the packet to itself.
- ✧ **200.200.202.0/24:** It indicates a subnet route. The destination is a subnet. If no host route matches the destination IP address included in a packet, the Device will use a subnet route that matches the network ID of the destination IP address. The subnet route forwards the packet to its gateway.
- ✧ **192.168.16.1/32:** It indicates a local host route (its interface is local). Once received a packet which matches the route, the Device will not forward it.
- ✧ **224.0.0.0/4:** It indicates a multicast route. Once received a multicast packet, the Device will make copies and send them to all receivers that have joined the corresponding multicast group.

5.6 Session Monitor

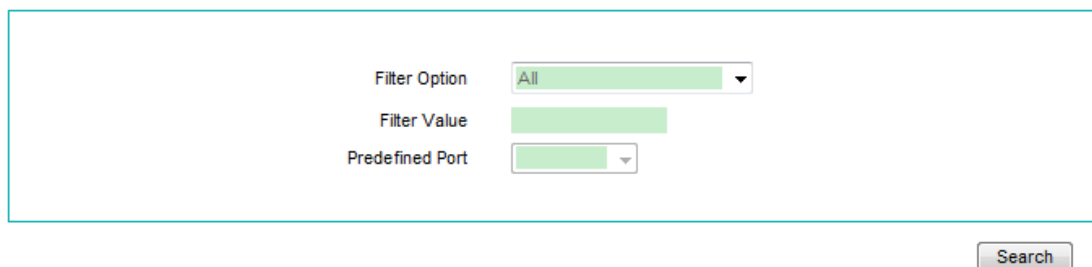
This section describes the **Status > Session Monitor** page, and it tells you how to monitor the Internet activities of the LAN users by the **NAT Session List**. This page displays the active NAT sessions on the Device, and it lets you filter and display sessions by certain criteria, such as source IP address, destination IP address/domain name, destination port, NAT translated IP address/domain name, and so on. It only displays the NAT sessions that are currently used by the LAN hosts, but doesn't display NAT statistics.

When receiving a request initiated by a LAN host, the Device will create a NAT session for the request to translate the host's local IP address to a public IP address. The NAT will translate incoming as well as outgoing packets belonging to the session.

Note

Only the administrator who has **Admin** privileges can open this page. You can go to the **System > Administrator** page to view and modify the administrator's privileges.

5.6.1 Session Monitor Settings



The screenshot shows a web form for Session Monitor Settings. It contains three input fields: 'Filter Option' (a dropdown menu with 'All' selected), 'Filter Value' (a text input field), and 'Predefined Port' (a dropdown menu). A 'Search' button is located at the bottom right of the form.

Figure 5-14 Session Monitor Settings

- ✧ **Filter Option:** It specifies an option for filtering and displaying the NAT sessions.
- **All:** Select it to display all the active NAT sessions on the Device. You can use this option to search the Internet activities of all the LAN users.
 - **WANx:** Select a WAN interface to display the active NAT sessions related to the interface. You can use this option to search the Internet activities of the LAN users who are using the Internet connection on the selected interface to access the Internet. Therein, x (value: 1, 2, 3, 4) indicates the corresponding WAN interface, and the number of WAN interfaces depends on the specific product

model.

- **Source IP:** Select it to display the active NAT sessions related to a LAN user, which is specified by entering his or her IP address in the **Filter Value** text box. You can use this option to search the Internet activities of the specified LAN user.
 - **Destination IP/Domain:** Select it to display the active NAT sessions related to an Internet site, which is specified by entering its IP address or domain name in the **Filter Value** text box. You can use this option to search the LAN users who are accessing the specified website.
 - **Destination Port:** Select it to display the active NAT sessions related to a network service, which is specified by entering the service port number in the **Filter Value** text box. You can use this option to search the LAN users who are accessing the specified service. The following provides port numbers of some well-known services: ftp-TCP21, ssh-TCP22, telnet-TCP23, smtp-TCP25, dns-UDP53, finger-TCP79, http-TCP80, pop3-TCP110, snmp-UDP161, etc. For more information, please refer to **Appendix D Common Service Ports**.
 - **NAT Translated IP/Domain:** Select it to display the active NAT sessions related to an Internet connection's IP address or domain name, which is specified in the **Filter Value** text box. When using multi-NAT (that is, you get multiple public IP addresses from your ISP), you can use this option to search the Internet activities of the LAN users who are using the specified public IP address to access the Internet.
- ✧ **Filter Value:** It specifies the filter value for filtering and displaying the NAT sessions. You should specify it according to the selected **Filter Option**.
- ✧ **Predefined Port:** It provides port numbers of some well-known services for you to choose. If you select **Destination Port** from the **Filter Option** drop-down list, you may select a service port number here.
- **Search:** After specifying the **Filter Option** and **Filter Value** (if needed), click the **Search** button to search and display all the active NAT sessions in accordance with your criteria in the **NAT Session List**.

5.6.2 NAT Session List

NAT Session List		Session Monitor Settings							
ID	Source IP	Source Port	Protocol	Dest IP	Dest Port	Tx Pkts	Rx Pkts	NAT IP	NAT Port
1	192.168.16.65	1660	T	200.200.200.251	139	1	3	200.200.202.134	1065
2	192.168.16.65	1665	T	207.46.124.166	msn	20	20	200.200.202.134	1048
3	192.168.16.65	1331	T	207.46.124.166	msn	41	42	200.200.202.134	1291
4	192.168.16.65	1292	T	99.163.197.242	52029	199	207	200.200.202.134	1238
5	192.168.16.65	1211	T	200.200.200.251	139	1	3	200.200.202.134	1060
6	192.168.16.65	4018	T	200.200.200.251	139	1	3	200.200.202.134	1070
7	192.168.16.65	3835	T	200.200.200.251	139	1	3	200.200.202.134	1093
8	192.168.16.65	3145	T	64.4.44.76	msn	376	254	200.200.202.134	1198
9	192.168.16.65	3122	T	200.200.200.228	445	169	158	200.200.202.134	1102
10	192.168.16.65	4025	T	200.200.200.251	139	1	3	200.200.202.134	1411
11	192.168.16.65	2708	T	200.200.200.129	139	1	3	200.200.202.134	1604
12	192.168.16.65	2331	T	200.200.200.251	139	1	3	200.200.202.134	1076
13	192.168.16.65	1899	T	200.200.200.228	445	3926	4572	200.200.202.134	1059
14	192.168.16.65	1061	T	207.46.124.64	msn	821	535	200.200.202.134	1145
15	192.168.16.68	3888	T	200.200.200.228	445	19	17	200.200.202.134	1062
16	192.168.16.68	512	I	200.200.200.228	1051	1	1	200.200.202.134	1061
17	192.168.16.68	63192	U	200.200.200.251	dns	1	1	200.200.202.134	1059
18	192.168.16.68	3859	T	200.200.200.129	445	128	125	200.200.202.134	1058
19	192.168.16.68	512	I	200.200.200.129	1057	1	1	200.200.202.134	1057
20	192.168.16.68	54763	U	200.200.200.251	dns	1	1	200.200.202.134	1056

Figure 5-15 NAT Session List

- ✧ **ID:** It is used to identify each entry in the list.
- ✧ **Source IP:** It displays the source IP address for the NAT session.
- ✧ **Source Port:** It displays the source port number for the NAT session.
- ✧ **Protocol:** It displays the protocol type (T:TCP, U:UDP, I:ICMP) or protocol number for the NAT session.
- ✧ **Dest IP:** It displays the destination IP address for the NAT session.
- ✧ **Dest Port:** It displays the destination port number or service name for the NAT session. There are some system predefined services, such as dns, ftp, www, smtp, pop3, msn, and so on.
- ✧ **Tx Pkts:** It displays the number of transmitted packets through the NAT session.
- ✧ **Rx Pkts:** It displays the number of received packets through the NAT session.
- ✧ **NAT IP:** The translated public IP address for the NAT session.
- ✧ **NAT Port:** The translated port for the NAT session. The Device uses this port number

to keep track of which hosts initiate data transfer. By keeping this record, the Device is able to correctly route responses.

- **Clear:** Click it to delete all of the dynamic NAT sessions in the list.



Note

The clear operation may disconnect the dynamic sessions that are being used now, so do it with caution.

5.6.3 Examples

5.6.3.1 Searching Internet Activities of the LAN User with IP Address 192.168.16.68/24

- Step 1** Go to the **Status > Session Monitor** page, see Figure 5-16.
- Step 2** Select **Source IP** from the **Filter Option** drop-down list.
- Step 3** Enter **192.168.16.68** in the **Filter Value** text box.
- Step 4** Click the **Search** button to search and display all the matching NAT sessions in the **NAT Session List**, see Figure 5-17.

The screenshot shows the 'Session Monitor Settings' page. At the top, there are two tabs: 'NAT Session List' (highlighted in yellow) and 'Session Monitor Settings'. Below the tabs, there are three filter fields: 'Filter Option' with a dropdown menu showing 'Source IP', 'Filter Value' with a text input field containing '192.168.16.68', and 'Predefined Port' with an empty dropdown menu. A 'Search' button is located at the bottom right of the form area.

Figure 5-16 Session Monitor Settings - Example1

Figure 5-18 Session Monitor Settings - Example2

The screenshot shows the 'Session Monitor Settings' tab in a web interface. At the top, there are two tabs: 'NAT Session List' and 'Session Monitor Settings'. Below the tabs, there are navigation controls: 'Lines/Page: 20', 'First', 'Prev', 'Next', 'Last', and a 'Search:' field. The main content is a table with the following columns: ID, Source IP, Source Port, Protocol, Dest IP, Dest Port, Tx Pkts, Rx Pkts, NAT IP, and NAT Port. The table contains 8 rows of data, all with Protocol 'T' and Dest IP '200.200.200.251'. The NAT IP is '200.200.202.134' for all rows. The NAT Port varies from 1085 to 1055. A 'Clear' button is located at the bottom right of the table.

ID	Source IP	Source Port	Protocol	Dest IP	Dest Port	Tx Pkts	Rx Pkts	NAT IP	NAT Port
1	192.168.16.65	1660	T	200.200.200.251	139	1	3	200.200.202.134	1085
2	192.168.16.65	1211	T	200.200.200.251	139	1	3	200.200.202.134	1060
3	192.168.16.65	4018	T	200.200.200.251	139	1	3	200.200.202.134	1070
4	192.168.16.65	3835	T	200.200.200.251	139	1	3	200.200.202.134	1083
5	192.168.16.65	4026	T	200.200.200.251	139	1	3	200.200.202.134	1411
6	192.168.16.65	2708	T	200.200.200.129	139	1	3	200.200.202.134	1604
7	192.168.16.65	2331	T	200.200.200.251	139	1	3	200.200.202.134	1076
8	192.168.16.68	3658	T	200.200.200.251	139	1	3	200.200.202.134	1055

Figure 5-19 NAT Session List - Example2

5.6.3.3 Searching the LAN Users Using MSN

- Step 1** Go to the **Status > Session Monitor** page, see Figure 5-20.
- Step 2** Select **Destination Port** from the **Filter Option** drop-down list.
- Step 3** Enter **1863** in the **Filter Value** text box, or select **1863 (MSN)** option from the **Predefined Port** drop-down list directly.
- Step 4** Click the **Search** button to search and display all the matching NAT sessions in the **NAT Session List**, see Figure 5-21.

When using multiple Internet connections, you can go to the **Basic > WAN** page to view the **WAN List** to find the WAN1 IP address.

- Step 1** Go to the **Status > Session Monitor** page, see Figure 5-22.
- Step 2** Select the **NAT Translated IP/Domain** from the **Filter Option** drop-down list.
- Step 3** Enter **200.200.202.134** in the **Filter Value** text box. The WAN1 IP address is 200.200.202.134 in this example.
- Step 4** Click the **Search** button to search and display all the matching NAT sessions in the **NAT Session List**, see Figure 5-23.

NAT Session List
Session Monitor Settings

Filter Option NAT Translated IP/Domain ▼

Filter Value 200.200.202.134

Predefined Port ▼

Search

Figure 5-22 Session Monitor Settings - Example3

NAT Session List
Session Monitor Settings

27/27 Lines/Page: 20 ▼ First Prev Next Last Search:

ID	Source IP	Source Port	Protocol	Dest IP	Dest Port	Tx Pkts	Rx Pkts	NAT IP	NAT Port
1	192.168.16.65	1660	T	200.200.200.251	139	1	3	200.200.202.134	1085
2	192.168.16.65	1655	T	207.46.124.165	msn	20	20	200.200.202.134	1048
3	192.168.16.65	1331	T	207.46.124.168	msn	41	42	200.200.202.134	1291
4	192.168.16.65	1282	T	99.183.197.242	52029	199	207	200.200.202.134	1238
5	192.168.16.65	1211	T	200.200.200.251	139	1	3	200.200.202.134	1050
6	192.168.16.65	4018	T	200.200.200.251	139	1	3	200.200.202.134	1070
7	192.168.16.65	3835	T	200.200.200.251	139	1	3	200.200.202.134	1093
8	192.168.16.65	3145	T	64.4.44.78	msn	375	254	200.200.202.134	1198
9	192.168.16.65	3122	T	200.200.200.228	445	169	158	200.200.202.134	1102
10	192.168.16.65	4026	T	200.200.200.251	139	1	3	200.200.202.134	1411
11	192.168.16.65	2708	T	200.200.200.129	139	1	3	200.200.202.134	1604
12	192.168.16.65	2331	T	200.200.200.251	139	1	3	200.200.202.134	1076
13	192.168.16.65	1899	T	200.200.200.228	445	3926	4572	200.200.202.134	1069
14	192.168.16.65	1061	T	207.46.124.64	msn	821	535	200.200.202.134	1145
15	192.168.16.68	3689	U	200.200.200.129	389	1	1	200.200.202.134	1034
16	192.168.16.68	63193	U	200.200.200.251	dns	1	1	200.200.202.134	1033
17	192.168.16.68	137	U	200.200.200.129	137	6	0	200.200.202.134	1031
18	192.168.16.68	512	I	200.200.200.129	1030	2	2	200.200.202.134	1030
19	192.168.16.68	3695	T	200.200.200.228	445	24	22	200.200.202.134	1062
20	192.168.16.68	3658	T	200.200.200.251	139	1	3	200.200.202.134	1055

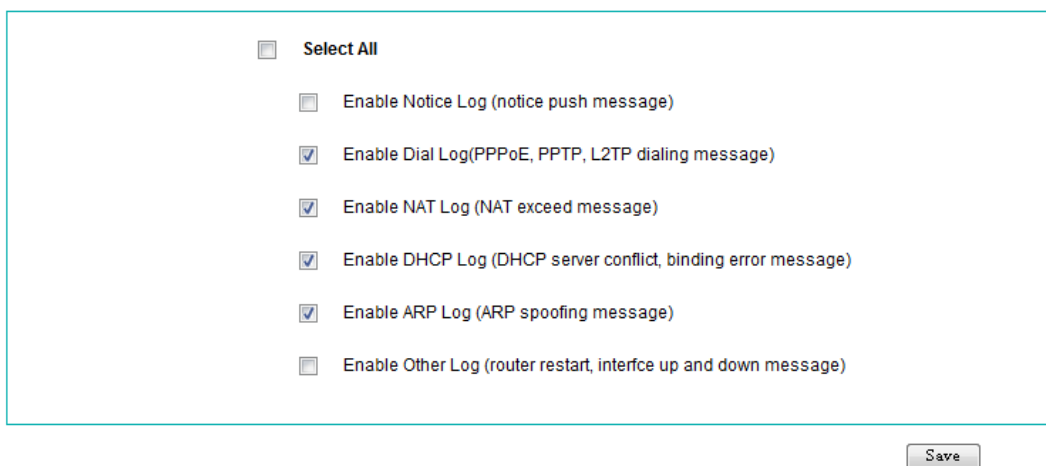
Clear

Figure 5-23 NAT Session List - Example4

5.7 System Log

In the **Status > System Log** page, you can view the system logs; also you can select the types of logs that you want the Device to store and display.

5.7.1 System Log Settings



The screenshot shows a configuration window for System Log Settings. At the top, there is a checkbox labeled "Select All". Below it, there are six individual checkboxes, each followed by a description of the log type and its associated messages. The checkboxes for "Enable Dial Log", "Enable NAT Log", "Enable DHCP Log", and "Enable ARP Log" are checked, while "Enable Notice Log" and "Enable Other Log" are unchecked. A "Save" button is located at the bottom right of the window.

Checkbox	Log Type	Message Description
<input type="checkbox"/>	Select All	
<input type="checkbox"/>	Enable Notice Log	(notice push message)
<input checked="" type="checkbox"/>	Enable Dial Log	(PPPoE, PPTP, L2TP dialing message)
<input checked="" type="checkbox"/>	Enable NAT Log	(NAT exceed message)
<input checked="" type="checkbox"/>	Enable DHCP Log	(DHCP server conflict, binding error message)
<input checked="" type="checkbox"/>	Enable ARP Log	(ARP spoofing message)
<input type="checkbox"/>	Enable Other Log	(router restart, interface up and down message)

Figure 5-24 System Log Settings

- ✧ **Select All:** It selects or unselects all the check boxes below. If you want to enable all the provided system log features at a time, please select this check box. If you want to disable all the provided system log features at a time, please clear the check box.
- ✧ **Enable Notice Log:** It allows you to enable or disable notice log. If you want the Device to store and display the notice related logs in the **System Log**, please select this check box.
- ✧ **Enable Dial Log:** It allows you to enable or disable dial log. If you want the Device to store and display the dial related logs in the **System Log**, please select this check box.
- ✧ **Enable NAT Log:** It allows you to enable or disable NAT log. If you want the Device to store and display the NAT related logs in the **System Log**, please select this check box.
- ✧ **Enable DHCP Log:** It allows you to enable or disable DHCP log. If you want the Device to store and display the DHCP related logs in the **System Log**, please select

this check box.

- ✧ **Enable ARP Log:** It allows you to enable or disable ARP log. If you want the Device to store and display the ARP related logs in the **System Log**, please select this check box.
- ✧ **Enable Other Log:** It allows you to enable or disable other log. If you want the Device to store and display other logs in the **System Log**, please select this check box.
- **Save:** Click it to save the system log settings.

5.7.2 Viewing System Logs

If you have enabled one or more system log features in the **Status > System Log > Log Settings** page, you can view the related logs in the **Status > System Log** page, see the following figure.

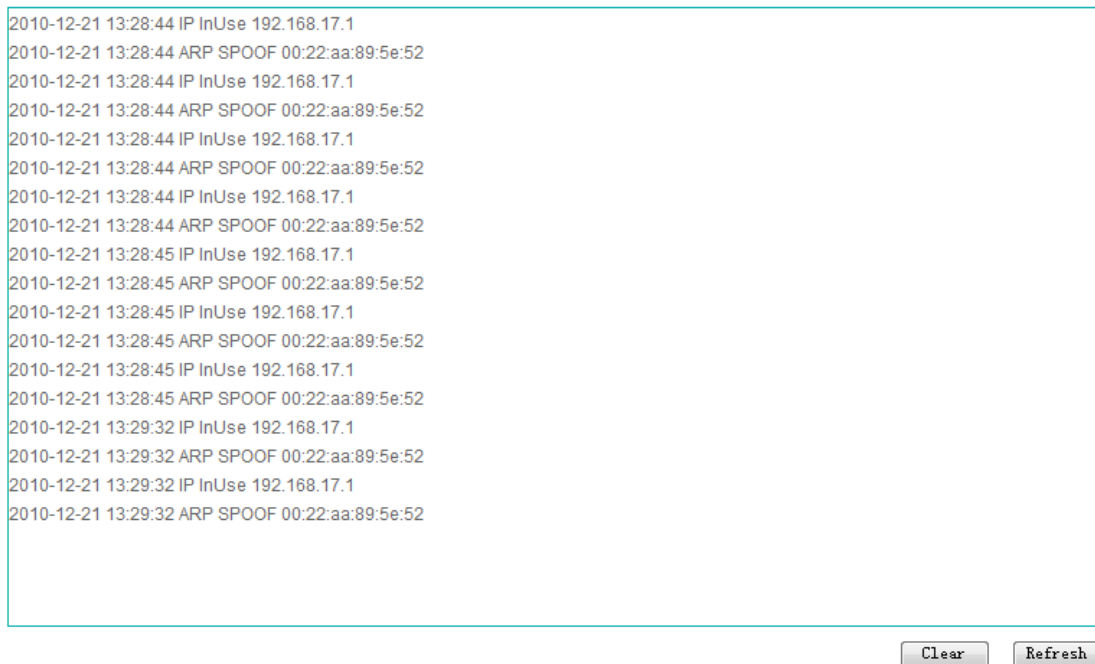


Figure 5-25 System Logs

- **Clear:** Click it to clear all the system logs.
- **Refresh:** Click it to view the latest system logs.

The following table describes some common types of system logs.

System Log		Meaning
Keyword	Sample	
Ethernet Up	ieX	The specified physical interface is enabled. ie0: LAN; ie1~ie4: WAN1~WAN4.
MAC New	00:22:aa:00:22:bb	The new MAC address of the specified user.
MAC Old	00:22:aa:00:22:aa	The old MAC address of the specified user.
ARP SPOOF	192.168.1.1	The MAC address of the user with IP address 192.168.1.1 has changed.
Session Up	PPPOE	The Device has successfully established a session whose name is PPPOE.
PPPoE Up	00:22:aa:5d:63:6f	The Device has successfully established a PPPoE connection with the remote device whose MAC address is 00:0c:f8:f9:66:c6.
Call Connected	@_netiNetworkStateChanged: 6244, on line 1, on channel 0	The physical layer data link layer connections have been established, but IP still couldn't be used.
Outgoing Call	@61:1-1	The Device started dialing out.
Call Terminated	@clearSession: 1	The Device failed to dial.
Outgoing Call	@61:1-1	The Device started dialing out.
Session down	Manually (PPPOE)	The session whose name is PPPOE was hanged up. Manually means it was hanged up by manual.

Session up	test	The Device has successfully established a session whose name is test.
Assigned to port	@answerIncomingCall:8012	The Device has successfully negotiated with the remote dial-in device, and has assigned a port to the remote device.
Call Connected	@_netiNetworkStateChanged: 6244, on line 1, on channel 0	The physical layer and data link layer connections have been established, but IP still couldn't be used.
Incoming Call	@_netiNetworkStateChanged: 6187, on line 1, on channel 0	The Device received a call from a remote device.
Route Up	ethX	The static routes bound to the specified physical interface became active. (Usually due to that the corresponding Internet connection became active.) eth1: LAN; eth2~eth5: WAN1~WAN4.
Route Down	ethX	The static routes bound to the specified physical interface became inactive. (Usually due to that the corresponding Internet connection became inactive.)
NAT exceeded	[IP Address]	The specified host has exceeded the maximum NAT sessions limited by the Device. Usually due to that this host is infected with a virus or it is using hacker attack software. If the host is working properly, please increase the maximum NAT sessions appropriately.
ARP exceeded	[IP Address]	The APR request for the specified IP address has been rejected due to the maximum ARP entries limit. If the ARP table is full, any new ARP request packet to the Device will be rejected and this log message generated.

DHCP:IP conflicted	[arp: IP Address]	A DHCP IP address conflict has occurred, that is, when acting as a DHCP server, the Device detected that the specified IP address is already used in the LAN before assigning it to a user, and then the Device assigned another IP address to this user.
notice	Give notice to user: 192.168.16.35	The device has given a notice to the user with IP address 192.168.16.35.

Table 5-1 System Logs List

5.8 Web Log

This section describes the **Status > Web Log** page.

In this page, it allows you to view web logs. A web log records the information of a web page access by a LAN user, which include: the access time, the LAN user's IP address, and the domain name of the web page.

5.8.1 Enable Web Log



Figure 5-26 Enable Web Log

- ✧ **Enable Web Log:** It allows you to enable or disable web log. If you want the Device to store and display the web logs in this page, please select this check box.
- **Save:** Click it to save your settings.

5.8.2 View Web Logs

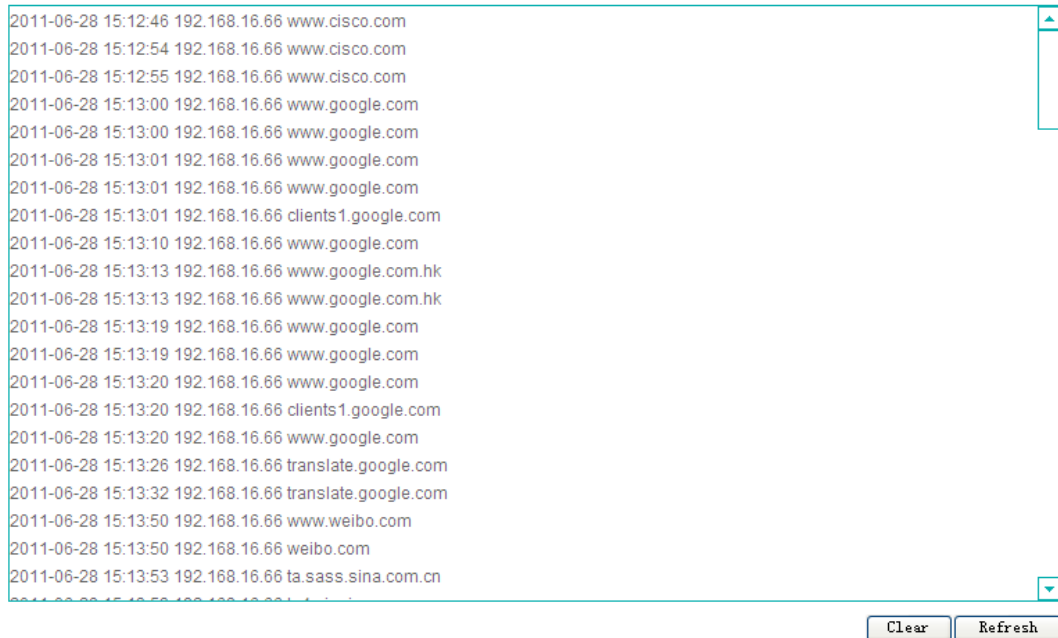


Figure 5-27 View Web Logs

A web log consists of date and time, an IP address of a LAN user, and a domain name.

- **Date and time:** It displays the date and time at which a LAN user accessed a web page.
- **IP address:** It displays the IP address of the LAN user who has accessed a web page.
- **Domain name:** It displays the domain name of a web page which is accessed by the LAN user.
- **Clear:** Click it to clear all the web logs in the list box.
- **Refresh:** Click it to view the latest web logs.



Note

To ensure that the date and time of the web logs are correct, you should synchronize

the system clock in the **System > Time** page.

5.9 Application Traffic Statistics

In the **Status > APP Traffic** page, you can view the traffic statistics of some predefined applications. For each application, you can view the traffic statistics of each WAN interface, and the traffic statistics of each LAN user.

5.9.1 Global Setup



Figure 5-28 Enable Application Traffic Statistics

- ✧ **Enable Application Traffic Statistics:** It allows you to enable or disable application traffic statistics. If you want to view the applications traffic statistics of the LAN users in the **APP Traffic Statistics** list, please select this check box to enable this feature.
- **Save:** Click it to save your settings.

5.9.2 Application Traffic Statistics List

Interface: WAN1 ▾

Application	Tx Rate(Kbit/s)	Rx Rate(Kbit/s)	Details
TCP	0	0	IP Address
UDP	0	0	IP Address
Web	0	0	IP Address
FTP	0	0	IP Address
P2P	0	0	IP Address
Game	0	0	IP Address

[Refresh](#)

Figure 5-29 Application Traffic Statistics List

- ✧ **Interface:** It allows you select a WAN interface to display the application traffic statistics of this interface.
- ✧ **Application:** It indicates the type of application traffic. The Device provides six types of application traffic, including TCP, UDP, Web, FTP, P2P and Game applications. Therein, there are multiple specific types of P2P and Game applications, please refer to **section 11.2 Internet Behavior Management** for more information.
- ✧ **Tx Rate:** It indicates the real-time uplink rate (in kilobits per second) of the given application traffic through the selected WAN interface.
- ✧ **Rx Rate:** It indicates the real-time downlink rate (in kilobits per second) of the given application traffic through the selected WAN interface.
- ✧ **Details:** Click the **IP Address** hyperlink to go to the **Status > APP Stats > User Traffic Statistics** page to view the given application traffic statistics of each LAN user.
- **Refresh:** Click it to view the latest information in the list.

5.9.3 User Traffic Statistics List

IP Address	Tx Rate(Kbit/s)	Rx Rate(Kbit/s)

Figure 5-30 User Traffic Statistics List

- ✧ **IP Address:** It indicates the IP address of the LAN host (i.e., LAN user).
- ✧ **Tx Rate:** It indicates the real-time rate (in kilobits per second) of the given application traffic sent by the LAN host.
- ✧ **Rx Rate:** It indicates the real-time rate (in kilobits per second) of the given application traffic received by the LAN host.
- **Back:** Click it to back to the **APP Traffic Statistics** list.
- **Refresh:** Click it to view the latest information in the list.

5.10 WAN Traffic Statistics

Through the **WAN Traffic Statistics** list in the **Status > WAN Traffic** page, you can view traffic and rate related information of each Internet connection.

WAN Traffic Statistics

Interface	Tx Bandwidth	Real-time Tx Rate	Average Tx Rate	Max Tx Rate	Rx Bandwidth	Real-time Rx Rate	Average Rx Rate	Max Rx Rate
WAN1	0Kbit/s	0Kbit/s	0Kbit/s	0Kbit/s	0Kbit/s	0Kbit/s	0Kbit/s	0Kbit/s

Figure 5-31 WAN Traffic Statistics List

- ✧ **Interface:** It specifies a WAN interface on which the Internet connection is established.
- ✧ **Tx Bandwidth:** It is the **Uplink Bandwidth** of the Internet connection configured in the **Basic > WAN** page.
- ✧ **Real-time Tx Rate:** It indicates the real-time uplink rate of the Internet connection.
- ✧ **Average Tx Rate:** It indicates the average uplink rate of the Internet connection since the Device was last started.
- ✧ **Max Tx Rate:** It indicates the maximum uplink rate of the Internet connection since the Device was last started.
- ✧ **Rx Bandwidth:** It is the **Downlink Bandwidth** of the Internet connection configured in the **Basic > WAN** page.
- ✧ **Real-time Rx Rate:** It indicates the real-time downlink rate of the Internet connection.
- ✧ **Average Rx Rate:** It indicates the average downlink rate of the Internet connection since the Device was last started.
- ✧ **Max Rx Rate:** It indicates the maximum downlink rate of the Internet connection since the Device was last started.
- **Refresh:** Click it to view the latest information in the list.

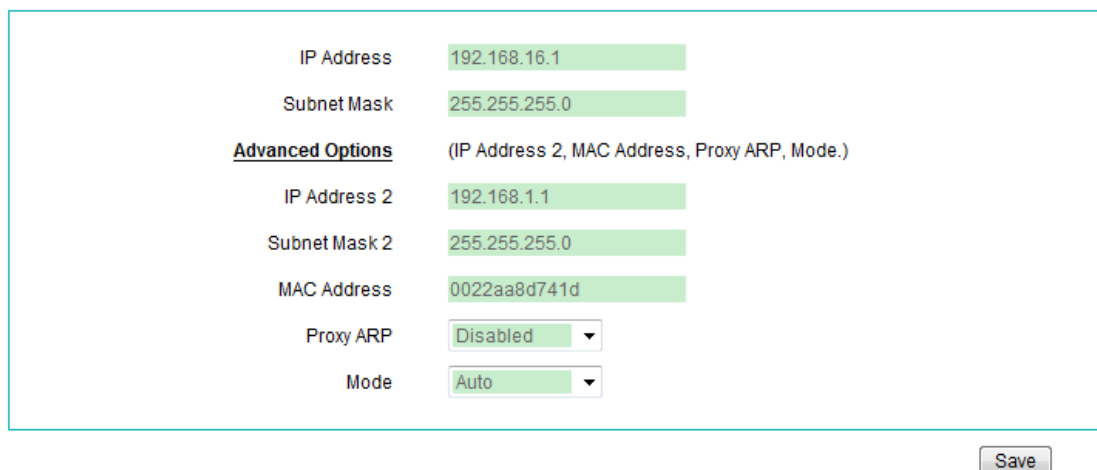
Chapter 6 Basic Setup

This chapter describes how to configure and use the basic features of the Device, which include LAN interface settings, WAN interface settings, load balancing (only multi-WAN products support it), DHCP and DNS features.

6.1 LAN Settings

This section describes the **Basic > LAN** page.

After you have configured the Internet Connection through the **Quick Wizard**, you can modify the IP address and subnet mask of the LAN interface in this page. Also, you can configure some other parameters, which include the **IP Address 2**, **Subnet Mask 2**, **MAC Address**, **Proxy ARP**, and **Mode**. Obviously, you can directly configure the **IP address** and **Subnet Mask** of the LAN interface in this page without using the **Quick Wizard**.



IP Address	192.168.16.1
Subnet Mask	255.255.255.0
Advanced Options	(IP Address 2, MAC Address, Proxy ARP, Mode.)
IP Address 2	192.168.1.1
Subnet Mask 2	255.255.255.0
MAC Address	0022aa8d741d
Proxy ARP	Disabled
Mode	Auto

Save

Figure 6-1 LAN Interface Settings

- ✧ **IP Address:** It specifies the IP address of the LAN interface.
- ✧ **Subnet Mask:** It specifies the subnet mask that defines the range of the LAN.
- **Advanced Options:** Click it to view and configure advanced parameters. In most cases, you need not configure them.
- ✧ **IP Address 2:** It specifies the secondary IP address of the LAN interface.
- ✧ **Subnet Mask 2:** It specifies the secondary subnet mask that defines the range of the secondary subnet.

- ✧ **MAC Address:** It specifies the MAC address of the LAN interface. In most cases, please leave the default value.
- ✧ **Proxy ARP:** It allows you to enable or disable proxy ARP on the LAN interface. The available options are **Disabled**, **Enabled** and **Nat**.
 - **Disabled:** Select it to disable the proxy ARP on the LAN interface.
 - **Enabled:** Select it to enable the proxy ARP on the LAN interface.
 - **Nat:** Select it to enable the NAT proxy ARP on the LAN interface.
- ✧ **Mode:** It specifies the speed and duplex mode of the LAN interface. The Device supports five or six modes (Note that only the gigabit LAN interface supports **1000M-HD**), which include **Auto** (Auto-negotiation), **100M-FD** (100M Full-Duplex), **100M-HD** (100M Half-Duplex), **10M-FD** (10M Full-Duplex), **10M-HD** (10M Half-Duplex), and **1000M-FD** (1000M Full-Duplex).

In most cases, please leave the default value. If a compatibility problem occurred, or the network device connected to the LAN interface doesn't support auto-negotiation function, you may modify it as required.
- **Save:** Click it to save the LAN interface settings.

**Note**

1. You can assign two IP addresses to the Device's LAN interface to connect two subnets. The hosts on the two subnets can communicate with each other.
2. If you have changed the LAN IP address and saved the change, you should use the new IP address to re-login to the Device. And the default gateway of each LAN host should be changed to this new IP address, thus the LAN hosts can access the Device and Internet.
3. The LAN interface integrates multiple switch ports, and you may go to the **Status > System Info** page to view each LAN port status.

6.2 WAN Settings

6.2.1 WAN List

After you have configured the Internet connection through the **Quick Wizard**, you can view its configuration and status in the **Basic > WAN > WAN List** page; also you can modify or delete it if needed.

WAN List											
WAN1			WAN2			WAN3			WAN4		
Interface	Type	Status	IP Address	Gateway	Rx Rate(bps)	Tx Rate(bps)	Operation	Edit			
WAN1	PPPoE(a) (Normal Mode)	Connected(Up time: :00:00:02:04)	10.0.0.2	10.0.0.2	19k	1k	Dial Hang Up Delete	Edit			
WAN2	None							Edit			
WAN3	None							Edit			
WAN4	None							Edit			

[Display Interface Statistics](#)

Figure 6-2 WAN Internet Connection List



Note

If you want to use multiple connections to access the Internet, please configure them in this page, and then go to the **Basic > Load Balancing** page to configure load balancing and failover.

6.2.1.1 Parameter Definitions

- ✧ **Type:** It displays the connection type. For the **PPPoE Internet connection**, it will also display its user name and dial mode.
- ✧ **Status:** It displays current status of the connection. We will describe the status of each connection status respectively.

1. PPPoE Connection Status

There are eight kinds of status for PPPoE connection (see Table 6-1). When it is connected, it will also display the elapsed time (days: hours: minutes: seconds) since connected.

Status	Description
Closed	The physical interface isn't connected, or doesn't dial up yet.
Dialing	Start dialing up, but not receive response yet.
Authenticating	Server responded and is authenticating.
Connected	Authentication succeeded, and the connection is established and ready for data transmission.
Disconnecting	The PPPoE session is disconnecting.
Hang up	Either peer has hanged up.
Disconnected	The PPPoE session has terminated, waiting for dialing up.
Internal Error	Undefined status.

Table 6-1 Description of PPPoE Connection Status

2. Static IP Connection Status

There are three kinds of status for Static IP connection (see Table 6-2).

Status	Description
Closed	The physical interface isn't connected.

Connected	The connection is established between the Device and peer device.
Internal Error	Undefined status.

Table 6-2 Description of Static IP Connection Status

3. DHCP Connection Status

There are four kinds of status for DHCP connection (see Table 6-3). When it is connected, it will also display the time left (days: hours: minutes: seconds) before the lease expires for the current IP address, which is assigned by your ISP's DHCP server.

Status	Description
Closed	The physical interface isn't connected. Or the connection has released the IP address but hasn't requested a new one yet.
Connecting	Requesting an IP address.
Connected	Has obtained an IP address, the connection is established successfully.
Internal Error	Undefined status.

Table 6-3 Description of DHCP Connection Status

6.2.1.2 List Function

- **Edit an Internet Connection:** If you want to modify a configured Internet connection, click its **Edit** hyperlink, the related information will be displayed in the setup page. Then modify it, and click the **Save** button.

- **Delete an Internet Connection:** If you want to delete a configured Internet connection, click **Delete** of the connection to delete it.

6.2.1.3 How to Dial and Hang up a PPPoE connection

For the PPPoE connection, the **Dial**, **Hang Up** and **Delete** are shown in the **Operation** column (see Figure 6-3).

If the PPPoE connection’s **Dial Type** is set to **Manual** (see **section 6.2.2.1**), you need click **Dial** to dial-up the Internet connection, and click **Hang Up** to hang it up.

- **Dial:** Click it to dial up the Internet connection manually. During dialing up, you can view the related status information in the **Status** column, which includes **Closed**, **Dialing**, **Authenticating** and **Connected**.
- **Hang Up:** Click it to hang the Internet connection up manually.

Interface	Type	Status	IP Address	Gateway	Rx Rate(bps)	Tx Rate(bps)	Operation	Edit
WAN1	PPPoE (Normal Mode)	Connected(Up time: :00:00:02:04)	10.0.0.2	10.0.0.2	19k	1k	Dial Hang Up Delete	Edit
WAN2	None							Edit
WAN3	None							Edit
WAN4	None							Edit

Display Interface Statistics Refresh

Figure 6-3 WAN List - PPPoE Internet Connection

6.2.1.4 How to Renew and Release a DHCP Connection

For the DHCP connection, the **Renew**, **Release** and **Delete** are shown in the **Operation** column (see Figure 6-4).

- **Renew:** Click it to re-obtain an IP address from the ISP’s DHCP server. The Device will automatically release the assigned IP address firstly, and then obtain a new IP address from the DHCP server. During renewing, you can view the related status information in the **Status** column, which includes **Closed**, **Connecting**, and **Connected**.
- **Release:** Click it to release the IP address obtained from the ISP’s DHCP server.

WAN List	WAN1	WAN2	WAN3	WAN4
----------	------	------	------	------

Interface	Type	Status	IP Address	Gateway	Rx Rate(bps)	Tx Rate(bps)	Operation	Edit
WAN1	DHCP	Connected(Left:00:00:59:50)	200.200.210.69	200.200.210.1	12k	336	Renew Release Delete	Edit
WAN2	None							Edit
WAN3	None							Edit
WAN4	None							Edit

[Display Interface Statistics](#)

Figure 6-4 WAN List DHCP Internet Connection

6.2.2 WAN Internet Connection Settings

This section describes how to configure PPPoE, Static IP and DHCP Internet connection respectively, and how to delete the connection.



Note

Only after you have configured the Internet connection on the WAN1, you can configure other connections. The system will automatically set these connections' **Primary DNS Server** to the IP address of the WAN1 Internet connection's **Primary DNS Server**, and you cannot modify them.

6.2.2.1 PPPoE Internet Connection Settings

Please select **PPPoE** from the **Connection Type** drop-down list if your ISP uses PPPoE to establish the Internet connection for you. Then the following page will be showed.

Connection Type:

 Tx Bandwidth: Kbit/s

 Rx Bandwidth: Kbit/s

 ISP:

 User Name:

 Password:

 Dial Mode:

 DNS Server:

Advanced Options (Service Name, Priority, Proxy ARP, Mode, MAC Address etc.)

 PPP Authentication:

 Service Name:

 MRU: bytes

 Dial Type:

 Dial Schedule:

 Online Schedule:

 Keepalive Period: milliseconds

 Idle Timeout: seconds

 Session Timeout: seconds

 Priority:

 Down Priority:

 Dial Sub-interface:

 Proxy ARP:

 Mode:

 MAC Address:

Figure 6-5 PPPoE Internet Connection Settings

- ✧ **Connection Type:** It specifies the type of the Internet connection. Here please select **PPPoE**.
- ✧ **Uplink Bandwidth:** It specifies the uplink bandwidth of the Internet connection, which is provided by your ISP. You may ask the ISP about the uplink bandwidth.
- ✧ **Downlink Bandwidth:** It specifies the downlink bandwidth of the Internet connection, which is provided by your ISP. You may ask the ISP about the downlink bandwidth.
- ✧ **ISP:** It specifies the Internet service provider (ISP) by which the Internet connection is provided.
- ✧ **User Name** and **Password:** They specify the PPPoE login user name and password provided by your ISP.
- ✧ **Dial Mode:** It specifies the dial mode of the PPPoE Internet connection. The default value is **Normal mode**. If the PPPoE connection isn't established successfully even

using correct user name and password, you may try to use another mode.

- ✧ **DNS Server:** It specifies the method by which you configure the DNS server(s). If you know the local DNS server IP address, you may select **Manual**, then enter the DNS server IP address in the **Primary DNS server** text box, and the secondary DNS server IP address in the **Secondary DNS Server** if available. Else, please select **Auto**, then the Device will automatically obtain the DNS server IP address.
- ✧ **Primary DNS Server:** It specifies the IP address of your ISP's primary DNS server.
- ✧ **Secondary DNS Server:** It specifies the IP address of your ISP's secondary DNS server. If it is available, you may set it. Else, please leave it 0.0.0.0.
- **Advanced Options:** Click it to view and configure advanced parameters. In most cases, you need not configure them.
- ✧ **PPP Authentication:** It specifies the PPP authentication mode of the PPPoE connection. The available options are **NONE**, **PAP**, **CHAP** and **Either**.
 - **PAP:** Password Authentication Protocol.
 - **CHAP:** Challenge Handshake Authentication Protocol.
 - **None:** It means that there is no protocol will be used.
 - **Either:** It means that the Device will automatically negotiate it with the peer device.
- ✧ **Service Name:** It specifies the service name provided by your ISP. In most cases, please leave it blank. If you have any questions, please contact the ISP.
- ✧ **MRU:** It specifies the largest packet size permitted for network receive. When dialing, the Device will automatically negotiate it with the peer device. Unless special application, please leave the default value of 1492 bytes.
- ✧ **Dial Type:** It specifies the dial type of the PPPoE connection. The available options are **Always On**, **Manual** and **On Demand**.
 - **Always On:** If you want the Device to establish a PPPoE connection when starting up and to automatically re-establish the PPPoE connection once disconnected, select this option.
 - **Manual:** If you want to dial and hang up a PPPoE connection manually, select this option. In this case, you should dial and hang up manually in the **WAN List** in the **Basic > WAN** page (see section 6.2.1.3).
 - **On Demand:** If you want the Device to establish a PPPoE connection only when it listens for packets destined for the Internet, select this option. In this case, the Device will terminate the connection after it has been inactive for the period of time specified by the **Idle Timeout**.

- ✧ **Dial Schedule:** It specifies a schedule during which the Device can dial up. If you select a schedule here, it will allow the Device to dial up only in the selected schedule range; else, the Device can always dial up. The schedule is configured in the **Security > Schedule** page.
- ✧ **Online Schedule:** It specifies a schedule during which the Device can access the Internet. If you select a schedule here, it will allow the Device to access the Internet only in the selected schedule range, and the Device will automatically terminate the PPPoE connection once beyond this schedule range; else, the Device will be always online. The schedule is configured in the **Security > Schedule** page.
- ✧ **Keepalive Period:** It specifies a period of time during which the Device will detect whether the link is available or not. If the connection is connected, the Device will periodically send keepalive packets to the peer device per 1000 milliseconds. If the Device does not receive a response during the specified period of time, it will terminate the connection. The default value is 15000 milliseconds.
- ✧ **Idle Timeout:** It specifies how long the PPPoE connection keeps connected since no Internet activity. The Device will automatically terminate the connection after it has been inactive for the specified period of time. The default value is zero, which means that the Device will not terminate it.
- ✧ **Session Timeout:** It specifies how long the PPPoE connection keeps connected since established. The Device will automatically terminate the connection after it has been connected for the specified period of time. The default value is zero, which means that the Device will not terminate it. In most cases, please leave the default value.
- ✧ **Priority:** It specifies the routing priority of the established connection. When there are several established connections, the Device will choose the connection with the highest priority to forward the packets. The lower value means the higher priority.
- ✧ **Down Priority:** It specifies the routing priority of the terminated connection. When there are several terminated connections, the connection with the highest priority will dial up preferentially. The lower value means the higher priority.
- ✧ **Dial Sub-interface:** It specifies a logical virtual interface which is subjected to the physical interface. You can create multiple sub-interfaces on a single physical interface. At present, the Device only supports that you create sub-interfaces on the WAN1, and these sub-interfaces are distinguished from one another by the 802.1Q VLAN identifier.
- ✧ **Proxy ARP:** It allows you to enable or disable proxy ARP on the WAN interface. The available options are **Disabled**, **Enabled** and **Nat**.
 - **Disabled:** Select it to disable the proxy ARP on the WAN interface.
 - **Enabled:** Select it to enable the proxy ARP on the WAN interface.

- **Nat:** Select it to enable the NAT proxy ARP on the WAN interface.
- ✧ **Mode:** It specifies the speed and duplex mode of the WAN interface. The Device supports five or six modes (Note that only the gigabit WAN interface supports **1000M-HD**), which include **Auto** (Auto-negotiation), **100M-FD** (100M Full-Duplex), **100M-HD** (100M Half-Duplex), **10M-FD** (10M Full-Duplex), and **10M-HD** (10M Half-Duplex) , **1000M-FD** (1000M Full-Duplex). In most cases, please leave the default value. If a compatibility problem occurred, or the network device connected to the WAN interface doesn't support auto-negotiation function, you may modify it as required.
- ✧ **MAC Address:** It specifies the MAC address of the WAN interface. In most cases, please leave the default value.
- **Save:** Click it to save the PPPoE Internet connection settings.

**Note**

1. The **Dial Sub-interface** can only be configured on the product that supports the IEEE 802.1Q tag-based VLAN feature. If you create multiple PPPoE Internet connections on a WAN Interface, some ISPs may forbid these connections to access their broadband access servers as they are using the same MAC address (that is, the WAN Interface's MAC address). You can use sub-interface feature to solve this problem: connect the WAN1 to a switch that provides 802.1Q tag-based VLAN feature, and then create multiple VALN sub-interfaces on the WAN1, lastly create a connection on each sub-interface respectively; then each connection will use a MAC address respectively
2. Compared with the PPPoE Internet connection setup page in the **Quick Wizard**, this page provides more configuration parameters, such as, **Dial Schedule, Online Schedule, Keepalive Period, Priority, Down Priority**, and so on.
3. In most cases, please leave the **Proxy ARP** the default value, that is, disable the proxy ARP on the interface. But in some cases, you need enable the proxy ARP. For example, when you enable PPTP or L2TP server feature on a WAN interface, and the IP addresses assigned to the mobile user clients are on the same subnet as the Device LAN interface, you need enable proxy ARP on this interface. Another example is that when using multi-NAT (that is, you get multiple public IP addresses from your ISP) on a WAN interface, you should enable NAT proxy ARP on this interface.

6.2.2.2 Static IP Internet Connection Settings

If you are required to use a static IP address, please select **Static IP** from the **Connection Type** drop-down list. Then the following page will be showed.

Connection Type	Static IP
Tx Bandwidth	0 Kbit/s
Rx Bandwidth	0 Kbit/s
ISP	Others
IP Address	200.200.200.202
Subnet Mask	255.255.255.0
Default Gateway	200.200.200.201
Primary DNS Server	202.106.46.188
Secondary DNS Server	202.106.46.151
Advanced Options (MAC Address, Proxy ARP, Gateway Binding etc.)	
MAC Address	0022aa8d7e2d
Proxy ARP	Nat
Mode	Auto
Gateway Binding Mode	None

Figure 6-6 Static IP Internet Connection Settings

- ✧ **Connection Type:** It specifies the type of the Internet connection. Here please select **Static IP**.
- ✧ **Uplink Bandwidth:** It specifies the uplink bandwidth of the Internet connection, which is provided by your ISP. You may ask the ISP about the uplink bandwidth.
- ✧ **Downlink Bandwidth:** It specifies the downlink bandwidth of the Internet connection, which is provided by your ISP. You may ask the ISP about the downlink bandwidth.
- ✧ **ISP:** It specifies the Internet service provider by which the Internet connection is provided.
- ✧ **IP Address:** It specifies the IP address of the WAN interface, which is provided by your ISP.
- ✧ **Subnet Mask:** It specifies the subnet mask of the WAN interface, which is provided by your ISP.
- ✧ **Default Gateway:** It specifies the IP address of the default gateway, which is provided by your ISP.

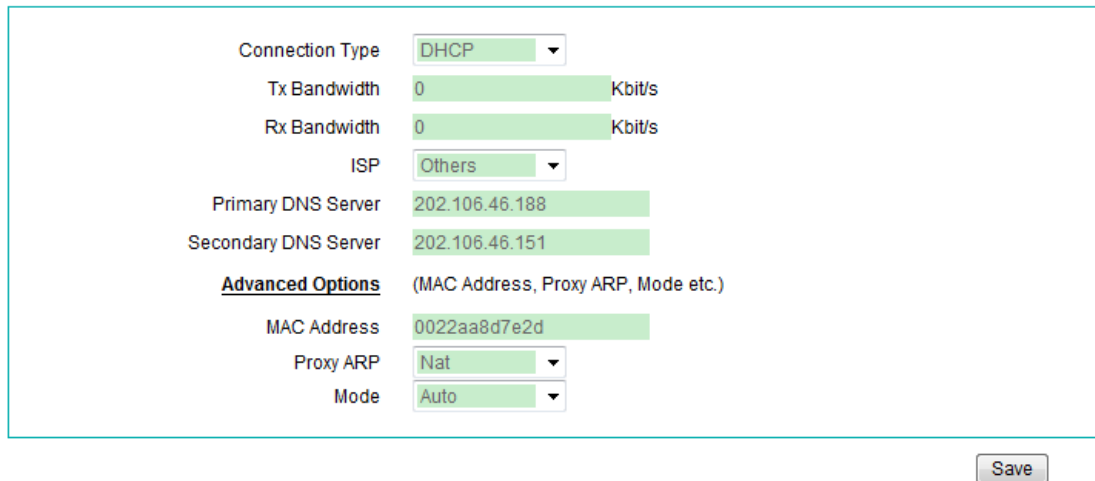
- ✧ **Primary DNS Server:** It specifies the IP address of your ISP's primary DNS server.
- ✧ **Secondary DNS Server:** It specifies the IP address of your ISP's secondary DNS server. If it is available, you may set it. Else, please leave it blank.
- **Advanced Options:** Click it to view and configure advanced parameters. In most cases, you need not configure them.
- ✧ **MAC Address:** It specifies the MAC address of the WAN interface. In most cases, please leave the default value.
- ✧ **Proxy ARP:** It allows you to enable or disable proxy ARP on the WAN interface. The available options are **Disabled**, **Enabled** and **Nat**.
 - **Disabled:** Select it to disable the proxy ARP on the WAN interface.
 - **Enabled:** Select it to enable the proxy ARP on the WAN interface.
 - **Nat:** Select it to enable the NAT proxy ARP the WAN interface.
- ✧ **Mode:** It specifies the speed and duplex mode of the WAN interface. The Device supports five or six modes (Note that only the gigabit WAN interface supports **1000M-HD**), which include **Auto** (Auto-negotiation), **100M-FD** (100M Full-Duplex), **100M-HD** (100M Half-Duplex), **10M-FD** (10M Full-Duplex), and **10M-HD** (10M Half-Duplex) , **1000M-FD** (1000M Full-Duplex). In most cases, please leave the default value. If a compatibility problem occurred, or the network device connected to the WAN interface doesn't support auto-negotiation function, you may modify it as required.
- ✧ **Gateway Binding Mode:** It determines whether the gateway's IP and MAC address pair will be bound or not. If you want to bind the gateway's IP and MAC address pair to protect the Device against external ARP spoofing, select **Manual** from this drop-down list, and enter the gateway's MAC address in the **Gateway MAC Address** text box. Else, select **None**.
- **Save:** Click it to save the static IP Internet connection settings.

**Note**

The WAN interface IP address and default gateway IP address should be on the same subnet. If they are not, please modify the **Subnet Mask** to make them be on the same subnet. If you don't have the subnet related knowledge, please ask a professional or UTT customer engineer for help.

6.2.2.3 DHCP Internet Connection Settings

If your ISP automatically assigns an IP address, please select **DHCP** from the **Connection Type** drop-down list. Then the following page will be showed.



The screenshot shows a configuration form for DHCP Internet Connection Settings. The fields are as follows:

Connection Type	DHCP
Tx Bandwidth	0 Kbit/s
Rx Bandwidth	0 Kbit/s
ISP	Others
Primary DNS Server	202.106.46.188
Secondary DNS Server	202.106.46.151
Advanced Options	(MAC Address, Proxy ARP, Mode etc.)
MAC Address	0022aa8d7e2d
Proxy ARP	Nat
Mode	Auto

Below the form is a "Save" button.

Figure 6-7 DHCP Internet Connection Settings

- ✧ **Connection Type:** It specifies the type of the Internet connection. Here please select **DHCP**.
- ✧ **Uplink Bandwidth:** It specifies the uplink bandwidth of the Internet connection, which is provided by your ISP. You may ask the ISP about the uplink bandwidth.
- ✧ **Downlink Bandwidth:** It specifies the downlink bandwidth of the Internet connection, which is provided by your ISP. You may ask the ISP about the downlink bandwidth.
- ✧ **ISP:** It specifies the Internet service provider by which the Internet connection is provided.
- ✧ **Primary DNS Server:** It specifies the IP address of your ISP's primary DNS server. If the Internet connection is refreshed, your ISP may update it to a new IP address.
- ✧ **Secondary DNS Server:** It specifies the IP address of your ISP's secondary DNS server. If it is available, you may set it. Else, please leave it blank.
- **Advanced Options:** Click it to view and configure advanced parameters. In most cases, you need not configure them.
- ✧ **MAC Address:** It specifies the MAC address of the WAN interface. In most cases, please leave the default value.
- ✧ **Proxy ARP:** It allows you to enable or disable proxy ARP on the WAN interface. The available options are **Disabled**, **Enabled** and **Nat**.

- **Disabled:** Select it to disable the proxy ARP on the WAN interface.
 - **Enabled:** Select it to enable the proxy ARP on the WAN interface.
 - **Nat:** Select it to enable the NAT proxy ARP on the WAN interface.
- ✧ **Mode:** It specifies the speed and duplex mode of the WAN interface. The Device supports five or six modes (Note that only the gigabit WAN interface supports **100M-HD**), which include **Auto** (Auto-negotiation), **100M-FD** (100M Full-Duplex), **100M-HD** (100M Half-Duplex), **10M-FD** (10M Full-Duplex), and **10M-HD** (10M Half-Duplex) , **1000M-FD** (1000M Full-Duplex). In most cases, please leave the default value. If a compatibility problem occurred, or the network device connected to the WAN interface doesn't support auto-negotiation function, you may modify it as required.
- **Save:** Click it to save the DHCP Internet connection settings.

6.2.2.4 How to Delete the Internet Connection

WAN List	WAN1	WAN2	WAN3	WAN4

Interface	Type	Status	IP Address	Gateway	Rx Rate(bps)	Tx Rate(bps)	Operation	Edit
WAN1	PPPoE(<input checked="" type="checkbox"/> Normal Mode)	Connected(Up time: 00:00:02.04)	10.0.0.2	10.0.0.2	19k	1k	Dial Hang Up Delete	Edit
WAN2	None							Edit
WAN3	None							Edit
WAN4	None							Edit

Display Interface Statistics

Figure 6-8 Delete the Internet Connection

If you want to delete a configured Internet connection, go to the **Basic > WAN > WAN List** page firstly, and then click **Delete** of the connection in the **WAN List**, see Figure 6-8. The system will pop up a prompt dialog box, see Figure 6-9. Then click **OK** to delete the connection, or click **Cancel** to cancel the operation.

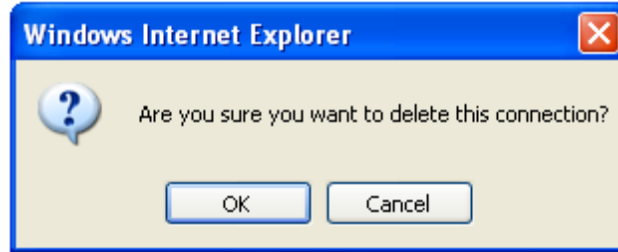


Figure 6-9 Prompt Dialog Box - Delete an Internet Connection

 **Note**

You can only delete one Internet connection at a time. And you can only delete the WAN1 Internet connection at last, that is, there is no any other connection in the **WAN List**.

6.2.2.5 Related Default Routes

After you have finished configuring the WAN1 Internet connection through the **Quick Wizard**, or configuring the WAN1 Internet connection and other connections in this page, the Device will automatically create a default route for each Internet connection respectively. You can go to the **Status > Route Stats** page to view their status information in the **Routing Table**. A default route's **Destination IP/Mask** is **0.0.0.0/0**.

6.3 Load Balancing

This section describes the **Basic > Load Balancing** page. Note that only after you have configured more than one Internet connections, the second level menu **Load Balancing** will be displayed.

When using multiple Internet connections, you can configure load balancing related parameters, such as, load balancing policy, load balancing mode, detection method, detection interval, retry times, and ID binding, and so on.

6.3.1 Introduction to Load Balancing and Failover

6.3.1.1 Internet Connection Detection Mechanism

When using multiple Internet connections, the Device should have the ability of real-time monitoring each Internet connection, and the network will not be interrupted even a connection is faulty. To this end, we design flexible automatic detection mechanism on the Device, and provide multiple detection methods to meet the actual requirements.

For the sake of convenience, we firstly introduce several related parameters including **Detection Target IP**, **Detection Interval**, **Retry Times**, and **Detection Period**.

- **Detection Target IP:** It indicates the IP address of a target device. The Device will monitor an Internet connection by sending the detection packets to the specified target IP address.
- **Detection Interval:** It indicates the time interval at which the Device periodically sends detection packets, one packet at a time. The default value is 1000 milliseconds. Especially, if you don't want to monitor an Internet connection, please set it to 0.
- **Retry Times:** It indicates the number of retries per detection period. The default value is 3.
- **Detection Period:** It indicates a period of time during which the Device detects whether the Internet connection is available or not. Its value is the product of **Detection Interval** and **Retry Times**. For example, by default, its value is 3000 (1000 × 3 = 3000) milliseconds.

For a normal Internet connection and a faulty Internet connection, the detection

mechanisms are different, the following describes them respectively.

For a normal Internet connection, the detection mechanism is as follows: The Device periodically sends a detection packet at the specified time interval to the target IP address. Once no response packet received during a detection period, the Device will consider that the connection is faulty and shield it immediately. For example, by default, if the Device has sent three detection packets but not received any response packet during a detection period, it will consider that the connection is faulty.

For a faulty Internet connection, the detection mechanism is as follows: Similarly, the Device also periodically sends a detection packet at the specified time interval to the target IP address. Once more than half of the response packets received during a detection period, the Device will consider that the connection is back to normal and enable it immediately. For example, by default, if the Device has sent three detection packets and received two packets during a detection period, it will consider that the connection is back to normal.



Note

If you don't want to monitor an Internet connection, please set its **Detection Interval** to 0.

6.3.1.2 Load Balancing Mode

The Device provides two connection groups: primary connection group and backup connection group. An Internet connection belonging to the primary connection group is a primary connection, while an Internet connections belonging to the backup connection group is a backup connection. By default, all the Internet connections are primary connections. It allows you to divide one or more connections into the backup connection group, but the WAN1 Internet connection can only be used as a primary connection.

The Device provides two load balancing modes: **Full Load Balancing** and **Partial Load Balancing**.

If you choose to use **Full Load Balancing**, all the Internet connections are used as primary connections. The operation principle is as follows:

1. If all the Internet connections are normal, the LAN users will use these connections to access the Internet.
2. If an Internet connection is faulty, the Device will shield it immediately, and the traffic

through the faulty connection will be distributed to other normal connections automatically.

3. Once the faulty connection is back to normal, the Device will enable it immediately, and the traffic will be redistributed automatically.

If you choose to use **Partial Load Balancing**, some Internet connections are used as primary connections, and others are used as backup connections. The operation principle is as follows:

1. As long as one or more primary connections are normal, the LAN users will use the primary connection(s) to access the Internet. In this case, if there is more than one primary connection, the Device will control and balance the traffic among these connections.
2. If all the primary connections are faulty, it will automatically switch to the backup connection(s) to let the LAN users use them to access the Internet. In this case, if there is more than one backup connection, the Device will control and balance the traffic among these connections.
3. Once one or more faulty primary connections are back to normal, it will automatically switch back to the primary connection(s).



Note

During connections switching, some user applications (such as some online games) may be interrupted unexpectedly due to the nature of TCP connection. UTT Technologies Co., Ltd. will not bear all the losses and legal proceedings caused by it.

6.3.1.3 Internet Connection Detection Method

The Device provides three detection methods: **ICMP**, **ARP** and **DNS**. It allows you to select one of them to monitor the Internet connections. Note that you can only select a single **Detection Method** for all the Internet connections, but can set different **Detection Target**, **Detection Interval**, and **Retry Times** for each Internet connection respectively. The descriptions of each detection mode are as follows:

- **ICMP**: The Device will monitor an Internet connection by sending ICMP echo request packets the target IP address you specify. In this case, the target IP address can be either the connection's default gateway IP address or another public IP address you specify.

- **ARP:** The Device will monitor an Internet connection by sending ARP request packets to the connection's default gateway IP address.
- **DNS:** The Device will monitor an Internet connection by sending DNS query packets to the public DNS server IP address you specify.

The following table describes detection target IP supported by each detection method, and the restriction of using each detection method. Therein, **Gateway IP Address** indicates the IP address of the Internet connection's default gateway; **Other IP Address** indicates an appropriate public IP address except gateway IP address.

Detection Method	Detection Target IP	Description
ICMP	Gateway IP Address	The detection target IP can be either the gateway IP address or other public IP address.
	Other IP Address	
ARP	Gateway IP Address	The detection target IP should be the gateway IP address. You cannot perform ARP request test on a PPPoE Internet connection.
DNS	Other IP Address	The detection target IP should be a public DNS server's IP address.

Table 6-4 Detection Method and Detection Target IP

In practice, it is suggested that you choose a detection method according to the following points:

1. As ICMP method has high sensitivity and accuracy, it is suggested that you choose ICMP method to perform ICMP echo test (Ping) on the Internet connection. In most cases, please use the connection's default gateway IP address as the detection target IP; but if ping response is disabled on the default gateway, you should choose other appropriate public IP address as the detection target IP.
2. The ARP method applies to a network environment in which ping response is

disabled. Note that when performing ARP request test, the detection target IP should be the gateway IP address; and you cannot perform ARP request test on a PPPoE Internet connection.

3. The DNS method applies to a network environment in which the Internet connection is connected always, but the access time is restricted by the ISP. Note that when performing DNS query test, the detection target IP should be an appropriate public DNS server IP address; and it is suggested that you use your ISP's DNS server IP address. Moreover, you cannot choose any DNS server used by the LAN hosts as the detection target; otherwise, those LAN hosts can only use the current Internet connection to access the Internet, but cannot use other Internet connections.
4. As a PPPoE connection automatically uses LCP (link control protocol) echo mechanism to validate link availability, the Device will not use ICMP, ARP or DNS method to monitor the PPPoE Internet connection by default (its **Detection Interval** is set to 0). If needed, the Device can perform ICMP echo or DNS query test on the PPPoE connection in addition to LCP echo mechanism, but the detection target cannot be the default gateway when choosing ICMP method.

6.3.2 The Operation Principle of Load Balancing

No matter what **Load Balancing Mode** you choose, as long as there are more than one primary Internet connections, the Device will implement load balancing among these connections. The following sections describe the operation principle and the characteristics of load balancing feature.

6.3.2.1 Allocating Traffic according to Connection Bandwidth

On the Device, it allows you designate the ratio of traffic that will be allocated to each Internet connection in advance. You can achieve this by specifying the Internet connection's **Weight**, the connection that has larger **Weight** will take more traffic than the connection that has smaller **Weight**. In most cases, to properly allocate traffic, you may specify each connection's **Weight** according to the ratio of each connection's bandwidth.

For example, we assume that a business has four Internet connections: connection A, connection B, connection C, and connection D. Their bandwidths are 10M, 6M, 4M and 4M respectively. There are two cases:

- In the case of **Full Load Balancing**, as all of the four Internet connections are used as primary connections, we may set each connection's **Weight** to 5, 3, 2, and 2

respectively.

- In the case of **Partial Load Balancing**, let's assume that connection A and B are used as primary connections, and connection C and D are used as backup connections, then we may set connection A's and B's **Weight** to 5 and 3 respectively, and set both connection C's and D's **Weight** to 1.

6.3.2.2 Two Load Balancing Policies

The **Load Balancing Policy** is used to control and balance the traffic among multiple Internet connections. And the Device provides two load balancing policies: load balancing based on IP address and load balancing based on NAT session. Their implementation mechanisms are as follows.

1. Load Balancing Based on IP Address

Note that here we assume that each LAN host only has one IP address.

If you choose IP address as the load balancing policy, the Device will assign the LAN hosts' IP addresses to each Internet connection in turn. The ratio of the numbers of the IP addresses assigned to each connection is the same with the ratio of connection's **Weight**. In this case, the NAT sessions initiated from the same IP address will use the same connection, that is, a LAN host will use only one Internet connection to access the Internet.

For example, there are three Internet connections whose **Weights** are 3, 2 and 1 respectively. Then in the sequence of accessing the Internet, the first, second and third LAN hosts will use the first connection, the fourth and fifth LAN hosts will use the second connection, the sixth LAN hosts will use the third connection; in turn the seventh, eighth and ninth LAN hosts will use the first connection ... and so on.

2. Load Balancing Based on NAT Session

If you choose NAT session as the load balancing policy, the Device will assign the NAT sessions to each Internet connection in turn. The ratio of the numbers of the NAT sessions assigned to each connection is the same with the ratio of each connection's **Weight**. In this case, the NAT sessions initiated from the same LAN host will use different connections, that is, a LAN host will use multiple connections to access the Internet.

For example, there are three Internet connections whose **Weights** are 3, 2 and 1 respectively. Then in the sequence of accessing the Internet, the first, second and third NAT sessions initiated from the LAN hosts will use the first connection, the fourth and fifth NAT sessions will use the second connection, the sixth NAT sessions will use the third connection; in turn the seventh, eighth and ninth NAT sessions will use the first connection ... and so on.

3. How to Choose the Load Balancing Policy

In most cases, it is suggested that you choose IP address as the load balancing policy. If you want to use some applications that need high bandwidth, such as the NetAnts, FlashGet, Net Transport, and other multi-threaded download managers (multi-threaded download means that it can split a file into several pieces and download the pieces simultaneously, and merge them together once downloaded), you may choose NAT session as the load balancing policy to take full advantage of multiple Internet connections' bandwidth to increase download speed. Note that even if you choose NAT session as the load balancing policy, due to that the related download website is busy or there are some other reasons, the bandwidth of each Internet connection cannot be aggregated fully, so some applications may be not running smoothly.

6.3.3 ID Binding

When using multiple Internet connections, if **Load Balancing Policy** is set to **NAT Session**, the NAT sessions of the same application will be assigned to the different connections, thus some applications (such as online banking, QQ, etc.) cannot be used normally due to the identity change. We provide ID binding feature to solve this problem: After you enable ID binding, the Device will assign the NAT sessions of the same application to the same Internet connection. For example, when a LAN user logs in to an online banking system, if the first NAT session is assigned to the WAN2 Internet connection, henceforth all the subsequent NAT sessions of the online banking application will be assigned to the WAN2 connection until the user logs out.

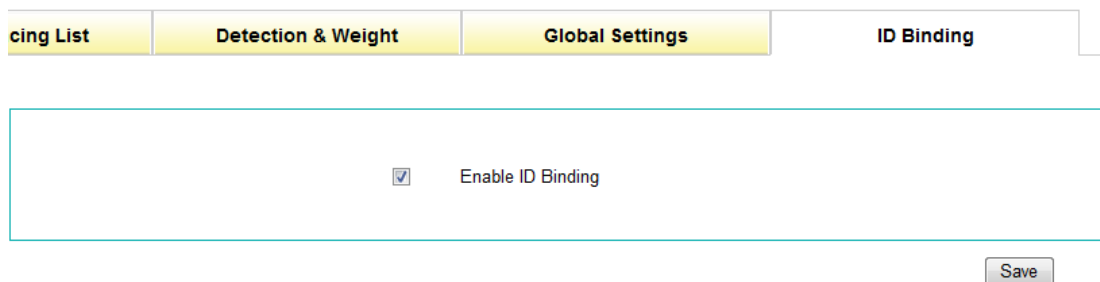


Figure 6-10 Enable ID Binding

- ✧ **Enable ID Binding:** It allows you to enable or disable ID binding. If you want to enable ID binding feature for some applications such as online banking, QQ, etc., please select this check box.
- **Save:** Click it to save your settings.

6.3.4 Load Balancing Global Settings

The following sections describe the global settings related to **Full Load Balancing** and **Partial Load Balancing** respectively. For more information about them, please refer to **section 6.3.1.2 Load Balancing Mode**.

6.3.4.1 Global Settings - Full Load Balancing

The screenshot shows a configuration interface with four tabs: 'Connection List', 'Detection & Weight', 'Global Settings', and 'ID Binding'. The 'Global Settings' tab is selected. The configuration area contains the following settings:

- Detection Method: ICMP (selected in a dropdown menu)
- Load Balancing Policy: NAT Session (selected in a dropdown menu)
- Load Balancing Mode:
 - Partial Load Balancing
 - Full Load Balancing

A 'Save' button is located at the bottom right of the configuration area.

Figure 6-11 Global Settings - Full Load Balancing

✧ **Detection Method:** It specifies the detection method which is used to monitor Internet connections. The Device provides three detection methods: **ICMP**, **ARP** and **DNS**. For more information about them, please refer to **section 6.3.1.3 Internet Connection Detection Method**.

- **ICMP:** The Device will monitor an Internet connection by sending ICMP echo request packets the target IP address you specify. In this case, the target IP address can be either the connection's default gateway IP address or another public IP address you specify.
- **ARP:** The Device will monitor an Internet connection by sending ARP request packets to the connection's default gateway IP address.
- **DNS:** The Device will monitor an Internet connection by sending DNS query packets to the public DNS server IP address you specify.

✧ **Load Balancing Policy:** It specifies the policy which is used to control and balance the traffic among multiple Internet connections. The available options are **IP Address**

and **NAT Session**, and the default value is **IP Address**. Refer to **section 6.3.2.2 Two Load Balancing Policies** for more information.

- ✧ **Load Balancing Mode:** It specifies the mode of load balancing. Here please select **Full Load Balancing**. Refer to **section 6.3.1.2 Load Balancing Mode** for more information.
- **Save:** Click it to save the load balancing global settings.

6.3.4.2 Global Settings --Partial Load Balancing

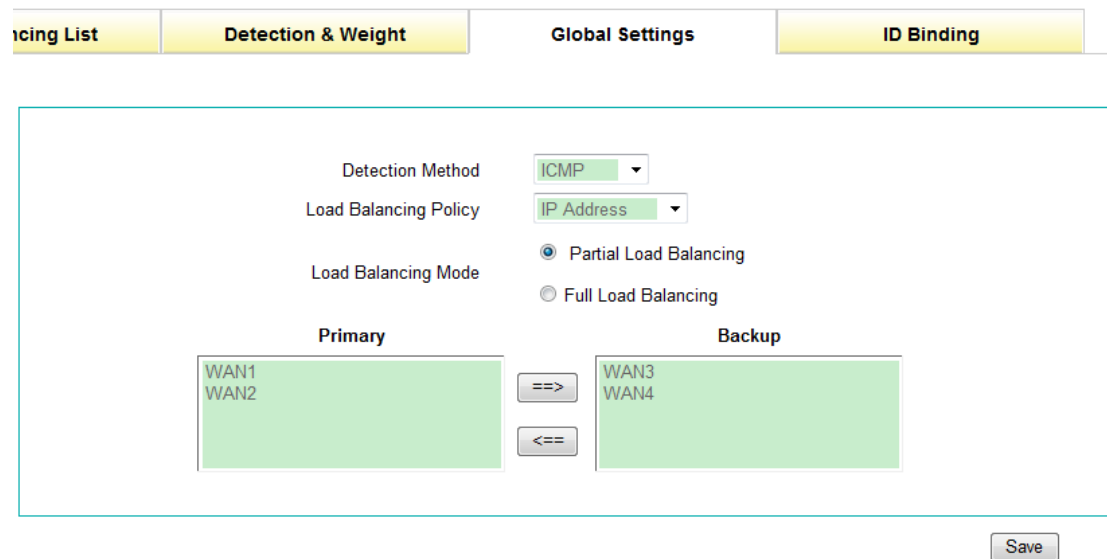


Figure 6-12 Global Settings - Partial Load Balancing

Please refer to section **6.3.4.1 Full Load Balancing** for detailed description of the **Detection Method** and **Load Balancing Policy**.

- ✧ **Load Balancing Mode:** It specifies the mode of load balancing. Here please select **Partial Load Balancing**. Refer to **section 6.3.1.2 Load Balancing Mode** for more information.
- ✧ **Primary:** It specifies the primary connection group. An Internet connection in the **Primary** list box is a primary connection. Refer to **section 6.3.1.2 Load Balancing Mode** for more information.
- ✧ **Backup:** It specifies the backup connection group. An Internet connection in the

Backup list box is a backup connection. Refer to **section 6.3.1.2 Load Balancing Mode** for more information.

- ✧ **==>**: Select one or more Internet connections in the **Primary** list box, and then click **==>** to move the selected connection(s) to the **Backup** list box.
- ✧ **<==**: Select one or more Internet connections in the **Backup** list box, and then click **==>** to move the selected connection(s) to the **Primary** list box.
- **Save**: Click it to save the load balancing global settings.

 **Note**

1. The **WAN1** Internet Connection can only be located in the **Primary** list box, that is, you cannot move it to the **Backup** list box.
2. If you change the **Load Balancing Mode** from **Partial Load Balancing** to **Full Load Balancing** and click the **Save** button to save the change, the Device will automatically move all the Internet connection(s) in the **Backup** list box to the **Primary** list box.
3. If you move all the Internet connection(s) in the **Backup** list box to the **Primary** list box and click the **Save** button to save change, or delete all the backup connections in the **Basic > WAN > WAN List** page, the Device will automatically switch the **Load Balancing Mode** from **Partial Load Balancing** to **Full Load Balancing**.

6.3.5 Detection and Weight Settings

 **Note**

In the **Basic > Load Balancing > Detection & Weight** page, you can configure the connection detection related parameters (**Detection Target IP**, **Detection Interval**, **Retry Times**) and **Weight** for each Internet connection respectively. The operation is as follows: Click the **Edit** hyperlink of an Internet connection in the **Load Balancing List** to go to **Detection & Weight** setup page, and then configure those parameters for the selected Internet connection, lastly click the **Save** button.

Binding List	Detection & Weight	Global Settings	ID Binding
WAN1(Static IP)			
Detection Target IP	Other IP Address	200.200.200.254	
Detection Interval	1000	milliseconds 0 means no detecting	
Retry Times	3		
Weight	1		
Save			

Figure 6-13 Detection and Weight Settings

- ✧ **Detection Target IP:** It indicates the IP address of a detection target device. The Device will monitor an Internet connection by sending the detection packets to the detection target IP address. If you select **Gateway IP Address** from the drop-down list, the Device will send the detection packets to the selected Internet connection's default gateway; If you select **Other IP Address** from the drop-down list, you need enter an appropriate public IP address in the associated text box, then the Device will send the detection packet to this IP address.
- ✧ **Detection Interval:** It specifies the time interval at which the Device periodically sends detection packets, one packet at a time. The default value is 1000 milliseconds. It should be between 1000 and 60000 milliseconds, or 0; and 0 means that connection detection is disabled on the selected Internet connection.
- ✧ **Retry Times:** It specifies the number of retries per detection period. The default value is 3.
- ✧ **Weight:** It specifies the weight of the selected Internet connection. Refer to **section 6.3.2.1 Allocating Traffic according to Connection Bandwidth** for more information about how to set it.
- **Save:** Click it to save the detection and weight settings of the selected Internet connection.



Note

The **Detection Target IP**, **Detection Interval**, and **Retry Times** are connection detection related parameters. For more information about them, please refer to **section 6.3.1.1 Internet Connection Detection Mechanism**.

6.3.6 Load Balancing List

Load Balancing List										
Detection & Weight				Global Settings			ID Binding			
Interface	Connection Type	Primary/Backup	Weight	Connection Status	Sessions Ratio	Detection Target Type	Detection Target IP	Detection Interval	Retry Times	Edit
WAN1	Static IP	Primary	1	Closed	0%	Other IP Address	200.200.200.254	1000	3	Edit
WAN2	DHCP	Primary	1	Closed	0%	Gateway IP Address	0.0.0.0	0	3	Edit
WAN3	PPPoE	Backup	1	Closed	0%	Other IP Address	202.202.199.133	1000	3	Edit
WAN4	PPPoE	Backup	1	Closed	0%	Gateway IP Address	0.0.0.0	0	3	Edit

Figure 6-14 Load Balancing List

- **Edit an Internet Connection:** If you want to configure or modify the detection related parameters and **Weight** of an Internet connection, click its **Edit** hyperlink, the related information will be displayed in the **Detection & Weight** page. Then configure or modify it, and click the **Save** button.
- **View Load Balancing List:** When you have configured load balancing global parameters, and detection and weight settings for one or more Internet connections, you can view the related configuration and status information in the **Load Balancing List**.
- **Refresh Load Balancing List:** Click the **Refresh** button to view the latest information in the list.

6.3.7 How to Configure Load Balancing

6.3.7.1 The Process of Configuring Load Balancing

Only after you have configured more than one Internet connections, the secondary menu of **Load Balancing** will be displayed. The process of configuring load balancing is as follows:

1. Go to the **Basic > WAN** page, configure the WAN1 Internet connection firstly, and then configure other Internet connection(s) as required. Note that you also can configure the WAN1 connection through the **Quick Wizard**.
2. Go to the **Basic > Load Balancing** page, click the **Edit** hyperlink of an Internet connection in the **Load Balancing List** to go to the **Detection & Weight** page to

configure detection related parameters and **Weight** for the selected connection. Then continue to configure these parameters for other connection(s) one by one.

3. Go to the **Basic > Load Balancing > Global Settings** page to configure global parameters as required.
4. Go to the **Basic > Load Balancing > ID Binding** page to enable ID binding feature if needed.

6.3.7.2 The Configuration Steps of Connection Detection and Weight

- Step 1** Go to the **Basic > Load Balancing** page.
- Step 2** Click the **Edit** hyperlink of an Internet connection in the **Load Balancing List** to go to the **Detection & Weight** page.
- Step 3** Configure the connection detection related parameters (**Detection Target IP, Detection Interval, Retry Times**) and **Weight** for the selected Internet connection as required.
- Step 4** Click the **Save** button to save the detection and weight settings for the selected Internet connection.
- Step 5** If you want to configure the connection detection related parameters and **Weight** for another Internet connection, please repeat the above steps.

6.3.7.3 The Configuration Steps of Load Balancing Global Settings

- Step 1** Go to the **Basic > Load Balancing > Global Settings** page.
- Step 2** Specify the **Detection Method** as required.
- Step 3** Specify the **Load Balancing Policy** as required.
- Step 4** Specify the **Load Balancing Mode** as required. If you choose **Partial Load Balancing** as **Load Balancing Mode**, you need move one or more Internet connections from the **Primary** list box to the **Backup** list box according to actual requirement. .
- Step 5** Click the **Save** button to save the load balancing global settings.

6.3.7.4 The Configuration Steps of ID Binding

- Step 1** Go to the **Basic > Load Balancing > ID Binding** page.
- Step 2** Select the **Enable ID Binding** check box if needed.
- Step 3** Click the **Save** button to save the ID binding settings.

6.3.8 Related Detection Route

When connection detection is enabled on an Internet connection (i.e., **Detection Interval** is more than 0), the Device will automatically create a detection route for the connection to ensure that the detection packets are forwarded through it. You can view the detection route configuration in the **Static Route List** on the **Advanced > Static Route** page. Refer to section **7.1.1.2 System Reserved Static Routes** for more information about detection routes.



Note

For a static IP or DHCP Internet connection, when its **Detection Target IP** is set to **Gateway IP Address**, the system will directly use its default route to forward detection packets to monitor the connection. That is, the default route also acts as a detection route.

6.4 DHCP & DNS

This section describes the **Basic > DHCP & DNS** page.

The Dynamic Host Configuration Protocol (DHCP) provides a framework for passing configuration information to hosts on a TCP/IP network. DHCP allows a host to be configured automatically, eliminating the need for intervention by a network administrator. The Device can act as a DHCP server to assign network addresses and deliver other TCP/IP configuration parameters (such as gateway IP address, DNS server IP address, WINS server IP address, etc.) to the LAN hosts.

6.4.1 DHCP Server

Setting	Value
Enable DHCP Server	<input checked="" type="checkbox"/>
Start IP Address	192.168.16.65
Subnet Mask	255.255.255.0
Number of Addresses	62
Default Gateway	192.168.16.1
Lease Time	3600 seconds
Primary DNS Server	192.168.1.99
Secondary DNS Server	202.106.46.151

Figure 6-15 DHCP Server Settings

- ✧ **Enable DHCP Server:** It allows you to enable or disable DHCP server. If you want to enable DHCP server on the Device, please select this check box.
- ✧ **Start IP Address:** It specifies the starting IP address assigned by the DHCP server. In most cases, this address should be on the same subnet as the Device's LAN IP address.
- ✧ **Subnet Mask:** It specifies the subnet mask of the IP addresses assigned by the DHCP server. In most cases, this subnet mask should be the same with the Device's LAN subnet mask.
- ✧ **Number of Addresses:** It specifies the maximum number of IP addresses that can be assigned by the DHCP server.

- ✧ **Default Gateway:** It specifies the IP address of the default gateway for a DHCP client. In most cases, this address should be the same with the Device's LAN IP address, that is, the Device is used as the default gateway for the LAN hosts.
- ✧ **Lease Time:** It specifies a length of time (in seconds) during which a client host can use an assigned IP address. If the lease expires, the client is automatically assigned a new dynamic IP address. Before the lease expires, the client typically needs to renew its address lease assignment with the server. The default value is 3600 seconds.
- ✧ **Primary DNS Server:** It specifies the IP address of the primary DNS server that is available to a DHCP client. If you have already set the **Primary DNS Server** through the **Quick Wizard** or in the **Basic > WAN** page, the Device will automatically set up the same value here.
- ✧ **Secondary DNS Server:** It specifies the IP address of the secondary DNS server that is available to a DHCP client. If you have already set the **Secondary DNS Server** through the **Quick Wizard** or in the **Basic > WAN** page, the Device will automatically set up the same value here.
- **Save:** Click it to save the DHCP server settings.

**Note**

If you want a LAN host to obtain an IP address and other TCP/IP parameters from the Device's built-in DHCP server, please select the **Obtain an IP address automatically** option in the **TCP/IP properties** dialog box on the host.

6.4.2 DHCP Auto Binding

If the hosts change frequently on your LAN, it is very troublesome to configure DHCP manual bindings. Using **ARP Spoofing Defense** (see **section 12.1.1 Internal Attack Defense**) feature also needs periodic maintenance. So usually there are some users who can't access the Device and Internet. To deal with these issues, the Device provides DHCP auto binding feature.

Once the DHCP auto binding is enabled, the Device will immediately scan the LAN to detect active hosts connected to the Device, learn dynamic ARP information and bind the related valid IP and MAC address pairs. After that, when a client host obtains an IP address from the Device that acts as a DHCP server, the Device will immediately bind this host's IP and MAC address pair. So it can effectively protect the Device and LAN hosts against ARP Spoofing.

Server DHCP Auto Binding DNS Proxy

Enable DHCP Auto Binding

Enable DHCP Auto Deleting

Save

Figure 6-16 DHCP Auto Binding

- ✧ **Enable DHCP Auto Binding:** It allows you to enable or disable DHCP auto binding. If you select this check box to enable DHCP auto binding, once a LAN host obtains an IP address from the Device that acts as a DHCP server, the Device will immediately bind this host's IP and MAC address pair. Else, the Device will not perform auto binding operation.
- ✧ **Enable DHCP Auto Deleting:** It allows you to enable or disable DHCP auto deleting. If you select this check box to enable DHCP auto deleting, the Device will automatically delete a DHCP auto binding entry if the corresponding host releases the IP address initiatively or its lease expires. Else, the Device will not perform auto deleting operation.
- **Save:** Click it to save your settings.

6.4.3 DNS Proxy

When acting as a DNS proxy, the Device listens for incoming DNS requests on the LAN interface, relays the DNS requests to the current public network DNS servers, and replies as a DNS resolver to the requesting LAN hosts.

Server DHCP Auto Binding DNS Proxy

Enable DNS Proxy

Save

Figure 6-17 Enable DNS Proxy

- ✧ **Enable DNS Proxy:** It allows you to enable or disable DNS proxy. If you want to enable DNS proxy on the Device, please select this check box.
- **Save:** Click it to save the DHCP proxy settings.

**Note**

1. If the DNS proxy is enabled on the Device, in order to use DNS proxy service normally, you need set the LAN hosts' primary DNS server to the Device's LAN IP address. Note: If the DHCP server is also enabled on the Device, the Device will assign its LAN IP address as the primary DNS server address to the LAN hosts automatically.
2. To ensure that the DNS proxy works well, you should at least specify the primary DNS server provided by your ISP on the Device. It is obvious that you can specify the secondary DNS server if it is provided by your ISP.
3. The Device can act as a DNS proxy server to all LAN users; this greatly simplifies the LAN hosts setup. For example, there is a LAN DNS proxy server on which a DNS proxy software is installed (e.g., Wingate), and the LAN users take this server's IP address as the primary DNS server address. Now, the Device will be used as a new gateway for the LAN hosts. In this case, in order to use DNS proxy service normally, the administrator only need change the Device's LAN IP address to the old proxy DNS server's IP address, and enable DNS proxy on the Device, without modify the LAN hosts' related settings.

Chapter 7 Advanced Setup

This chapter describes how to configure and use the Device advanced features, which include static route, policy-based routing, DNS redirection, Plug and Play, SNMP, SYSLOG, DDNS, and switch, and so on.

7.1 Static Route

This section describes the **Advanced > Static Route** page.

In this page, you can configure not only static routes, but also static route PDBs (PDB: Policy Database). Using static route PDBs, you can create a large batch of static routes at a time, thus the traffic destined for one ISP's servers will be forwarded through this ISP's connection, but not another ISP's connection.

The following describes how to configure and user static route and static route PDB.

7.1.1 Static Route

7.1.1.1 Introduction to Static Route

A static route is manually configured by the network administrator, which is stored in a routing table. By using routing table, the Device can select an optimal transmission path for each received packet, and forward the packet to the destination site effectively. The proper usage of static routes can not only improve the network performance, but also achieve other benefits, such as traffic control, provide a secure network environment.

The disadvantage of using static routes is that they cannot dynamically adapt to the current operational state of the network. When there is a change in the network or a failure occurs, some static routes will be unreachable. In this case, the network administrator should update the static routes manually.

7.1.1.2 System Reserved Static Routes

In the system, there are two types of reserved static routes: default route and detection

route. The following describes them respectively.

1. Default Routes

A default route is used to forward packets that don't match any other route in the routing table. The packets will be forwarded to the default gateway specified by the default route. The default route's destination IP address and subnet mask both are 0.0.0.0.

After you have finished configuring the WAN1 Internet connection through the **Quick Wizard**, or configuring the WAN1 Internet connection and other connections in the **Basic > WAN** page, the Device will automatically create a default route for each Internet connection respectively. You can go to the **Status > Route Stats** page to view their status information in the **Routing Table**. A default route's **Destination IP/Mask** is **0.0.0.0/0**.

2. Detection Routes

If connection detection is enabled on an Internet connection (i.e., the **Detection Interval** is more than 0) in the **Basic > Load Balancing** page, the Device will automatically create a detection route for the connection to ensure that the detection packets are forwarded through it. You can view the detection route configuration in the **Static Route List** on this page. Table 7-1 provides the IDs of detection routes for the Internet connections with different interfaces and connection types.



Note

For a static IP or DHCP Internet connection, when its **Detection Target IP** is set to **Gateway IP Address**, the system will directly use its default route to forward detection packets to monitor the connection. That is, the default route also acts as a detection route.

Internet Connection		Detection Route ID
Physical Interface	Connection Type	
WAN1	Static IP	Detect
	DHCP	Detect
	PPPoE	Detect
WAN2	Static IP	DETEFIX_03
	DHCP	DETEDYN_03
	PPPoE	DETEPPP_01

WAN3	Static IP	DETEFIX_04
	DHCP	DETEDYN_04
	PPPoE	DETEPPP_02
WAN4	Static IP	DETEFIX_05
	DHCP	DETEDYN_05
	PPPoE	DETEPPP_03

Table 7-1 Reserved Detection Route Name

7.1.1.3 Static Route Settings

Route List

Route Settings

Predefined	<input type="text" value="None"/>	
Destination IP	<input type="text" value="200.200.200.12"/>	
Subnet Mask	<input type="text" value="255.255.255.0"/>	
Gateway IP Address	<input type="text" value="0.0.0.0"/>	
Bind to	<input type="text" value="LAN"/>	
Description	<input type="text"/>	
Advanced Options	<small>(Detection Interval, Priority and Metric)</small>	
Detection Interval	<input type="text" value="0"/>	milliseconds
Priority	<input type="text" value="60"/>	
Metric	<input type="text" value="1"/>	

Figure 7-1 Static Route Settings

- ✧ **Predefined:** When creating a static route, please leave the default value of **None**. Else, select one predefined route PDB (policy database).
- ✧ **Destination IP:** It specifies the IP address of the destination network or destination host.
- ✧ **Subnet Mask:** It specifies the subnet mask associated with the destination network.

- ✧ **Gateway IP Address:** It specifies the IP address of the next hop gateway or router to which to forward the packets.
- ✧ **Bind to:** It specifies an outbound interface through which the packets are forwarded to the next hop gateway or router. The available options are the name of each physical interface, and **Local**. **Local** means internal soft-route interface, and the packets will be forwarded to the Device itself.
- ✧ **Description:** It specifies the description of the static route. When creating a static route, you may enter the description for it. Else, the description is provided by the system.
- ✧ **Detection Interval:** It is same with the **Detection Interval** in the **Basic > Load Balancing > Detection & Weight** page. Only the detection route needs it. It specifies the time interval at which the Device sends the detection packets to detecting the corresponding Internet connection status. Refer to **section 6.3.5 Detection and Weight Settings** for more information.
- ✧ **Priority:** It indicates the priority of the route. If there are multiple routes to the same destination with different priorities, the Device will choose the route with the highest priority to forward the packets. The smaller the value, the higher the priority.
- ✧ **Metric:** It indicates the cost of using the route, which is typically the number of hops to the IP destination. If there are multiple routes with same priority to the same destination, the Device will choose the route with the lowest metric to forward the packets.
- **Save:** Click it to save the static route settings.

**Note**

1. When creating a static route, you should specify the next hop IP address by the **Gateway IP Address** or **Bind to**. If the outbound interface is a physical interface, you should specify the **Gateway IP Address**, but may not specify the **Bind to** (i.e., leave it blank). In this case, the Device can select an optimal transmission path. If the outbound interface is a dial interface related to a dial connection (e.g., PPPoE connection), you should select the corresponding physical interface from the **Bind to** drop-down list, but need not specify the **Gateway IP Address** (i.e., leave it the default value **0.0.0.0**). In this case, the next hop IP address is assigned by a dial server (e.g., PPPoE server).
2. In most cases, please don't modify the system reserved static route (e.g., Default, Detect) to avoid surfing the Internet abnormally.

7.1.1.4 Static Route List

ID	Predefined	Destination IP	Subnet Mask	Gateway IP Address	Detection Interval	Priority	Metric	Bind to	Description	Edit
<input type="checkbox"/> Default	None	0.0.0.0	0.0.0.0	200.200.200.1	1000	60	1	WAN1		Edit
<input type="checkbox"/> Detect	None	200.200.200.254	255.255.255.255	200.200.200.1	0	60	1	WAN1		Edit
<input type="checkbox"/> 1	None	1.1.3.0	255.255.255.0	192.168.16.1	0	60	1	LAN		Edit
<input type="checkbox"/> DYNRT_03	None	0.0.0.0	0.0.0.0	0.0.0.0	0	60	1	WAN2		Edit
<input type="checkbox"/> 3	None	200.200.200.12	255.255.255.0	0.0.0.0	0	60	1	WAN1		Edit
<input type="checkbox"/> DETEPPP_02	None	202.202.199.133	255.255.255.255	0.0.0.0	1000	60	1	WAN3		Edit

Figure 7-2 Static Route List

- **Add a Static Route:** If you want to add a new static route, click the **New** button or select the **Route Settings** tab to go to the setup page, and then configure it, lastly click the **Save** button.
- **View Static Routes:** When you have configured some static routes, you can view them in the **Static Route List**.
- **Edit a Static Route:** If you want to modify a configured static route, click its **Edit** hyperlink, the related information will be displayed in the setup page. Then modify it, and click the **Save** button.
- **Delete Static Route(s):** If you want to delete one or more static routes, select the leftmost check boxes of them, and then click the **Delete** button.
- **Display Routing Table:** Click this hyperlink to go to the **Status > Route Stats** page to view the current status of all the active routes in the **Routing Table**.

7.1.1.5 How to Add the Static Routes

If you want to add one or more static routes, do the following:

- Step 1** Go to the **Advanced > Static Route** page.
- Step 2** Click the **New** button or select the **Route Settings** tab to go to the setup page.
- Step 3** Specify the **Destination IP** and **Subnet Mask** for the static route.

Step 4 Specify the next hop IP address by the **Gateway IP Address** or **Bind to**.

If the outbound interface is a physical interface, you should specify the **Gateway IP Address**, but may leave the **Bind to** blank. In this case, the Device will select an optimal transmission path.

For example, a static route's destination network is 192.168.1.0/24, gateway IP address is 192.168.1.254, and the outbound interface is a physical interface. Here you should enter **192.168.1.254** in the **Gateway IP Address** text box, but may leave the **Bind to** blank. The Device will select an optimal transmission path. The detailed settings are shown in the following figure.

Route Settings	
Predefined	None
Destination IP	192.168.1.0
Subnet Mask	255.255.255.0
Gateway IP Address	192.168.1.254
Bind to	
Description	
<u>Advanced Options</u>	(Detection Interval, Priority and Metric)

Save

Figure 7-3 Static Route Settings - Example One

If the outbound interface is a dial interface, you should select the corresponding physical interface from **Bind to** drop-down list, but need leave the **Gateway IP Address** the default value **0.0.0.0**. In this case, the next hop IP address is assigned by a dial server (e.g., PPPoE server).

For example, a static route's destination network is 218.19.213.45/24, the outbound interface is a PPPoE dial interface, and the corresponding physical interface is WAN2. Here you should select **WAN2** from the **Bind to** drop-down list, but need leave the **Gateway IP Address** the default value **0.0.0.0**. The next hop IP address is assigned by your ISP's PPPoE server. The detailed settings are shown in the following figure.

ute List Route Settings

Predefined	<input type="text" value="None"/>
Destination IP	<input type="text" value="218.19.213.45"/>
Subnet Mask	<input type="text" value="255.255.255.0"/>
Gateway IP Address	<input type="text" value="0.0.0.0"/>
Bind to	<input type="text" value="WAN2"/>
Description	<input type="text"/>
<u>Advanced Options</u>	(Detection Interval, Priority and Metric)

Figure 7-4 Static Route Settings - Example Two

- Step 5** Specify the **Detection Interval** if you want to detect connection status.
- Step 6** Specify the **Priority** and **Metric** for the static route as required.
- Step 7** Click the **Save** button to save the settings. You can view the static route in the **Static Route List**.
- Step 8** If you want to add another new static route, please repeat the above steps.

 **Note**

If you want to delete one or more static routes, select the leftmost check boxes of them in the **Static Route List**, and then click the **Delete** button.

7.1.2 Static Route Policy Database

 **Note**

The policy database is called PDB for short in this document.

7.1.2.1 Introduction to Static Route PDB

A user (e.g., Internet Café or Business) using multiple Internet connections usually applies

for them from different ISPs, for example, one is TEL Internet connection, and another is CNC Internet connection. In some cases, if packets accessing one ISP's servers are forwarded through another ISP's connection, the access rate may be very slow, or the access even be forbidden. To ensure that the LAN hosts access the servers normally, the traffic destined for one ISP's servers should be forwarded through this ISP's connection, but not another ISP's connection. You can easily achieve this by using static route PDBs.

The system provides three predefined route PDBs whose names are **TEL**, **CNC** and **ChinaMobile**. The TEL PDB is used to access the TEL servers (i.e., the servers provided by China Network Communications Corporation), the CNC PDB is used to access the CNC servers (i.e., the servers provided by China Network Communications Corporation), and the ChinaMobile PDB is used to access the China Mobile servers (i.e., the servers provided by China Mobile Communications Corporation). The TEL PDB encapsulates many TEL subnets information (IP addresses and subnet masks), the CNC PDB encapsulates many CNC subnets information, and the ChinaMobile PDB encapsulates many China Mobile subnets information. By introducing route PDB, the users don't need add static routes one by one, but instead create a large batch of static routes at a time. Then the traffic destined for TEL servers will be forwarded through the TEL connection, the traffic destined for CNC servers will be forwarded through the CNC Internet connection, and the traffic destined for China Mobile servers will be forwarded through the China Mobile connection.

UTT Technologies Co., Ltd. will successively provide more route PDBs according to actual user requirements. You may go to the **Restriction > Policy Database** page to view the route PDBs status information in the **Policy Database List**, such as version, reference status, and so on.

In addition, as the IP addresses of ISP servers often change, the UTT's technical engineers will acquire the related information and provide the latest route PDBs aperiodically as required. In order to facilitate using PDBs, we provide PDB online update function. That is, you only need go to the **Restriction > Policy Database** page, and click the **Update** hyperlink of a route PDB entry in the **Policy Database List**. Then the Device will download the latest PDB from designated web site and apply it automatically.

7.1.2.2 Static Route PDB Settings

Predefined	CNC
Gateway IP Address	200.200.200.1
Bind to	WAN2
Description	Routing PDB
Advanced Options	(Detection Interval, Priority and Metric)

Figure 7-5 Static Route PDB Settings

Because each static route PDB encapsulates many IP addresses and subnet masks, you needn't configure the **Destination IP** and **Subnet Mask** when creating a static route PDB entry as shown in Figure 7-5.

As a route PDB entry's **Gateway IP Address**, **Bind to**, **Detection Interval**, **Priority** and **Metric** are the same with a static route's, please refer to **section 7.1.1.3 Static Route Setup** for detailed description.

- ✧ **Predefined:** You should select a PDB option when creating a static route PDB entry. The available options are **TEL**, **CNC** and **ChinaMobile**. Note that the **TEL** PDB should be bound to a TEL connection, the **CNC** PDB should be bound to a CNC connection, and the **ChinaMobile** PDB should be bound to a China Mobile connection.
- ✧ **Detection Interval:** Its value should be 0 for a route PDB entry.
- ✧ **Description:** Its value is **Routing PDB**, which is provided by the system automatically when creating a static route PDB.
- ✧ **Save:** Click it to save the static route PDB entry settings.

When you have created a route PDB entry here, the system will automatically create many static routes that have the following characteristics:

- Their **Destination IP** and **Subnet Mask** are predefined by the route PDB.
- Each static route has same **Gateway IP Address**, **Bind to**, **Detection Interval**, **Priority** and **Metric**, that is, the same with the route PDB. Note: As the **Detection Interval** can only be set to 0 when creating the PDB entry, so each static route's **Detection Interval** is 0.

- ID values are 1, 2, 3 ... incrementally.



Note

If there is a static route PDB entry bound to an Internet connection, once the connection is activated, all the static routes created by the route PDB entry will take effect immediately. You can go to the **Status > Route Stats** page to view the settings and status of these static routes in the **Routing Table**.

7.1.2.3 How to Add the Static Route PDB Entries

If you want to add one or more static route PDB entries, do the following:

- Step 1** Go to the **Advanced > Static Route** page.
- Step 2** Click the **New** button or select the **Route Settings** tab to go to the setup page.
- Step 3** Select a PDB option from the **Predefined** drop-down list.
- Step 4** Specify the next hop IP address by the **Gateway IP Address** or **Bind to**.

If the outbound interface is a physical interface, you should specify the **Gateway IP Address**, but may leave the **Bind to** blank. In this case, the Device will select an optimal transmission path.

For example, you want to create a TEL route PDB entry. The TEL Internet connection is static IP connection (that is, the outbound interface is a physical interface), and gateway IP address is 200.200.200.254. Here you should enter **200.200.200.254** in the **Gateway IP Address** text box, but may leave the **Bind to** blank. The Device will select an optimal transmission path. The detailed settings are shown in the following figure.

Route List	Route Settings
	<p>Predefined: TEL</p> <p>Gateway IP Address: 200.200.200.254</p> <p>Bind to: </p> <p>Description: Routing PDB</p> <p><u>Advanced Options</u>: (Detection Interval, Priority and Metric)</p> <p>Save</p>

Figure 7-6 Static Route PDB Settings - Example One

If the outbound interface is a dial interface, you should select the corresponding physical interface from the **Bind to** drop-down list, but need leave the **Gateway IP Address** the default value **0.0.0.0**. In this case, the next hop IP address is assigned by a dial server (e.g., PPPoE server).

For example, you want to create a CNC route PDB entry. The CNC Internet connection is PPPoE connection (that is, the outbound interface is a dial interface), and the corresponding physical interface is WAN2. Here you should select **WAN2** from the **Bind to** drop-down list, but need leave the **Gateway IP Address** the default value **0.0.0.0**. The next hop IP address is assigned by your ISP's PPPoE server. The detailed settings are shown in the following figure.

The screenshot shows the 'Route Settings' configuration page. It includes the following fields:

- Predefined:** CNC (selected in a dropdown menu)
- Gateway IP Address:** 0.0.0.0 (text input)
- Bind to:** WAN2 (selected in a dropdown menu)
- Description:** Routing PDB (text input)
- Advanced Options:** (Detection Interval, Priority and Metric) (text input)

A 'Save' button is located at the bottom right of the configuration area.

Figure 7-7 Static Route PDB Settings - Example Two

- Step 5** Specify the priority and metric for the static route PDB entry as required. In most cases, please leave the default values.
- Step 6** Click the **Save** button to save the settings. You can view the static route PDB entry in the **Static Route List**.
- Step 7** If you want to add another new static route PDB entry, please repeat the above steps.



Note

If you want to delete one or more static route PDB entries, select the leftmost check boxes of them in the **Static Route List**, and then click the **Delete** button.

7.1.2.4 How to Update a System Default Static Route PDB

As mentioned earlier, if you want to update a system default static route PDB, please go to

the **Restriction > Policy Database** page, and click the **Update** hyperlink of the route PDB in the **Policy Database List**. Then the Device will download the latest PDB from designated web site and apply it automatically.

Note that if the route PDB has been referenced, you should reference it again in this page to let the related settings take effect. The steps are as follows: At first click the **Edit** hyperlink of the route PDB, and then select the PDB from the **Predefined** drop-down list again, lastly click the **Save** button to make the related settings take effect.

7.2 Policy-Based Routing

This section describes the **Advanced > PBR** page.

PBR (policy-based routing) provides a tool for forwarding and routing data packets based on the user-defined policies. Different from the traditional destination-based routing mechanism, PBR enables you to use policies based on source and destination address, protocol, port, schedule, and other criteria to route packets flexibly.

7.2.1 Policy-Based Routing Settings

The screenshot shows the 'PBR Settings' configuration page. It is divided into three main sections: 'PBR Rule', 'Address', and 'Service'.
 - **PBR Rule:** 'Bind to' is set to 'WAN1'. 'Schedule' is set to 'Always'. There is an 'Edit Schedule' link. The 'Description' field is empty.
 - **Address:** 'Source' has 'Addresses From' selected with empty input fields, and 'Address Group' selected with 'Any Address' in a dropdown and an 'Edit Address Group' link. 'Destination' has 'Addresses From' selected with empty input fields, and 'Address Group' selected with 'Any Address' in a dropdown and an 'Edit Address Group' link.
 - **Service:** 'Ports From' is selected with empty input fields. 'Service Group' is selected with 'Any Service' in a dropdown and an 'Edit Service Group' link. The 'Protocol' dropdown is set to 'ICMP'.
 A 'Save' button is located at the bottom right of the form.

Figure 7-8 Policy-Based Routing Settings

- ✧ **Bind to:** It specifies an outbound interface through which the packets matching the PBR entry are forwarded.
- ✧ **Schedule:** It specifies a schedule to restrict when the PBR entry is in effect. The default value is **Always**, which means the PBR entry will be in effect always.

- ✧ **Description:** It specifies the description of the PBR entry. It is usually used to describe the purpose of the entry.
- ✧ **Source:** It specifies the source IP addresses of the packets to which the PBR entry applies. There are two options:
 - **Addresses:** Select it to enter the start and end addresses in the associated text boxes.
 - **Address Group:** Select it to choose an address group from the associated drop-down list. By default, the **Address Group** radio button is selected, and its value is **Any Address**.
- ✧ **Destination:** It specifies the destination IP addresses of the packets to which the PBR entry applies. There are two options:
 - **Addresses:** Select it to enter the start and end IP addresses in the associated text boxes.
 - **Address Group:** Select it to choose an address group from the associated drop-down list. By default, the **Address Group** radio button is selected, and its value is **Any Address**.
- ✧ **Service:** It specifies a range of ports or a service group to which the PBR applies. There are two options:
 - **Ports:** Select it to enter the start and end port numbers in the associated text boxes, and select a protocol type from **Protocol** drop-down list. The port number is between 1 and 65535, and the protocols include TCP, UDP and ICMP.
 - **Service Group:** Select it to choose a service group or predefined service from the associated drop-down list. The Device provides some well-known services, such as telnet, smtp, web, pop3, and so on. By default, the **Service Group** radio button is selected, and its value is **Any Service**.
- **Edit Schedule:** Click it to go to the **Security > Schedule** page to add, view, modify or delete the schedules.
- **Edit Address Group:** Click it to go to the **Security > Address Group** page to add, view, modify or delete the address groups.
- **Edit Service Group:** Click it to go to the **Security > Service Group** page to add, view, modify or delete the service groups.
- **Save:** Click it to save the PBR entry settings.

 **Note**

PBR (Policy-based routing) takes precedence over the Device’s normal destination-based routing. That is, if a packet matches all the criteria (source address, destination address, protocol type, port, etc.) specified in a PBR entry, it will be forwarded through the outbound interface specified in the PDB entry. If no match is found in the PBR list, the packet will be forwarded through normal routing channel (in other words, destination-based routing is performed).

7.2.2 Enable Policy-Based Routing

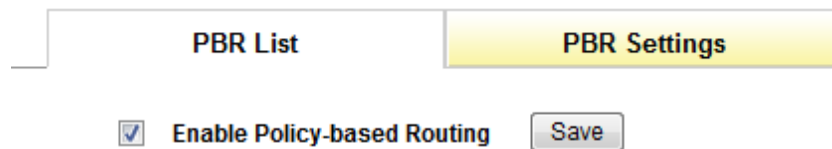


Figure 7-9 Enable Policy-Based Routing

- ✧ **Enable Policy-based Routing:** It allows you to enable or disable policy-based routing. If you select the check box to enable policy-based routing, the configured PBR entries will take effect. Else the PBR entries will be of no effect.
- **Save:** Click it to save your settings.

7.2.3 Policy-Based Routing List

ID	Enable	Schedule	Source Address	Destination Address	Service	Bind to	Description	Edit
1	<input checked="" type="checkbox"/>	Always	[192.168.16.10-192.168.16.100]	Any Address	Destination Port21-23 Protocol TCP	WAN2		Edit
3	<input checked="" type="checkbox"/>	Always	Any Address	Any Address	Any Service	WAN1		Edit

2/20 Lines/Page: 10 First Prev Next Last Search:

Select All

Move before

Figure 7-10 PBR List

- **Add a PBR Entry:** If you want to add a new PBR entry, click the **New** button or select the **PBR Settings** tab to go to the setup page, and then configure it, lastly click the **Save** button.
- **Enable a PBR Entry:** The **Enable** check box is used to enable or disable the corresponding PBR entry. The default value is selected, which means the PBR entry is in effect. If you want to disable the PBR entry temporarily instead of deleting it, please click it to remove the check mark.
- **View PBR Entry(s):** When you have configured some PBR entries, you can view them in the **PBR List**.
- **Edit a PBR Entry:** If you want to modify a configured PBR entry, click its **Edit** hyperlink, the related information will be displayed in the setup page. Then modify it, and click the **Save** button.
- **Delete PBR Entry(s):** If you want to delete one or more PBR entries, select the leftmost check boxes of them, and then click the **Delete** button.
- **Move a PBR Entry:** The Device allows you to move a PBR entry before another entry in the list, the operation is as follows: Select the ID of a PBR entry that you want to move from the **Move** drop-down list, and another entry's ID from the **before** drop-down list, lastly click **OK**. Note that moving a PBR entry in the list doesn't change its ID number.

7.3 DNS Redirection

This section describes the **Advanced > DNS Redirection** page.

7.3.1 Introduction to DNS Redirection

DNS redirection is used to redirect domain names directly to the specified IP addresses, that is, the domain names aren't resolved by DNS server, but are queried in a user-defined list of names-to-addresses mappings. Once you have configured some DNS redirection entries, a DNS redirection list that contains the names-to-addresses mappings will be created. When receiving a DNS request, the Device lookups the requested domain name in the DNS redirection list. If a match is found, the Device will send a DNS response that contains the IP mapped address to the requester. Else, the Device will resolve the domain name by looking up local DNS cache or external DNS servers.

7.3.2 Enable DNS Redirection

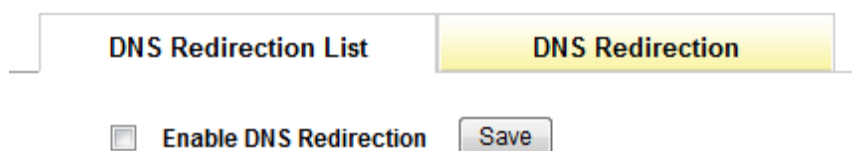


Figure 7-11 Enable DNS Redirection

- ✧ **Enable DNS Redirection:** It allows you to enable or disable DNS redirection. The default value is unselected, which means the configured DNS redirection entries are of no effect. If you want the DNS redirection entries to take effect, please select this check box to enable DNS redirection.
- **Save:** Click it to save your settings.

7.3.3 DNS Redirection List

ID	Enable	Domain Name	Redirecting IP Address	Description	Edit
2	<input checked="" type="checkbox"/>	www.163.com ; www.google.com ; www.baidu.com.cn ;	192.168.1.2	Block 163, google, baidu	Edit
1	<input checked="" type="checkbox"/>	www.sina.com ;	192.168.1.1	Block Sina	Edit

Figure 7-12 DNS Redirection List

- **Add a DNS Redirection Entry:** If you want to add a new DNS redirection entry, click the **New** button or select the **DNS Redirection Settings** tab to go to the setup page, and then configure it, lastly click the **Save** button.
- **Enable a DNS Redirection Entry:** The **Enable** check box is used to enable or disable the corresponding DNS redirection entry. The default value is selected, which means the DNS redirection entry is in effect. If you want to disable the DNS redirection entry temporarily instead of deleting it, please click it to remove the check mark.
- **View DNS Redirection Entry(s):** When you have configured some DNS redirection entries, you can view them in the **DNS Redirection List**.
- **Edit a DNS Redirection Entry:** If you want to modify a configured DNS redirection entry, click its **Edit** hyperlink, the related information will be displayed in the setup page. Then modify it, and click the **Save** button.
- **Delete DNS Redirection Entry(s):** If you want to delete one or more DNS redirection entries, select the leftmost check boxes of them, and then click the **Delete** button.



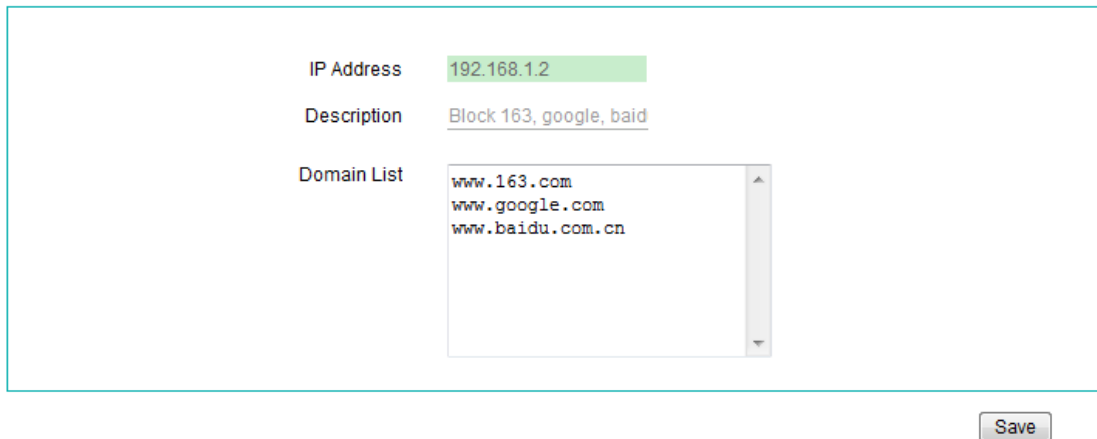
Note

1. A DNS redirection entry whose domain name contains the wildcard character * has lower priority, in other words, the domain name has the highest accuracy will be matched first. For example, there are two DNS redirection entries in the list, the first entry's domain name is www.sina.com, and the second entry's is www.sina.*. When

accessing www.sina.com, the Device will redirect www.sina.com to the IP address specified by the first entry because of higher accuracy.

2. For the entries whose domain names have the same accuracy, in reverse chronological order of creation, the last created entry will be matched first.

7.3.4 DNS Redirection Settings



IP Address: 192.168.1.2

Description: Block 163, google, baid

Domain List: www.163.com, www.google.com, www.baidu.com.cn

Save

Figure 7-13 DNS Redirection Settings

- ✧ **IP Address:** It specifies the IP address to which the specified domain name(s) are redirected.
- ✧ **Description:** It specifies the description of the DNS redirection entry. It is usually used to describe the purpose of the entry.
- ✧ **Domain List:** Each DNS redirection entry has a domain list. You can enter a domain name or multiple domain names that you want to redirect in the **Domain List** box. It supports up to ten different domain names.
- **Save:** Click it to save the DNS redirection entry settings.



Note

1. Different DNS redirection entries can have the same IP addresses or domain names.
2. The domain names that contain the wildcard character * should be different.

3. The domain names that belong to the same **Domain List** should be different.

7.3.5 How to Configure DNS Redirection

Do the following to configure DNS Redirection.

- Step 1** Go to the **Advanced > DNS Redirection** page.
- Step 2** Click the **New** button or select the **DNS Redirection Settings** tab to go to the setup page.
- Step 3** Specify the **IP Address, Description** and **Domain List** for a DNS Redirection entry.
- Step 4** Click the **Save** button to save the settings. You can view the DNS Redirection entry in the **DNS Redirection List**.
- Step 5** If you want to add another new DNS Redirection entry, please repeat the above steps.
- Step 6** Select the **Enable DNS Redirection** check box to enable the DNS redirection, thus all the DNS redirection entries you have created will take effect immediately.

Once you have configured DNS redirection, all the DNS request packets received by the Device will be processed by DNS redirection module firstly.



Note

Please make ensure that **Enable DNS Redirection** check box is selected, else the configured DNS redirection entries will not be in effect.

7.4 Plug and Play

This section describes the **Advanced > Plug and Play** page.

7.4.1 Introduction to Plug and Play

Plug and Play is a new feature of UTT series security firewalls. If you enable plug and play feature on the Device, the LAN users can access the Internet through the Device without changing any network parameters, no matter what IP address, subnet mask, default gateway and DNS server they might have. Obviously, this feature can greatly facilitate the users. As this feature is suitable for hotel network, we also call it hotel special version.

7.4.2 Enable Plug and Play

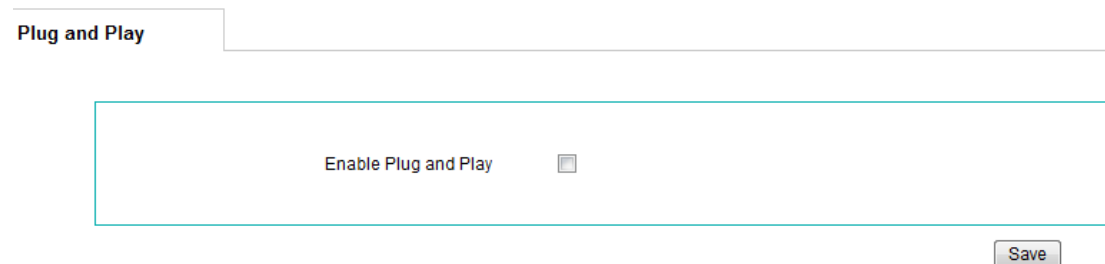


Figure 7-14 Enable Plug and Play

- ✧ **Enable Plug and Play:** It allows you to enable or disable plug and play. By default it is disabled. If you select the check box to enable this feature, no matter what IP address, subnet mask, default gateway and DNS server the LAN users might have, they are able to access the Internet through the Device.
- **Save:** Click it to save your settings.

 **Note**

1. The LAN hosts basic TCP/IP parameters (including IP address, subnet mask, gateway IP address, and DNS server IP address) should be set properly; otherwise, plug and play feature cannot act on those hosts.

2. Once plug and play is enabled, the Device will automatically enable proxy ARP, enable DNS proxy, and disable IP spoofing defense.
3. Once plug and play is enabled, the Device will allow those non-IP/MAC binding users to access the Device and Internet.
4. The users with the same IP address cannot access the Internet at the same time. For example, if a LAN user with IP address 1.1.1.1 has connected to the Device to access the Internet, another user with IP address 1.1.1.1 cannot access the Internet through the Device.
5. A LAN user's IP address cannot be the same with the Device's LAN/WAN interface IP address, gateway IP address, and primary/secondary DNS server IP address; otherwise, the user cannot access the Device and Internet.

7.5 SNMP

This section describes the **Advanced > SNMP** page.

SNMP (Simple Network Management Protocol) is an application layer protocol for collecting information about devices on the network. It is part of the TCP/IP protocol suite which enables network administrators to monitor, configure, and troubleshoot the network devices.

If you enable the SNMP agent on the Device, you can use the SNMP manager software to monitor and manage the Device remotely. The Device supports SNMP v1/v2c and Management Information Base II (MIBII) groups.

To ensure security, the SNMP manager can read the information about the Device but can't change anything.

SNMP Settings

Enable SNMP	<input checked="" type="checkbox"/>
Community Name	uTt22aA
System Name	
System Contact	
System Location	
Allowed SNMP NMSs	<input checked="" type="checkbox"/>
Host 1 IP Address	192.168.16.25
Host 2 IP Address	0.0.0.0
Host 3 IP Address	0.0.0.0

Figure 7-15 SNMP Settings

- ✧ **Enable SNMP:** It allows you to enable or disable the SNMP agent. If you want to enable the SNMP agent on the Device, please select this check box.
- ✧ **Community Name:** It specifies a community name to restrict access to the Device. The SNMP community name is used as a shared secret for SNMP managers to access the SNMP agent. The default value is uTt22aA. To ensure security, it is recommended that you modify it to prevent intruder from using SNMP requests to get the information from the Device.
- ✧ **System Name:** It specifies the host name of the Device.
- ✧ **System Contact:** It specifies the system contact information (such as a name or phone number).
- ✧ **System Location:** It specifies the physical location information of the Device.
- ✧ **Allowed SNMP NMSs:** If you select this check box, you can specify up to three SNMP network management stations (i.e., hosts), and only they can access and manage the Device. Else, any host can use SNMP to manage the Device.
- ✧ **Host 1 IP Address ~ Host 3 IP Address:** They specify the IP addresses of the hosts that can use SNMP to manage the Device.
- **Save:** Click it to save the SNMP settings.

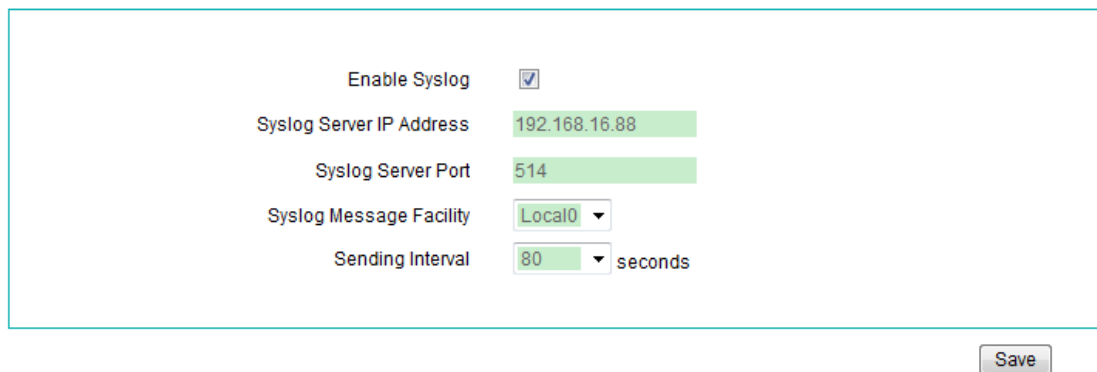
**Note**

If you want to use SNMP Manager to manage the Device via Internet, please select the **SNMP** check box in the **System > Remote Admin** page first.

7.6 SYSLOG

This section describes the **Advanced > SYSLOG** page.

Syslog is a standard protocol used to capture a lot of running information about network activity. The Device supports this protocol and can send its activity logs to an external syslog server. It helps the network administrator monitor, analyze and troubleshoot the Device and network.



Enable Syslog	<input checked="" type="checkbox"/>
Syslog Server IP Address	192.168.16.88
Syslog Server Port	514
Syslog Message Facility	Local0
Sending Interval	80 seconds

Save

Figure 7-16 SYSLOG Settings

- ✧ **Enable Syslog:** It allows you to enable or disable syslog feature. If you want to enable syslog feature on the Device, please select this check box.
- ✧ **Syslog Server IP address:** It specifies the IP address or domain name of the syslog server to which the Device sends syslog messages.
- ✧ **Syslog Server Port:** It specifies the port used by the syslog server to communicate with the Device. In most cases, please leave the default value of **514**, which is a well-known port number.
- ✧ **Syslog Message Facility:** It specifies the facility level used for logging. The facilities are used to distinguish different classes of syslog messages. The available options are local0, local1 through local7.
- ✧ **Sending Interval:** It specifies the time interval (in seconds) at which the Device periodically sends heartbeat messages. If you select the option other than zero, the Device will periodically send heartbeat messages to the syslog server to indicate that it is still alive. The default value is 0, which means the Device will not send heartbeat messages.
- **Save:** Click it to save the Syslog settings.



Note

So far, only the Xport HiPER Manager software of UTT Technologies Co., Ltd. can identify the heartbeat message.

7.7 DDNS

This section describes the **Advanced > DDNS** page.



Note

To ensure that DDNS operates properly, you should synchronize the system clock in the **System > Time** page.

7.7.1 Introduction to DDNS

Dynamic Domain Name Service (DDNS) is a service used to map a domain name which never changes to a dynamic IP address which can change quite often. For example, if you have applied for a PPPoE connection with a dynamically assigned IP address from the ISP's PPPoE server, you can use DDNS to allow the external hosts to access the Device by a constant domain name.

In order to use DDNS service, you should apply for a DDNS account from a DDNS service provider. Each DDNS provider offers its own specific network services. The DDNS service provider reserves the right to change, suspend or terminate your use of some or all network services at any time for any reason. The DDNS service providers supported by UTT Technologies Co., Ltd. currently provide free DDNS services, but they may charge for the DDNS services in the future. In this case, UTT Technologies Co., Ltd. will notify you as soon as possible; if you refuse to pay for the services, you will no longer be able to use them. During the free phase, UTT Technologies Co., Ltd. does not guarantee that the DDNS services can meet your requirements and will be uninterrupted, and UTT does not guarantee the timeliness, security and accuracy of the services.

So far, UTT Technologies Co., Ltd. only supports two DDNS service providers: iplink.com.cn and 3322.org. It will successively support other DDNS service providers in the future.

7.7.2 DDNS Service Offered by iplink.com.cn

7.6.1.1 Apply for a DDNS Account from iplink.com.cn

To use DDNS offered by iplink.com.cn on the Device, you should login to <http://www.utt.com.cn/ddns> to apply for a DDNS account, which includes a fully qualified

domain name (FQDN) with suffix of iplink.com.cn and a key.

注册新主机

主机信息

主机名: .iplink.com.cn

注册号/序列号:

域名用途: 网站 VPN VoIP 其它:

备案号:

Figure 7-17 Apply for a DDNS Account from IPLink.com.cn

- ✧ **Host Name:** It specifies a unique host name of the Device. The suffix of iplink.com.cn will be appended to the host name to create a fully qualified domain name (FQDN) for the Device. For example, if the Device's host name is **test**, then its FQDN is **test.iplink.com.cn**; and it allows you to use **test.iplink.com.cn** to access the Device. Note that to avoid duplication, you had better use the Device's globally unique serial number (SN) as the host name. The SN is the same with the **Registration Number** displayed in the **Advanced > DDNS > DDNS Settings** page.
- ✧ **Registration Number/Serial Number:** It specifies the registration number (i.e., serial number) of the Device. It should be the same with the **Registration Number** displayed in the **Advanced > DDNS > DDNS Settings** page.
- **Register:** Click it to register a DDNS account. Once clicked the **Register** button, you can get a key that matches the registered domain name of the Device.

<input type="checkbox"/>	主机名	域名	产品S/N	密钥 (enkey)	用途	注册时间	备案序号
<input type="checkbox"/>	abcd110	.iplink.com.cn	12132111	QRogDpwtEC29g/FADjdDHS+0oiYbxHJDOEnnKc8Vzauv	测试	2009-10-14 13:07:56	

 **Note**

A domain name can only be registered once; and as each Device has its own unique serial number, you will get different keys if you register the same domain name for different Devices. Thus when you want to replace your Device and use the existing domain name for the new Device, you need login to <http://www.utt.com.cn/ddns> to delete the domain name, and then register it again.

7.7.2.1 DDNS Settings Related to iplink.com.cn

The screenshot shows the DDNS Settings configuration page. At the top, there are two tabs: 'Status' and 'DDNS Settings'. The 'DDNS Settings' tab is active. Below the tabs is a form with the following fields:

- Interface: WAN1 (dropdown menu)
- Registry Website: <http://www.utt.com.cn/ddns> (text field)
- Registration Number: 9270301 (text field)
- Service Provider: iplink.com.cn (dropdown menu)
- Host Name: zhaolili.iplink.com.cn (text field)
- Key: [Redacted with dots]
- Confirm Key: [Redacted with dots]

A 'Save' button is located at the bottom right of the form area.

Figure 7-18 DDNS Settings Related to iplink.com.cn

- ✧ **Interface:** It specifies the WAN interface on which DDNS service is applied. All the WAN interfaces support DDNS feature, and you can use DDNS service on each WAN interface at the same time.
- ✧ **Registry Website:** It allows you to click <http://www.utt.com.cn/ddns> to go to this website to register a DDNS account for the Device.
- ✧ **Registration Number:** It specifies the registration number of the Device.
- ✧ **Service Provider:** It specifies the DDNS service provider who offers services to the Device. Now the Device only supports two DDNS service providers: **iplink.com.cn** and **3322.org**. Here please select **iplink.com.cn**.
- ✧ **Host Name:** It specifies the host name of the Device. It should be the same with the host name that you entered when registering the DDNS account on the website of <http://www.utt.com.cn/ddns>.
- ✧ **Key:** It specifies the key that you got when registering the DDNS account on the website of <http://www.utt.com.cn/ddns>.
- ✧ **Confirm Key:** You should re-enter the key.
- **Save:** Click it to save the DDNS settings.

7.7.3 DDNS Service Offered by 3322.org

7.7.3.1 Apply for a DDNS Account from 3322.org

To use DDNS offered by 3322.org on the Device, you should login to <http://www.3322.org> to apply for a fully qualified domain name (FQDN) with suffix of 3322.org.

希网动态域名 用户创建动态域名 (DynDns)
请正确输入下表的内容
请正确输入域名!

主机名:	<input type="text" value="bed"/>	<input type="text" value="3322.org"/>	<input type="button" value="HELP"/>
IP地址:	<input type="text" value="200.200.254.151"/>	<input type="button" value="HELP"/>	
邮件服务器 (mx):	<input type="text"/>	<input type="button" value="HELP"/>	
备份邮件服务器:	<input type="checkbox"/>	<input type="button" value="HELP"/>	
通配符:	<input type="button" value="是"/>	<input type="button" value="HELP"/>	
			<input type="button" value="确定"/>

Figure 7-19 Apply for a DDNS Account from 3322.org

- ✧ **Host Name:** It specifies a unique host name of the Device. The suffix of `iplink.com.cn` will be appended to the host name to create a fully qualified domain name (FQDN) for the Device. For example, if the Device's host name is **test**, then its FQDN is **test.3322.org**; and it allows you to use **test.3322.org** to access the Device. Note that to avoid duplicate, you had better use the Device's globally unique serial number (SN) as the host name.
- ✧ **IP Address:** It specifies the IP address mapped to the registered domain name of the Device.
- ✧ **OK:** Click it to register the domain name.

7.7.3.2 DDNS Settings Related to 3322.org

status DDNS Settings

Interface WAN1

Registry Website <http://www.3322.org>

Service Provider 3322.org

Host Name UTTtest . 3322.org

User Name zhaolili

Password

Save

Figure 7-20 DDNS Settings Related to 3322.org

- ✧ **Interface:** It specifies the WAN interface on which DDNS service is applied. All the WAN interfaces support DDNS feature, and you can use DDNS service on each WAN interface at the same time.
- ✧ **Registry Website:** It allows you to click <http://www.3322.org> to go to this website to register a DDNS account for the Device.
- ✧ **Service Provider:** It specifies the DDNS service provider who offers services to the Device. Now the Device only supports two DDNS service providers: **iplink.com.cn** and **3322.org**. Here please select **3322.org**.
- ✧ **Host Name:** It specifies the host name of the Device. It should be the same with the host name that you entered when registering the DDNS account on the website of <http://www.3322.org>.
- ✧ **User Name:** It specifies the user name that you entered when registering your user account on the website of <http://www.3322.org>.
- ✧ **Password:** It specifies the password which is created by the website when registering your user account on the website of <http://www.3322.org>.
- **Save:** Click it to save the DDNS settings.



Note

It also allows you to login to <http://www.3322.org> to apply for a domain name (FQDN) with suffix of 2288.org, 6600.org, 7700.org, 8800.org, 8866.org, or 9966.org for the

Device. Refer to **section 7.6.3.1 Apply for a DDNS Account from 3322.org** for detailed operation.

7.7.4 DDNS Verification

To verify whether DDNS is updated successfully, you can use the ping command at the MS-DOS command prompt on the PC, for example: **ping abc.iplink.com.cn**

If the displayed page is similar to the screenshot below: the domain name is resolved to an IP address successfully (200.200.202.152 in this example), DDNS is updated successfully.

```
C:\>ping abc.iplink.com.cn

Pinging abc.iplink.com.cn [200.200.202.152] with 32 bytes of data:

Reply from 200.200.202.152: bytes=32 time<1ms TTL=64
Reply from 200.200.202.152: bytes=32 time<1ms TTL=64
Reply from 200.200.202.152: bytes=32 time<1ms TTL=64
Reply from 200.200.202.152: bytes=32 time<1ms TTL=64

Ping statistics for 200.200.202.152:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```



Note

1. After you have finished configuring an Internet connection, the Device will automatically enable NAT. Then when you ping the Device's domain name from the Internet, the domain name can be resolved to its mapped IP address successfully, but the Device will not respond to the ping request. If you want to ping this IP address, please go to the **Security > Attack Defense > External Defense** page to select the **Enable WAN Ping Respond** check box.
2. Only when the WAN interface IP address is a public IP address, the Internet users can use its mapped domain name to access the Device normally.
3. DDNS feature can help you implement VPN tunnels using dynamic IP addresses on the Device.

7.8 Advanced DHCP

This section describes the **Advanced > DHCP** pages.

7.8.1 Introduction to DHCP

7.8.1.1 Overview

The Dynamic Host Configuration Protocol (DHCP) provides a framework for passing configuration information to hosts on a TCP/IP network. DHCP allows a host to be configured automatically, eliminating the need for intervention by a network administrator. DHCP is built on a client/server model, where one or more DHCP servers assign network addresses and deliver other TCP/IP configuration parameters to DHCP clients (hosts). In addition, DHCP can guarantee to avoid allocation of duplicate IP addresses, and to reassign the IP addresses that are no longer used.

DHCP supports three mechanisms for IP address allocation:

- Automatic allocation: DHCP server assigns a permanent IP address to a client.
- Dynamic allocation: DHCP server assigns an IP address to a client for a limited period of time, which is called a lease. The client may extend its lease with subsequent request, and it may release the address back to the server.
- Manual allocation: A network administrator assigns an IP address to a client, and DHCP server is used simply to convey the assigned address to the client.

A particular network will use one or more of these mechanisms, according to the actual requirements. The dynamic allocation is the only mechanism that allows automatic reuse of addresses that are no longer needed by the client.

7.8.1.2 DHCP Operation Process

The following describes the basic operation principle of DHCP, including the process of requesting for a new IP address, the process of renewing an IP address, and the process of releasing an IP address.

1. Requesting for an IP Address

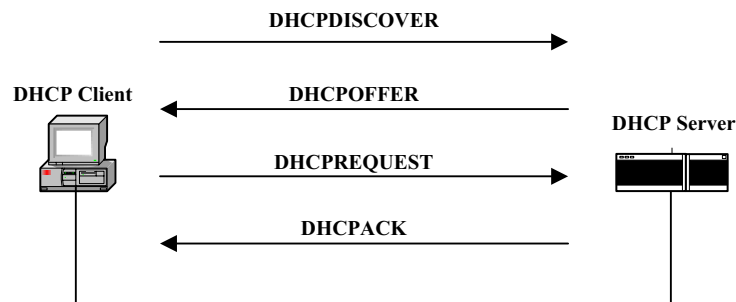


Figure 7-21 Requesting for an IP Address from a DHCP Server

As shown in Figure 7-20, the process of a DHCP client requesting for an IP address from a DHCP server falls into four basic phases:

- **DHCP Discover:** It is the phase that the DHCP client locates a DHCP server to ask for an IP address. The client broadcasts a DHCPDISCOVER message on its local physical subnet. Only DHCP server(s) will respond it.
- **DHCP Inform:** It is the phase that one or more DHCP servers) offer an IP address to the DHCP client. Once received the DHCPDISCOVER message, a DHCP server will send a DHCPOFFER unicast message which includes configuration parameters (such as an IP address, a domain name, a lease, and so on) to the DHCP client.
- **DHCP Request:** It is the phase that the DHCP client accepts the offer, chooses an IP address and requests the address. The client may receive DHCPOFFER messages from more than one DHCP server. Then the client chooses one from them, and broadcasts a DHCPREQUEST message to formally request the offered IP address. The DHCPREQUEST message also includes the server identifier option to indicate which message it has selected, implicitly declining all other DHCPOFFER messages. Once received the DHCPREQUEST message, those servers not selected will release the IP addresses offered to the client.

If the configuration parameters sent to the client in the DHCPOFFER unicast message by the DHCP Server are invalid (a misconfiguration error exists), the client returns a DHCPDECLINE broadcast message to the DHCP Server to reject the configuration assigned.

- **DHCP Acknowledgement:** It is the phase that the DHCP server officially assigns the address to the client. Once received the DHCPREQUEST message, the selected DHCP server will respond with a DHCPACK unicast message containing the IP address and other configuration parameters for the requesting client. Then the client will accept and apply the IP address and other configuration parameters.

2. Renewing an IP Address

- An IP address dynamically allocated by a DHCP server for a client has a lease. The

DHCP server will reclaim the IP address if the lease expires, so the client has to renew the lease in order to use the IP address longer. When one half of the lease time has expired, the client will send a DHCPREQUEST message to the DHCP server, asking to extend the lease for the given configuration. The DHCP server will respond with a DHCPACK message if it agrees to renew the lease.

If the requesting IP address in the DHCPREQUEST message is inconsistent with the allocated IP address whose lease doesn't expire, the DHCP server will respond with a DHCPNAK message.

3. Releasing the IP Address

- When a DHCP client no longer needs the IP address assigned by a DHCP server, it relinquishes the address by sending a DHCPRELEASE message to the DHCP server. The address returns to the address pool for reassignment. Besides the DHCP client sets its IP address to 0.0.0.0.

7.8.1.3 DHCP Message types

DHCP is built on a client/server model. A client and a server may exchange the types of messages listed in the below table.

Message Type	Description
DHCPDISCOVER	Broadcast by a client to find available DHCP servers.
DHCPOFFER	Response from a server to a DHCPDISCOVER message and offering IP address and other parameters.
DHCPREQUEST	<p>Message from a client to servers that does one of the following:</p> <ul style="list-style-type: none"> • Requests the parameters offered by one of the servers, which implicitly declines all other offers. • Requests the extension of a lease on a particular address. • Verifies a previously allocated address after a system or network change (a restart for example).

DHCPDECLINE	Message from a client to server indicating that the offered address is already in use.
DHCPACK	Acknowledgement message from a server to a client with configuration parameters, including IP address.
DHCPNAK	Negative acknowledgement message from a server to a client, refusing the request for parameters. If the client receives a DHCPNAK message, it will restart the configuration process.
DHCPRELEASE	Message from a client to a server cancelling remainder of a lease and relinquishing network address.
DHCPINFORM	Message from a client that already has an IP address (manually configured, for example), requesting further network configuration parameters (DNS server's IP address, for example) from the DHCP server. This message is used very rare.

Table 7-2 DHCP Message Types

7.8.2 Introduction to DHCP Feature of the Device

According to the different settings, the Device can act as a DHCP client, DHCP server or DHCP relay agent. The following sections describe their characteristics respectively.

Note

If the DHCP client is enabled on a physical interface, neither the DHCP server nor DHCP relay agent function can be enabled on it. If both the DHCP server and DHCP relay agent function are enabled on the interface, the DHCP server has higher priority. That is, the Device will chose the DHCP server to process the DHCP messages preferentially; and it will chose the DHCP relay agent to process the messages only when the DHCP server isn't able to process them.

7.8.2.1 Introduction to DHCP Server

When acting as a DHCP server, the Device can allocate network addresses and deliver other TCP/IP configuration parameters (such as gateway IP address, DNS server IP address, WINS server IP address, etc.) to the LAN hosts.

7.8.2.1.1 Address Conflict Detection Method

In order to prevent the DHCP server from assigning duplicate addresses that cause the address conflict, the DHCP server should probe the address before assigning an address to a DHCP client. The device supports two address detection methods: ARP and ICMP. ARP is the system default method which is enabled forever and is not configurable. ICMP method is configurable, and can be disabled.

- **ARP Method:** Before assigning an address to a DHCP client, DHCP will send ARP packets to the address to detect whether it is already in use firstly. After sending two ARP packets in succession, if no response is received, the DHCP server assumes that the address is free. Else, the DHCP server assumes that the address is in use, and will try another address and so on, until it finds a free address.
- **ICMP Method:** Once passed the ARP detection, the address needs to be detected further by ICMP. The DHCP server will send ICMP ECHO REQUEST packets (one packet at a time) to detect if it is already in use. After sending the specified maximum number of ICMP packets in succession, if no response is received, the DHCP server assumes that the address is free and assigns the address to the requesting client. Else, the DHCP server assumes that the address is in use, and will try another address and so on, until it finds a free address and assigns it to the client.

The maximum number of ICMP ECHO REQUEST packets is specified by the parameter **ICMP Ping Packets**, and the maximum amount of time the DHCP server waits for a ping reply packet is specified by the parameter **ICMP Ping Timeout**. By default, the value of **ICMP Ping Packets** is 2, and the value of **DHCP Ping Timeout's** value is 500 milliseconds. If you want to disable the ICMP detection, please set the **DHCP Ping Packets** to 0.

7.8.2.1.2 DHCP Address Pool

The DHCP server assigns an IP address to a requesting client from a DHCP address pool, which also can be configured to provide other TCP/IP configuration parameters to the client, such as the DNS Server, gateway IP address, etc. The Device supports multiple address pools, so you can easily define multiple subnets in the LAN. Before configuring an address pool, you should specify a physical interface to which the pool is bound.

7.8.2.1.3 DHCP Manual Binding

Through DHCP manual binding, you can assign a static IP address to a specific host (client). You may create a manual binding by mapping the IP address to the host's MAC address, Remote ID or Client ID. The DHCP server will always assign the specified IP address to the host that matches the manual binding.

7.8.2.1.4 IP Address Allocation Policy

A DHCP server assigns an IP address to a client based on some parameters contained in the message sent by the client. The parameters are Remote ID, Circuit ID (i.e., Relay Agent ID), giaddr (i.e., Relay Agent IP), Client ID and MAC address, and the priorities of them are descending. Only the highest priority parameter will be effect when more than one parameter is configured. When a matching parameter is found, the DHCP server will assign an address according to this parameter related configuration. If no matching parameter is found, the DHCP server will find an IP address that can be allocated according to the default sequence.

Specifically, a DHCP server assigns an IP address to a client according to the following sequence:

- 1) If the message sent by the client contains Remote ID option, the DHCP server will search the DHCP manual binding list to find out if there is an IP address bound to this Remote ID. If a match is found, the DHCP server will assign the specified IP address to the client. Else, do the next step.
- 2) If the message sent by the client contains Circuit ID option, the DHCP server will search the DHCP address pool list to find out if there is an address pool which is configured with this Circuit ID. If a match is found, the DHCP server will assign an IP address from this address pool. Else, do the next step.
- 3) If the giaddr field contained in a message sent by a client is not 0, the DHCP server will search the DHCP address pool list to find out if there is an address pool which is configured with this giaddr. If a match is found, the DHCP server will assign an IP address from this address pool. Else, do the next step.
- 4) If the message sent by the client contains Client ID option, the DHCP server will search the DHCP manual binding list to find out if there is an IP address bound to this Client ID. If a match is found, the DHCP server will assign the specified IP address to the client. Else, do the next step.
- 5) The DHCP server will search the DHCP manual binding list to find out if there is an IP address bound to the MAC address of the client. If a match is found, the DHCP server will assign the specified IP address to the client. Else, do the next step.
- 6) If the message sent by the client contains Requested IP Address option, the DHCP server will search the DHCP address pool list to find out if there is an address pool contains this Requested IP Address. If a match is found, and this Requested IP

Address is free, the DHCP server will assign it to the client. If a match is found, but this Requested IP address is in use, the DHCP server will try to assign another address dynamically from the address pool. Else, do the next step.

- 7) If no matching parameter found, the DHCP server will find an assignable IP address from each DHCP address pool in the chronological order of creation. Once an assignable IP address is found, the DHCP server will assign it to the client.
- 8) If no IP address is assignable, the DHCP server will report an error.

**Note**

- 1) You may create a manual binding by mapping an IP address to a host's MAC address, Remote ID or Client ID. The priorities of Remote ID, Client ID and MAC Address are descending. Only the highest priority parameter will be in effect when two or three of them are configured. For example, if there is a manual binding that contains an IP address bound to Remote ID and Client ID, the Client ID will be of no effect. That is, if a message sent by a client contains a mismatched Remote ID option, even if it contains a matched Client ID option, the client can't obtain the specified IP address.
- 2) If a message sent by a client contains Circuit ID or giaddr option that matches a DHCP address pool, the DHCP server will search the manual bindings belong to this address pool to find out if there is a DHCP manual binding contains the client's Client ID or MAC address. If a match is found, the DHCP server will assign the specified IP address to the client. Else, the DHCP server will try to find out if there is a DHCP manual binding contains this Requested IP Address. If a match is found, the DHCP server will assign it to the client. Else, the DHCP server will try to assign an address dynamically from this address pool.
- 3) If a message sent by a client matches a DHCP manual binding, but doesn't match the Circuit ID or giaddr option that is specified in the related DHCP address pool, the DHCP server will assign the address that is specified in this DHCP manual binding to the client.
- 4) If a message sent by a client matches a DHCP manual binding, but the specified IP address is already in use by another client (that is, an address conflict is detected), the DHCP server won't assign any IP address to the client.
- 5) If a message sent by a client contains Circuit ID or giaddr option that matches a DHCP address pool, but there is no free address in this pool, the DHCP server will assign an address from other DHCP address pools to the client.

7.8.2.2 Introduction to DHCP Client

When acting as a DHCP client, the Device can dynamically obtain an IP address and

other TCP/IP configuration parameters from a DHCP server. All of the physical interfaces support DHCP client feature, and you can enable DHCP client on each interface at the same time.

In order to meet different needs, DHCP client can use client ID to identify itself, send DHCPREQUEST messages in broadcast or unicast mode, and require DHCP server to respond in broadcast or unicast mode.

The Device also supports AutoIP feature, that is, if the DHCP client cannot obtain an IP address via DHCP, it will automatically assign an IP address (in the range of 169.254.1.0/16 through 169.254.254.0/16) to itself. And the DHCP client can ascertain that the address is not used by another host.

7.8.2.3 Introduction to DHCP Relay Agent

When acting as a DHCP relay agent, the Device can forwards DHCP messages between DHCP servers and clients. DHCP relay agents are used to forward requests and replies between clients and servers when they are not on the same physical subnet. Then the DHCP clients that reside on multiple physical subnets can use the same DHCP server. Using DHCP relay agent can help you save cost and achieve centralized management.

The following describes the basic operation principle of DHCP relay agent.

1. When starting, a DHCP client will start the DHCP initialization procedure during that a DHCPDISCOVER message will be broadcasted on its local physical subnet.
2. If a DHCP server that resides on the local subnet and is configured and operating correctly, the DHCP client will directly obtain configuration parameters such as an IP address from it. In this case, no DHCP relay agent is required.
3. If a DHCP server that doesn't reside on the local subnet, there must be a DHCP relay agent on the local subnet to receive the message and then generate a new DHCP message to send to the specified DHCP server that resides on another subnet.
4. After receiving the DHCPREQUEST message, the DHCP sever will unicast a DHCPOFFER message to the DHCP relay agent, which includes an IP address and other configuration parameters. After receiving the DHCPOFFER message, the DHCP relay agent will process and forward the message to the requesting client.
5. There are multiple such interactions during the configuration process.

The Device provides the parameters of **Option** and **Policy** to specify the forwarding policy of DHCP messages. When a DHCP relay agent receives a client-originated DHCP

message, it will process message according to the settings of these two parameters, see the following table for detailed description:

Option	Policy	The message is from another relay agent, and already contains option 82.	The message is from a client directly, and doesn't contain option 82.
insert	drop	Drop the message.	The relay agent will insert option 82 into the message before forwarding it.
	keep	The relay agent will retain the existing option 82 in the message and forward it.	
	replace	The relay agent will replace (overwrite) the existing option 82 with its option 82 in the message before forwarding it.	
disabled	drop	Drop the message.	Forward directly.
	keep	Forward directly.	
	replace	Forward directly.	

Table 7-3 DHCP Relay Agent Forwarding Policies

The following explains the meanings of the parameters in the above table.

Option 82: It indicates the relay agent information option.

Option: It is used to enable or disable the Device to insert option 82 before forwarding a client-originated DHCP message that doesn't contain option 82. By default, the relay agent will forward the message directly. If you want to insert option 82 into the message before forwarding it, please select **insert**. Note that, when the **Option** is set to **disabled**, the DHCP relay agent will drop or forward the message directly.

Policy: It is used to configure the reforwarding policy for a DHCP relay agent (what a relay agent should do if a message already contains option 82). A DHCP relay agent may receive a message from another relay agent that already contains relay information. By default, the relay agent will retain the existing option 82 in the message and forward it. If this behavior is not suitable for your network, you can set **Policy** to change it.

7.8.2.4 Introduction to Raw Option

DHCP provides a framework for passing configuration information to hosts on a TCP/IP network. Configuration parameters and other control information are carried in tagged

data items that are stored in the options field of the DHCP message. The data items themselves are also called options. For detailed information about DHCP options, see RFC 2132, with updates in RFC 3942.

Most DHCP options are predefined in RFC, although new options will come out with DHCP development. The Device provides Raw Option feature to support for the predefined options, and also new options. The raw options can be applied to both DHCP sever and DHCP client.

7.8.3 DHCP Client

Go to the **Advanced > DHCP** page firstly, and then select the **DHCP Client** radio button (see the following figure) to go to the **DHCP Client** page, which includes the **DHCP Client List** and **DHCP Client Settings** subpages.



Figure 7-22 Select DHCP Client

7.8.3.1 DHCP Client Settings

ent List
DHCP Client Settings

Interface WAN ▾

Enable DHCP Client

Enable PnP

Request Mode Broadcast ▾

Required Response Mode Unicast ▾

Client ID hex ▾ 010022aa123456

Enable AutoIP

Figure 7-23 DHCP Client Settings

✧ **Interface:** It specifies a physical interface on which the DHCP client is applied.

- ✧ **Enable DHCP Client:** It allows you to enable or disable DHCP client. If you want to enable DHCP client on the specified interface, please select this check box.
- ✧ **Enable PnP:** It allows you to enable or disable PnP. If you select this check box to enable PnP, the DHCP client can obtain IP address and subnet mask, and other TCP/IP configuration parameters such as default gateway address, DNS server addresses and so on. Else, the DHCP client can only obtain IP address and subnet mask.
- ✧ **Request Mode:** It specifies a mode in which the DHCP client sends the DHCPREQUEST messages. The available options are **Unicast** and **Broadcast**.
 - **Unicast:** It indicates that the DHCP client unicasts the DHCPREQUEST messages.
 - **Broadcast:** It indicates that the DHCP client broadcasts the DHCPREQUEST messages.
- ✧ **Required Response Mode:** It specifies a mode in which DHCP server sends the DHCP response message. The available options are **Unicast** and **Broadcast**.
 - **Unicast:** It indicates that the DHCP client requires DHCP server to respond in unicast mode.
 - **Broadcast:** It indicates that the DHCP client requires DHCP server to respond in broadcast mode.
- ✧ **Client ID:** It specifies the client identifier. There are three types of formats.
 - **hex:** It is used to specify a hexadecimal string. It should be between 1 and 25 characters long.
 - **ascii:** It is used to specify an ASCII character string. It should be between 1 and 27 characters long.
 - **ip:** It is used to specify an IP address.
- ✧ **Allow AutoIP:** You can allow or deny the DHCP client to use AutoIP. AutoIP means if the DHCP client cannot obtain an IP address via DHCP, it will automatically assign an IP address (in the range of 169.254.1.0/16 through 169.254.254.0/16) to itself. And the DHCP client can ascertain that the address is not used by another host.
- **Save:** Click it to save the DHCP client settings.

7.8.3.2 DHCP Client List

DHCP Client List		DHCP Client Settings							
Interface	Status	IP Address	Lease Left	PnP	Request Mode	Required Response Mode	Client ID	AutoIP	Edit
<input type="checkbox"/>	LAN	Disabled	192.168.16.1	-	Enabled	Broadcast	Unicast		Enabled Edit
<input type="checkbox"/>	WAN	Disabled	200.200.200.28	-	Enabled	Broadcast	Unicast	hex:010022aa123456	Enabled Edit
<input type="checkbox"/>	DMZ	Enabling ...	169.254.23.193	-	Enabled	Broadcast	Unicast		Enabled Edit

Select All

Figure 7-24 DHCP Client List

- **Configure DHCP Client:** If you want to apply DHCP client function on a physical interface, select the **DHCP Client Settings** tab to go to the setup page, and then select the interface and configure other parameters, lastly click the **Save** button.
- **View DHCP Client Information:** When you have configured DHCP client on one or more physical interfaces, you can view the related configuration and status information in the **DHCP Client List**.
- **Edit DHCP Client:** If you want to modify DHCP client applied on a physical interface, click its **Edit** hyperlink, the related information will be displayed in the setup page. Then modify it, and click the **Save** button.
- **Release:** If you want to release the current IP address of the DHCP client applied on a physical interface, select its leftmost check box, and then click the **Release** button.

7.8.3.3 How to Configure DHCP Client

If you want to configure DHCP client, do the following:

- Step 1** Go to the **Advanced > DHCP** page, select the **DHCP Client** radio button and then select the **DHCP Client Settings** tab to go to the setup page.
- Step 2** From the **Interface** drop-down list, select a physical interface on which the DHCP client will be applied.
- Step 3** Select the **Enable DHCP Client** check box to enable DHCP client on the specified interface.

- Step 4** In most cases, select the **Enable PnP** check box to enable PnP for the client.
- Step 5** Specify the **Request Mode** and **Required Response Mode** if required.
- Step 6** Specify the **Client ID** if required.
- Step 7** In most cases, select the **Allow AutoIP** check box to allow the DHCP client to use AutoIP.
- Step 8** Click the **Save** button to save the settings. Till now you have finished configuring the DHCP client applied on the specified interface, and then you can view the related configuration and status in the **DHCP Client List**.

 **Note**

If you want to disable DHCP client on a physical interface, please click its **Edit** hyperlink in the **DHCP Client List**, and then unselect the **Enable DHCP Client** check box, lastly click the **Save** button.

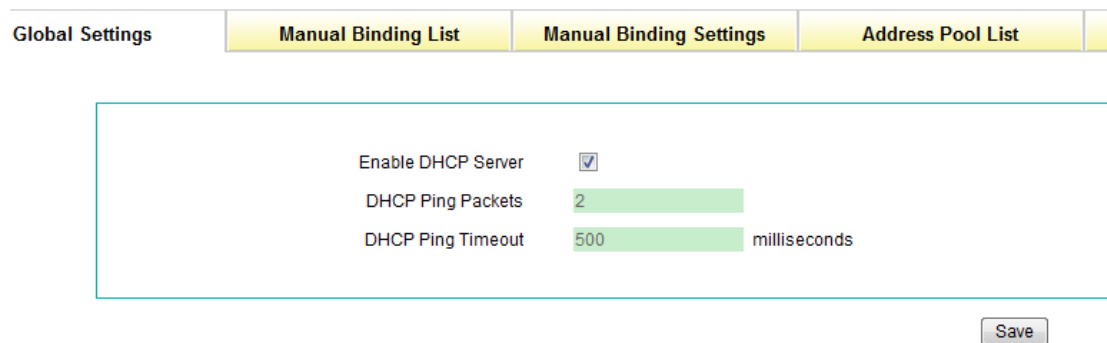
7.8.4 DHCP Server

Go to the **Advanced > DHCP** page firstly, and then select the **DHCP Server** radio button (see the following figure) to go to the **DHCP Server** page, which includes the **Global Settings**, **Manual Binding List**, **Manual Binding Settings**, **Address Pool List** and **Address Pool Settings** subpages.



Figure 7-25 Select DHCP Server

7.8.4.1 DHCP Server Global Settings



bindings, you can view them in the **Manual Binding List**.

- **Edit DHCP Manual Binding:** If you want to modify a configured DHCP manual binding, click its **Edit** hyperlink, the related information will be displayed in the setup page. Then modify it, and click the **Save** button.
- **Delete DHCP Manual Binding(s):** If you want to delete one or more DHCP manual bindings, select the leftmost check boxes of them, and then click the **Delete** button.



Note

The IP/MAC bindings created in the **Advanced > IP/MAC Binding** page will also display in the **Manual Binding List**, because they are DHCP manual bindings too.

7.8.4.3 DHCP Manual Binding Settings

Through DHCP manual binding, you can assign a static IP address to a specific host (client). You may create a manual binding by mapping the IP address to the host's MAC address, Remote ID or Client ID. The priorities of Remote ID, Client ID and MAC Address are descending. Only the highest priority parameter will be in effect when two or three of them are configured. The DHCP server will always assign the specified IP address to the host that matches the manual binding.

Settings	Manual Binding List	Manual Binding Settings	Address Pool List
----------	---------------------	-------------------------	-------------------

<table style="width: 100%;"> <tr> <td>Bind to</td> <td><input type="text" value="pool1"/></td> </tr> <tr> <td>User Name</td> <td><input type="text" value="192.168.16.101"/></td> </tr> <tr> <td>IP Address</td> <td><input type="text" value="192.168.16.101"/></td> </tr> <tr> <td>MAC Address</td> <td><input type="text" value="0026c7505a92"/></td> </tr> <tr> <td>Client ID</td> <td><input type="text" value="hex"/> <input type="text" value="010026c7505a92"/></td> </tr> <tr> <td>Remote ID</td> <td><input type="text" value="hex"/> <input type="text"/></td> </tr> <tr> <td>Host Name</td> <td><input type="text" value="zhaolili"/></td> </tr> </table> <p style="text-align: center;"><input type="button" value="Save"/></p>	Bind to	<input type="text" value="pool1"/>	User Name	<input type="text" value="192.168.16.101"/>	IP Address	<input type="text" value="192.168.16.101"/>	MAC Address	<input type="text" value="0026c7505a92"/>	Client ID	<input type="text" value="hex"/> <input type="text" value="010026c7505a92"/>	Remote ID	<input type="text" value="hex"/> <input type="text"/>	Host Name	<input type="text" value="zhaolili"/>	<div style="border: 1px solid #ccc; padding: 5px; background-color: #e0f0e0;"> <p style="margin: 0;">192.168.16.101 (00:26:c7:50:5a:92)</p> </div> <p style="text-align: center;"><input type="button" value="Show ARP Table"/></p>
Bind to	<input type="text" value="pool1"/>														
User Name	<input type="text" value="192.168.16.101"/>														
IP Address	<input type="text" value="192.168.16.101"/>														
MAC Address	<input type="text" value="0026c7505a92"/>														
Client ID	<input type="text" value="hex"/> <input type="text" value="010026c7505a92"/>														
Remote ID	<input type="text" value="hex"/> <input type="text"/>														
Host Name	<input type="text" value="zhaolili"/>														

Figure 7-28 DHCP Manual Binding Settings

- ✧ **Bind to:** It specifies a DHCP address pool to which the DHCP manual binding

belongs.

- ✧ **User Name:** It specifies a unique name for the DHCP manual binding. It is used to identify the host that want to be assigned a static IP address. It should be between 1 and 31 characters long.
- ✧ **IP Address:** It specifies the IP address for the DHCP manual binding. It must be a valid IP address of the related address pool. The requesting host that matches the manual binding will be assigned this specified address.
- ✧ **MAC Address:** It specifies the MAC address of the DHCP client.
- ✧ **Client ID:** It specifies the Client ID of the DHCP client. There are three types of formats.
 - **hex:** It is used to specify a hexadecimal string. It should be between 1 and 25 characters long.
 - **ascii:** It is used to specify an ASCII character string. It should be between 1 and 27 characters long.
 - **ip:** It is used to specify an IP address.
- ✧ **Remote ID:** It specifies the Remote ID of the DHCP client. There are three types of formats.
 - **hex:** It is used to specify a hexadecimal string. It should be between 1 and 25 characters long.
 - **ascii:** It is used to specify an ASCII character string. It should be between 1 and 27 characters long.
 - **ip:** It is used to specify an IP address.
- ✧ **Host Name:** It specifies the local host name of the DHCP client. It should be between 1 and 31 characters long.
- **Save:** Click it to save the DHCP manual binding settings.
- **Show ARP Table:** Click it to display the hosts' dynamic ARP information learned by the LAN interface. Note: It will only display dynamic ARP information, but not display static ARP information (that is, the IP and MAC address pairs have been bound manually).

7.8.4.4 How to Add the DHCP Manual Bindings

If you want to add one or more DHCP manual bindings, do the following:

- Step 1** Go to the **Advanced > DHCP** page, and select the **DHCP Server** radio button to go to the **DHCP Server** page.
- Step 2** Select the **Manual Binding Settings** tab to go to the setup page.
- Step 3** From the **Bind to** drop-down list, select a DHCP address pool to which this DHCP manual binding belongs.
- Step 4** Specify the **User Name**, **IP Address** and **MAC Address** as required.
- Step 5** Specify the **Client ID**, **Remote ID** or **Host Name** if needed.
- Step 6** Click the **Save** button to save the settings. You can view the DHCP manual binding in the **Manual Binding List**.
- Step 7** If you want to add another new DHCP manual binding, please repeat the above steps.



Note

If you want to delete one or more DHCP manual bindings, select the leftmost check boxes of them in the **Manual Binding List**, and then click the **Delete** button.

7.8.4.5 DHCP Address Pool List

Pool Name	Start IP	Subnet Mask	Number of Addresses	Gateway	Lease Time	Primary DNS	Secondary DNS	Primary WINS	Secondary WINS	Interface	Edit
<input type="checkbox"/> pool1	192.168.16.65	255.255.255.0	62	192.168.16.1	3600	192.168.1.99	202.106.46.151	0.0.0.0	0.0.0.0	LAN	Edit
<input type="checkbox"/> pooltest	192.168.1.2	255.255.255.0	100	192.168.1.1	3600	202.96.209.5	202.96.199.133	0.0.0.0	0.0.0.0	LAN	Edit

Figure 7-29 DHCP Address Pool List

- **Add a DHCP Address Pool:** If you want to add a new DHCP address pool, select the **Address Pool Settings** tab, and then configure it, lastly click the **Save** button.
- **View DHCP Address Pool(s):** When you have configured some DHCP address pools, you can view them in the **Address Pool List**.
- **Edit DHCP Address Pool:** If you want to modify a configured DHCP address pool, click its **Edit** hyperlink, the related information will be displayed in the setup page. Then modify it, and click the **Save** button.
- **Delete DHCP Address Pool(s):** If you want to delete one or more DHCP address pools, select the leftmost check boxes of them, and then click the **Delete** button.

7.8.4.6 DHCP Address Pool Settings

The DHCP server assigns an IP address to a requesting client from a DHCP address pool, which also can be configured to provide other TCP/IP configuration parameters to the client, such as the Gateway IP address, DNS Server and WINS Server addresses, lease time, etc. The Device supports multiple address pools, so you can easily define multiple subnets in LAN.

Before configuring a DHCP address pool, you should specify a physical interface to which the pool is bound.

Interface	LAN
Pool Name	pooltest
Start IP Address	192.168.1.2
Number of Addresses	100
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.1
Lease Time	3600 seconds
Primary DNS Server	202.96.209.5
Secondary DNS Server	202.96.199.133
Primary WINS Server	0.0.0.0
Secondary WINS Server	0.0.0.0
Advanced Options	
Domain Name	
Relay Agent IP	0.0.0.0
Enable AutoIP	<input checked="" type="checkbox"/>
Response Mode	Broadcast
NetBIOS Node Type	B-Node
Relay Agent ID	hex

Figure 7-30 DHCP Address Pool Settings

- ✧ **Interface:** It specifies a physical interface to which the DHCP address pool is bound.
- ✧ **Pool Name:** It specifies a unique name for the DHCP address pool. It should be between 1 and 11 characters long.
- ✧ **Start IP Address:** It specifies the starting IP address assigned from the DHCP address pool.
- ✧ **Number of Addresses:** It specifies the maximum number of IP addresses that can be assigned from the DHCP address pool. The addresses can be assigned dynamically or manually by the DHCP server.
- ✧ **Subnet Mask:** It specifies the subnet mask of the IP addresses assigned from the DHCP address pool.
- ✧ **Default Gateway:** It specifies the IP address of the default gateway for a DHCP client.
- ✧ **Lease Time:** It specifies the length of time (in seconds) during which each IP address assigned by a DHCP server is valid. If the lease expires, the client is automatically assigned a new dynamic IP address. Before the lease expires, the client typically

needs to renew its address lease assignment with the server. The duration for a lease determines when it will expire and how often the client needs to renew it with the server. The default value is 3600 seconds.

- ✧ **Primary DNS Server:** It specifies the IP address of the primary DNS server that is available to a DHCP client.
- ✧ **Secondary DNS Server:** It specifies the IP address of the secondary DNS server that is available to a DHCP client.
- ✧ **Primary WINS Server:** It specifies the IP address of the primary NetBIOS WINS server that is available to a Microsoft DHCP client.
- ✧ **Secondary WINS Server:** It specifies the IP address of the secondary NetBIOS WINS server that is available to a Microsoft DHCP client.
- ✧ **Domain Name:** It specifies the DNS domain name for a DHCP client. This is usually an organization name followed by a period and an extension that indicates the type of organization, such as `utt.com.cn`. This domain name is appended to the local host name to create the fully qualified domain name (FQDN) for the host. When querying for a host name, the system will append this domain name to the host name for name resolution, thus the DHCP client host who has a host name can access the network.
- ✧ **DHCP Relay IP:** It specifies the relay agent IP address for the DHCP address pool. It can be a parameter used by address allocation policy. Refer to **section 7.7.2.1.4 IP Address Allocation Policy** for details.
- ✧ **Enable AutoIP:** It allows you to enable or disable AutoIP. Select it to permit the address obtained by a DHCP client through AutoIP to coexist with the address assigned by a DHCP server.
- ✧ **Response Mode:** It specifies the mode in which DHCP server sends the DHCP response messages to the client. The available options are **Client Determine**, **Unicast** and **Broadcast**.
 - **Client Determine:** It indicates that the DHCP server sends the DHCP response messages in the mode required by the client.
 - **Unicast:** It indicates that the DHCP server unicasts the DHCP response messages to the client.
 - **Broadcast:** It indicates that the DHCP server broadcasts the DHCP response messages to the client.
- ✧ **NetBIOS Node Type:** It specifies the NetBIOS node type for Microsoft DHCP clients. There are four NetBIOS nodes types, and each node type resolves NetBIOS names differently.

- **B-Node:** It indicates a broadcast node that uses broadcasts for name resolution.
 - **P-Node:** It indicates a peer-to-peer node that uses a WINS server to resolve NetBIOS names. P-Node does not use broadcasts but queries the WINS server directly.
 - **M-Node:** It indicates a mixed node that is a combination of a B-Node and P-Node. By default, an M-Node functions as a B-Node firstly. If the broadcast name query is unsuccessful, it uses a WINS server.
 - **H-Node:** It indicates a hybrid node that is a combination of a P-Node and B-Node. By default, an H-Node functions as a P-Node firstly. If the unicast name query to the WINS server is unsuccessful, it uses broadcasts.
- ✧ **Relay Agent ID:** It specifies the relay agent identifier for the DHCP address pool. It can be a parameter used by address allocation policy. Refer to **section 7.7.2.1.4 IP Address Allocation Policy** for details. There are three types of formats.
- **hex:** It is used to specify a hexadecimal string. It should be between 1 and 25 characters long.
 - **ascii:** It is used to specify an ASCII character string. It should be between 1 and 27 characters long.
 - **ip:** It is used to specify an IP address.
- **Save:** Click it to save the DHCP address pool settings.

**Note**

The Device provides a default address pool whose name is **pool1**. The **pool1** is editable, but can't be deleted. Also, you can configure and view it in the **Basic > DHCP & DNS** page.

7.8.4.7 How to Add the DHCP Address Pools

If you want to add one or more DHCP address pools, do the following:

- Step 1** Go to the **Advanced > DHCP** page, and select the **DHCP Server** radio button to go to the **DHCP Server** page.
- Step 2** Select the **Address Pool Settings** tab to go to the setup page.

- Step 3** From the **Interface** drop-down list, select a physical interface to which the DHCP address pool is bound.
- Step 4** Specify the **Pool Name**, **Start IP Address**, **Number of Addresses** and **Primary DNS Server**.
- Step 5** Specify the **Subnet Mask**, **Default Gateway** and **Lease Time** as required.
- Step 6** Specify the **Secondary DNS Server**, **Primary WINS Server** and **Secondary WINS Server** if needed.
- Step 7** Specify the **Domain Name**, **DHCP Relay IP** and **Relay Agent ID** if needed.
- Step 8** In most cases, select the **Enable AutoIP** check box.
- Step 9** Specify the **Response Mode** and **NetBIOS Node Type** if needed
- Step 10** Click the **Save** button to save the settings. You can view the DHCP address pool in the **Manual Binding List**.
- Step 11** If you want to add another new DHCP address pool, please repeat the above steps.

**Note**

If you want to delete one or more DHCP address pools except the **Pool1**, select the leftmost check boxes of them in the **Address Pool List**, and then click the **Delete** button.

7.8.5 DHCP Relay Agent

Go to the **Advanced > DHCP** page firstly, and then select the **DHCP Relay Agent** radio button (see the following figure) to go to the **DHCP Relay Agent** page, which includes the **DHCP Relay Agent List** and **Relay Agent Settings** subpages.



Figure 7-31 Select DHCP Relay Agent

7.8.5.1 DHCP Relay Agent Settings

Agent List
Relay Agent Settings

Interface	<input type="text" value="DMZ"/>
Enable DHCP Relay	<input type="checkbox"/>
DHCP Server 1	<input type="text" value="200.200.200.88"/>
DHCP Server 2	<input type="text" value="0.0.0.0"/>
DHCP Server 3	<input type="text" value="0.0.0.0"/>
Option	<input type="text" value="disabled"/>
Policy	<input type="text" value="keep"/>
Max. Packet Size	<input type="text" value="1024"/>
Relay Agent ID	<input type="text" value="hex"/> <input type="text" value="010022aa112233"/>
Response Mode	<input type="text" value="Broadcast"/>

Figure 7-32 DHCP Relay Agent Settings

- ✧ **Interface:** It specifies physical interface on which the DHCP relay agent is applied.
- ✧ **Enable DHCP Relay Agent:** It allows you to enable or disable DHCP relay agent. If you want to enable DHCP relay agent on the specified interface, please select this check box.
- ✧ **DHCP Server 1 ~ 3:** It specifies one or more DHCP servers for the relay agent. You can specify up to three DHCP servers for the relay agent. The DHCP relay agent will unicast the DHCP request messages to all the specified servers respectively.
- ✧ **Option:** It specifies whether the DHCP relay agent inserts option 82 (DHCP relay agent information option) into a client-originated DHCP message before forwarding it to a DHCP server or not.
- ✧ **Policy:** It specifies the reforwarding policy for the DHCP relay agent, that is, what the relay agent should do if a message already contains option 82.
- ✧ **Max. Packet Size:** It specifies the maximum size of packet (in bytes) that the DHCP relay agent can forward. The default is 1024 bytes.
- ✧ **Relay Agent ID:** It specifies the relay agent identifier. There are three types of formats:
 - **hex:** It is used to specify a hexadecimal string. It should be between 1 and 25

characters long.

- **ascii:** It is used to specify an ASCII character string. It should be between 1 and 27 characters long.
- **ip:** It is used to specify an IP address.

✧ **Response Mode:** It specifies the mode in which DHCP relay agent sends the DHCP response messages to the client. The available options are **Client Determine**, **Unicast** and **Broadcast**.

- **Client Determine:** It indicates that the DHCP relay agent sends the DHCP response messages in the mode required by the client.
- **Unicast:** It indicates that the DHCP relay agent unicasts the DHCP response messages to the client.
- **Broadcast:** It indicates that the DHCP relay agent broadcasts the DHCP response messages to the client.

➤ **Save:** Click it to save the DHCP relay agent settings.



Note

For more information about **Option** and **Policy**, please refer to **section 7.7.2.3 Introduction to DHCP Relay Agent**.

7.8.5.2 DHCP Relay Agent List

DHCP Relay Agent List		Relay Agent Settings									
Interface	Status	DHCP Server 1	DHCP Server 2	DHCP Server 3	Option	Policy	Max. Packet Size	Relay Agent ID	Response Mode	Edit	
<input checked="" type="checkbox"/>	LAN	Enabled	200.200.200.254	0.0.0.0	0.0.0.0	Insert	Keep	1024	ascii.Test_Relay1	Broadcast	Edit
<input checked="" type="checkbox"/>	WAN	Disabled	0.0.0.0	0.0.0.0	0.0.0.0	Disabled	Keep	1024		Broadcast	Edit
<input checked="" type="checkbox"/>	DMZ	Disabled	0.0.0.0	0.0.0.0	0.0.0.0	Disabled	Keep	1024		Broadcast	Edit
<input type="checkbox"/>											
<input type="checkbox"/>											
<input type="checkbox"/>											
<input type="checkbox"/>											
<input type="checkbox"/>											

Figure 7-33 DHCP Relay Agent List

- **Configure DHCP Relay Agent:** If you want to apply DHCP relay agent function on a physical interface, select the **Relay Agent Settings** tab to go to the setup page, and then select the interface and configure other parameters, lastly click the **Save** button.
- **View DHCP Relay Agent Information:** When you have configured DHCP relay agent on one or more physical interfaces, you can view the related information in the **DHCP Relay Agent List**.
- **Edit DHCP Client:** If you want to modify DHCP relay agent on a physical interface, click its **Edit** hyperlink, the related information will be displayed in the setup page. Then modify it, and click the **Save** button.

7.8.5.3 How to Configure DHCP Relay Agent

If you want to configure DHCP relay agent, do the following:

- Step 1** Go to the **Advanced > DHCP** page, and select the **DHCP Relay Agent** radio button to go to the **DHCP Relay Agent** page.
- Step 2** Select the **Relay Agent Settings** tab to go to the setup page.
- Step 3** From the **Interface** drop-down list, select a physical interface on which the DHCP relay agent is applied.
- Step 4** Select the **Enable DHCP Relay Agent** check box to enable DHCP relay agent on the specified interface.
- Step 5** Specify the **DHCP Server 1**, and specify **DHCP Server 2** and **DHCP Server 3** if needed.
- Step 6** Specify the **Option** and **Policy** if needed.
- Step 7** Specify the **Max. Packet Size**, **Relay Agent ID** and **Policy** if needed.
- Step 8** Click the **Save** button to save the settings. Till now you have finished configuring the DHCP relay agent which is applied on the specified interface, and then you can view the related configuration and status information in the **DHCP Relay Agent List**.



Note

If you want to disable DHCP relay agent on a physical interface, please click its **Edit** hyperlink in the **DHCP Relay Agent List**, and then unselect the **Enable DHCP Relay Agent** check box, lastly click the **Save** button.

7.8.6 Raw Option

Go to the **Advanced > DHCP** page firstly, and then select the **Raw Option** radio button (see the following figure) to go to the **Raw Option** page, which includes the **Raw Option List** and **Raw Option Settings** subpages.

DHCP Client
 DHCP Server
 DHCP Relay Agent
 Raw Option

Figure 7-34 Select Raw Option

7.8.6.1 Raw Option Settings

In this page, you can easily create DHCP raw options. Once a raw option is defined, the DHCP server or client on the specified interface will add it into the options field of the DHCP messages before sending them.

Raw Option List Raw Option Settings

Option Name:

Option Code: (1-254)

Option Value:

Interface:

Figure 7-35 Raw Option Settings

- ✧ **Option Name:** It specifies a unique name of the raw option. It should be between 1 and 31 characters long.
- ✧ **Option Code:** It specifies the code of the raw option. It is used to uniquely identify the option type. It should be a number between 1 and 254.
- ✧ **Option Value:** It specifies the associated values of the raw option. There are three types of formats.
 - **hex:** It is used to specify a hexadecimal string. It should be between 1 and 25 characters long.

- **ascii:** It is used to specify an ASCII character string. It should be between 1 and 27 characters long.
 - **ip:** It is used to specify an IP address.
- ✧ **Interface:** It specifies the physical interface on which the DHCP raw option is applied.
- **Save:** Click it to save the DHCP raw option settings.



Note

For detailed information about DHCP options, see RFC 2132, with updates in RFC 3942.

7.8.6.2 Raw Option List

Option Name	Option Code	Option Value	Interface	Edit
ven_inf	43	asciiTest	LAN	Edit

Figure 7-36 Raw Option List

- **Add a Raw Option:** If you want to add a new DHCP raw option, click the **New** button or select the **Raw Option Settings** tab to go to the setup page, and then configure it, lastly click the **Save** button.
- **View Raw Option(s):** When you have configured some DHCP raw options, you can view them in the **Raw Option List**.
- **Edit a Raw Option:** If you want to modify a configured DHCP raw option, click its **Edit** hyperlink, the related information will be displayed in the setup page. Then modify it, and click the **Save** button.
- **Delete Raw Option(s):** If you want to delete one or more DHCP raw options, select

the leftmost check boxes of them, and then click the **Delete** button.

7.8.6.3 How to Add the DHCP Raw Options

If you want to add one or more DHCP raw options, do the following:

- Step 1** Go to the **Advanced > DHCP** page, and select the **Raw Option** radio button to go to the **Raw Option** page.
- Step 2** Select the **Raw Option Settings** tab or click the **New** button to go to the setup page.
- Step 3** Specify the **Option Name**, **Option Code** and **Option Value**.
- Step 4** From the **Interface** drop-down list, select a physical interface on which the DHCP raw option is applied.
- Step 5** Click the **Save** button to save the settings. You can view the DHCP raw option in the **Raw Option List**.
- Step 6** If you want to add another new DHCP raw option, please repeat the above steps.



Note

If you want to delete one or more DHCP raw options, select the leftmost check boxes of them in the **Raw Option List**, and then click the **Delete** button.

7.8.7 Configuration Examples for DHCP

7.8.7.1 Configuration Example for the DHCP Server

There are two typical types of DHCP network topologies:

- The DHCP server(s) and DHCP clients are on the same subnet so they can directly exchange DHCP messages.
- The DHCP server(s) and DHCP clients are not on the same subnet so they need communicate via a DHCP relay agent.

The DHCP server configuration for these two types is the same.

1. Network Requirements

In this example, the Device acts as a DHCP server to dynamically assign the IP addresses to the clients that reside on the same subnet. The Device's LAN interface IP address is 192.168.16.1/24.

We need to create two address pools (pool1 and pool2). The pool1's address range is from 192.168.16.2/24 to 192.168.16.101/24, primary and secondary DNS servers IP addresses are 202.96.209.5 and 202.96.199.133, domain name is utt.com.cn and lease time is 3600 seconds. And it uses Device's LAN IP address (that is, 192.168.16.1/24) as the default gateway address. Leave the default values for the other parameters.

The pool2's address range is from 192.168.16.102/24 to 192.168.16.254/24 and lease time is 7200 seconds. The pool2's primary and secondary DNS servers, domain name, and default gateway IP address have the same values with pool1's.

Besides, we need to create a DHCP manual binding to the host that needs a static IP address. The host's MAC address is 000795a81c3d, client ID is 01000795a81c3d which is formed by concatenating the media type and MAC address, and host name is test. The host wants to use 192.168.16.10/24 as its IP address and binding1 as its user name. It is obvious that the host belongs to the **pool1**.

2. Network Topology

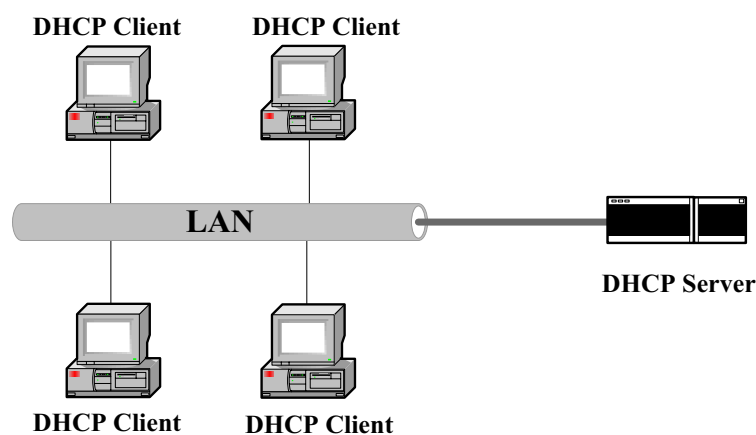


Figure 7-37 Network Topology where DHCP Server and Clients on Same Subnet

3. Configuration Procedure

1) Configuring DHCP Server Global Parameters

Step 1 Go to the **Advanced > DHCP** page, and then select the **DHCP Server** radio button to go to the **DHCP Server** page.

Step 2 Select the **Global Settings** tab to go to the setup page.

Step 3 Select the **Enable DHCP Server** check box, see the following figure.

Global Settings	Manual Binding List	Manual Binding Settings	Address Pool List	
-----------------	---------------------	-------------------------	-------------------	--

Enable DHCP Server	<input checked="" type="checkbox"/>
DHCP Ping Packets	<input type="text" value="2"/>
DHCP Ping Timeout	<input type="text" value="500"/> milliseconds

Figure 7-38 DHCP Server Global Settings - Example

Step 4 Click the **Save** button to save the settings. Till now you have finished configuring DHCP server global settings.

2) Configuring the DHCP Address Pool - pool1

As mentioned earlier, the **pool1** is the default address pool provided by the Device. And it is editable, but can't be deleted. So you could modify the **pool1** according to your requirements. The steps are as follows:

Step 1 Go to the **Advanced > DHCP** page, and then select the **DHCP Server** radio button to go to **DHCP Server** page.

Step 2 Select the **Address Pool List** tab to go to related subpage, and then click the **Edit** hyperlink of the **pool1**, the related information will be displayed in the setup page.

Interface	LAN
Pool Name	pool1
Start IP Address	192.168.16.2
Number of Addresses	100
Subnet Mask	255.255.255.0
Default Gateway	192.168.16.1
Lease Time	3600 seconds
Primary DNS Server	202.96.209.5
Secondary DNS Server	202.96.199.133
Primary WINS Server	0.0.0.0
Secondary WINS Server	0.0.0.0
Advanced Options	
Domain Name	utt.com.cn
Relay Agent IP	0.0.0.0
Enable AutoIP	<input checked="" type="checkbox"/>
Response Mode	Broadcast
NetBIOS Node Type	B-Node
Relay Agent ID	hex

Save

Figure 7-39 DHCP Address Pool Settings - Example (pool1)

Step 3 Enter **192.168.16.2** in the **Start IP Address** text box, enter **100** in the **Number of Addresses** text box, enter **192.168.16.1** in the **Default Gateway** text box, enter **202.96.209.5** in the **Primary DNS Server** text box, enter **202.96.199.133** in **Secondary DNS Server** text box, and enter **utt.com.cn** in the **Domain Name** text box. Leave the default values for the other parameters.

Step 4 Click the **Save** button to save the settings. Till now you have finished configuring the **pool1**, and then you can view its configuration in the **Address Pool List**.

3) Configuring the DHCP Address Pool - pool2

Step 1 Go to the **Advanced > DHCP** page, and then select the **DHCP Server** radio button to go to the **DHCP Server** page.

Step 2 Select the **Address Pool Settings** tab to go to the setup page, see the following figure.

Interface	LAN
Pool Name	pool2
Start IP Address	192.168.16.102
Number of Addresses	153
Subnet Mask	255.255.255.0
Default Gateway	192.168.16.1
Lease Time	7200 seconds
Primary DNS Server	202.96.209.5
Secondary DNS Server	202.96.199.133
Primary WINS Server	0.0.0.0
Secondary WINS Server	0.0.0.0
Advanced Options	
Domain Name	utt.com.cn
Relay Agent IP	0.0.0.0
Enable AutoIP	<input checked="" type="checkbox"/>
Response Mode	Broadcast
NetBIOS Node Type	B-Node
Relay Agent ID	hex

Figure 7-40 DHCP Address Pool Settings - Example (pool2)

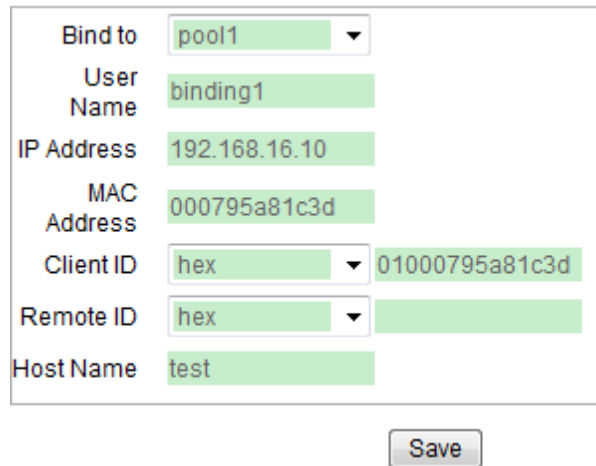
Step 3 Enter **192.168.16.102** in the **Start IP Address** text box, enter **153** in the **Number of Addresses** text box, enter **192.168.16.1** in the **Default Gateway** text box, enter **7200** in the **Lease Time** text box, enter **202.96.209.5** in the **Primary DNS Server** text box, enter **202.96.199.133** in the **Secondary DNS Server** text box, and enter **utt.com.cn** in the **Domain Name** text box. Leave the default values for the other parameters.

Step 4 Click the **Save** button to save the settings. Till now you have finished configuring the **pool2**, and then you can view its configuration in the **Address Pool List**.

4) Configuring the DHCP Manual Binding

Step 1 Go to the **Advanced > DHCP** page, and then select the **DHCP Server** radio button to go to the **DHCP Server** page.

Step 2 Select the **Manual Binding Settings** tab to go to the setup page, see the following figure.



The screenshot shows a configuration form for DHCP Manual Binding. The fields are as follows:

Bind to	pool1
User Name	binding1
IP Address	192.168.16.10
MAC Address	000795a81c3d
Client ID	hex 01000795a81c3d
Remote ID	hex
Host Name	test

Below the form is a "Save" button.

Figure 7-41 DHCP Manual Binding Settings - Example

- Step 3** Select **pool1** from the **Bind to** drop-down list, enter **binding1** in the **User Name** text box, enter **192.168.16.10** in the **IP Address** text box and enter **000795a81c3d** in the **MAC Address** text box.
- Step 4** Select **hex** from the **Client ID** drop-down list and enter **01000795a81c3d** in the associated text box, enter **test** in the **Host Name** text box. Leave the default values for the other parameters.
- Step 5** Click the **Save** button to save the settings. Till now you have finished configuring the DHCP manual binding, and then you can view its configuration in the **Manual Binding List**.

7.8.7.2 Configuration Example for the DHCP Client

As mentioned earlier, each physical interface of the Device supports DHCP client, and it allows you to enable DHCP client on each interface at the same time. In this example, the DHCP client is applied on the WAN interface.

1. Network Requirements

In this example, we connect the Device's WAN interface to the LAN that contains a DHCP server. The LAN network ID is 200.200.200.0/24. The Device acts as a DHCP client which is enabled on the WAN interface, then the WAN interface will obtain an IP address from the DHCP server dynamically. The WAN interface's MAC address is 0022aa123456, and its client ID is 010022aa123456 which is formed by concatenating the media type and MAC address.

2. Network Topology

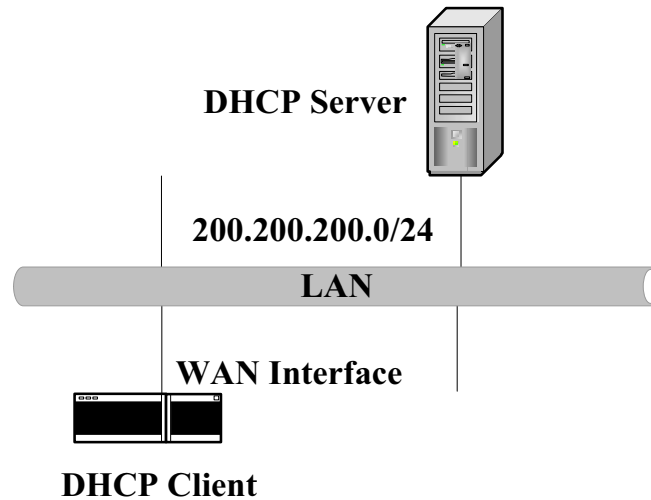


Figure 7-42 Network Topology Where DHCP Client is Applied on WAN Interface

3. Configuration Procedure

Step 1 Go to the **Advanced > DHCP** page, select the **DHCP Client** radio button and then select the **DHCP Client Settings** tab to go to the setup page, see the following figure.

The screenshot shows the "DHCP Client Settings" configuration page. At the top, there are two tabs: "DHCP Client Settings" (selected) and "DHCP Client List". The configuration area contains the following settings:

- Interface: WAN (dropdown menu)
- Enable DHCP Client:
- Enable PnP:
- Request Mode: Broadcast (dropdown menu)
- Required Response Mode: Unicast (dropdown menu)
- Client ID: hex (dropdown menu) with the value 010022aa123456 (text input)
- Enable AutoIP:

A "Save" button is located at the bottom right of the configuration area.

Figure 7-43 DHCP Client Settings - Example

- Step 2** Select **WAN** from the **Interface** drop-down list.
- Step 3** Select the **Enable DHCP Client**, **Enable PnP** and **Allow AutoIP** check boxes.
- Step 4** Select **hex** from the **Client ID** drop-down list and enter **010022aa123456** in the associated text box. Leave the default values for the other parameters.

- Step 5** Click the **Save** button to save the settings. Till now you have finished configuring the DHCP client, and then you can view its configuration and status in the **DHCP Client List**.

7.8.7.3 Configuration Example for the DHCP Relay Agent

1. Network Requirements

In this example, the DHCP clients reside on the subnet 192.168.16.0/24, and the DHCP server's IP address is 200.200.200.254/24. Because the DHCP server and DHCP clients reside on the different subnets, the Device acting as a DHCP relay agent is deployed to forward DHCP messages between the DHCP server and DHCP clients. The DHCP relay agent is enabled on the LAN interface, which is connected to the subnet where DHCP clients reside. Then DHCP clients can obtain an IP address and other TCP/IP configuration parameters from the DHCP server dynamically.

Note that in order to assign appropriate IP addresses to the DHCP clients, on the DHCP server you should create a DHCP address pool whose address range is from 192.168.16.2 to 192.168.16.254. And also you should create a static route whose destination network is 192.168.16.0/24. For more information about static route, please refer to **section 7.1.1 Static Route**.

2. Network Topology

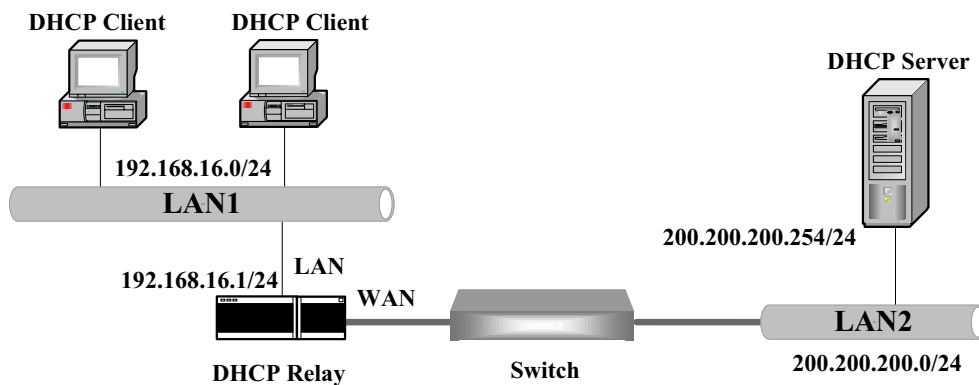


Figure 7-44 Network Topology Where the Device Acting as a DHCP Relay Agent

3. Configuration Procedure

- Step 1** Go to the **Advanced > DHCP** page, and select the **DHCP Relay Agent** radio button.
- Step 2** Select the **Relay Agent Settings** tab to go to the setup page, see the following figure.

Agent List

Relay Agent Settings

Interface	LAN
Enable DHCP Relay	<input checked="" type="checkbox"/>
DHCP Server 1	200.200.200.254
DHCP Server 2	0.0.0.0
DHCP Server 3	0.0.0.0
Option	disabled
Policy	keep
Max. Packet Size	1024
Relay Agent ID	hex
Response Mode	Broadcast

Figure 7-45 DHCP Relay Agent Settings - Example

- Step 3** Select **LAN** from the **Interface** drop-down list.
- Step 4** Select the **Enable DHCP Relay Agent** check box.
- Step 5** Enter **200.200.200.254** in the **DHCP Server 1** text box. Leave the default values for the other parameters.
- Step 6** Click the **Save** button to save the settings. Till now you have finished configuring the DHCP relay agent, and then you can view its configuration and status in the **DHCP Relay Agent List**.

7.8.7.4 Configuration Example for the Raw Option

1. Requirements

In this example, we need to create a raw option whose option name is ven_inf, option code is 43 (that is, vendor-specific information) and option value is Test in ASCII format. And it is applied on the LAN interface.

2. Configuration Procedure

- Step 1** Go to **Advanced > DHCP** page, and select the **Raw Option** radio button.
- Step 2** Select the **Raw Option Settings** tab to go to the setup page, see the following figure.

Raw Option List Raw Option Settings

Option Name ven_inf

Option Code 43 (1-254)

Option Value ascii Test

Interface LAN

Save

Figure 7-46 Raw Option Settings - Example

- Step 3** Enter **ven_inf** in the **Option Name** text box, enter **43** in the **Option Code** text box, select **ascii** from the **Option Value** drop-down list and enter **Test** in the associated text box.
- Step 4** Select **LAN** from the **Interface** drop-down list.
- Step 5** Click the **Save** button to save the settings. Till now you have finished configuring the DHCP raw option, and then you can view its configuration in the **Raw Option List**.

7.8.7.5 Comprehensive Example for DHCP

When acting as a DHCP server, the Device supports up to ten DHCP address pools. You can use different Relay agent IP addresses or IDs to distinguish them. In most cases, the DHCP server will assign the addresses from the same address pool to the clients that have the same relay agent IP address or ID with this pool's, then these clients will reside on the same subnet.

1. Network Requirements

In this example, there is a college who wants to realize the unified management of the campus network hosts. We plan to divide the campus network into several subnets, one subnet per building (office or dormitory building), so that the hosts residing on the same building will be on the same subnet. We deploy a Device acting as a DHCP server on the network center, and deploy a Devices acting as a DHCP relay agent on each building. Each DHCP relay agent Device is connected to the center DHCP server Device. And the hosts residing on each building are connected to a relay agent Device, so that these hosts can access the network center through the related relay agent Device.

See the following network topology, we respectively call these buildings building1,

building2 ... building10, and call the Devices residing on each building DHCP Relay1, DHCP Realy2 ... DHCP Realy10. Each relay agent Device has its own ID.

The Device residing on the center network acts as a DHCP server, and the DHCP address pools are bound to the LAN interface with IP address 200.200.200.254/24.

The Devices residing on each building act as the DHCP relay agents. The DHCP relay agent is enabled on each Device's LAN interface. The hosts residing on each building are connected to the related Device's LAN interface respectively, and they will act as clients to request addresses from the DHCP server. The following table lists the name, relay agent ID, WAN IP address and LAN IP address for each relay agent Device. Also it lists the IP address space of each subnet where the client hosts reside.

Name	WAN IP address	LAN IP Address	Client Subnet	Relay Agent ID
DHCP Relay1	200.200.200.1/24	192.168.1.1/24	192.168.1.0/24	Test_Relay1
DHCP Relay2	200.200.200.2/24	192.168.2.1/24	192.168.2.0/24	Test_Relay2
DHCP Relay3	200.200.200.3/24	192.168.3.1/24	192.168.3.0/24	Test_Relay3
DHCP Relay4	200.200.200.4/24	192.168.4.1/24	192.168.4.0/24	Test_Relay4
DHCP Relay5	200.200.200.5/24	192.168.5.1/24	192.168.5.0/24	Test_Relay5
DHCP Relay6	200.200.200.6/24	192.168.6.1/24	192.168.6.0/24	Test_Relay6
DHCP Relay7	200.200.200.7/24	192.168.7.1/24	192.168.7.0/24	Test_Relay7
DHCP Relay8	200.200.200.8/24	192.168.8.1/24	192.168.8.0/24	Test_Relay8
DHCP Relay9	200.200.200.9/24	192.168.9.1/24	192.168.9.0/24	Test_Relay9
DHCP Relay10	200.200.200.10/24	192.168.10.1/24	192.168.10.0/24	Test_Relay10

Table 7-4 DHCP Relay Agent IP Addresses and IDs - Comprehensive Example

In order to ensure that the hosts residing on each building obtain the addresses in the range of the specified subnet respectively, we need to create ten DHCP address pools on the DHCP server Device. These DHCP address pools' settings are as follows:

- Every DHCP address pool is bound to the LAN interface.
- Their pool names are pool1, pool2 ... pool10 respectively.
- Their starting IP addresses are 192.168.1.2, 192.168.2.2 ... 192.168.10.2 respectively.

- Every DHCP address pool's number of addresses is 253, which is the maximum number of valid addresses in each subnet where the client hosts reside.
- Every DHCP address pool's lease time is 3600 seconds, primary and secondary DNS servers' IP addresses are 202.96.209.6 and 202.96.199.133.
- Their relay agent IDs are Test_Relay1, Test_Relay2 ... Test_Relay10 respectively, which are in ASCII format.

Note that you also should create ten static routes whose destination networks are the subnets where the client hosts reside. For more information about static route, please refer to **section 7.1.1 Static Route**.

For those DHCP relay agent Devices, the DHCP relay agent settings are as follows:

- Every DHCP relay agent is applied on the **LAN** interface.
- Every DHCP relay agent's **DHCP Server 1** is **200.200.200.254**.
- Every DHCP relay agent's **Option** is **insert**.
- Their **Relay Agent IDs** are **Test_Relay1, Test_Relay2 ... Test_Relay10** respectively, which are in ASCII format.

Note that since the DHCP server uses the relay agent ID to distinguish each address pool, we need set **Option** to **insert** for each relay agent. The DHCP relay agent will insert relay agent ID before forwarding a client-originated DHCP message; thus the DHCP server can select a matched address pool according to the relay agent ID to assign an address to the requesting client.

2. Network Topology

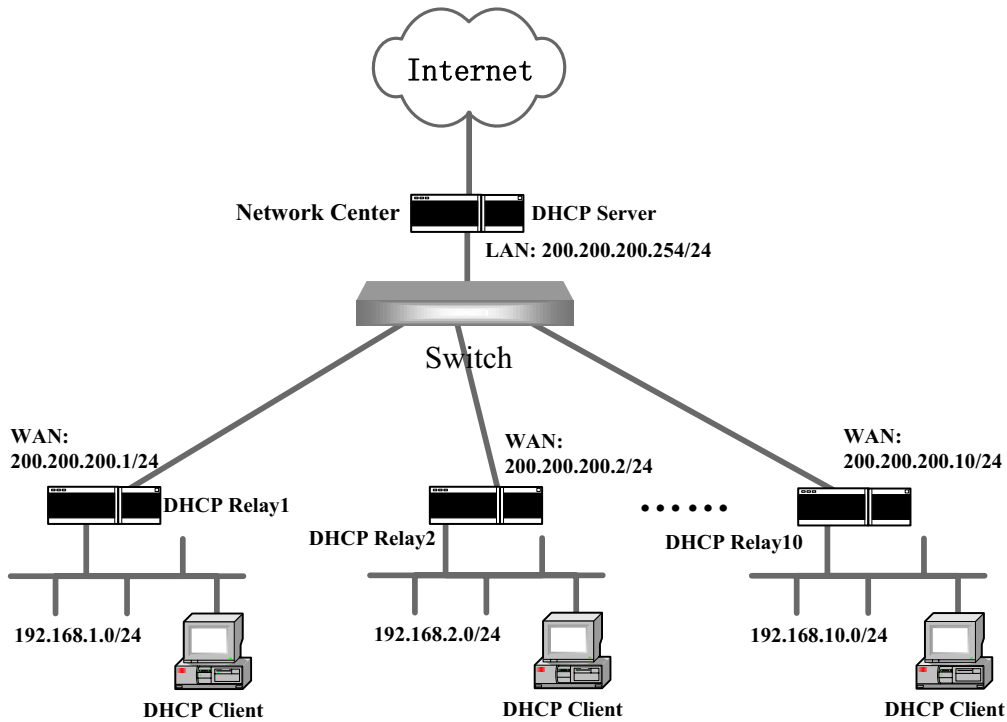


Figure 7-47 Network Topology for DHCP Comprehensive Example

3. Configuration Procedure

As DHCP address pools have the similar configuration procedure, here we will take DHCP address **pool1** for example to describe how to configure the DHCP address pool.

As DHCP relay agents have the similar configuration procedure, here we will take **DHCP Relay1** for example to describe how to configure the DHCP relay agent.

1) Configuring DHCP server

a) Configuring DHCP Server Global Parameters

Step 1 Go to the **Advanced > DHCP** page, and then select the **DHCP Server** radio button to go to the **DHCP Server** page.

Step 2 Select the **Global Settings** tab to go to the setup page.

Step 3 Select the **Enable DHCP Server** check box, see the following figure.

Global Settings	Manual Binding List	Manual Binding Settings	Address Pool List
-----------------	---------------------	-------------------------	-------------------

Enable DHCP Server	<input checked="" type="checkbox"/>
DHCP Ping Packets	<input type="text" value="2"/>
DHCP Ping Timeout	<input type="text" value="500"/> milliseconds

Figure 7-48 DHCP Server Global Settings - Comprehensive Example

Step 4 Click the **Save** button to save the settings. Till now you have finished configuring DHCP server global settings.

b) Configuring the DHCP Address Pool - pool1

As mentioned earlier, the **pool1** is the system default address pool. And it is editable, but can't be deleted. So you could modify the **pool1** according to your requirements. The steps are as follows:

Step 1 Go to the **Advanced > DHCP** page, and then select the **DHCP Server** radio button to go to the **DHCP Server** page.

Step 2 Select the **Address Pool List** tab, and then click the **pool1**'s **Edit** hyperlink in the **Address Pool List**, the related information will be displayed in the setup page.

Interface	LAN
Pool Name	pool1
Start IP Address	192.168.1.2
Number of Addresses	253
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.1
Lease Time	3600 seconds
Primary DNS Server	202.96.209.5
Secondary DNS Server	202.96.199.133
Primary WINS Server	0.0.0.0
Secondary WINS Server	0.0.0.0
Advanced Options	
Domain Name	
Relay Agent IP	0.0.0.0
Enable AutoIP	<input checked="" type="checkbox"/>
Response Mode	Broadcast
NetBIOS Node Type	B-Node
Relay Agent ID	ascii Test_Relay1

Figure 7-49 DHCP Address Pool Settings - Comprehensive Example (pool1)

- Step 3** Enter **192.168.1.2** in the **Start IP Address** text box, enter **253** in the **Number of Addresses** text box, enter **192.168.1.1** in the **Default Gateway** text box, enter **202.96.209.5** in the **Primary DNS Server** text box and enter **202.96.199.133** in the **Secondary DNS Server** text box.
- Step 4** Select **ascii** from the **Relay Agent ID** drop-down list and enter **Test_Relay1** in the associated text box. Leave the default values for the other parameters.
- Step 5** Click the **Save** button to save the settings. Till now you have finished configuring the **pool1**, and then you can view its configuration in the **Address Pool List**.

c) Configuring the Other DHCP Address Pools (pool2 ~ pool10)

The other DHCP address pools' configuration procedures are very similar to that of the **Pool1**. The difference is that each DHCP address pool has different **Pool Name**, **Start IP Address**, **Default Gateway** and **Relay Agent ID**. Since the other DHCP address pools' configuration procedures are so similar to that of the **pool1**, the user is directed to review the configuration procedure of the **pool1**.

2) Configuring DHCP Relay1

Step 1 Go to the **Advanced > DHCP** page, select the **DHCP Relay Agent** radio button and then select the **Relay Agent Settings** tab to go to the setup page, see the following figure.

Agent List	Relay Agent Settings
Interface	LAN
Enable DHCP Relay	<input checked="" type="checkbox"/>
DHCP Server 1	200.200.200.254
DHCP Server 2	0.0.0.0
DHCP Server 3	0.0.0.0
Option	insert
Policy	keep
Max. Packet Size	1024
Relay Agent ID	ascii Test_Relay1
Response Mode	Broadcast
Save	

Figure 7-50 DHCP Relay Agent Settings - Comprehensive Example (DHCP Relay1)

- Step 2** Select **LAN** from the **Interface** drop-down list.
- Step 3** Select the **Enable DHCP Relay Agent** check box.
- Step 4** Enter **200.200.200.254** in the **DHCP Server 1** text box. Select **insert** from the **Option** text box, select **ascii** from the **Relay Agent ID** drop-down list and enter **Test_Relay1** in the associated text box. Leave the default values for the other parameters.
- Step 5** Click the **Save** button to save the settings. Till now you have finished configuring the DHCP relay agent, and then you can view its configuration in the **DHCP Relay Agent List**.

3) Configuring the Other DHCP Agent Relays (DHCP Relay2 ~ Realy10)

The other DHCP relay agents' configuration procedures are very similar to that of the **DHCP Relay1**. The difference is that each DHCP relay agent has different **Relay Agent ID**. Since the other DHCP relay agents' configuration procedures are so similar to that of the **DHCP Relay1**, the user is directed to review the configuration procedure of the **DHCP Relay1**.

7.9 Switch

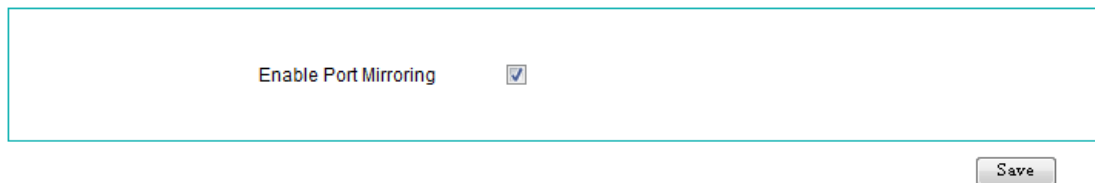
This section describes **Advanced > Switch** page.

7.9.1 Port Mirroring

7.9.1.1 Introduction to Port Mirroring

The port mirroring allows an administrator to mirror and monitor network traffic. It copies the traffic from the specified ports to another port where the traffic can be monitored with an external network analyzer. Then the administrator can perform traffic monitoring, performance analysis and fault diagnosis.

7.9.1.2 Port Mirroring Setup



Enable Port Mirroring

Save

Figure 7-51 Port Mirroring Settings

- ✧ **Enable Port Mirroring:** It allows you enable or disable port mirroring. If you want to enable port mirroring on the Device, please select this check box. By default, the LAN Port 1 is the mirroring port that can't be changed. If the port mirroring is enabled, the LAN Port 1 will mirror the traffic of the other LAN ports
- Click the **Save** button to save the port mirroring settings.



Note

If the LAN switch ports belong to different VLANs, only the traffic of the ports on the same VLAN as the Port 1 can be mirrored.

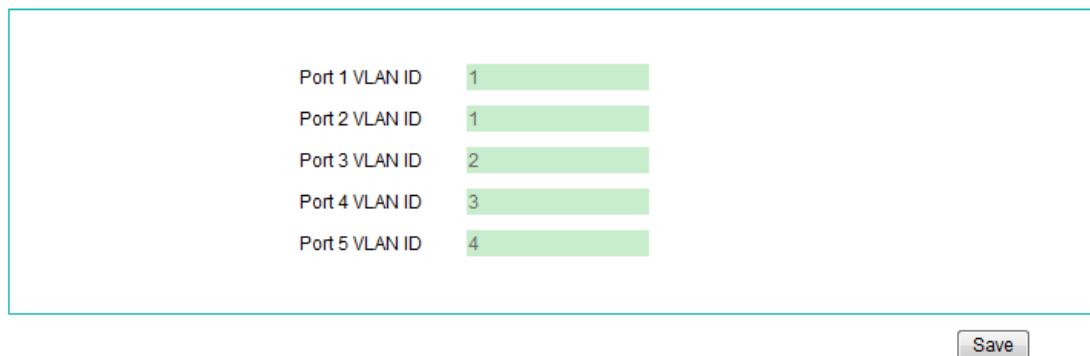
7.9.2 Port-Based VLAN

7.9.2.1 Introduction to VLAN

A VLAN (Virtual Local Area Network) is a group of devices that form a logical LAN segment, that is, a broadcast domain. The members on the same VLAN can communicate with each other. The traffic will not disturb among different VLANs, that is, any traffic (unicast, broadcast or multicast) within a VLAN doesn't flow to another VLAN. The VLAN feature offers the benefits of both security and performance. VLAN is used to isolate traffic between different users which provides better security. Limiting the broadcast traffic within the same VLAN broadcast domain also enhances performance.

The Device provides port-based VLAN, which is defined according to the switch ports on the Device. You can set a VLAN ID to each switch port. The ports that have the same VLAN ID will be grouped into a VLAN. The ports that belong to the same VLAN can communicate with each other, but the ports that belong to the different VLANs can't communicate. For example, if a port belongs to VLAN 1 and another port belongs to VLAN 2, the two ports will not be able to communicate with each other.

7.9.2.2 Port-Based VLAN Setup



Port 1 VLAN ID	1
Port 2 VLAN ID	1
Port 3 VLAN ID	2
Port 4 VLAN ID	3
Port 5 VLAN ID	4

Save

Figure 7-52 Port-Based VLAN Setup

- ✧ **Port 1 VLAN ID ~ Port 5 VLAN ID:** They specify the VLAN IDs of the five switch ports. It allows you to set a VLAN ID to each switch port for each switch port respectively. The ports that have the same VLAN ID will be grouped into a VLAN, which is independent of the other ports.
- **Save:** Click it to save the VLAN settings.

**Note**

1. The ports that have the same VLAN ID will be grouped into a VLAN. The ports on the same VLAN can communicate with each other, but the ports that belong to the different VLANs can't communicate.
2. By default, all the LAN switch ports are members of the same VLAN. The most complex case is that each port is grouped into a VLAN respectively. For example, see Figure 7-52, Port 1 and Port 2 are grouped into a VLAN (VLAN 1), Port 3, Port 4 and Port 5 are grouped to the different VLANs (VLAN 2, VLAN 3 and VLAN 4) respectively.
3. The ports within a LAG should be grouped into the same VLAN.

7.10 Miscellaneous

This section describes **Advanced > Miscellaneous** page, which include **Miscellaneous**, **Scheduled Task List**, and **Scheduled Task Settings** subpages.

7.10.1 Miscellaneous

Miscellaneous

Enable Internet Connection Sharing Protection Shield

Enable Traffic Destined for Same IP Address via Different WANs

[Display Scheduled Task](#)

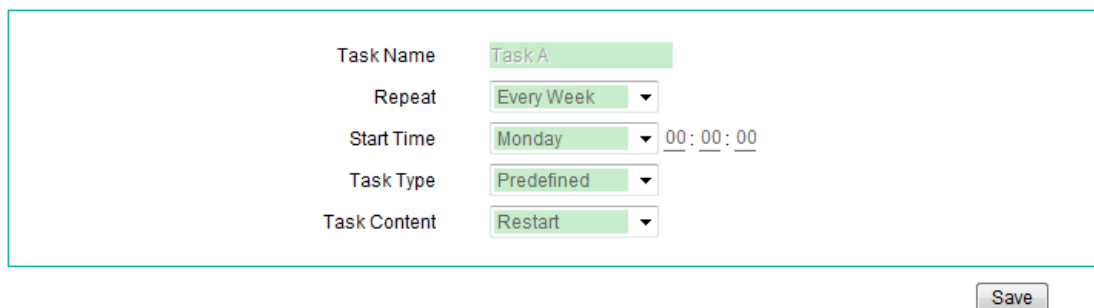
Figure 7-53 Miscellaneous

- ✧ **Enable Internet Connection Sharing Protection Shield:** It allows you to enable or disable Internet connection sharing protection shield. When your ISP forbid you from sharing a single Internet connection, you can select the check box to enable this feature, then all your LAN hosts still can share the Internet connection to access the Internet.

- ✧ **Enable Traffic Destined for Same IP Address via Different WANs:** It allows you to enable or disable traffic destined for same IP address via different WANs. When using multiple Internet connections to access the Internet, if you select this check box, the packets destined for the same IP address will be transmitted through different Internet connections to implement load balancing.
- **Save:** Click it to save your settings.

7.10.2 Scheduled Task

By default, if you click the **Display Scheduled Task** hyperlink in the **Advanced > Miscellaneous** page (see Figure 7-53), it will jump to the **Scheduled Task Settings** page, see Figure 7-54. But if you have created one or more scheduled tasks, it will jump to the **Scheduled Task List** page.



Task Name	Task A
Repeat	Every Week
Start Time	Monday 00:00:00
Task Type	Predefined
Task Content	Restart

Figure 7-54 Scheduled Task Settings

- ✧ **Task Name:** It indicates the sequence number of the task, and it is read-only.
- ✧ **Repeat:** It specifies how often or when the Device will perform the task. The available options are **Every Week**, **Every Day**, **Every Hour**, **Every Minute**, or **When Starting**.
- ✧ **Start Time:** It specifies the time at which the Device will start to perform the task. Its settings will change according to the value of **Repeat**.
- ✧ **Task Type:** It specifies the type of the task. The available options are **Predefined** and **User-defined**.
 - **Predefined:** If you want to add a new predefined task, please select this option, and then select a predefined task from the **Task Content**. Now the Device provides two predefined scheduled tasks: **Bind All** and **Restart**; therein, **Bind All** means that the Device will bind all the IP/MAC address pairs periodically; **Restart** means that the Device will restart itself periodically.

- **User-defined:** If you want to add a new user-defined task, please select this option, and then enter the related CLI command in the **Task Content**. Note that you can only enter one command for one task.

- ✧ **Task Content:** It specifies the content of the task.

- **Save:** Click it to save the scheduled task settings.

Chapter 8 NAT

This chapter describes how to configure and use NAT features, including port forwarding, DMZ hosts, NAT rule and UPnP.

8.1 Port Forwarding

This section describes the **NAT > Port Forwarding** page, which allows you to configure port forwarding rules.

8.1.1 Introduction to Port Forwarding

By default, NAT is enabled on the Device, so the Device will block all the requests initiated from outside users. In some cases, the outside users want to access the LAN internal servers through the Device. To achieve this purpose, you need to create port forwarding rules or DMZ hosts on the Device.

Using port forwarding, you can create the mapping between <external IP address: external port> and <internal IP address: internal port>, then all the requests from outside users to the specified external IP address: port on the Device will be forwarded to the mapped local server, so the outside users can access the service offered by the local server.

For example, if you want to allow the local SMTP server (IP address: 192.168.16.88) to be available to the outside users, you can create a port forwarding rule: external IP address is WAN1 IP address (200.200.201.88 in this example), external port is 2100, internal IP address is 192.168.16.88, and internal port is 25. Then all the requests for SMTP from outside users to 200.200.201.88:2100 will be forwarded to 192.168.16.88:25.

8.1.2 Port Forwarding Settings

The screenshot shows the 'Port Forwarding Settings' configuration page. It features two tabs at the top: 'Port Forwarding List' (highlighted in yellow) and 'Port Forwarding Settings'. The main content area is a form with the following fields:

- Protocol: TCP (dropdown menu)
- Start External Port: 2025 (text input)
- Internal IP Address: 192.168.16.88 (text input)
- Start Internal Port: 25 (text input)
- Port Count: 1 (text input)
- Bind to: WAN1 (dropdown menu)
- Description: SMTP (text input)

A 'Save' button is located at the bottom right of the form area.

Figure 8-1 Port Forwarding Settings

- ✧ **Protocol:** It specifies the transport protocol used by the service. The available options are **TCP**, **UDP** and **GRE**.
- ✧ **Start External Port:** It specifies the lowest port number provided by the Device. The external ports are opened for outside users to access.
- ✧ **Internal IP Address:** It specifies the IP address of the local host that provides the service.
- ✧ **Start Internal Port:** It specifies the lowest port number of the service provided by the LAN host. The **Start External Port** and **Start Internal Port** can be different.
- ✧ **Port Count:** It specifies the number of service ports provided by the LAN host. If the service uses only one port number, enter 1. The maximum value is 20. For example, if the start internal port is 21, the start external port is 2001 and the port count is 10, then the internal port range is from 21 to 30, and the external port range is from 2001 to 2010.
- ✧ **Bind to:** It specifies the NAT rule to which this port forwarding rule is bound. The port forwarding rule will use the NAT rule's external IP address as its external IP address. The available options are:
 - Each **EasyIP** NAT rule's **ID**: it stands for the corresponding NAT rule respectively.
 - **WANx** (x: 1, 2, 3, 4): It stands for the system reserved NAT rule bound to the Internet connection on the selected WAN interface. The reserved NAT rule uses the WAN interface's IP address as its external IP address.

- ✧ **Description:** It specifies the description of the port forwarding rule.
- **Save:** Click it to save the port forwarding rule settings.



Note

1. If you choose the **Protocol** as **GRE**, you should set the **Start External Port** and **Start Internal Port** to 0, and set the **Port Count** to 1.
2. After you have enabled some features (such as, HTTP management in the **System > Remote Admin** page), the system will automatically create some port forwarding rules, which cannot be modified or deleted.

8.1.3 Port Forwarding List

Port Forwarding List Port Forwarding Settings

3/100 Lines/Page: 10 First Prev Next Last Search:

ID	Protocol	Internal IP Address	Start Internal Port	Start External Port	Port Count	Bind to	Description	Edit
<input type="checkbox"/> i2tp	UDP	192.168.16.1	1701	1701	1	WAN1		Edit
<input type="checkbox"/> pptp	TCP	192.168.16.1	1723	1723	1	WAN1		Edit
<input type="checkbox"/> 1	UDP	192.168.16.88	25	2025	1	WAN1	SMTP	Edit

Select All

Figure 8-2 Port Forwarding List

- **Add a Port Forwarding Rule:** If you want to add a new port forwarding rule, click the **New** button or select the **Port Forwarding Settings** tab to go to the setup page, and then configure it, lastly click the **Save** button.
- **View Port Forwarding Rule(s):** When you have configured some port forwarding rules, you can view them in the **Port Forwarding List**.
- **Edit a Port Forwarding Rule:** If you want to modify a configured port forwarding rule, click its **Edit** hyperlink, the related information will be displayed in the setup page. Then modify it, and click the **Save** button.
- **Delete Port Forwarding Rule(s):** If you want to delete one or more port forwarding rules, select the leftmost check boxes of them, and then click the **Delete** button.

8.1.4 How to Add the Port Forwarding Rules

If you want to add one or more port forwarding rules, do the following:

- Step 1** Go to the **NAT > Port Forwarding** page, and then click the **New** button or select the **Port Forwarding Settings** tab to go to the setup page.
- Step 2** Specify the **Protocol**, **Internal IP Address** and **Start Internal Port** as required.
- Step 3** Specify the **Start External Port** as required. The **Start External Port** and **Start Internal Port** can be different.
- Step 4** If the open service uses a range of consecutive ports, you need specify the **Port Count**.
- Step 5** Select a NAT rule from the **Bind to** drop-down list as required. The port forwarding rule will use the selected NAT rule's external IP address as its external IP address.
- Step 6** Click the **Save** button to save the settings. You can view the port forwarding rule in the **Port Forwarding List**.
- Step 7** If you want to add another new port forwarding rule, please repeat the above steps.



Note

If you want to delete one or more port forwarding rules, select the leftmost check boxes of them in the **Port Forwarding List**, and then click the **Delete** button.

8.1.5 Configuration Examples for Port Forwarding

8.1.5.1 Example One

An organization wants a LAN server (IP Address: 192.168.16.88) to open syslog service (Protocol: UDP; Port: 514) to the outside users. And the Device will use 2514 as the external port and the WAN1 IP address (200.200.200.88 in this example) as the external IP address. Then all the requests for syslog from outside users to 200.200.200.88:2514 will be forwarded to 192.168.16.99:514.

The following figure shows the detailed settings.

Protocol	UDP
Start External Port	2514
Internal IP Address	192.168.16.88
Start Internal Port	514
Port Count	1
Bind to	WAN1
Description	Syslog

Figure 8-3 Port Forwarding Settings - Example One

8.1.5.2 Example Two

An organization wants a LAN server (IP Address: 192.168.16.100) to open ftp service (Protocol: TCP; Port: 20, 21) to the outside users. And the Device will use 2020 and 2021 as the external ports and the WAN2 IP address (200.200.201.18 in this example) as the external IP address. As the ftp service uses two ports, so we need set the **Port Count** to 2. Then all the requests for ftp from outside users to 200.200.201.18:2020 or 200.200.201.18:2021 will be forwarded to 192.168.16.100:20 or 192.168.16.100:21.

The following figure shows the detailed settings.

Protocol	TCP
Start External Port	2020
Internal IP Address	192.168.16.100
Start Internal Port	20
Port Count	2
Bind to	WAN2
Description	FTP

Figure 8-4 Port Forwarding Settings - Example Two

8.1.5.3 Example Three

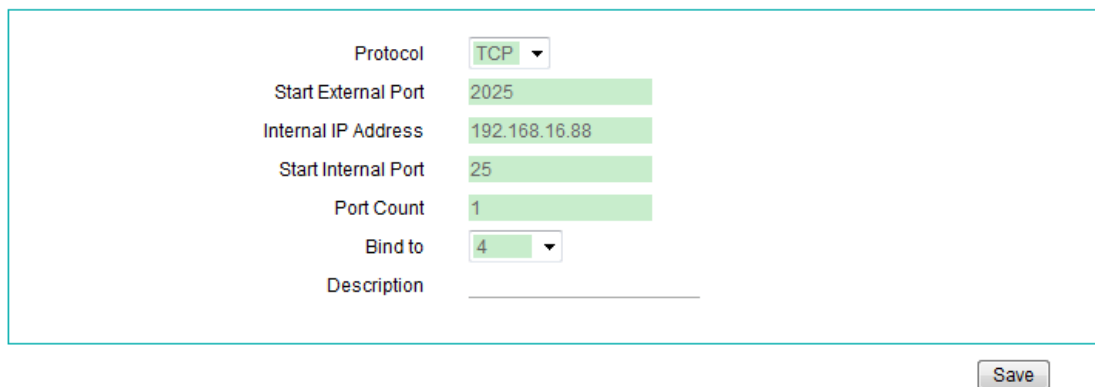
An organization obtains eight public IP addresses (from 218.1.21.0/29 to 218.1.21.7/29)

from the ISP. Therein, 218.1.21.1/29 is used as the Internet connection's gateway IP address, 218.1.21.2/29 is used as the Device's WAN1 interface's IP address.

The organization wants a LAN server (IP Address: 192.168.16.88) to open SMTP service (Protocol: TCP; Port: 25) to the outside users. And the Device will use 2025 as the external port and 218.1.21.3 as the external IP address.

Firstly, we need to create a NAT rule, and set its **External IP Address** to 218.1.21.3, see section 8.3.5 **How to Add the NAT Rules** for detailed information. Then we need to create the port forwarding rule, and select the NAT rule's **ID (4** in this example) from the **Bind to** drop-down list.

The following figure shows the detailed settings.



The screenshot displays a configuration window for port forwarding. It includes the following fields and values:

Protocol	TCP
Start External Port	2025
Internal IP Address	192.168.16.88
Start Internal Port	25
Port Count	1
Bind to	4
Description	

A "Save" button is located at the bottom right of the configuration area.

Figure 8-5 Port Forwarding Settings - Example Three

8.2 DMZ Host

This section describes the **NAT > DMZ** page.

8.2.1 Introduction to DMZ host

The DMZ (Demilitarized Zone) host allows one local host to be exposed to the Internet for the use of a special service such as online game or video conferencing. When receiving the requests initiated from outside users, the Device will directly forward these requests to the specified DMZ host.

For the Device that has multiple WAN interfaces, it allows you to create one global DMZ host, and several interface DMZ hosts which are bound to each WAN interface respectively.

- **Global DMZ host:** You can access the global DMZ host through different Internet connections at the same time.
- **Interface DMZ host:** You can only access the interface DMZ host through the corresponding Internet connection.

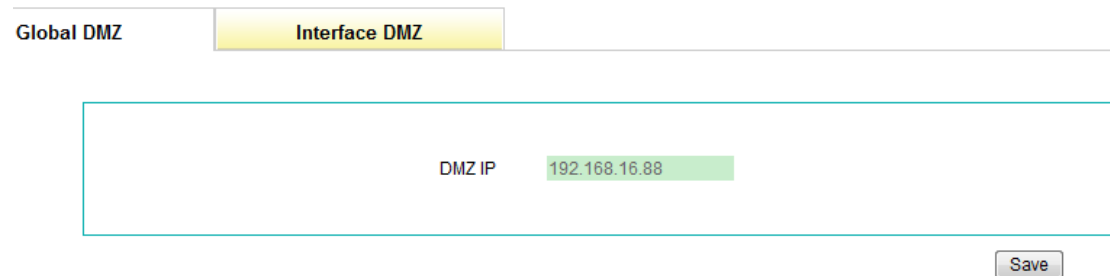


Note

When a local host is designated as the DMZ host, it loses firewall protection provided by the Device. As the DMZ host is exposed to many exploits from the Internet, it may be used to attack your network.

8.2.2 DMZ Host Settings

8.2.2.1 Global DMZ Host Settings



Global DMZ Interface DMZ

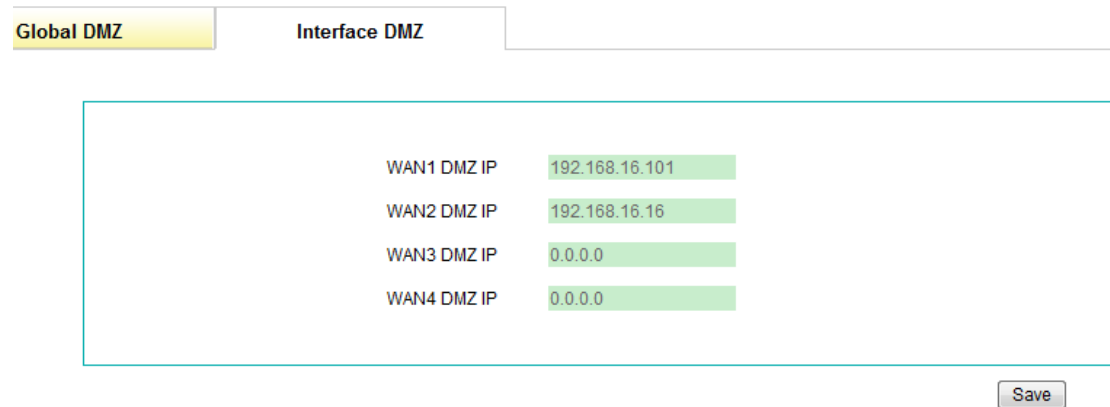
DMZ IP 192.168.16.88

Save

Figure 8-6 Global DMZ Host Settings

- ✧ **DMZ IP:** It specifies the private IP address of the global DMZ host.
- **Save:** Click it to save the global DMZ host settings.

8.2.2.2 Interface DMZ Host Settings



Global DMZ Interface DMZ

WAN1 DMZ IP 192.168.16.101

WAN2 DMZ IP 192.168.16.16

WAN3 DMZ IP 0.0.0.0

WAN4 DMZ IP 0.0.0.0

Save

Figure 8-7 Interface DMZ Host Settings

- ✧ **WANx DMZ IP:** It specifies the private IP address of the interface DMZ host which is bound to the WAN interface. Therein, x (value: 1, 2, 3, 4) indicates the corresponding WAN interface, and the number of WAN interfaces depends on the specific product model.
- **Save:** Click it to save the interface DMZ host settings.

8.2.3 The Priorities of Port Forwarding and DMZ Host

The port forwarding has higher priority than the DMZ host. When receiving a request packet initiated from an outside user, the Device will firstly search the **Port Forwarding List** to find out if there is a port forwarding rule matching the destination IP address and port of the packet. If a match is found, the Device will forward the packet to the mapped local host. Else, the Device will try to find out if there is an available DMZ host.

And the interface DMZ host has higher priority than the global DMZ host. Only when there is no interface DMZ host available to the request packet, the Device will choose the global DMZ host.

8.3 NAT Rule

8.3.1 Introduction to NAT

The NAT (Network Address Translation) is an Internet standard that is used to map one IP address space (i.e., Intranet) to another IP address space (i.e., Internet). The NAT is designed to alleviate the shortage of IP addresses, that is, it allows all the LAN hosts to share a single or a small group of IP addresses: On the Internet, there is only a single device using a single or a small group of public IP addresses; but the LAN hosts can use any range of private IP addresses, and these IP addresses are not visible from the Internet. As the internal network can be effectively isolated from the outside world, the NAT can also provide the benefit of network security assurance.

The Device provides flexible NAT features, and the following sections will describe them in detail.

8.3.1.1 NAT Address Space Definitions

To ensure that NAT operates properly, the Device uses and maintains two address spaces:

- **Internal IP address:** It indicates the IP address that is assigned to a LAN host by the administrator. It is usually a private IP address.
- **External IP address:** It indicates the IP address that is assigned to the Device's Internet connection by the ISP. It is a legal public IP address that can represent one or more internal IP addresses to the outside world.

8.3.1.2 NAT Types

The Device provides three types of NAT: **One2One**, **EasyIP** and **Passthrough**.

- **One2One (One to One):** It indicates static network address translation. It is always referred to as Basic NAT, which provides a one to one mapping between an internal and an external IP address. In this type of NAT, IP address need be changed, but port needn't.

One to One NAT can be used to allow the outside users to access a LAN server: In the

local network, the LAN server still use the private IP address, which is provided to the LAN hosts to access; and on the Internet, the Device will assign an external IP address to the local server, then the outside users can using this external IP address to access the server through the Device.

- **EasyIP:** It indicates network address and port translation (NAPT). Since it is the most common type of NAT, it is often simply referred to as NAT. NAPT provides many-to-one mappings between multiple internal IP addresses and a single external IP addresses, that is, these multiple internal IP addresses will be translated to the same external IP address. In this type of NAT, to avoid ambiguity in the handling of returned packets, it must dynamically assign a TCP/UDP port to an outgoing session and change the packets' source port to the assigned port before forwarding them. Besides, the Device must maintain a translation table so that return packets can be correctly translated back.
- **Passthrough:** It indicates bypassing NAT when NAT is enabled. If you enable NAT, the LAN hosts must match a NAT rule when accessing outside hosts. So if you do not want to perform NAT for some LAN hosts, you can use this function to bypass NAT for those hosts. It is often used for some particular applications that do not support NAT well, such as, online game or video conferencing. To ensure that these applications run properly, you can divide a voice and video area in the LAN, and create a **Passthrough** NAT rule for the hosts in this area. Then the Device will not perform NAT for them, that is, the packets sent by these hosts to the outside hosts will be directly routed and forwarded.

When you obtain multiple public IP addresses from your ISP, you can create more than one NAT rule for each type of NAT. In actual network environment, different types of NAT rules are often used together.

8.3.1.3 The Relations of Internet Connection, NAT Rule and Port Forwarding Rule

On the Device, the relations of the Internet connection, NAT rule and port forwarding rule are as follows:

- A NAT rule should be bound to an Internet connection. It allows you bind multiple NAT rules to the same Internet connection.
- A port forwarding rule should be bound to an **EasyIP** NAT rule (that is, the NAT rule's type is **EasyIP**), and the port forwarding rule will use the NAT rule's external IP address

as its external IP address. It allows you bind multiple port forwarding rules to the same **EasyIP** NAT rule.

- Only after you have configured an Internet connection, you can create a NAT rule which is bound to this Internet connection; and only after you have configured an **EasyIP** NAT rule, you can create a port forwarding rule which is bound to this **EasyIP** NAT rule.

8.3.1.4 System Reserved NAT Rules

After you have finished configuring the WAN1 Internet connection through the **Quick Wizard**, or configuring the WAN1 Internet connection and other connections in the **Basic > WAN** page, the Device will automatically create a NAT rule for each Internet connection respectively.

For convenience, we call them system reserved NAT rules in the manual. You can view them in the **NAT Rule List**. By default, a system reserved NAT rule's **Type** is **EasyIP**, **Bind to** is the WAN interface on which the Internet connection is established, external IP Address is **0.0.0.0** which means this NAT rule will directly use the WAN interface's IP address as its external IP address.

8.3.2 NAT and Multi-WAN Load Balancing

8.3.2.1 Overview

The **section 6.3 Load Balancing** describes load balancing among multiple Internet connections. In actual, that feature implementation is based on NAT feature.

8.3.2.2 Assigning Preferential Channel according to Source IP

Here, the channel stands for the NAT rule, which determines NAT type, external IP address and Internet connection used by the LAN hosts to surf the Internet.

On the Device, you can assign a preferential channel to some LAN hosts in advance by specifying the NAT rule's **Start Internal IP Address** and **End Internal IP Address**, then the LAN hosts belong to the specified address range will preferentially use the assigned NAT rule to access the Internet. If the assigned NAT rule is in effect, these LAN hosts can only use this NAT rule to access the Internet. Else, the Device will take them as the free

LAN hosts (that is, the hosts that have not been assigned a preferential channel) to process. On the Device, you can assign different preferential channel for different LAN hosts.

8.3.2.3 Allocating Traffic according to Connection Bandwidth

On the Device, you can designate the ratio of traffic that will be allocated to each Internet connection in advance. You can achieve this by specifying the Internet connection's **Weight**, the connection that has larger **Weight** will take more traffic than the connection that has smaller **Weight**. In most cases, to properly allocate traffic, you may specify each connection's **Weight** according to the ratio of each connection's bandwidth.

Note that if several EasyIP NAT rules are bound to an Internet connection with multiple IP addresses, then the Internet connection's **Weight** is the sum of each EasyIP NAT rule's **Weight**.

Besides, when you have designated preferential channels for some LAN hosts, if you specify each connection's **Weight** according to the ratio of each connection's bandwidth, the ratio of each connection's actual traffic and the ratio of each connection's bandwidth may be quite different. In this case, you can adjust each connection's **Weight** according to the actual situation.

8.3.2.4 Two Load Balancing Policies



Note

In this section, those hosts that have not been assigned a preferential NAT rule are called **free LAN hosts**.

The **Load Balancing Policy** is used to control and balance the traffic among multiple Internet connections. Note that the load balancing policy only acts on the free LAN hosts. The **Load Balancing Policy** is configured in the **Basic > Load Balancing > Global Settings** page, and the Device provides two load balancing policies: load balancing based on IP address and NAT session. Their implementation mechanisms are as follows.

1. Load Balancing Based on IP Address

Note that here we assume that each LAN host only has one IP address.

If you choose IP address as the load balancing policy, the Device will assign the free LAN hosts' IP addresses to each **EasyIP** NAT rule in turn. The ratio of the numbers of the IP addresses assigned to each **EasyIP** NAT rule is the same with the ratio of each rule's

Weight. In this case, the NAT sessions initiated from the same IP address will use the same NAT rule, that is, a LAN host will use only one NAT rule to access the Internet.

For example, there are three **EasyIP** NAT rules whose **Weights** are 3, 2 and 1 respectively. Then in the sequence of accessing the Internet, the first, second and third free hosts will use the first rule, the fourth and fifth free hosts will use the second rule, the sixth free hosts will use the third rule; then the seventh, eighth and ninth free hosts will use the first rule ... and so on.

2. Load Balancing Based on NAT Session

If you choose NAT session as the load balancing policy, the Device will assign the NAT sessions to each **EasyIP** NAT rule in turn. The ratio of the numbers of the NAT sessions assigned to each **EasyIP** NAT rule is the same with the ratio of each rule's **Weight**. In this case, the NAT sessions initiated from the same LAN host will use different NAT rules, that is, a LAN host will use several NAT rules to access the Internet.

For example, there are three **EasyIP** NAT rules whose **Weights** are 3, 2 and 1 respectively. Then in the sequence of accessing the Internet, the first, second and third NAT sessions initiated from the free LAN hosts will use the first rule, the fourth and fifth NAT sessions will use the second rule, the sixth NAT sessions will use the third rule; then the seventh, eighth and ninth NAT sessions will use the first rule ... and so on.

3. How to Choose the Load Balancing Policy

In most cases, it is suggested that you choose IP address as the load balancing policy. If you want to use some applications that need high bandwidth, such as the NetAnts, FlashGet, Net Transport, and other multi-threaded download managers (multi-threaded download means that it can split a file into several pieces and download the pieces simultaneously, and merge them together once downloaded), you may choose NAT session as the load balancing policy to take full advantage of multiple Internet connections' bandwidth to increase download speed. Note that even you choose NAT session as the load balancing policy, due to that the related download website is busy or there are some other reasons, the bandwidth of each Internet connection cannot be aggregated fully, so some applications may be not running smoothly.

8.3.2.5 The Priorities of NAT Rules

When receiving a request packet initiated from a LAN host to access the Internet, the Device will firstly search the **NAT Rule List** to find out if there is a NAT rule matching the source IP address or the packet, that is, the host's IP address belongs to the address range specified by the **Start Internal IP Address** and **End Internal IP Address** of the NAT rule. If a match is found, the Device will assign the matched NAT rule to the host, and then the host will use this rule to access the Internet. Else, the Device will assign the **EasyIP** NAT rule to the host. If there are several **EasyIP** NAT rules, the Device will assign

the IP addresses or NAT sessions to each **EasyIP** NAT rule in turn. Then the Device will effectively control and balance the traffic among multiple Internet connections.

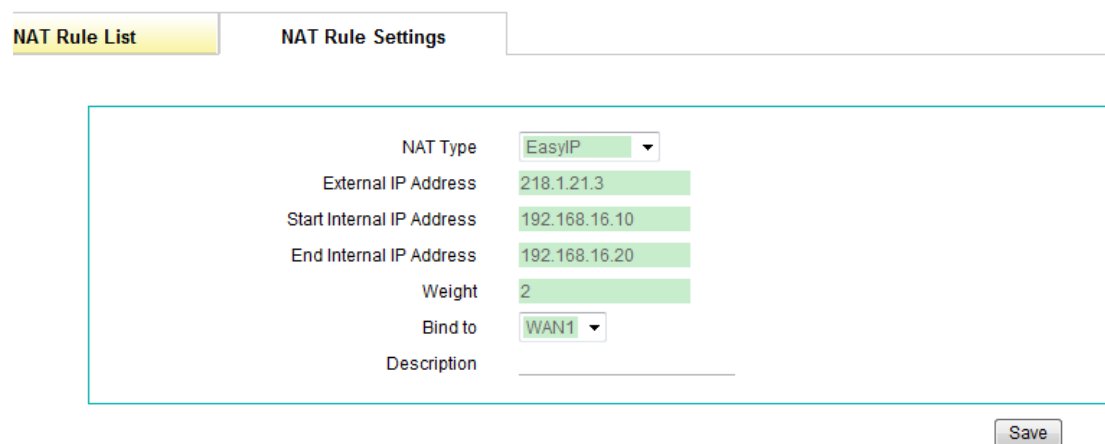
8.3.3 NAT Rule Settings

The following sections describe three types of NAT rules respectively, which include: **EasyIP** NAT (see Figure 8-8), **One2One** NAT (see Figure 8-9), and **Passthrough** NAT (see Figure 8-10).

Note

When using multi-NAT (that is, you get multiple public IP addresses from your ISP) on a WAN interface, you should enable NAT proxy ARP on the interface. The operation is as follows: Go to the **Basic > WAN > WAN List** page, click the **Edit** hyperlink of the related Internet connection to go to its setup page, click the **Advanced Options**, and then select **Nat** from the **Proxy ARP** drop-down list, lastly click the **Save** button.

8.3.3.1 EasyIP NAT Rule Settings



NAT Type	EasyIP
External IP Address	218.1.21.3
Start Internal IP Address	192.168.16.10
End Internal IP Address	192.168.16.20
Weight	2
Bind to	WAN1
Description	

Save

Figure 8-8 EasyIP NAT Rule Settings

- ✧ **NAT Type:** It specifies the type of the NAT rule. The available options are **EasyIP**, **One2One**, and **Passthrough**. Here please select **EasyIP**.
- ✧ **External IP Address:** It specifies the external IP address to which the LAN hosts' IP addresses are mapped. A system reserved NAT rule's external IP address is **0.0.0.0**, which means that the rule will use the related WAN interface's IP address as its

external IP address; and it is non-editable. A user-defined NAT rule's external IP address can be neither 0.0.0.0 nor the WAN interface's IP address, that is, you can only use the other public IP addresses provided by your ISP as its external IP addresses.

- ✧ **Start Internal IP Address** and **End Internal IP Address**: They specify the internal address range of the NAT rule. The LAN hosts that belong to this address range will preferential use the NAT rule.
- ✧ **Weight**: It specifies the weight of the NAT rule. It should be a number between 1 and 255. The default value is 1.
- ✧ **Bind to**: It specifies an Internet connection to which the NAT rule is bound. The LAN hosts that match the NAT rule will access the Internet through this Internet connection.
- ✧ **Description**: It specifies the description of the NAT rule.
- **Save**: Click it to save the NAT rule settings.

8.3.3.2 One2One NAT Rule Settings

The screenshot displays the 'NAT Rule Settings' configuration page. At the top, there are two tabs: 'NAT Rule List' and 'NAT Rule Settings', with the latter being active. The main configuration area contains the following fields:

- NAT Type**: A dropdown menu set to 'One2One'.
- Start External IP Address**: A text input field containing '202.1.1.3'.
- Start Internal IP Address**: A text input field containing '192.168.16.100'.
- End Internal IP Address**: A text input field containing '192.168.16.106'.
- Bind to**: A dropdown menu set to 'WAN1'.
- Description**: An empty text input field.

A 'Save' button is positioned at the bottom right of the configuration area.

Figure 8-9 One2One NAT Rule Settings

- ✧ **NAT Type**: It specifies the type of the NAT rule. The available options are **EasyIP**, **One2One**, and **Passthrough**. Here please select **One2One**.
- ✧ **Start External IP Address**: It specifies the start external IP address to which the start internal IP address is mapped.
- ✧ **Start Internal IP Address** and **End Internal IP Address**: They specify the internal address range of the NAT rule. The LAN hosts that belong to this address range will use the NAT rule.

- ✧ **Bind to:** It specifies an Internet connection to which the NAT rule is bound. The LAN hosts that match the NAT rule will access the Internet through this Internet connection.
- ✧ **Description:** It specifies the description of the NAT rule.
- **Save:** Click it to save the NAT rule settings.

Note

1. When creating a **One2One** NAT rule, you should set the **Start External IP Address**, and the number of the external IP addresses is the same with the number of internal IP addresses, which is determined by the **Start Internal IP Address** and **End Internal IP Address**. For example, if the **Start Internal IP Address** is 192.168.16.6, **End Internal IP Address** is 192.168.16.8, and **Start External IP Address** is 200.200.200.116, then 192.168.16.6, 192.168.16.7, and 192.168.16.8 will be mapped to 200.200.200.116, 200.200.200.117, and 200.200.200.118 respectively.
2. In order to make both LAN hosts and Internet hosts can access a **One2One** NAT rule's external IP addresses (that is, public IP addresses), after you finished configuring the **One2One** NAT rule, the Device will automatically create the related static routes and enable NAT proxy ARP (by selecting **Nat** from **Proxy ARP** drop-down list) on the related WAN interface. You can go to the **Advanced > Static Route** page to view those static routes in the **Static Route List**, therein, the static route's **Destination IP** is a public IP addresses, **Gateway IP** is the related WAN interface's IP address.

8.3.3.3 Passthrough NAT Rule Settings

NAT Rule List

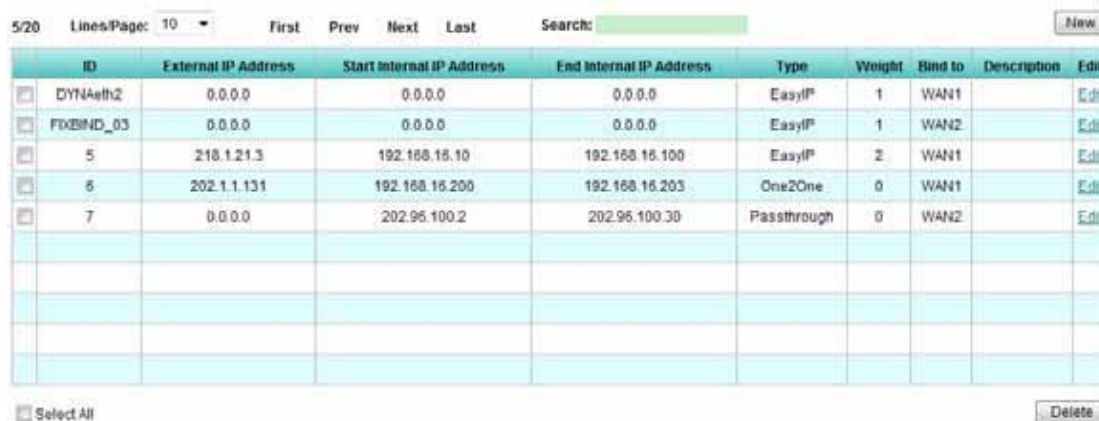
NAT Rule Settings

NAT Type	<input type="text" value="Passthrough"/>
Start Internal IP Address	<input type="text" value="202.96.100.2"/>
End Internal IP Address	<input type="text" value="202.96.100.30"/>
Bind to	<input type="text" value="WAN2"/>
Description	<input type="text"/>

Figure 8-10 Passthrough NAT Rule Settings

- ✧ **NAT Type:** It specifies the type of the NAT rule. The available options are **EasyIP**, **One2One**, and **Passthrough**. Here please select **Passthrough**.
- ✧ **Start Internal IP Address** and **End Internal IP Address:** They specify the internal address range of the NAT rule. They are usually public IP addresses provided by the ISP. The LAN hosts that belong to this address range will use the **Passthrough** NAT rule; that is, the Device will not perform NAT for them, so the packets sent by these hosts to the outside hosts will be directly routed and forwarded. Note that the internal address range of a **Passthrough** NAT rule should not overlap with the external address range of any **EasyIP** or **One2One** NAT rule.
- ✧ **Bind to:** It specifies an Internet connection to which the NAT rule is bound. The LAN hosts that match the NAT rule will access the Internet through this Internet connection.
- ✧ **Description:** It specifies the description of the NAT rule.
- **Save:** Click it to save the NAT rule settings.

8.3.4 NAT Rule List



ID	External IP Address	Start Internal IP Address	End Internal IP Address	Type	Weight	Bind to	Description	Edit
<input type="checkbox"/> DYNAuth2	0.0.0.0	0.0.0.0	0.0.0.0	EasyIP	1	WAN1		Edit
<input type="checkbox"/> FIXBIND_03	0.0.0.0	0.0.0.0	0.0.0.0	EasyIP	1	WAN2		Edit
<input type="checkbox"/> 5	218.1.21.3	192.168.16.10	192.168.16.100	EasyIP	2	WAN1		Edit
<input type="checkbox"/> 6	202.1.1.131	192.168.16.200	192.168.16.203	One2One	0	WAN1		Edit
<input type="checkbox"/> 7	0.0.0.0	202.96.100.2	202.96.100.30	Passthrough	0	WAN2		Edit

Figure 8-11 NAT Rule List

- **Add a NAT Rule:** If you want to add a new NAT rule, click the **New** button or select the **NAT Rule Settings** tab to go to the setup page, and then configure it, lastly click the **Save** button.
- **View NAT Rule(s):** When you have configured some NAT rules, you can view them in the **NAT Rule List**.
- **Edit a NAT Rule:** If you want to modify a configured NAT rule, click its **Edit** hyperlink,

the related information will be displayed in the setup page. Then modify it, and click the **Save** button.

- **Delete NAT Rule(s):** If you want to delete one or more NAT rules, select the leftmost check boxes of them, and then click the **Delete** button.

8.3.5 How to Add the NAT Rules

If you want to add one or more NAT rules, do the following:

- Step 1** Please decide the type of the NAT rule.
- Step 2** Go to the **NAT > NAT Rule** page, and then click the **New** button or select the **NAT Rule Settings** tab to go to the setup page.
- Step 3** Select a type from the **NAT Type** drop-down list as required.
- Step 4** There are three cases:
 - 1) If the NAT rules' type is **EasyIP**, please specify the **External IP Address**, **Start Internal IP Address**, **End Internal IP Address**, and **Weight** as required.
 - 2) If the NAT rules' type is **One2One**, please specify the **Start External IP Address**, **Start Internal IP Address**, and **End Internal IP Address** as required.
 - 3) If the NAT rules' type is **Passthrough**, please specify the **Start Internal IP Address** and **End Internal IP Address** as required.
- Step 5** Select an Internet connection from the **Bind to** drop-down list as required.
- Step 6** Click the **Save** button to save the settings. You can view the NAT rule in the **NAT Rule List**.
- Step 7** If you want to add another new NAT rule, please repeat the above steps.



Note

1. If you want to delete one or more NAT rules, select the leftmost check boxes of them in the **NAT Rule List**, and then click the **Delete** button. Note that you cannot delete the system reserved NAT rules here.

2. A system reserved NAT rule's external IP address is 0.0.0.0, which means that the rule will use the related WAN interface's IP address as its external IP address; and it is non-editable. A user-defined NAT rule's external IP address can be neither 0.0.0.0 nor the related WAN interface's IP address, that is, you can only use the other public IP addresses provided by your ISP as its external IP addresses.
3. The internal IP address range of each NAT rule should not overlap, and the external IP address range of each NAT rule should not overlap too; and the internal IP address range of a **Passthrough** NAT rule should not overlap with the external IP address range of any **EasyIP** or **One2One** NAT rule.

8.3.6 Configuration Examples for NAT Rule

8.3.6.1 An Example for Configuring EasyIP NAT Rule

1. Requirements

In this example, an Internet café has a single Internet connection, and obtains eight public IP addresses (from 218.1.21.0/29 to 218.1.21.7/29) from the ISP. Therein, 218.1.21.1/29 is used as the Internet connection's gateway IP address, 218.1.21.2/29 is used as the Device's WAN1 interface's IP address. Note that 218.1.21.0/29 and 218.1.21.7/29 cannot be used as they are the subnet number and broadcast address respectively.

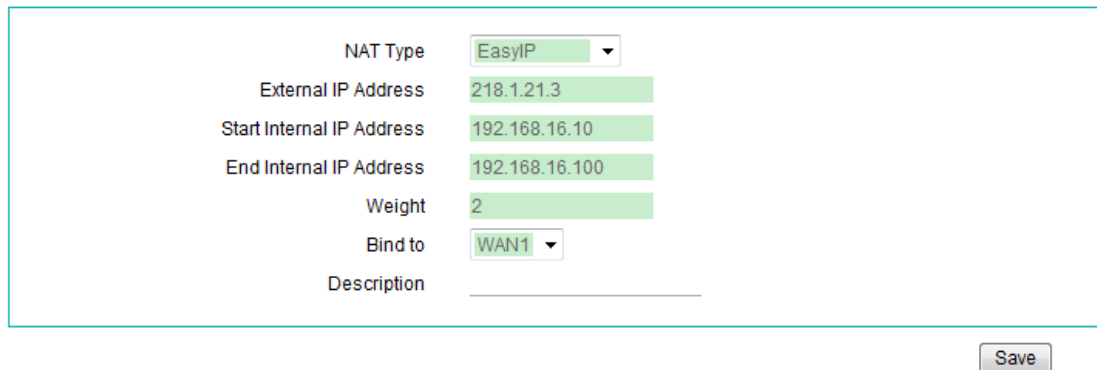
The administrator want the hosts in the online game area (its address range is from 192.168.16.10/24 to 192.168.16.100/24) to use 218.1.21.3/29 to access the Internet. To achieve this purpose, he should create an **EasyIP** NAT rule for them. The rule's **External IP Address** is 218.1.21.3, **Start Internal IP address** is 192.168.16.10, **End Internal IP Address** is 192.168.16.100, and **Bind to** is WAN1. And we assume that the **Weight** is 2.

2. Configuration Procedure

The configuration steps are the following:

Step 1 Go to the **NAT > NAT Rule** page, and select the **NAT Rule Settings** tab to go to the setup page.

Step 2 Select **EasyIP** from the **NAT Type** drop-down list, see the following figure.



The screenshot shows a configuration form for an EasyIP NAT rule. The fields are as follows:

NAT Type	EasyIP
External IP Address	218.1.21.3
Start Internal IP Address	192.168.16.10
End Internal IP Address	192.168.16.100
Weight	2
Bind to	WAN1
Description	

A "Save" button is located at the bottom right of the form.

Figure 8-12 EasyIP NAT Rule Settings - Example

- Step 3** Enter **218.1.21.3** in the **External IP Address** text box, enter **192.168.16.10** in the **Start Internal IP address** text box, and enter **192.168.16.100** in the **End Internal IP address** text box.
- Step 4** Enter **2** in the **Weight** text box.
- Step 5** Select **WAN1** from the **Bind to** drop-down list.
- Step 6** Click the **Save** button to save the settings. Till now you have finished configuring the NAT rule, and then you can view its configuration in the **NAT Rule List**.

8.3.6.2 An Example for Configuring One2One NAT Rule

1. Requirements

In this example, see Figure 8-13, a business has a single static IP Internet connection, and obtains eight public IP addresses (from 202.1.1.128/29 to 202.1.1.135/29) from the ISP. Therein, 202.1.1.129/29 is used as the Internet connection's gateway IP address, 202.1.1.130/2 is used as the Device's WAN1 interface's IP address. Note that 202.1.1.128/29 and 202.1.1.135/29 cannot be used as they are the subnet number and broadcast address respectively.

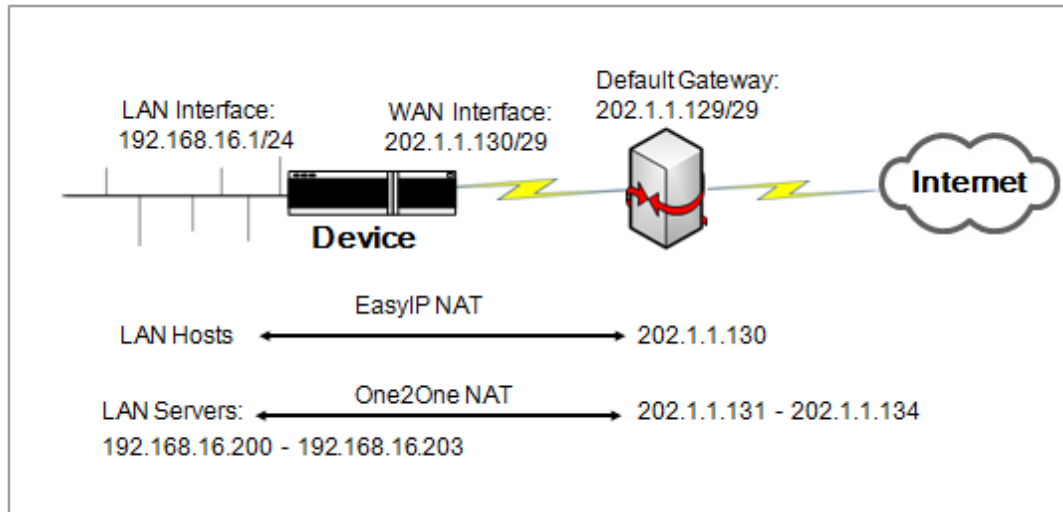


Figure 8-13 Network Topology for One2One NAT Rule Configuration Example

The business employees will share a single public IP address of 202.1.1.130/29 to access the Internet. The LAN's subnet number is 192.168.16.0, and subnet mask is 255.255.255.0. And the business want to use the remaining four public IP addresses (from 202.1.1.131/29 to 202.1.1.134/29) to create a **One2One** rule for the four local servers, then the outside users can use these public addresses to access the local servers through the Device. The four local servers IP addresses are from 192.168.16.200/24 to 192.168.16.203/24, which are mapped to 202.1.1.131/29, 202.1.1.132/29, 202.1.1.133/29, 202.1.1.134/29 respectively.

2. Analysis

Firstly we need configure a static IP Internet connection on the WAN1 interface in the **Basic > WAN** page or through the **Quick Wizard**. After you have configured the Internet connection, the Device will automatically create a related system reserved NAT rule, and also enable NAT.

Secondly, we need to create a One2One NAT rule for the four local servers. After you have configured this rule, the Device will automatically create the related static route and enable NAT proxy ARP on the WAN1 interface. Please see **section 8.3.3.2 One2One NAT Rule Settings** for detailed description.

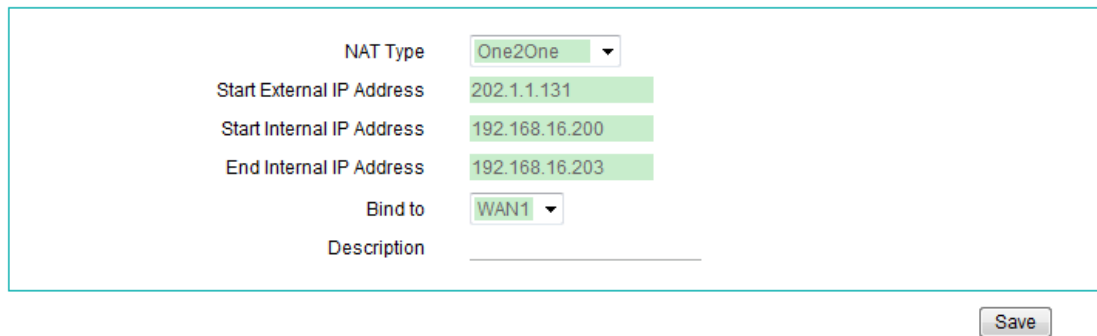
3. Configuration Procedure

Here we only describe how to create the **One2One** NAT rule.

The configuration steps are the following:

Step 1 Go to the **NAT > NAT Rule** page, and select the **NAT Rule Settings** tab to go to the setup page.

Step 2 Select **One2One** from the **NAT Type** drop-down list, see the following figure.



The screenshot shows a configuration form for a One2One NAT rule. The fields are as follows:

NAT Type	One2One
Start External IP Address	202.1.1.131
Start Internal IP Address	192.168.16.200
End Internal IP Address	192.168.16.203
Bind to	WAN1
Description	

A "Save" button is located at the bottom right of the form.

Figure 8-14 One2One NAT Rule Settings - Example

- Step 3** Enter **202.1.1.131** in the **Start External IP Address** text box, enter **192.168.16.200** in the **Start Internal IP address** text box, and enter **192.168.16.203** in the **End Internal IP address** text box.
- Step 4** Select **WAN1** from the **Bind to** drop-down list.
- Step 5** Click the **Save** button to save the settings. Till now you have finished configuring the NAT rule, and then you can view its related configuration in the **NAT Rule List**.

8.3.6.3 An Example for Configuring Passthrough NAT Rule

1. Requirements

In this example, see Figure 8-15, a business has a single static IP Internet connection. The connection IP address is 202.96.97.2/30, and the connection's gateway IP address is 202.96.97.1/30. The business employees will share the IP address of 202.96.97.2/30 to access the Internet. The LAN's subnet number is 192.168.16.0, and subnet mask is 255.255.255.0.

Furthermore, the ISP has assigned a range of IP addresses (from 202.96.100.0/27 to 202.96.100.31/27) to the business. The business wants to assign these public IP addresses for some local servers, and create a **Passthrough** NAT rule for these local servers. Note that 202.96.100.0/27 and 202.96.100.31/27 cannot be used as they are the subnet number and broadcast address respectively.

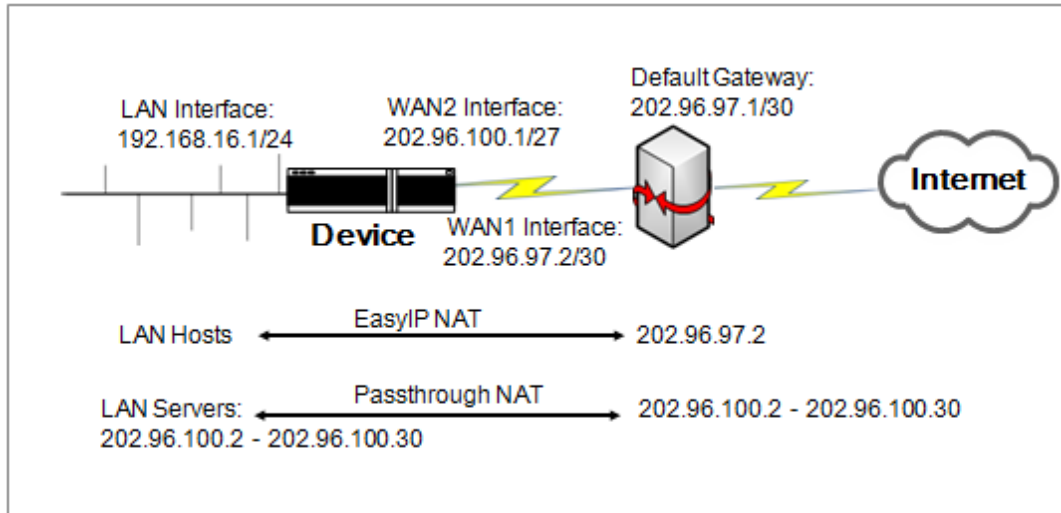


Figure 8-15 Network Topology for Passthrough NAT Rule Configuration Example

2. Analysis

Firstly we need to configure a static IP Internet connection on the WAN1 interface in the **Basic > WAN** page or through the **Quick Wizard**. After you have configured the Internet connection, the Device will automatically create the related system reserved NAT rule, and also enable NAT.

Secondly, in order to make the opened local servers be routed directly, we need to connect the servers to the Device's WAN2 interface over a switch, set the WAN2 interface IP address to 202.96.100.1/27, set each server's IP address to an IP address in the range of 202.96.100.2/27 through 202.96.100.30/27, and set each server's default gateway IP address to 202.96.100.1/27.

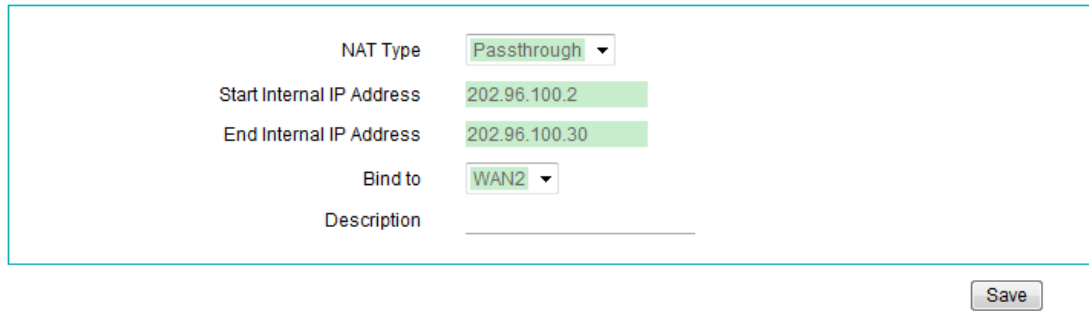
Lastly, we need to create a **Passthrough** NAT rule for the opened local servers.

3. Configuration Procedure

Here we only describe how to create the **Passthrough** NAT rule.

The configuration steps are the following:

- Step 1** Go to the **NAT > NAT Rule** page, and select the **NAT Rule Settings** tab to go to the setup page.
- Step 2** Select **Passthrough** from the **NAT Type** drop-down list, see the following figure.



NAT Type	Passthrough
Start Internal IP Address	202.96.100.2
End Internal IP Address	202.96.100.30
Bind to	WAN2
Description	

Save

Figure 8-16 Passthrough NAT Rule Settings - Example

- Step 3** Enter **202.96.100.2** in the **Start Internal IP address** text box, and enter **202.96.100.30** in the **End Internal IP address** text box.
- Step 4** Select **WAN2** from the **Bind to** drop-down list.
- Step 5** Click the **Save** button to save the settings. Till now you have finished configuring the NAT rule, and then you can view its configuration in the **NAT Rule List**.

8.4 UPnP

This section describes the **NAT > UPnP** page.

The Universal Plug and Play (UPnP) is architecture that implements zero configuration networking, that is, it provides automatic IP configuration and dynamic discovery of the UPnP compatible devices from various vendors. A UPnP compatible device can dynamically join a network, obtain an IP address, announce its name, convey its capabilities upon request, and learn about the presence and capabilities of other devices on the network.

The Device can implement NAT traversal by enabling UPnP. When you enable UPnP, the Device allows any LAN UPnP-enabled device to perform a variety of actions, including retrieving the public IP address, enumerate existing port mappings, and add or remove port mappings. By adding a port mapping, a UPnP-enabled device opens the related service ports on the Device to allow the Internet hosts access. Windows Messenger is an example of an application that supports NAT traversal and UPnP.

The Device provides the **UPnP Port Forwarding List**, which lists all the port forwarding rules established using UPnP. You can view each port forwarding rule's detailed information in the list, which includes internal IP address, internal port, protocol, remote IP address, external port, and description.

8.4.1 Enable UPnP

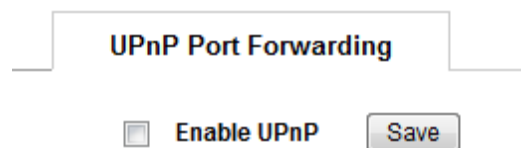


Figure 8-17 Enable UPnP

- ✧ **Enable UPnP:** It allows you to enable or disable UPnP. If you want to enable UPnP, please select this check box.
- **Save:** Click it to save your settings.



Note

The UPnP is enabled on the LAN interface by default.

8.4.2 UPnP Port Forwarding List

ID	Internal IP	Internal Port	Protocol	Remote IP	External Port	Description
<input type="checkbox"/> 1	192.168.1.22	4672	UDP	0.0.0.0	4672	[title 0.49.1] [UDP: 4672]
<input type="checkbox"/> 2	192.168.1.22	4662	TCP	0.0.0.0	4662	[title 0.49.1] [TCP: 4662]

Select All

Figure 8-18 UPnP Port Forwarding List

- ✧ **ID:** It is used to identify each UPnP port forwarding rule in the list.
- ✧ **Internal IP:** It displays the IP address of the LAN host.
- ✧ **Internal Port:** It displays the service port provided by the LAN host.
- ✧ **Protocol:** It displays the transport protocol used by the service.
- ✧ **Remote IP:** It displays the IP address of the remote host.
- ✧ **External Port:** It displays the external port of the UPnP port forwarding, which is opened for outside user to access.
- ✧ **Description:** It displays the description of the UPnP port forwarding rule.
- **Delete:** If you want to delete one or more UPnP port forwarding rules, select the leftmost check boxes of them, and then click the **Delete** button.

Chapter 9 PPPoE Server

9.1 Introduction to PPPoE

The PPPoE stands for Point-to-Point Protocol over Ethernet, which uses client/server model. The PPPoE provides the ability to connect the Ethernet hosts to a remote Access Concentrator (AC) over a simple bridging access device. And it provides extensive access control management and accounting benefits to ISPs and network administrators.

The PPPoE is a network protocol for encapsulating PPP frames in Ethernet frames to provide point-to-point connection over an Ethernet network.

9.1.1 PPPoE Stages

As specified in RFC 2516, the PPPoE has two distinct stages: a discovery stage and a PPP session stage. The following describes them respectively.

9.1.2 PPPoE Discovery Stage

In the PPPoE discovery stage, a PPPoE client will find a proper server, and then build the connection. When a client initiates a PPPoE session, it should perform discovery to identify the PPPoE server's Ethernet MAC address, and establish a PPPoE session ID.

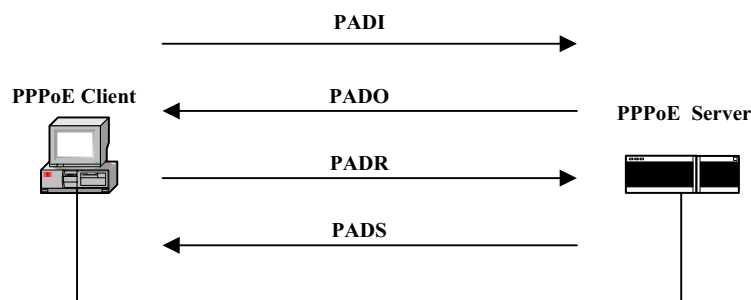


Figure 9-1 PPPoE Discovery Stage Flows

See Figure 9-1, the discovery stage includes the following four steps:

1. **PADI (PPPoE Active Discovery Initiation):** At the beginning, a PPPoE client broadcasts a PADI packet to find all the servers that can be connected possibly. Until it receives PADO packets from one or more servers. The PADI packet must contain a service name which indicates the service requested by the client.
2. **PADO (PPPoE Active Discovery Offer):** When a PPPoE server receives a PADI packet in its service range, it will send a PADO response packet. The PADO packet must contain the server's name, and a service name identical to the one in the PADI, and any number of other service names which indicate other services that the PPPoE server can offer. If a PPPoE server receives a PADI packet beyond its service range, it cannot respond with a PADO packet.
3. **PADR (PPPoE Active Discovery Request):** The client may receive more than one PADO packet as the PADI was broadcast. The client chooses one server according to the server's name or the services offered. Then the host sends a PADR packet to the selected server. The PADR packet must contain a service name which indicates the service requested by the client.
4. **PADS (PPPoE Active Discovery Session- confirmation):** When a PPPoE server receives a PADR packet; it prepares to begin a PPP session. It generates a unique PPPoE session ID, and respond to the client with a PADS packet. The PADS packet must contain a service name which indicates the service provided to the client.

When the discovery stage completes successfully, both the server and client know the PPPoE session ID and the peer's Ethernet MAC address, which together define the PPPoE session uniquely.

9.1.3 PPP Session Stage

In the PPP session stage, the server and client perform standard PPP negotiation to establish a PPP connection. After the PPP connection is established successfully, the original datagram are encapsulated in PPP frames, and PPP frames are encapsulated in PPPoE session frames, which have the Ethernet type 0x8864. Then these Ethernet frames are sent to the peer. In a PPPoE session frame, the session ID must be the value assigned in the Discovery stage, and cannot be changed in this session.

9.1.4 PPPoE Session Termination

After a session is established, either the server or client may send a PADT (PPPoE Active Discovery Terminate) packet at anytime to indicate the session has been terminated. The PADT packet's SESSION-ID must be set to indicate which session is to be terminated. Once received a PADT, no further PPP packets (even normal PPP termination packets) are allowed to be sent using the specified session. A PPP peer should use the PPP protocol itself to terminate a PPPoE session, but can use the PADT packet to terminate the PPPoE session if PPP cannot be used.

9.2 PPPoE Server Settings

The UTT Series Security Firewalls support PPPoE server to allow LAN hosts acting as the PPPoE clients to dial up to the Device.

The UTT Series Security Firewalls provide rich PPPoE server features, which include PPPoE server global settings, PPPoE account settings, static and dynamic address allocation, PPPoE account and MAC address binding, PPPoE account and IP address binding, PPPoE IP/MAC binding, PPPoE status viewing, and so on.

9.2.1 PPPoE Server Global Settings

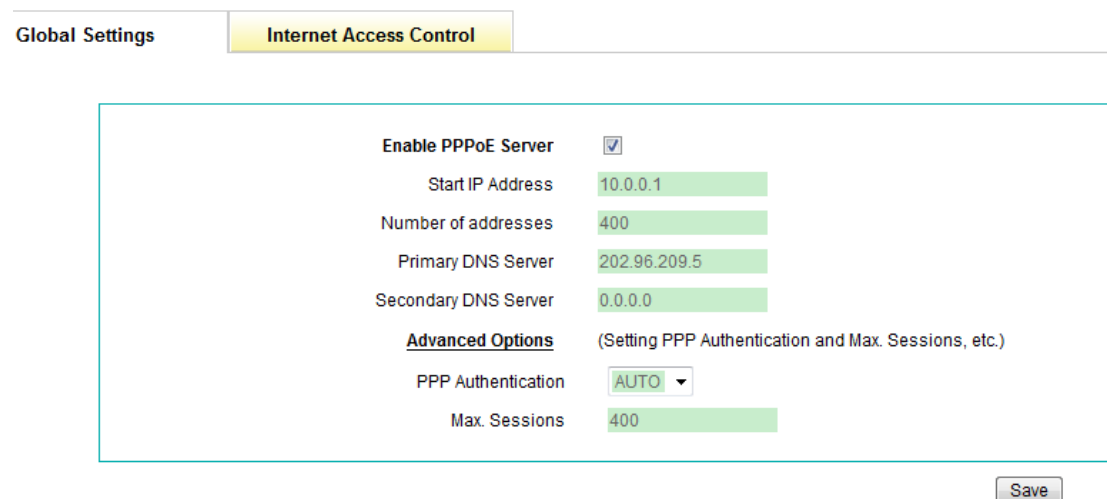
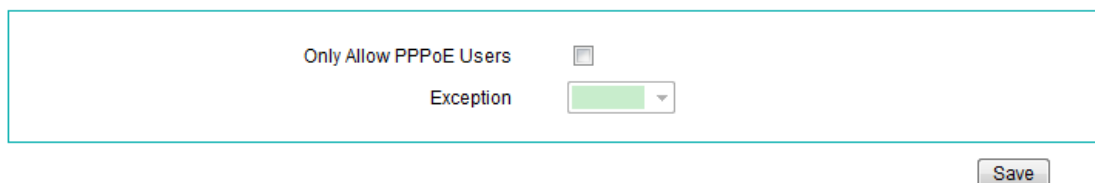


Figure 9-2 PPPoE Server Global Settings

- ✧ **Enable PPPoE Server:** It allows you to enable or disable PPPoE server. If you want to enable PPPoE server on the Device, please select this check box. Only after you have enabled PPPoE server, you can configure the other parameters in this page.
- ✧ **Start IP Address:** It specifies the starting IP address that is assigned by the PPPoE server.
- ✧ **Number of Addresses:** It specifies the maximum number of IP addresses that can be assigned to the PPPoE clients. The addresses can be assigned dynamically or manually by the PPPoE server.
- ✧ **Primary DNS Server:** It specifies the IP address of the primary DNS server that is available to a PPPoE client.
- ✧ **Secondary DNS Server:** It specifies the IP address of the secondary DNS server that is available to a PPPoE client.
- **Advanced Options:** Click it to view and configure advanced parameters. In most cases, you need not configure them.
- ✧ **PPP Authentication:** It specifies the PPP authentication mode by which the PPPoE server authenticates a PPPoE client. The available options are **NONE**, **PAP**, **CHAP** and **Either**. In most cases, please leave the default value of **Either**, which means that the Device will automatically choose **PAP** or **CHAP** to authenticate the PPPoE client.
- ✧ **Max. Sessions:** It specifies the maximum number of PPPoE sessions that can be created on the Device. The maximum value of **Max. Sessions** depends on the specific product model.
- **Save:** Click it to save the PPPoE server global settings.

9.2.2 Internet Access Control



Only Allow PPPoE Users

Exception

Save

Figure 9-3 Internet Access Control Settings

- ✧ **Only Allow PPPoE Users:** It allows you to enable or disable **Only Allow PPPoE Users**, that is, only the PPPoE dial-in users can access the Internet through the Device. If you want to only allow the PPPoE dial-in users to access the Internet

through the Device, please select this option. The one exception is that you select an address group from **Exception** drop-down list.

- ✧ **Exception:** It specifies an address group that is exempt from the restriction of **Only Allow PPPoE Users**. If you select an address group here, the LAN users that belong to this address group are exempt from the restriction of **Only Allow PPPoE Users**, that is, whether it is enabled or not, those users may access the Internet through the Device even they aren't PPPoE dial-in users. The address group is configured in the **Security > Address Group** page.
- **Save:** Click it to save the Internet access control settings.

9.3 PPPoE Account

This section describes the **PPPoE > PPPoE Account** page, which includes the **PPPoE Account Settings**, **PPPoE Account List**, **Import Accounts** and **PPPoE Account Billing**.

9.3.1 PPPoE Account Settings

In the **PPPoE > PPPoE Account > PPPoE Account Settings** page, you can configure PPPoE account related parameters, which include basic parameters, rate limit parameters and security parameters.

Basic	<p>User Name <input type="text"/></p> <p>Password <input type="password"/></p> <p>Description <input type="text"/></p> <p>Advanced Options (Idle Time, Session Timeout, Dialing Schedule, etc.)</p> <p>Idle Timeout <input type="text" value="0"/> seconds</p> <p>Session Timeout <input type="text" value="0"/> seconds</p> <p>Dialing Schedule <input type="text" value=""/> <input type="button" value="v"/></p>
Rate Limit	<p>(Before configure PPPoE Rate Limit, please make sure the Rate Limit function is enabled in QoS - Global Settings.)</p> <p>Tx Bandwidth <input type="text" value="0"/> kbit/s <input type="text" value="NoLimit"/> <input type="button" value="v"/></p> <p>Rx Bandwidth <input type="text" value="0"/> kbit/s <input type="text" value="NoLimit"/> <input type="button" value="v"/></p>
Accounting	<p>Accounting Mode <input type="text" value="None"/> <input type="button" value="v"/></p>
Security	<p>Max. Sessions <input type="text" value="1"/></p> <p>Account/MAC Binding <input type="text" value="None"/> <input type="button" value="v"/></p> <p>Account/IP Binding <input type="text" value="0.0.0.0"/> (The priority of Account/IP Binding is lower than the one of IP/MAC Binding.)</p>

Figure 9-4 PPPoE Account Settings

- ✧ **User Name:** It specifies a unique user name of the PPPoE account. It should be between 1 and 31 characters long. The PPPoE server will use **User Name** and **Password** to identify the PPPoE client.
- ✧ **Password:** It specifies the password of the PPPoE account.
- ✧ **Description:** It specifies the description of the PPPoE account.
- **Advanced Options:** Click it to view and configure advanced parameters. In most cases, you need not configure them.
- ✧ **Idle Timeout:** It specifies how long the PPPoE session keeps connected since no packets are transmitted through the PPPoE session. The Device will automatically terminate the session after it has been inactive for the specified period of time. It should be between 0 and 65535 seconds. The default value is zero, which means that the Device will not terminate it.
- ✧ **Session Timeout:** It specifies how long the PPPoE session keeps connected since established. The Device will automatically terminate the session after it has been connected for the specified period of time. It should be between 0 and 65535 seconds. The default value is zero, which means that the Device will not terminate it.
- ✧ **Dialing Schedule:** It specifies a schedule during which a PPPoE client can use the current PPPoE account to dial up. If you select a schedule here, it will allow the PPPoE client to dial up only in the selected schedule range. Else, the PPPoE client can always dial up. The schedule is configured in the **Security > Schedule** page.
- ✧ **Tx Bandwidth:** It specifies the maximum upload bandwidth of a PPPoE dial-in user that uses the current PPPoE account.
- ✧ **Rx Bandwidth:** It specifies the maximum download bandwidth of a PPPoE dial-in user that uses the current PPPoE account.
- ✧ **Accounting Mode:** UTT Series support Account Billing of PPPoE Server. It offer account billing based on different mode of By Date, By Hour and By Traffic.
 - **None:** If you don't want to bill a PPPoE Account, please select this option. The default value is **None**.
 - **By Date:** Account will expire at the specified date. Refer to section **9.3.4 PPPoE Account Billing** for more information.
 - **By Hours:** Account will expire after accumulative online time reaches the specified hours. Refer to section **9.3.4 PPPoE Account Billing** for more information.
 - **By Traffic:** Account will expire after accumulative upload or download traffic

reaches the specified megabytes. Refer to section **9.3.4 PPPoE Account Billing** for more information.

- ✧ **Max. Sessions:** It specifies the maximum number of PPPoE sessions that can be created by using the current PPPoE account.
- ✧ **Account/MAC Binding:** It specifies the type of PPPoE account and MAC address binding. The available options are **None**, **Auto** and **Manual**.
 - **None:** If you don't want to create account/MAC binding for the current PPPoE account, select this option, then a PPPoE client with any MAC address can use the current PPPoE account to dial up.
 - **Auto:** If you want to create account/MAC binding for the current PPPoE account automatically, select this option. That is, the Device will automatically bind the PPPoE account to the MAC address of the user who uses this account to establish a PPPoE session firstly. After that only this user can use the account.
 - **Manual:** If you want to create account/MAC binding for the current PPPoE account manually, select this option, and configure up to four MAC addresses that are bound to the account. Then only the users with one of these MAC addresses can use the account.
- ✧ **MAC Address:** It specifies the MAC address that is bound to the current PPPoE account. If you select **Manual** from the **Account/MAC Binding** drop-down list, this parameter will be displayed. In this case, you should enter a MAC address that is bound to the account in the text box.
- ✧ **MAC Address 2, MAC Address 3, and MAC address 4:** It specifies another three MAC addresses that are bound to the current PPPoE account. If you select **Manual** from the **Account/MAC Binding** drop-down list, you can configure more than one MAC address (up to four) if needed.
- ✧ **Account/IP Binding:** It specifies a static IP address that is assigned to the user who uses the current PPPoE account. It must be a valid IP address in the range of address pool configured in the **PPPoE > Global Settings** page.
- **Save:** Click it to save the PPPoE account settings.



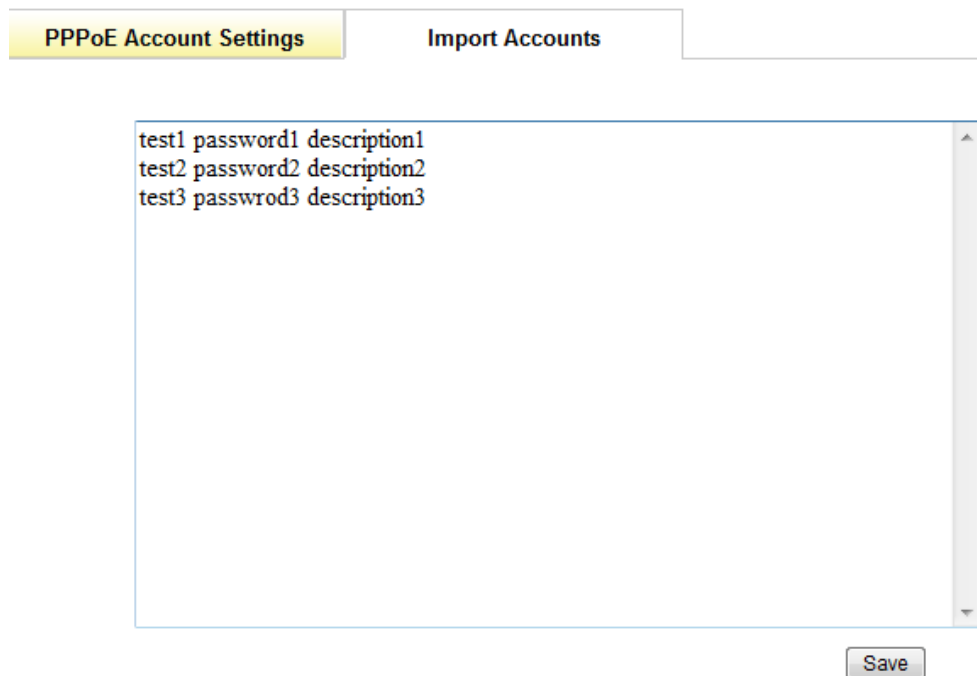
Note

1. If you want to assign a static IP address to the user that uses a PPPoE account to establish a PPPoE session, you should enter the IP address in the **Account/IP Binding** text box, and should set the **Max. Sessions** to 1.

select the leftmost check boxes of them, and then click the **Delete** button.

9.3.3 Import Accounts

The **PPPoE > PPPoE Account > Import Accounts** page provides PPPoE accounts import function to simplify operation. When you want to create a great deal of PPPoE accounts, you can import them at a time in the page. You can edit them in Notepad, and then copy them to the **Import Accounts** list box; also you can directly enter them in the **Import Accounts** list box. The import contents are: User Name, Password, and Description of each PPPoE account, one PPPoE account per line; and the import format of a PPPoE account is: User Name<Space>Password<Space>Description<Enter>.



PPPoE Account Settings Import Accounts

```
test1 password1 description1
test2 password2 description2
test3 passwrod3 description3
```

Save

Figure 9-6 PPPoE Accounts Import

- **Save:** After you have entered the PPPoE accounts in the **Import Accounts** list box, click the **Save** button to save them to the Device, and then you can view them in the **PPPoE Account List**.

 **Note**

To avoid unnecessary data loss due to computer crashes, you can copy the entered PPPoE accounts to a Notepad file in your local PC before saving them to the Device.

9.3.4 PPPoE Account Billing

9.3.4.1 Introduction to PPPoE Account Billing Mechanism

PPPoE Account Billing is a specific function of UTT Series Security Firewalls. It provides a billing mechanism. According to different **Accounting Mode**, the UTT Device will start to run the billing mechanism **by Date, Hour or Traffic**. Together with PPPoE Account Expiration Notice to alert the user to renew the account, PPPoE Account Billing can be a very helpful Billing tool especially for Communication. When the PPPoE account expires, the account will be no longer available unless the user renew the account. Here provide the billing mechanism picture, see Figure 9-7.

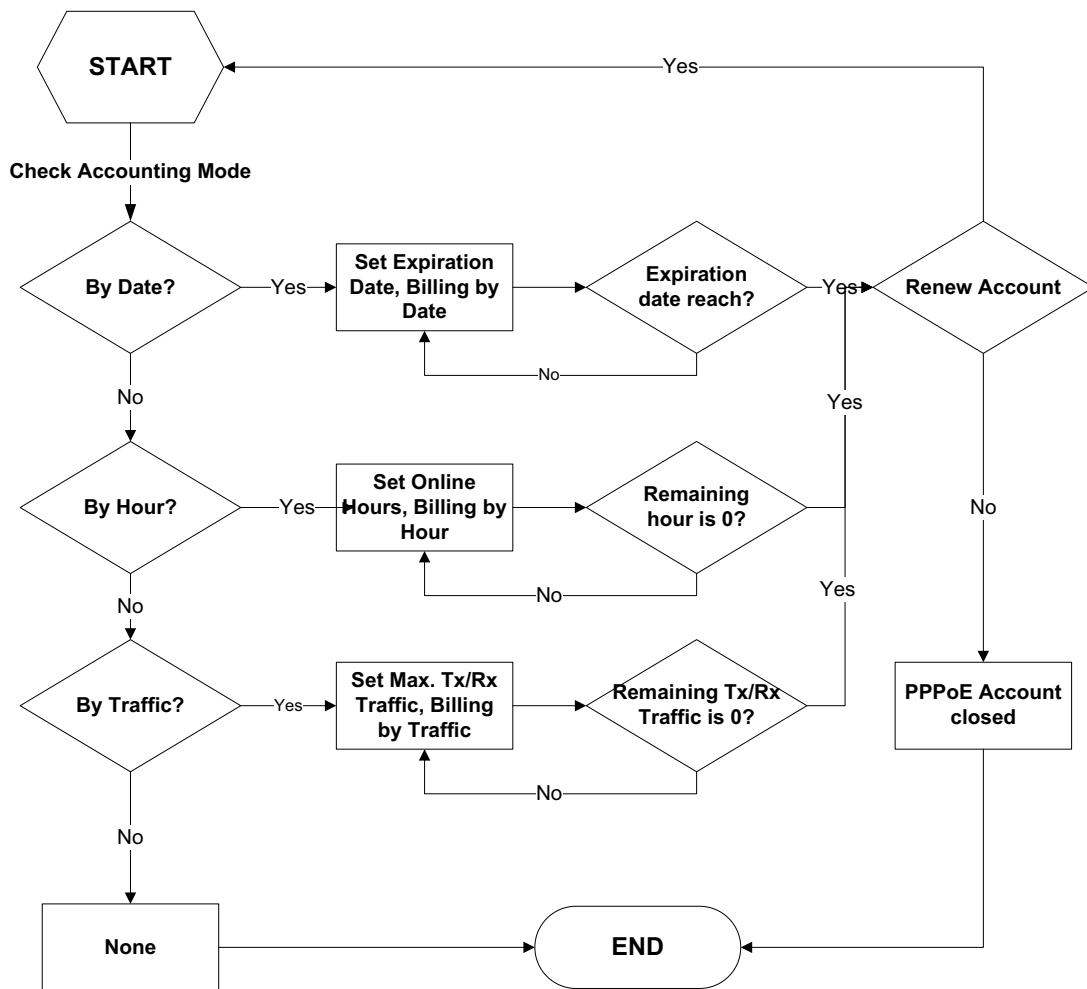
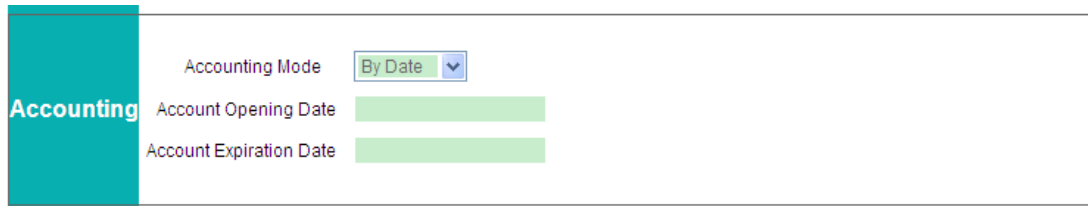


Figure 9-7 PPPoE Account Billing mechanism

9.3.4.2 PPPoE Account Billing By Date

If you want to create a PPPoE Billing Account by date, you can go to **PPPoE > PPPoE Account > PPPoE Account Settings** page and set the **Accounting Mode** as **By Date**, see **Figure**.



The screenshot shows a web interface for configuring PPPoE account settings. On the left, there is a teal sidebar with the word "Accounting" in white. The main content area has a white background. At the top, there is a label "Accounting Mode" followed by a dropdown menu currently set to "By Date". Below this, there are two input fields: "Account Opening Date" and "Account Expiration Date", both of which are currently empty and have a light green border.

Figure 9-8 PPPoE Account Billing By Date

- ✧ **Accounting Mode:** It specify the accounting mode of the PPPoE billing account. Here select By Date.
- ✧ **Account Opening Date:** It specify the opening date of the PPPoE account. If the current date is before the **Account Opening Date**, the account cannot be used because it's been disabled by the UTT device.
- ✧ **Account Expiration Date:** It specify the expiration(end) date of the PPPoE account. If the current date is after the **Account Expiration Date**, the account cannot be used because it's been disabled by the UTT device.

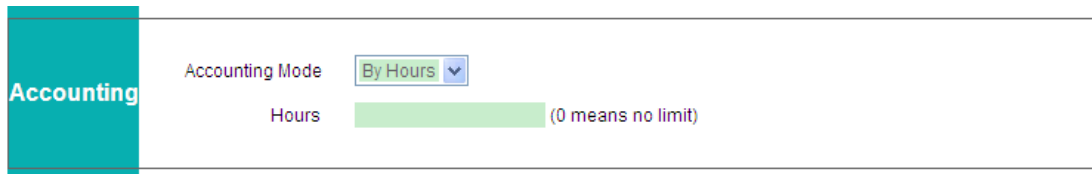


Note

1. To ensure that PPPoE Account Billing operates properly, you should synchronize the system clock in the **System > Time** page.
2. Before the PPPoE Account expires, if you have also set the PPPoE Account Expiration Notice (refer to section **9.7 PPPoE Account Expiration Notice** for more information), the device will push a notice to the user. If the user decide to renew the account(Accounting Mode is By Date), the Administrator should set the **Account Opening Date** and **Account Expiration Date** to new dates.

9.3.4.3 PPPoE Account Billing By Hour

If you want to create a PPPoE Billing Account by hour, you can go to **PPPoE > PPPoE Account > PPPoE Account Settings** page and set the **Accounting Mode** as **By Hour**.



Accounting Mode: (dropdown)

Hours: (0 means no limit)

Figure 9-9 PPPoE Account Billing By Hour

- ✧ **Accounting Mode:** It specify the accounting mode of the PPPoE billing account. Here select By Hour.
- ✧ **Hours:** It specify the max online time(by hour) of the PPPoE account. The device will accumulate the online time of the PPPoE account, once the online time reaches the max online time, the account cannot be used because it's been disabled by the UTT device. 0 means no limit, the account will be always enabled.

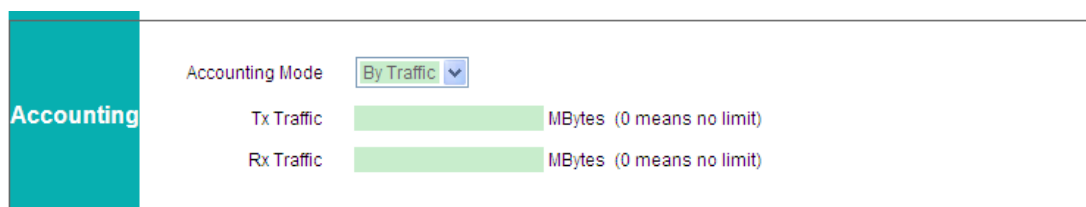


Note

1. To ensure that PPPoE Account Billing operates properly, you should synchronize the system clock in the **System > Time** page.
2. Before the PPPoE Account expires, if you have also set the PPPoE Account Expiration Notice(refer to section **9.7 PPPoE Account Expiration Notice** for more information), the device will push a notice to the user. If the user decide to renew the account(Accounting Mode is By Hour), the Administrator should set the **Hours** to a new value.

9.3.4.4 PPPoE Account Billing By Traffic

If you want to create a PPPoE Billing Account by traffic, you can go to **PPPoE > PPPoE Account > PPPoE Account Settings** page and set the **Accounting Mode** as **By Traffic**.



Accounting Mode: (dropdown)

Tx Traffic: MBytes (0 means no limit)

Rx Traffic: MBytes (0 means no limit)

Figure 9-10 PPPoE Account Billing By Traffic

- ✧ **Accounting Mode:** It specify the accounting mode of the PPPoE billing account. Here select By Traffic.

- ✧ **Tx. Traffic:** It specify the max Tx. Traffic of the PPPoE account. The device will accumulate the upload traffic of the PPPoE account, once the accumulative upload traffic reaches the **Tx. Traffic**, the account cannot be used because it's been disabled by the UTT device. 0 means no limit for upload traffic.
- ✧ **Rx. Traffic:** It specify the max Rx. Traffic of the PPPoE account. The device will accumulate the download traffic of the PPPoE account, once the accumulative download traffic reaches the **Rx. Traffic**, the account cannot be used because it's been disabled by the UTT device. 0 means no limit for download traffic.

**Note**

Before the accumulative upload/download traffic reaches the **Tx./Rx. Traffic**, if you have also set the PPPoE Account Expiration Notice(refer to section **9.7 PPPoE Account Expiration Notice** for more information), the device will push a notice to the user. If the user decide to renew the account(Accounting Mode is By Traffic), the Administrator should set the **Tx. Traffic and Rx. Traffic** to new value.

9.4 PPPoE IP/MAC Binding

In the **PPPoE > PPPoE IP/MAC > IP/MAC Binding Settings** page, you can create a binding by mapping a static IP address to a host's MAC address, and then the PPPoE server will always assign this IP address to the specified host.

9.4.1 PPPoE IP/MAC Binding Settings

Binding List	IP/MAC Binding Settings
IP Address	192.168.16.88
MAC Address	0022aa115566
Description	test
<input type="button" value="Save"/>	

Figure 9-11 PPPoE IP/MAC Binding Settings

- ✧ **IP Address:** It specifies the IP address for the PPPoE IP/MAC binding. The PPPoE

server will always assign this address to the PPPoE dial-in host specified by the **MAC Address**. It must be a valid IP address in the range of address pool configured in the **PPPoE > Global Settings** page.

- ✧ **MAC Address:** It specifies the MAC address of a PPPoE dial-in host.
- ✧ **Description:** It specifies the description of the PPPoE IP/MAC binding.
- **Save:** Click it to save the PPPoE IP/MAC binding settings.

Note

1. If you create an IP/MAC binding for a PPPoE dial-in user, the PPPoE server will always assign the specified IP address to the user.
2. The PPPoE IP/MAC binding has higher priority than the PPPoE account/IP binding, that is, if an IP/MAC binding and account/IP binding have the same IP address, the Device will assign this IP address to the user that matches the IP/MAC binding. The account/IP binding is configured in the **PPPoE > PPPoE Account > PPPoE Account Settings** page.

9.4.2 PPPoE IP/MAC Binding List

When you have configured some PPPoE IP/MAC bindings, you can view them in the PPPoE **IP/MAC Binding List**, and check whether a static IP address is assigned to the specified host or not.



ID	IP Address	MAC Address	Status	Description	Edit
1	192.168.16.0/8	0022aa115566	Unassigned	test	

Figure 9-12 PPPoE IP/MAC Binding List

- **Add a PPPoE IP/MAC Binding:** If you want to add a new PPPoE IP/MAC binding, click the **New** button or select the **IP/MAC Binding Settings** tab to go to the setup page, and then configure it, lastly click the **Save** button.
- **Edit a PPPoE IP/MAC Binding:** If you want to modify a configured PPPoE IP/MAC binding, click its **Edit** hyperlink, the related information will be displayed in the setup page. Then modify it, and click the **Save** button.
- **Delete PPPoE IP/MAC Binding(s):** If you want to delete one or more PPPoE IP/MAC bindings, select the leftmost check boxes of them, and then select **Delete** from the drop-down list on the lower right corner of the **IP/MAC Binding List**, lastly click **OK**.
- **Delete All:** If you want to delete all the PPPoE IP/MAC bindings at a time, select **Delete All** from the drop-down list on the lower right corner of the list, and then click **OK**. Then the PPPoE server will assign IP addresses to the dial-in users dynamically.

9.5 PPPoE Status

In the **PPPoE > PPPoE Status** page, you can view the status and usage information of each online PPPoE dial-in user. If a PPPoE dial-in user has established the PPPoE session to the Device successfully, you can view the assigned IP address, MAC address, Rx Rate and Tx Rate of the user, online time and session ID of the PPPoE session.

User Name	Status	IP Address	MAC Address	Online Time	Rx Rate(KByte/s)	Tx Rate(KByte/s)	Session ID
<input type="checkbox"/> admin	Connected	10.0.0.1	1c:8f:65:ed:8a:12	00:00:02:52	0	0	1

1/50 Lines/Page: 20 First Prev Next Last Search:

Select All

Figure 9-13 PPPoE Status List

- ✧ **User Name:** It displays the PPPoE user name. The PPPoE dial-in user uses it to dial-up and establish the PPPoE session to the Device.
- ✧ **Status:** It displays the PPPoE account status. If a PPPoE dial-in user has established the PPPoE session to the Device successfully with the PPPoE account, it displays Connected; Else, it displays Disconnected.
- ✧ **IP Address:** It displays the PPPoE dial-in user's IP address that is assigned by the PPPoE server.
- ✧ **MAC Address:** It displays the PPPoE dial-in user's MAC address.
- ✧ **Online Time:** It displays the elapsed time since the PPPoE session was established successfully.
- ✧ **Rx Rate:** It displays the real-time download rate (in kilobytes per second) of the PPPoE dial-in user.
- ✧ **Tx Rate:** It displays the real-time upload rate (in kilobytes per second) of the PPPoE dial-in user.
- ✧ **Session ID:** It displays the session ID of the PPPoE Session, which uniquely identifies a PPPoE session.
- **Disconnect:** If you want to hang the established PPPoE session up manually, select the leftmost check box of this PPPoE session, and then click the **Disconnect** button.
- **Refresh:** Click it to view the latest information in the list.

9.6 Configuration Example for PPPoE Server

1. Requirements

In this example, an organization's administrator wants the LAN users to act as the PPPoE clients to dial up to the Device. And it only allows the PPPoE dial-in users to access the Internet through the Device. The exception is the CEO with IP address **192.168.16.2**.

When acting as a PPPoE server, the Device dynamically will assign the IP addresses to the LAN users. The start IP address assigned to the dial-in user is 10.0.0.1, the maximum number of dial-in users is 100, the primary DNS server IP address is 202.101.10.10, and the maximum number of PPPoE sessions that can be created on the Device is 100.

The administrator need to create two PPPoE accounts: one is universal account which is used by the normal employees, and its **Rx** and **Tx bandwidth** are both 512 Kbit/s, its **Max. Sessions** is 90; the other is advanced account, its **Max. Sessions** is 10.

And the administrator wants the LAN user with MAC address 0021859b4544 to use a static IP address: 10.0.0.50, so he needs to create a PPPoE IP/MAC binding for this user.

2. Configuration Procedure

1) Configuring PPPoE Server Global Parameters

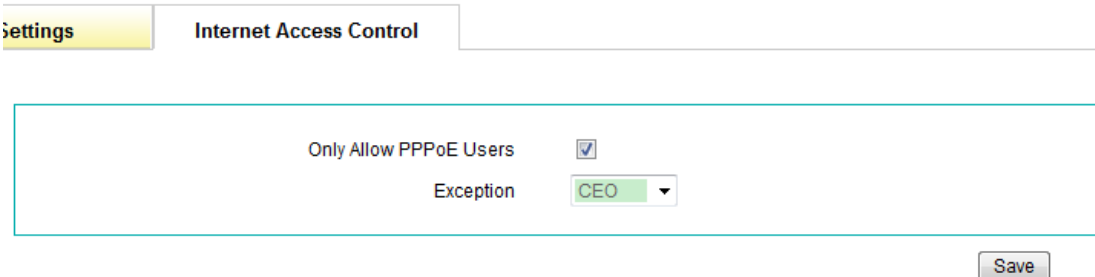
Step 1 Go to the **PPPoE > Global Settings** page.

Step 2 See the following figure, select the **Enable PPPoE Server** check box, enter **10.0.0.1** in the **Start IP Address**, enter **100** in the **Number of Addresses**, enter **202.101.10.10** in the **Primary DNS Server**, and enter **100** in the **Max. Sessions** text box. Leave the default values for the other parameters. Then click the **Save** button to save the settings.

Enable PPPoE Server	<input checked="" type="checkbox"/>
Start IP Address	10.0.0.1
Number of addresses	100
Primary DNS Server	202.101.10.10
Secondary DNS Server	0.0.0.0
Advanced Options (Setting PPP Authentication and Max. Sessions, etc.)	
PPP Authentication	AUTO
Max. Sessions	100

Figure 9-14 PPPoE Server Global Settings - Example

Step 3 Go to the **PPPoE > Global Settings > Internet Access Control** page, select the **Only Allow PPPoE Users** check box, and select **CEO** from the **Exception** drop-down list. The **CEO** address group only includes one IP address: 192.168.16.2, which is configured in the **Security > Address Group** page.



The screenshot shows a web interface with a navigation bar at the top containing 'Settings' and 'Internet Access Control'. Below this, a configuration area is highlighted with a red border. It contains a checkbox labeled 'Only Allow PPPoE Users' which is checked, and a dropdown menu labeled 'Exception' with 'CEO' selected. A 'Save' button is located at the bottom right of the configuration area.

Figure 9-15 Internet Control Settings - Example

2) Configuring PPPoE Accounts

Step 1 Go to the **PPPoE > PPPoE Account > PPPoE Account Settings** page.

Step 2 Creating the universal PPPoE Account whose user name is All. See the following figure, enter **All** in the **User Name**, enter **test** in the **Password**, enter **universal account** in the **Description**, enter **512** in the **Tx Bandwidth** and **Rx Bandwidth**, and enter **90** in the **Max. Sessions** text box. Leave the default values for the other parameters. Then click the **Save** button to save the settings. Note that you should enable rate limit in the **QoS > Global Settings** page to make rate limit for this PPPoE account take effect.

Basic	User Name <input type="text" value="All"/> Password <input type="password" value="••••"/> Description <input type="text" value="universal account"/> <u>Advanced Options</u> (Idle Time,Session Timeout,Dialing Schedule, etc.)
Rate Limit	(Before configure PPPoE Rate Limit, please make sure the Rate Limit function is enabled in QoS - Global Settings .) Tx Bandwidth <input type="text" value="512"/> kbit/s <input type="text" value="512K"/> <input type="button" value="v"/> Rx Bandwidth <input type="text" value="512"/> kbit/s <input type="text" value="512K"/> <input type="button" value="v"/>
Accounting	Accounting Mode <input type="text" value="None"/> <input type="button" value="v"/>
Security	Max. Sessions <input type="text" value="90"/> Account/MAC Binding <input type="text" value="None"/> <input type="button" value="v"/> Account/IP Binding <input type="text" value="0.0.0.0"/> (The priority of Account/IP Binding is lower than the one of IP/MAC Binding.)

Figure 9-16 Configuring the Universal PPPoE Account - Example

Step 3 Creating the advanced PPPoE Account whose user name is Advanced. See the following figure, enter **Advanced** in the **User Name**, enter **test2** in the **Password**, enter **advanced account** in the **Description**, and enter **10** in the **Max. Sessions** text box. Leave the default values for the other parameters. Then click the **Save** button to save the settings.

Basic	User Name <input type="text" value="Advanced"/> Password <input type="password" value="*****"/> Description <input type="text" value="advanced account"/> <u>Advanced Options</u> (Idle Time, Session Timeout, Dialing Schedule, etc.)
Rate Limit	(Before configure PPPoE Rate Limit, please make sure the Rate Limit function is enabled in QoS - Global Settings .) Tx Bandwidth <input type="text" value="0"/> kbit/s <input type="button" value="NoLimit"/> Rx Bandwidth <input type="text" value="0"/> kbit/s <input type="button" value="NoLimit"/>
Accounting	Accounting Mode <input type="button" value="None"/>
Security	Max. Sessions <input type="text" value="10"/> Account/MAC Binding <input type="button" value="None"/> Account/IP Binding <input type="text" value="0.0.0.0"/> (The priority of Account/IP Binding is lower than the one of IP/MAC Binding.)

Figure 9-17 Configuring the Advanced PPPoE Account - Example

3) Configuring a PPPoE IP/MAC Binding

Step 1 Go to the **PPPoE > PPPoE IP/MAC > IP/MAC Binding Settings** page.

Step 2 See the following figure, enter **10.0.0.50** in the **IP Address**, and enter **0021859b4544** in the **MAC Address**, then click the **Save** button to save the settings.

IP Address	<input type="text" value="10.0.0.50"/>
MAC Address	<input type="text" value="0021859b4544"/>
Description	<input type="text"/>

Figure 9-18 Configuring a PPPoE IP/MAC Binding – Example

9.7 PPPoE Account Expiration Notice

The UTT series security firewalls provide PPPoE account expiration notice feature to remind a PPPoE dial-in user periodically that his/her account is going to expire. Then the user can avoid the loss due to the account expiration.

When you have enabled PPPoE account expiration notice and the account is going to expire, the Device will pop up a notice message to remind the user. The notice is sent one time per day, at the time user first access a webpage.

In the **PPPoE > PPPoE Notice > Expiration Notice** page, you can configure PPPoE account expiration notice feature. The Device supports three PPPoE account expiration notice modes:

- **By Date:** Account will expire at the specified date.
- **By Hours:** Account will expire after accumulative online time reaches the specified hours.
- **By Traffic:** Account will expire after accumulative upload or download traffic reaches the specified megabytes.

You should select the proper mode here according to the accounting mode of a PPPoE account, which is configured in the **PPPoE > PPPoE Account > PPPoE Account Settings** page.

9.7.1 PPPoE Account Expiration Notice by Date

PPPoE Account Expiration Notice Mode:

Enable Notice by Date:

Remaining Days: Day(s)

Notice Title:

Signature:

Notice Content

```
Hello,  
Your account is going to expire soon.  
In order to access the Internet properly, please recharge in time.  
If you have any questions, please contact the administrator.
```

Figure 9-19 PPPoE Account Expiration Notice by Date

- ✧ **PPPoE Account Expiration Notice Mode:** It specifies the PPPoE account expiration notice mode. Here select **By Date**.
- ✧ **Enable Notice by Date:** It allows you to enable or disable the PPPoE account expiration notice by date. If you want to enable this feature, please select this check box.
- ✧ **Remaining Days:** It specifies the remaining days before account expires. If the actual remaining days is less than the configured remaining days, the Device will pop up the notice message one time per day; else not.
- ✧ **Notice Title:** It specifies the title of the notice message.
- ✧ **Signature:** It specifies the signature of the notice message.
- ✧ **Notice Content:** It specifies the content of the notice message.
- **Save:** Click it to save your settings.

- **Preview:** Click it to preview the notice message you just configured. The following figure shows an example of a notice message.

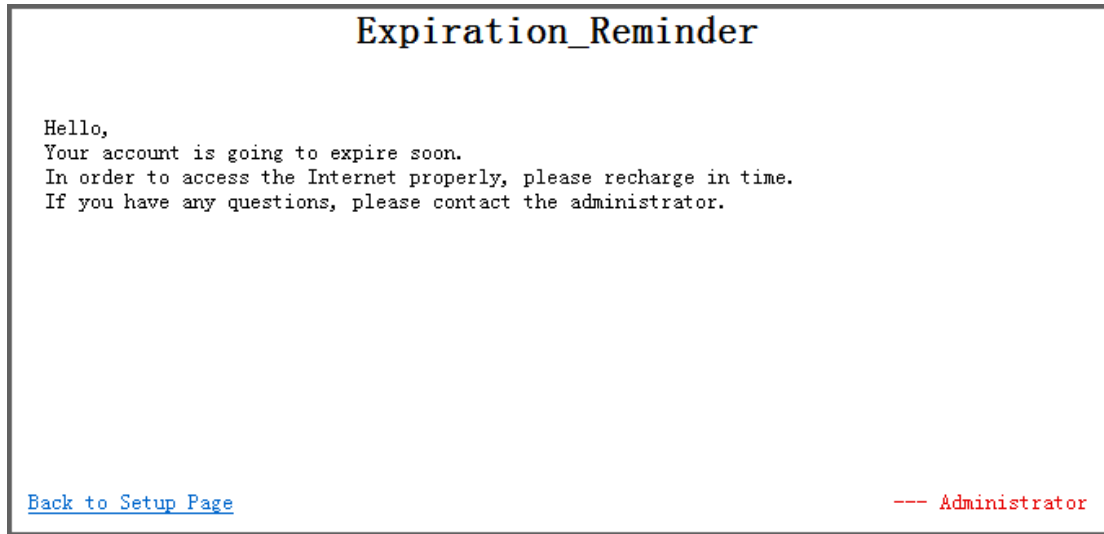


Figure 9-20 PPPoE Account Expiration Notice Preview – Example 1

- **Back to Setup Page:** Click it to go back to the **PPPoE > PPPoE Notice > Expiration Notice** page.

9.7.2 PPPoE Account Expiration Notice by Hours

PPPoE Account Expiration Notice Mode:

Enable Notice by Hours:

Remaining Hours: Hour(s)

Notice Title:

Signature:

Notice Content

```
Hello,  
Your account is going to expire as the remaining online time is less than 10 hours.  
In order to access the Internet properly, please recharge in time.  
If you have any questions, please contact the administrator.
```

Figure 9-21 PPPoE Account Expiration Notice by Hours

- ✧ **PPPoE Account Expiration Notice Mode:** It specifies the PPPoE account expiration notice mode. Here select **By Hours**.
- ✧ **Enable Notice by Hours:** It allows you to enable or disable the PPPoE account expiration notice by hours. If you want to enable this feature, please select this check box.
- ✧ **Remaining Hours:** It specifies the remaining hours before account expires. If the actual remaining hours is less than the configured remaining hours, the Device will pop up the notice message one time per day; else not.
- ✧ **Notice Title:** It specifies the title of the notice message.
- ✧ **Signature:** It specifies the signature of the notice message.
- ✧ **Notice Content:** It specifies the content of the notice message.
- **Save:** Click it to save your settings.

- **Preview:** Click it to preview the notice message you just configured. The following figure shows an example of a notice message.

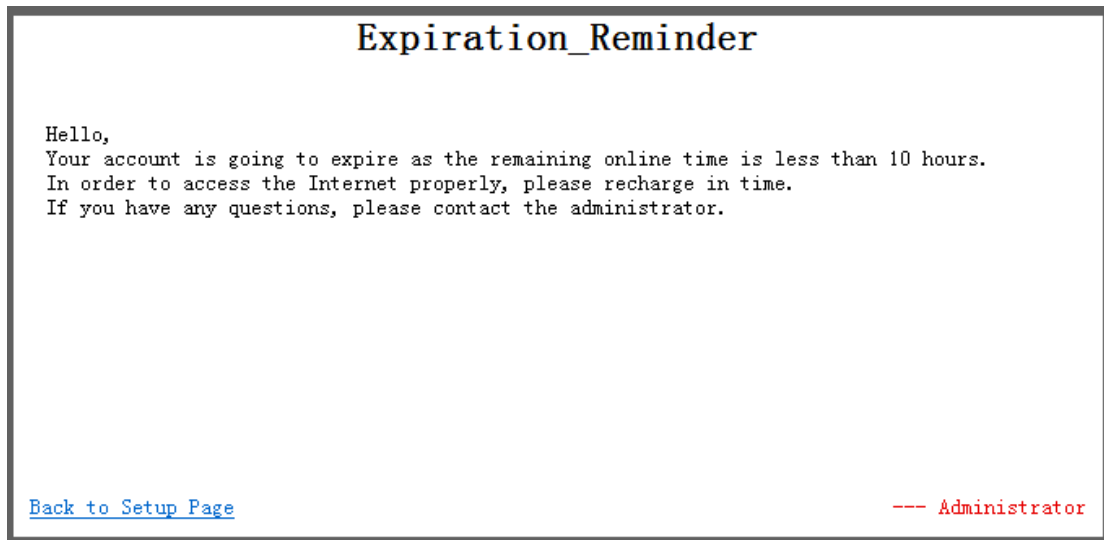


Figure 9-22 PPPoE Account Expiration Notice Preview – Example 2

- **Back to Setup Page:** Click it to go back to the **PPPoE > PPPoE Notice > Expiration Notice** page.

9.7.3 PPPoE Account Expiration Notice by Traffic

PPPoE Account Expiration Notice Mode:

Enable Notice by Traffic:

Remaining Upload Traffic: MBytes

Remaining Download Traffic: MBytes

Notice Title:

Signature:

Notice Content

```
Hello,  
Your account is going to expire as the traffic will be exhausted.  
In order to access the Internet properly, please recharge in time.  
If you have any questions, please contact the administrator.
```

Figure 9-23 PPPoE Account Expiration Notice by Traffic

- ✧ **PPPoE Account Expiration Notice Mode:** It specifies the PPPoE account expiration notice mode. Here select **By Traffic**.
- ✧ **Enable Notice by Traffic:** It allows you to enable or disable the PPPoE account expiration notice by traffic. If you want to enable this feature, please select this check box.
- ✧ **Remaining Upload Traffic:** It specifies the remaining upload traffic (in Megabytes) before account expires. If the actual remaining upload traffic is less than the configured remaining upload traffic, the Device will pop up the notice message one time per day; else not.
- ✧ **Remaining download Traffic:** It specifies the remaining download traffic (in Megabytes) before account expires. If the actual remaining download traffic is less than the configured remaining download traffic, the Device will pop up the notice message one time per day; else not.

- ✧ **Notice Title:** It specifies the title of the notice message.
- ✧ **Signature:** It specifies the signature of the notice message.
- ✧ **Notice Content:** It specifies the content of the notice message.
- **Save:** Click it to save your settings.
- **Preview:** Click it to preview the notice message you just configured. The following figure shows an example of a notice message.

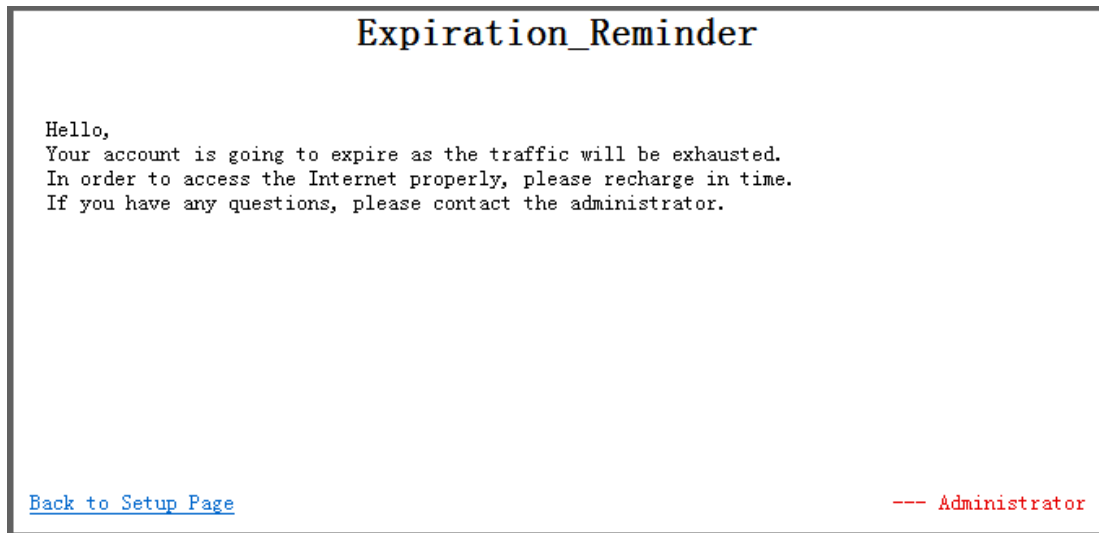


Figure 9-24 PPPoE Account Expiration Notice Preview – Example 3

 **Note**

1. The PPPoE account expiration notice function will take effect only when the accounting function of a PPPoE account is enabled.
2. If you select **By Date** from the **Notice Mode** drop-down list, you should configure correct system time and time zone in the **System > Time** page to ensure the PPPoE account expiration notice by date function work properly.
3. After you selected an option from the **Notice Mode** drop-down list, you should enable the corresponding PPPoE account expiration notice feature to make it take effect. Else, it will be of no effect.
4. The PPPoE account expiration notice by date, PPPoE account expiration notice by hours, and PPPoE account expiration notice by traffic can be enabled at the same time.
5. If a PPPoE account is used by multiple users at the same time, the notice message will only be popped up to the first user that access a webpage, but not to any other LAN user

Chapter 10 QoS

This chapter describes how to control and manage Internet bandwidth of the LAN users, including global settings, rate limit rule settings and P2P rate limit settings.

10.1 Introduction to Bandwidth Management

10.1.1 Why We Need Bandwidth Management

With the growing popularity of P2P, Internet users are able to quickly download high definition movies and video clips, massively multiplayer online games, and hundreds of megabytes of data, also share them with others. But at the same time, as the P2P has the nature of seizing bandwidth, it can maximize the consumption of bandwidth, and thus it has been given a name of “network vampire”. Using P2P applications in the LAN will impact the other users accessing the Internet, even cause network congestion and performance deterioration, which will ultimately lead to that those users can't access the Internet. Therefore, in order to restrain the aggressive consumption of network resources by P2P applications to provide a stable and secure network to the users, we need to effectively limit the maximum bandwidth for the LAN users and applications. However, if we only limit the maximum bandwidth, the bandwidth will be wasted when the network is idle, which will undoubtedly greatly reduce bandwidth utilization. To solve this problem, we introduce a new feature of intelligent bandwidth management on the UTT products to provide users a more reasonable network bandwidth management solution.

The UTT products support intelligent bandwidth management based on token bucket algorithm. It allows you to create rate limit rules based on source IP address, destination IP address, protocol type (TCP, UDP or ICMP), port, schedule, and so on. Through the user-defined capacity and actual network conditions, the Device will get an idea whether the network is idle, normal, busy and exhausted; besides, it can flexibly control the upload and download bandwidth for each LAN host according to the network status and user-defined rate limit rules. In short, using intelligent bandwidth management feature can help you truly implement intelligent and flexible bandwidth management.

10.1.2 Token Bucket Algorithm

As bandwidth management feature provided by the UTT products is based on token bucket algorithm, this section describe token bucket in brief.

Token bucket algorithm is one of the most common algorithms which are used for network traffic shaping and rate limiting. Typically, token bucket algorithm is used to control the amount of data injected into a network, and it allows bursts of data to be sent.

The token bucket is a control mechanism that dictates when traffic can be transmitted, based on the presence of tokens in the bucket. The bucket contains tokens, each of which can represent a byte. If tokens are present, traffic can be transmitted; else, traffic cannot be transmitted. Therefore, if the burst threshold is configured appropriately and there are adequate tokens in the bucket, traffic can be transmitted in its peak burst rate.

The basic process of token bucket algorithm is as follows:

- The token rate is r , that is, a token is added to the bucket every $1/r$ seconds.
- The bucket can hold at the most β tokens. If a token arrives when the bucket is full, it is discarded.
- When a packet of n bytes arrives, n tokens are removed from the bucket, and the packet is sent to the network.
- If fewer than n tokens are available, no tokens are removed from the bucket, and the packet is considered to be non-conformant.
- Although the algorithm allows for the burst of up to β bytes of traffic, over the long run the output of conformant packets is limited by the constant rate, r .

Non-conformant packets can be treated in various ways:

- They may be dropped.
- They may be enqueued for subsequent transmission when sufficient tokens have accumulated in the bucket.
- They may be transmitted, but marked as being non-conformant, possibly to be dropped subsequently if the network is overloaded.

In conclusion, the token bucket algorithm allows bursts of up to β bytes, but over the long run the output of conformant packets is limited to the constant rate, r .

10.1.3 Implementation of Bandwidth Management

Using intelligent bandwidth management based on token bucket algorithm, the Device can flexibly control the upload and download bandwidth of the LAN hosts. There are four process mechanisms depending on the bandwidth utilization:

1. When the bandwidth utilization level is idle, each LAN host is likely to obtain its maximum bandwidth.
2. When the bandwidth utilization level is normal, each LAN host can obtain a bandwidth between its guaranteed and maximum bandwidth, and the bandwidth allocated to the LAN hosts are closest to their maximum bandwidth.
3. When the bandwidth utilization level is busy, each LAN host can only obtain its guaranteed bandwidth.
4. When the bandwidth utilization level is exhausted, only the LAN hosts with high priority can obtain their guaranteed bandwidth, any other LAN host can only obtain a bandwidth lower than the guaranteed bandwidth.

Depending on the ratio of the actual capacity (i.e., total number of network devices connected to the Device) to the user-defined capacity (set by **Capacity** in the **QoS > Global Settings** page), we divide the bandwidth utilization into four levels: Idle, Normal, Busy, and Exhausted.

- Idle: The ratio is below 50%.
- Normal: The ratio is between 50% and 95%.
- Busy: The ratio is between 95% and 100%.
- Exhausted: The ratio is above 100%.

The intelligent bandwidth management feature can help you effectively solve the network congestion problem due to network abuse by the LAN users, and ensure full bandwidth utilization without affecting the other users. In short, this feature can help you truly implement intelligent and flexible bandwidth management.

10.2 Rate Limit Global Settings

Global Settings

Enable Rate Limit

Capacity

Figure 10-1 Rate Limit Global Settings

- ✧ **Enable Rate Limit:** It allows you to enable or disable rate limit. If you select the check box to enable rate limit, the configured rate limit rules will take effect. Else the rate limit rules will be of no effect.
- ✧ **Capacity:** It specifies the maximum number of network devices (PC or other network device) that can be connected to the Device at the same time. Depending on the ratio of the actual capacity (i.e., total number of network devices connected to the Device) to this user-defined capacity, we divide the bandwidth utilization into four levels: Idle, Normal, Busy, and Exhausted. Refer to **10.1.3 Implementation of Bandwidth Management** for more information.
- **Save:** Click it to save the rate limit global settings.

Note

The units of bandwidth and rate generally are Kbit/s (Kilobit per second) and KByte/s or KB/s (Kilobyte per second). The conversion formulas are as follows:

- Byte = 8 bits
- Kilobyte = 1024 bytes or 8192 (8 x 1024) bits
- Megabyte = 1024 Kilobytes or 1.048.576 (1024 x 1024) bytes or 8.388.608 bits
- Gigabyte = 1024 Megabytes or 1.073.741.824 bytes or 8.589.934.592 bits

For example, 10 Mbit/s = 10240 Kbit/s = 10240/8 KByte/s = 1280 KByte/s

10.3 Rate Limit Rule

You can create rate limit rules based on source IP address, destination IP address, protocol type (TCP, UDP or ICMP), port, schedule, and so on.

Note that if you want the rate limit rules to take effect, please make sure that the **Enable Rate Limit** check box is selected in the **QoS > Global Settings** page.

10.3.1 Rate Limit Rule Settings

Before creating the rate limit rules, you may do the following tasks:

- Go to the **Security > Address Group** page to create the address groups that will be referenced by the rules. The addresses within an address group are used to match the source or destination IP addresses of packets that are received by the Device.
- Go to the **Security > Service Group** page to create the service groups that will be referenced by the rules. Note that only the service groups whose **Service Type** is **General Service** can be referenced by the rate limit rules.
- Go to the **Security > Schedule** page to create the schedules that will be referenced by the rules.

If the source IP addresses are consecutive, you also can directly specify the source IP addresses for a rate limit rule in this page. The following describes the definitions of a rule's parameters.

Source Addresses From To

Address Group [Edit Address Group](#)

Destination Address Group [Edit Address Group](#)

Min. Tx Bandwidth Kbit/s

Min. Rx Bandwidth Kbit/s

Max. Tx Bandwidth Kbit/s

Max. Rx Bandwidth Kbit/s

Description _____

Advanced Options (Service Group, Priority, Schedule, etc.)

Each Assign Bandwidth to Each Specified Host or Application

Share All Specified Hosts or Applications Share Bandwidth

Service Group [Edit Service Group](#)

Bandwidth Priority

Bind to

Schedule [Edit Schedule](#)

Figure 10-2 Rate Limit Rule Settings

- ✧ **Source:** It specifies the IP addresses of the LAN hosts to which the rate limit rule applies. There are two available options:
 - **Addresses:** Select it to enter the start and end addresses in the associated text boxes.
 - **Address Group:** Select it to choose an address group from the associated drop-down list. By default, the **Address Group** radio button is selected, and its value is **Any Address**.
- ✧ **Destination Address Group:** It allows you to select an address group to specify the destination IP addresses of the traffic to which the rate limit rule applies.
- ✧ **Min. Tx Bandwidth:** It specifies the guaranteed upload bandwidth allocated to the LAN hosts or applications that match the rate limit rule. Note that you can set the **Min. Tx Bandwidth**, **Min. Rx Bandwidth**, **Max. Tx Bandwidth** and **Max. Rx Bandwidth** through two ways.
 - Enter a value in the associated text box. If you don't want to specify a bandwidth, please enter **0**.
 - Select an option from the associated drop-down list. If you don't want to specify a

bandwidth, please select **NoLimit**.

- ✧ **Min. Rx Bandwidth:** It specifies the guaranteed download bandwidth allocated to the LAN hosts or applications that match the rate limit rule.
- ✧ **Max. Tx Bandwidth:** It specifies the maximum upload bandwidth allocated to the LAN hosts or applications that match the rate limit rule.
- ✧ **Max. Rx Bandwidth:** It specifies the maximum download bandwidth allocated to the LAN hosts or applications that match the rate limit rule.
- ✧ **Description:** It specifies the description of the rate limit rule. It is usually used to describe the purpose of the rule.
- **Advanced Options:** Click it view and configure advanced parameters. In most cases, you need not configure them.
- **Each:** If you select this radio button, the Device will assign the specified bandwidths to each LAN host or application that matches the rule. For example, if the **Min. Tx Bandwidth** is set to 1M and there are 10 LAN hosts match the rule, each host will be ensured with at least 1M upload bandwidth.
- **Share:** If you select this radio button, all the LAN hosts or applications that match the rule will share the specified bandwidths. For example, if the **Min. Tx Bandwidth** is set to 1M and there are 10 LAN hosts match the rule, the total upload bandwidth allocated to all the hosts is at least 1M.
- ✧ **Service Group:** It allows you to select a service group to specify the protocol type (TCP, UDP or ICMP) and ports of the traffic to which the rate limit rule applies. Note that only the service groups whose **Service Type** is **General Service** can be referenced by the rate limit rules. The default value is **Any Service**, which means any protocol type and port.
- ✧ **Bandwidth Priority:** It specifies the bandwidth priority of the traffic to which the rate limit rule applies. There are three options: **Low**, **Mid**, and **High**. The Device will preferentially assign idle bandwidth to the traffic with higher priority; when the network is busy, the Device will firstly ensure the guaranteed bandwidth for the traffic with high priority.
- ✧ **Bind to:** It specifies an Internet connection to which the rate limit rule is bound.
- ✧ **Schedule:** It specifies a schedule to restrict when the rate limit rule is in effect. The default value is **Always**, which means the rate limit rule is in effect always. Note that after the selected schedule has expired, the rule will be in effect always.
- **Edit Schedule:** Click it to go to the **Security > Schedule** page to add, view, modify or delete schedules.
- **Edit Address Group:** Click it to go to the **Security > Address Group** page to add,

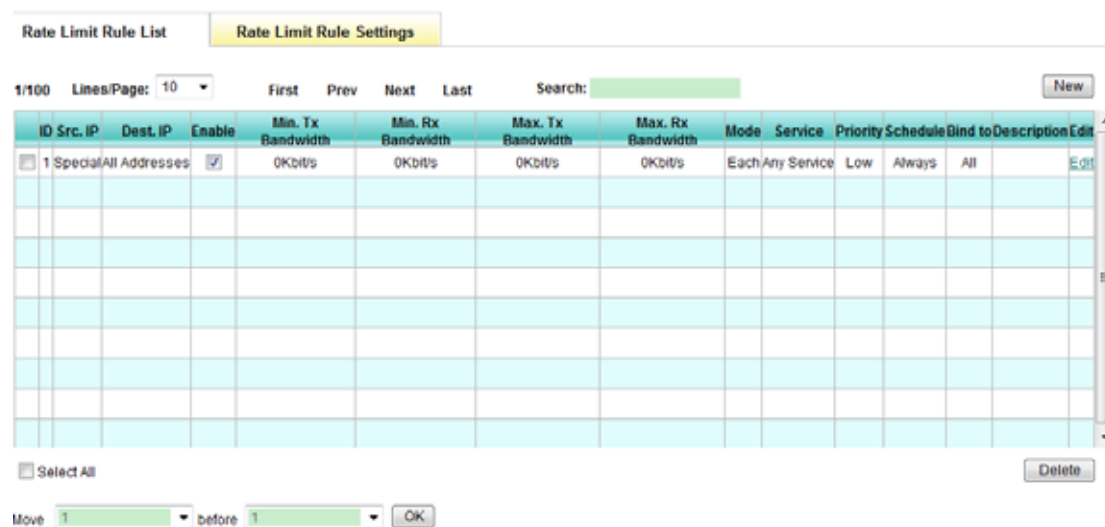
view, modify or delete address groups.

- **Edit Service Group:** Click it to go to the **Security > Service Group** page to add, view, modify or delete service groups.
- **Save:** Click it to save the rate limit rule settings.

Note

If the sum of specified **Min. Tx/Rx Bandwidth** is larger than the Internet connection's **Uplink/Downlink Bandwidth** (configured in the **Basic > WAN** page), the Device cannot guarantee the specified hosts or applications with minimum upload/download bandwidth.

10.3.2 Rate Limit Rule List



ID	Src. IP	Dest. IP	Enable	Min. Tx Bandwidth	Min. Rx Bandwidth	Max. Tx Bandwidth	Max. Rx Bandwidth	Mode	Service	Priority	Schedule	Bind to	Description	Edit
1	Special	All Addresses	<input checked="" type="checkbox"/>	0Kbit/s	0Kbit/s	0Kbit/s	0Kbit/s	Each/Any	Service	Low	Always	All		Edit

Figure 10-3 Rate Limit Rule List

- **Add a Rate Limit Rule:** If you want to add a new rate limit rule, click the **New** button or select the **Rate Limit Rule Settings** tab to go to the setup page, and then configure it, lastly click the **Save** button.
- **Enable a Rate Limit Rule:** The **Enable** check box is used to enable or disable the corresponding rate limit rule. The default value is selected, which means the rate limit rule is in effect. If you want to disable the rate limit rule temporarily instead of deleting it, please click it to remove the check mark.
- **View Rate Limit Rule(s):** When you have configured some rate limit rules, you can

view them in the **Rate Limit Rule List**.

- **Edit a Rate Limit Rule:** If you want to modify a configured rate limit rule, click its **Edit** hyperlink, the related information will be displayed in the setup page. Then modify it, and click the **Save** button.
- **Move a Rate Limit Rule:** The Device allows you to move a rate limit rule to above another rule in the list, the operation is as follows: Select the ID of a rule that you want to move from the **Move** drop-down list, and another rule's ID from the **before** drop-down list, lastly click **OK**. Note that moving a rule in the list doesn't change its ID number.
- **Delete Rate Limit Rule(s):** If you want to delete one or more rate limit rules, select the leftmost check boxes of them, and then click the **Delete** button.

10.3.3 The Execution Order of Rate Limit Rules

When receiving a packet initiated from LAN, the Device will analyze the packet by extracting its source IP address, destination IP address, protocol type (TCP, UDP or ICMP), port number, and the date and time at which the packet was received, and then compare them with each rule in the order in which the rules are listed in **Rate Limit Rule List** to find out if there is a rule matches the packet. The first matched rule will apply to the packet, and no further rules will be checked. If no rule matches, the packet will not be restricted by any rate limit rule.

Note that in the **Rate Limit Rule List**, the rate limit rules are listed in reverse chronological order of creation, the later the rule is created, the upper the rule is listed; and the Device allows you to manually move a rule to a different position in the list.

10.4 P2P Rate Limit

This section describes the **QoS > P2P Rate Limit** page.

P2P rate limit feature is specially designed for P2P application. The P2P rate limit has the highest priority, that is, even if you have created rate limit rules for some LAN users in the **QoS > Rate Limit Rule** page, the P2P traffic of these users is still restricted by P2P rate limit settings. Using P2P rate limit, you can effectively reduce network congestion caused by the usage of P2P applications without the expense of the other LAN users' traffic and bandwidth.

P2P Rate Limit

Enable P2P Rate Limit

Max Tx Rate Kbit/s

Max. Rx Rate Kbit/s

Rate Limit Mode
 Each (Limit Each Host P2P Traffic to Max. Rate)
 Share (Limit All Hosts Total P2P Traffic to Max. Rate)

Exception

Save

Figure 10-4 P2P Rate Limit Settings

- ✧ **Enable P2P Rate Limit:** It allows you to enable or disable P2P rate limit. If you want to enable P2P rate limit, please select this check box. P2P applications include Bit Spirit, Bit Comet, Thunder, Tuotu, and so on.
- ✧ **Max. Tx Rate:** It specifies the maximum upload rate of the P2P traffic.
- ✧ **Max. Rx Rate:** It specifies the maximum download rate of the P2P traffic.
- ✧ **Rate Limit Mode:** It specifies the mode by which the Device will limit the maximum Tx/Rx rate of the LAN hosts.
 - **Each:** If you select this radio button, the Tx/Rx rate of each LAN host's P2P traffic can reach the value specified by the **Max. Tx/Rx Rate** at most.
 - **Share:** If you select this radio button, the total Tx/Rx rate of all the LAN hosts' P2P traffic can reach the value specified by the **Max. Tx/Rx Rate** at most.

- ✧ **Exception:** It specifies an address group that is exempt from the restriction of P2P rate limit settings. If you select an address group here, the P2P traffic of the LAN users in the group will be exempt from the restriction of P2P rate limit settings. The address group is configured in the **Security > Address Group** page.
- **Save:** Click it to save the P2P rate limit settings.

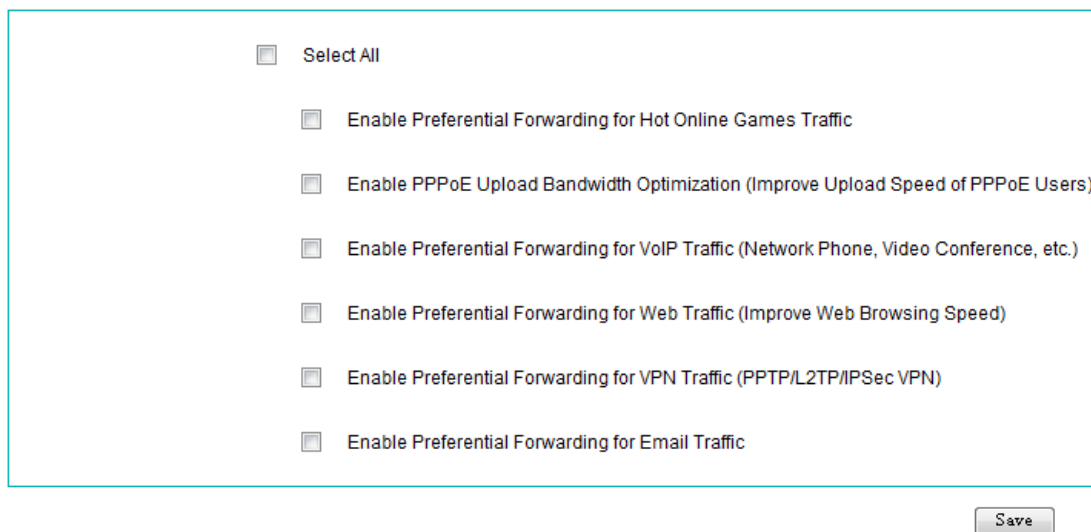
**Note**

1. The P2P rate limit has higher priority than the rate limit rules configured in the **QoS > Rate Limit Rule** page.
2. Only after you have enabled rate limit in the **QoS > Global Settings** page, the P2P rate limit settings can take effect.

10.5 Application QoS

This section describes the **QoS > APP QoS** page.

The Device provides preferential forwarding for some predefined special applications traffic, that is, these applications traffic will be exempt from the restrictions of the rate limit rules configured in the **QoS > Rate Limit Rule** page. The predefined applications include hot online games, VoIP, Web browsing, VPN and Email. In this page, it allows you enable preferential forwarding for one or more predefined applications as required. Moreover, it allows you to enable PPPoE upload bandwidth optimization feature.



The screenshot shows a configuration page with a list of checkboxes. At the top, there is a checkbox labeled "Select All". Below it are seven checkboxes, each with a corresponding label:

- Select All
- Enable Preferential Forwarding for Hot Online Games Traffic
- Enable PPPoE Upload Bandwidth Optimization (Improve Upload Speed of PPPoE Users)
- Enable Preferential Forwarding for VoIP Traffic (Network Phone, Video Conference, etc.)
- Enable Preferential Forwarding for Web Traffic (Improve Web Browsing Speed)
- Enable Preferential Forwarding for VPN Traffic (PPTP/L2TP/IPSec VPN)
- Enable Preferential Forwarding for Email Traffic

At the bottom right of the form area, there is a "Save" button.

Figure 10-5 Preferential Forwarding for Some Applications Traffic

- ✧ **Select All:** It selects or unselects all the check boxes below. If you want to enable all the features provided in this page at a time, please select this check box. If you want to disable all the features provided in this page at a time, please clear the check box.
- ✧ **Enable Preferential Forwarding for Hot Online Games Traffic:** It allows you to enable or disable preferential forwarding for hot online games traffic. If you select the check box to enable this feature, the LAN users' hot online games traffic will be exempt from the restriction of the rate limit rules. The online games mainly include: WOW, Aion, MHXY, BNB, Jade Dynasty, QQGame, CGA, Zhengtu, Perfect World, Audition, Kartrider Rush, and so on.
- ✧ **Enable PPPoE Upload Bandwidth Optimization:** It allows you to enable or disable PPPoE upload bandwidth optimization. If you want to improve the upload speed of the LAN PPPoE dial-in users, please select the check box to enable this feature.
- ✧ **Enable Preferential Forwarding for VoIP Traffic:** It allows you to enable or disable

preferential forwarding for VoIP traffic. If you select the check box to enable this feature, the LAN users' VoIP traffic will be exempt from the restriction of the rate limit rules. The VoIP applications mainly include: Network Phone, Video Conference, etc.

- ✧ **Enable Preferential Forwarding for Web Traffic:** It allows you to enable or disable preferential forwarding for Web traffic. If you select the check box to enable this feature, the LAN users' Web traffic will be exempt from the restriction of the rate limit rules, thus the web browsing speed of the LAN users will be improved.
- ✧ **Enable Preferential Forwarding for VPN Traffic:** It allows you to enable or disable preferential forwarding for VPN traffic. If you select the check box to enable this feature, the LAN users' VPN traffic (including PPTP, L2TP and IPSec VPN traffic) will be exempt from the restriction of the rate limit rules.
- ✧ **Enable Preferential Forwarding for Email Traffic:** It allows you to enable or disable preferential forwarding for Email traffic. If you select the check box to enable this feature, the LAN users' Email traffic will be exempt from the restriction of the rate limit rules.
- **Save:** Click it to save your settings.



Note

Only after you have enabled rate limit in the **QoS > Global Settings** page, the Device can preferentially forward the selected applications traffic.

10.6 Configuration Examples for QoS

10.6.1 Example One

1. Requirements

In this example, a business has a single Internet connection with uplink bandwidth 10 Mbit/s and downlink bandwidth 20 Mbit/s. And the number of network devices is approximately 100.

The requirements are as follows: All the LAN users want to access the Internet smoothly, and the bandwidth will not be wasted when the network is idle. Besides, the administrator wants to limit the rate of the P2P applications for each LAN host: **Max. Tx Rate** is 64 Kbit/s, **Max. Rx Rate** is 128 Kbit/s.

2. Analysis

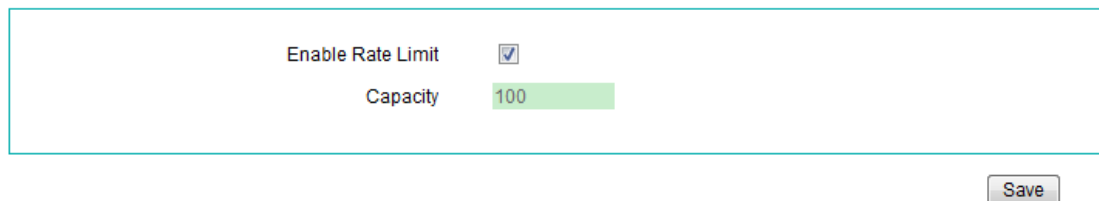
We need to do the following settings:

- Set the Internet connection's **Uplink Bandwidth** and **Downlink Bandwidth** to **10240** Kbit/s and **20480** Kbit/s respectively.
- Enable rate limit and set the **Capacity** to **100** in the **QoS > Global Settings** page.
- Create one rate limit rule to set guaranteed bandwidth for each LAN host: **Min. Tx Bandwidth** is **100** Kbit/s, and **Min. Rx Bandwidth** is **200** Kbit/s.
- Enable P2P rate limit feature, and limit the P2P traffic rate for each LAN host: **Max. Tx Rate** is 64 Kbit/s, **Max. Rx Rate** is 128 Kbit/s.

3. Configuration Procedure

Step 1 Go to the **Basic > WAN > WAN1** page, enter **10240** in the **Uplink Bandwidth** text box, and enter **20480** in the **Downlink Bandwidth** text box.

Step 2 Go to the **QoS > Global Settings** page (see Figure 10-6), select the **Enable Rate Limit** check box, and then enter **100** in the **Capacity** text box, lastly click the **Save** button.



The screenshot shows a configuration interface with two main settings: 'Enable Rate Limit' which is checked with a small square icon, and 'Capacity' which is set to the value '100' in a text input field. Below these settings is a 'Save' button.

Figure 10-6 Rate Limit Global Settings - Example One

Step 3 Go to **QoS > Rate Limit Rule > Rate Limit Rule Settings** page (see Figure 10-7), enter **100** in the **Min. Tx Bandwidth** text box, and enter **200** in the **Min. Rx Bandwidth** text box. Leave the default values for the other parameters. Lastly click the **Save** button.

Source Addresses From To

Address Group [Edit Address Group](#)

Destination Address Group [Edit Address Group](#)

Min. Tx Bandwidth Kbit/s

Min. Rx Bandwidth Kbit/s

Max. Tx Bandwidth Kbit/s

Max. Rx Bandwidth Kbit/s

Description

Advanced Options (Service Group, Priority, Schedule, etc.)

Each Assign Bandwidth to Each Specified Host or Application

Share All Specified Hosts or Applications Share Bandwidth

Service Group [Edit Service Group](#)

Bandwidth Priority

Bind to

Schedule [Edit Schedule](#)

Figure 10-7 Rate Limit Rule Settings - Example One

Step 4 Go to the **QoS > P2P Rate Limit** page (see Figure 10-8), select the **Enable P2P Rate Limit** check box, and select **64K** from the **Max. Tx Rate** drop-down list, and select **128K** from the **Max. Rx Rate** drop-down list. Leave the default values for the other parameters. Lastly click the **Save** button.

Enable P2P Rate Limit

Max Tx Rate Kbit/s

Max. Rx Rate Kbit/s

Rate Limit Mode Each (Limit Each Host P2P Traffic to Max. Rate)

Share (Limit All Hosts Total P2P Traffic to Max. Rate)

Exception

Figure 10-8 P2P Rate Limit Settings - Example One

10.6.2 Example Two

1. Requirements

In this example, an Internet café has a single Internet connection with uplink bandwidth 50 Mbit/s and downlink bandwidth 100 Mbit/s. And the number of network devices is approximately 100. The Internet café consists of three areas: Video Area, Online Game Area, and Common Area. There are 30 hosts in Video Area, 30 hosts in Online Game Area, and 40 hosts in Common Area. The IP address ranges of the areas are as follows:

- Video Area: 192.168.16.2~192.168.16.40
- Online Game Area: 192.168.16.41~192.168.16.80
- Common Area: the remaining IP addresses

The requirements are as follows: The hosts in Video Area have high bandwidth demand, the hosts in Online Game Area have mid bandwidth demand, and the hosts in Common Area have low bandwidth demand (that is, the bandwidth just need to meet the requirements of web browsing and any other general operation); furthermore, the LAN users' Web traffic has the highest priority.

2. Analysis

We need to do the following settings:

- Set the Internet connection's **Uplink Bandwidth** and **Downlink Bandwidth** to **51200** Kbit/s and **102400** Kbit/s respectively.
- Enable rate limit and set **Capacity** to **100** in the **QoS > Global Settings** page.
- Create rate limit rule 1 for all the LAN users: **Min. Tx Bandwidth** is **256** Kbit/s, **Min. Rx Bandwidth** is **512** Kbit/s, and **Bandwidth Priority** is **Low**. Note that as this rule has lowest priority, it should be created at first.
- Create rate limit rule 2 for the hosts in the Online Game Area: **Min. Tx Bandwidth** is **1** Mbit/s, **Min. Rx Bandwidth** is **2** Mbit/s, and **Bandwidth Priority** is **Mid**.
- Create rate limit rule 3 for the hosts in the Video Area: **Min. Tx Bandwidth** is **2** Mbit/s, **Min. Rx Bandwidth** is **4** Mbit/s, and **Bandwidth Priority** is **High**.
- Enable preferential forwarding for Web traffic feature in the **QoS > APP** QoS page.

3. Configuration Procedure

- Step 1** Go to **Security > Address Group** page to create two address groups: One is for the Video Area, and it contains the IP addresses from 192.168.16.2 to 192.168.16.40; the other is for the Online Game Area, and it contains the IP addresses from 192.168.16.41 to 192.168.16.80; and here we assume their names are **video** and **game** respectively.
- Step 2** Go to the **Basic > WAN > WAN1** page, enter **51200** in the **Uplink Bandwidth** text box, and enter **102400** in the **Downlink Bandwidth** text box.
- Step 3** Go to the **QoS > Global Settings** page, select the **Enable Rate Limit** check box, and then enter **100** in the **Capacity** text box, lastly click the **Save** button to save the settings.
- Step 4** Creating rate limit rule 1: Go to the **QoS > Rate Limit Rule > Rate Limit Rule Settings** page (see Figure 10-9), enter **256** in the **Min. Tx Bandwidth** text box, and enter **512** in the **Min. Rx Bandwidth** text box. Leave the default values for the other parameters. Lastly click the **Save** button.

Source Addresses From To

Address Group [Edit Address Group](#)

Destination Address Group [Edit Address Group](#)

Min. Tx Bandwidth Kbit/s

Min. Rx Bandwidth Kbit/s

Max. Tx Bandwidth Kbit/s

Max. Rx Bandwidth Kbit/s

Description

Advanced Options (Service Group, Priority, Schedule, etc.)

Each Assign Bandwidth to Each Specified Host or Application

Share All Specified Hosts or Applications Share Bandwidth

Service Group [Edit Service Group](#)

Bandwidth Priority

Bind to

Schedule [Edit Schedule](#)

Figure 10-9 Rate Limit Rule 1 Settings - Example Two

- Step 5** Creating rate limit rule 2: Go to the **QoS > Rate Limit Rule > Rate Limit Rule Settings** page (see Figure 10-10), select **game** from the **Source Address Group**, select **1M** from the **Min. Tx Bandwidth** drop-down list, select **2M** from

the **Min. Rx Bandwidth** drop-down list, and select **Mid** from the **Bandwidth Priority** drop-down list. Leave the default values for the other parameters. Lastly click the **Save** button.

Source Addresses From To

Address Group [Edit Address Group](#)

Destination Address Group [Edit Address Group](#)

Min. Tx Bandwidth Kbit/s

Min. Rx Bandwidth Kbit/s

Max. Tx Bandwidth Kbit/s

Max. Rx Bandwidth Kbit/s

Description _____

Advanced Options (Service Group, Priority, Schedule, etc.)

Each Assign Bandwidth to Each Specified Host or Application

Share All Specified Hosts or Applications Share Bandwidth

Service Group [Edit Service Group](#)

Bandwidth Priority

Bind to

Schedule [Edit Schedule](#)

Figure 10-10 Rate Limit Rule 2 Settings - Example Two

Step 6 Creating rate limit rule 3: Go to the **QoS > Rate Limit Rule > Rate Limit Rule Settings** page (see Figure 10-11), select **video** from the **Source Address Group**, select **2M** from the **Min. Tx Bandwidth** drop-down list, select **4M** from the **Min. Rx Bandwidth** drop-down list, select **High** from the **Bandwidth Priority** drop-down list. Leave the default values for the other parameters. Lastly click the **Save** button.

Source Addresses From To

Address Group [Edit Address Group](#)

Destination Address Group [Edit Address Group](#)

Min. Tx Bandwidth Kbit/s

Min. Rx Bandwidth Kbit/s

Max. Tx Bandwidth Kbit/s

Max. Rx Bandwidth Kbit/s

Description

Advanced Options (Service Group, Priority, Schedule, etc.)

Each Assign Bandwidth to Each Specified Host or Application

Share All Specified Hosts or Applications Share Bandwidth

Service Group [Edit Service Group](#)

Bandwidth Priority

Bind to

Schedule [Edit Schedule](#)

Figure 10-11 Rate Limit Rule 3 Settings - Example Two

Step 7 Go to the **QoS > APP QoS** page (see Figure 10-12), select the **Enable Preferential Forwarding for Web Traffic** check box, and then click the **Save** button.

Select All

Enable Preferential Forwarding for Hot Online Games Traffic

Enable PPPoE Upload Bandwidth Optimization (Improve Upload Speed of PPPoE Users)

Enable Preferential Forwarding for VoIP Traffic (Network Phone, Video Conference, etc.)

Enable Preferential Forwarding for Web Traffic (Improve Web Browsing Speed)

Enable Preferential Forwarding for VPN Traffic (PPTP/L2TP/IPSec VPN)

Enable Preferential Forwarding for Email Traffic

Figure 10-12 Enable Preferential Forwarding for Web Traffic- Example Two

Chapter 11 Restriction

This chapter describes how to configure personal settings for each LAN user, Internet behavior management, policy database, QQ whitelist, notice and Web Authentication feature; and how to view the related status information.

11.1 User Admin

This section describes how to view the current status information of LAN users (hosts); and how to configure personal settings for each user individually, including rate limit settings and Internet behavior management settings.

11.1.1 User Status List

Through the **User Status List** in the **Restriction > User Admin** page, you can view the status information of each LAN user (host).

ID	Description	IP Address	MAC Address	Enable Personal Settings	Binding Status	Rx Rate(Kbit/s)	Tx Rate(Kbits)	NAT Sessions	User Type	Online Status
1	test	192.168.16.89	00:22:aa:11:55:66	<input type="checkbox"/>	Yes	0	0	1	PPPOE	Offline
2		192.168.16.191	00:26:c7:50:5a:92	<input type="checkbox"/>	No	0	0	0	Static IP	Online

Figure 11-1 User Status List

- ✧ **ID:** It is used to identify each entry in the list.
- ✧ **Description:** If the LAN user is an IP/MAC binding user, it displays the description of the user; else it is blank.
- ✧ **IP Address:** It displays the IP address of the LAN user. If you click **IP Address** hyperlink, it will jump to the **Restriction > User Admin > Rate Limit** page, and then you can individually limit the maximum upload and download rates of the user;

moreover, you can go to the **Restriction > User Admin > Internet Behavior** page to configure the personal Internet behavior management parameters for the user. If you move your mouse over the **IP Address** hyperlink, it will display the current effective settings of the user.

- ✧ **MAC Address:** It displays the MAC address of the LAN user.
- ✧ **Binding Status:** It indicates whether the LAN user is binding or not. If the user is an IP/MAC binding user, DHCP binding user, or PPPoE IP/MAC binding user, it displays **Yes**; else, it displays **No**.
- ✧ **Rx Rate:** It displays the real-time download rate (in kilobits per second) of the LAN user.
- ✧ **Tx Rate:** It displays the real-time upload rate (in kilobits per second) of the PPPoE LAN user.
- ✧ **NAT Sessions:** It displays the number of NAT sessions that are being used by the LAN host now.
- ✧ **User Type:** It displays the access type of the LAN user. The possible values are **PPPoE**, **DHCP** and **Static IP**. If the user is a PPPoE dial-in user, it displays **PPPoE**; if the user is a DHCP client user, it displays **DHCP**; else, it displays **Static IP**.
- ✧ **Online Status:** It displays online status of the LAN user. If the user is connected to the Device, it displays **Online**; if the user is an IP/MAC binding user, DHCP binding user, or PPPoE IP/MAC binding user, and isn't connected to the Device, it displays **Offline**. Note that the list doesn't display the status information of those non-binding users who aren't connected to the Device.
- **Enable Personal Settings:** The **Enable Personal Settings** check box is used to enable or disable the personal settings of the LAN user. If you want to configure and enable the personal settings of a LAN user, please select this check box. Note that as mentioned earlier, it allows you to click **IP Address** hyperlink to configure, view and modify personal settings. If you want to disable the LAN user's personal settings temporarily instead of deleting them, please click it to remove the check mark.
- **Display IP/MAC Binding:** Click it to go to the **Security > IP/MAC Binding** page to view the **IP/MAC Binding List**.
- **Delete Selected Personal Settings:** If you want to delete personal settings of one or more LAN users, select the leftmost check boxes of them, and then select **Delete Selected Personal Settings** from the drop-down list on the lower right corner of the list, lastly click **OK**.
- **Delete All Personal Settings:** If you want to delete all the personal settings at a time, select **Delete All Personal Settings** from the drop-down list on the lower right corner of the list, and then click **OK**.

✔ Note

You can configure IP/MAC binding users in the **Security > IP/MAC Binding > IP/MAC Binding Settings** page, configure PPPoE IP/MAC binding users in the **PPPoE > PPPoE IP/MAC > IP/MAC Binding Settings** page, and configure DHCP manual binding users in the **DHCP > DHCP Server > Manual Binding Settings** page.

11.1.2 Personal Rate Limit

If you want to individually limit the maximum upload and download rates of a LAN user, go to the **Restriction > User Admin > User Status List** page firstly, and then select the user's **Enable Personal Settings** check box or click its **IP Address** hyperlink to go to the **Restriction > User Admin > Rate Limit** page to specify the **Max. Tx Rate** and **Max. Rx Rate** for the selected user.

The screenshot shows a web interface for configuring user settings. At the top, there are three tabs: 'Status List', 'Rate Limit', and 'Internet Behavior'. The 'Rate Limit' tab is selected. Below the tabs, the current IP address is displayed as '192.168.16.88'. The main content area contains two rows of settings: 'Max Tx Rate' with a value of '1024' and 'Kbit/s', and 'Max Rx Rate' with a value of '2048' and 'Kbit/s'. A 'Save' button is located at the bottom right of the settings area.

Figure 11-2 Personal Rate Limit Settings

- ✧ **Max. Tx Rate:** It specifies the maximum upload rate of the selected LAN user.
- ✧ **Max. Rx Rate:** It specifies the maximum download rate of the selected LAN user.
- **Save:** Click it to save your settings.

11.1.3 Personal Internet Behavior Management

Moreover, it allows you to go to the **Restriction > User Admin > Internet Behavior** page to configure, modify and view the personal Internet behavior management settings for the

selected user, see Figure 11-3. For detailed description of the related parameters, refer to **section 11.2.1 Internet Behavior Management Settings**.

User List	Rate Limit	Internet Behavior
Current IP Address:192.168.16.88		
IM	<input type="checkbox"/> Block QQ <input type="checkbox"/> Block MSN <input type="checkbox"/> Block Ali Wangwang <input type="checkbox"/> Block Web QQ <input type="checkbox"/> Block Fention	
P2P	<input type="checkbox"/> Block BT (BitSpirit,BitComet) <input type="checkbox"/> Block Thunder Search <input type="checkbox"/> Block QQLive <input type="checkbox"/> Block PPS <input type="checkbox"/> Block Sogou Search <input type="checkbox"/> Block PPLive <input type="checkbox"/> Block QVOD	
Game	<input type="checkbox"/> Block QQGame <input type="checkbox"/> Block BNB <input type="checkbox"/> Block Zhengtu <input type="checkbox"/> Block Jade Dynasty <input type="checkbox"/> Block MHXY <input type="checkbox"/> Block Audition <input type="checkbox"/> Block CGA <input type="checkbox"/> Block WOW <input type="checkbox"/> Block Aion <input type="checkbox"/> Block Kartrider Rush	
Web Element	<input type="checkbox"/> Block Files View <input type="checkbox"/> Block Submit	
DNS	<input type="checkbox"/> Block Game Websites View <input type="checkbox"/> Block Stock Websites View	
Others	<input type="checkbox"/> Block HTTP Proxy <input type="checkbox"/> Block SOCKS4 Proxy <input type="checkbox"/> Block SOCKS5 Proxy	

Figure 11-3 Personal Internet Behavior Management Settings

11.2 Internet Behavior Management

This section describes the **Restriction > Behavior Mgmt** page.

In this page, you can easily control and manage the Internet behaviors of the LAN users, which include: allow or block the LAN users from using popular IM (e.g., QQ, MSN) and P2P applications (e.g., Bit Comet, Bit Spirit, Thunder Search), downloading the files with the extension .exe, .dll, .vbs, .com, .bat or .sys over HTTP, playing online games, accessing stock and game websites, submitting input in the webpage, using HTTP proxy, and so on.

Moreover, it allows you to configure Internet behaviors management policies based on address group and schedule.

11.2.1 Internet Behavior Management Policy Settings

B a s i c	Address Group Any Address Schedule Always	
	Select All <input type="checkbox"/>	Description <input type="text"/>
I M	<input type="checkbox"/> Block QQ <input type="checkbox"/> Block MSN <input type="checkbox"/> Block Ali Wangwang <input type="checkbox"/> Block Web QQ <input type="checkbox"/> Block Fention	
P 2 P	<input type="checkbox"/> Block BT (BitSpirit, BitComet) <input type="checkbox"/> Block Thunder Search <input type="checkbox"/> Block QQLive <input type="checkbox"/> Block PPS <input type="checkbox"/> Block Sogou Search <input type="checkbox"/> Block PPLive <input type="checkbox"/> Block QVOD	
G a m e	<input type="checkbox"/> Block QQGame <input type="checkbox"/> Block BNB <input type="checkbox"/> Block Zhengtu <input type="checkbox"/> Block Jade Dynasty <input type="checkbox"/> Block MHXY <input type="checkbox"/> Block Audition <input type="checkbox"/> Block CGA <input type="checkbox"/> Block WOW <input type="checkbox"/> Block Aion <input type="checkbox"/> Block Kartrider Rush	
W e b	<input type="checkbox"/> Block Files View <input type="checkbox"/> Block Submit	
D N S	<input type="checkbox"/> Block Game Websites View <input type="checkbox"/> Block Stock Websites View	
O t h e r s	<input type="checkbox"/> Block HTTP Proxy <input type="checkbox"/> Block SOCKS4 Proxy <input type="checkbox"/> Block SOCKS5 Proxy	
<input type="button" value="Save"/>		

Figure 11-4 Internet Behavior Management Policy Settings

- ✧ **Address Group:** It specifies an address group to which the Internet behavior management policy applies. The Device will control and manage the Internet behaviors of the LAN users that belong to this address group according to the policy. The address group is configured in the **Security > Address Group** page.
- ✧ **Schedule:** It specifies a schedule to restrict when the Internet behavior management policy is in effect. The default value is **Always**, which means the policy is in effect always. Note that after the selected schedule has expired, the policy will be in effect always. The schedule is configured in the **Security > Schedule** page.

- ✧ **Description:** It specifies the description of the Internet behavior management policy. It is usually used to describe the purpose of the policy.
- ✧ **IM:** You can allow or block some popular IM (Instant Message) applications, which include QQ, MSN, Ali Wangwang, WebQQ and Fetion.
 - **Block QQ:** Allow or block QQ application. If you want to block the specified LAN users (set by **Address Group**) from using QQ to chat with others, please select this check box.
 - **Block MSN:** Allow or block MSN Messenger. If you want to block the specified LAN users from using MSN Messenger to chat with others, please select this check box.
 - **Block Ali Wangwang:** Allow or block Ali Wangwang application. If you want to block the specified LAN users from using Ali Wangwang, please select this check box.
 - **Block WebQQ:** Allow or block WebQQ application. If you want to block the specified LAN users from using WebQQ to chat with others, please select this check box.
 - **Block Fetion:** Allow or block Fetion application. If you want to block the specified LAN users from using Fetion to chat with others, please select this check box.
- ✧ **P2P:** You can allow or block some popular P2P applications, which include BT (Bit Comet, Bit Spirit), Thunder Search, QQLive, PPS, Sogou Search, PPLive and QVOD.
 - **Block BT (BitSpirit, BitComet):** Allow or block BitSpirit and BitComet applications. If you want to block the specified LAN users from using BitSpirit or BitComet to download files, please select this check box.
 - **Block Thunder Search:** Allow or block Thunder search application. If you want to block the specified LAN users from using Thunder to search resources, please select this check box.
 - **Block QQLive:** Allow or block QQLive application. If you want to block the specified LAN users from using QQLive to play videos, please select this check box.
 - **Block PPS:** Allow or block PPS (i.e., PPStream) application. If you want to block the specified LAN users from using PPS to play videos, please select this check box.

- **Block Sogou Search:** Allow or block Sogou search application. If you want to block the specified LAN users from using Sogou to search resources, please select this check box.

- **Block PPLive:** Allow or block PPLive application. If you want to block the specified LAN users from using PPLive to play videos, please select this check box.

- **Block QVOD:** Allow or block QVOD (Quasi Video on Demand) application. If you want to block the specified LAN users from using QVOD to play videos, please select this check box.

- ◇ **Game:** You can allow or block some popular online game applications, which include QQGame, BNB, Zhengtu, Perfect World, Jade Dyna, MHXY, Audition, CGA, WOW, Aion and Kartrider Rush.
 - **Block QQGame:** Allow or block QQGame application. If you want to block the specified LAN users from playing QQGame, please select this check box.

 - **Block BNB:** Allow or block BNB application. If you want to block the specified LAN users from playing BNB game, please select this check box.

 - **Block Zhengtu:** Allow or block Zhengtu application. If you want to block the specified LAN users from playing Zhengtu game, please select this check box.

 - **Block Jade Dynasty:** Allow or block Jade Dynasty and Perfect World applications. If you want to block the specified LAN users from playing Jade Dynasty or Perfect World game, please select this check box.

 - **Block MHXY:** Allow or block MHXY application. If you want to block the specified LAN users from playing MHXY game, please select this check box.

 - **Block Audition:** Allow or block Audition application. If you want to block the specified LAN users from playing Audition game, please select this check box.

 - **Block CGA:** Allow or block CGA application. If you want to block the specified LAN users from playing CGA game, please select this check box.

 - **Block WOW:** Allow or block WOW application. If you want to block the specified LAN users from playing WOW game, please select this check box.

 - **Block Aion:** Allow or block Aion application. If you want to block the specified

LAN users from playing Aion game, please select this check box.

- **Block Kartrider Rush:** Allow or block Kartrider Rush application. If you want to block the specified LAN users from playing Kartrider Rush game, please select this check box.
- ✧ **Web:** You can allow or block downloading some predefined types of files over HTTP, and submitting input in the webpage.
- **Block Files:** Allow or block downloading some predefined types of files over HTTP. If you want to block the specified LAN users from downloading the files with the extension .exe, .dll, .vbs, .com, .bat or .sys over HTTP, please select this check box. It allows you to click **View** hyperlink to view all the predefined file types.
 - **Block Submit:** Allow or block submitting input in the webpage. If you want to block the specified LAN users from submitting input in the webpage, such as logging in to a website, posting messages on a forum, etc.
- ✧ **DNS:** You can allow or block some predefined game and stock websites by DNS filtering.
- **Block Game Websites:** Allow or block some predefined game websites. If you want to block the specified LAN users from accessing those predefined game websites, please select this check box. It allows you to click the **View** hyperlink to view all the predefined game websites.
 - **Block Stock Websites:** Allow or block some predefined stock websites. If you want to block the specified LAN users from accessing those predefined stock websites, please select this check box. It allows you to click the **View** hyperlink to view all the predefined stock websites.
- ✧ **Others:** Allow or block some other applications such as HTTP Proxy, SOCK Proxy.
- **Block HTTP Proxy:** Allow or block HTTP Proxy application. If you want to block the specified LAN users from using HTTP Proxy, please select this check box.
 - **Block SOCK4 Proxy:** Allow or block SOCK4 Proxy application. If you want to block the specified LAN users from using SOCK4 Proxy, please select this check box.
 - **Block SOCK5 Proxy:** Allow or block SOCK4 Proxy application. If you want to block the specified LAN users from using SOCK5 Proxy, please select this check

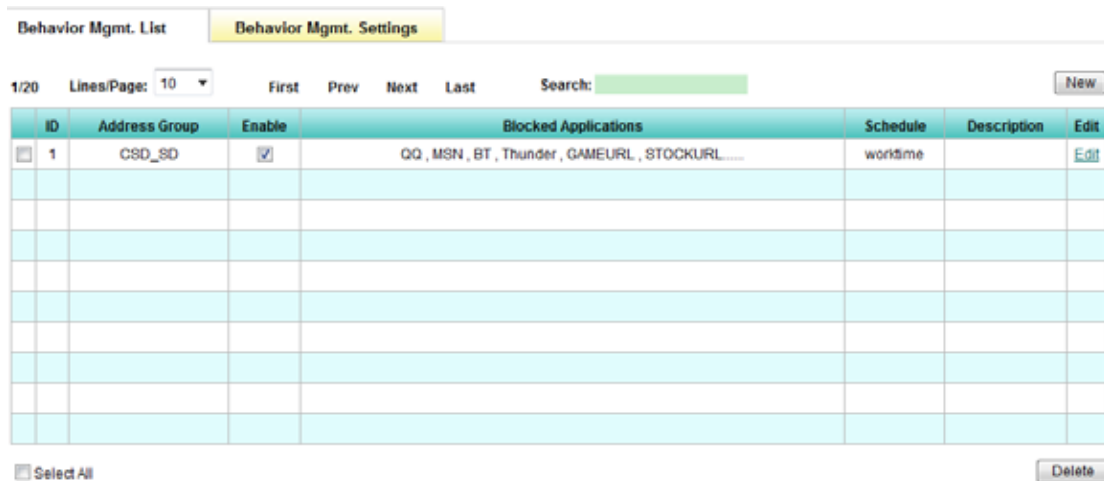
box.

- **Save:** Click it to save the Internet behavior management policy settings.

 **Note**

1. If a function option of an internet behavior management policy is not in effect as desired, please go to the **Restriction > Policy Database > Policy Database List** to check whether its corresponding policy database is the latest or not. Refer to **section 11.3.2 Policy Database List** for more information about how to update a policy database.
2. When using Internet behavior management feature, the Device will search the Internet behavior management policy list to find out if there is a matched policy for each LAN user. It will check the user’s IP address against each policies in the order in which the policies are listed. The first matched policy will apply to the LAN user, and no further policies will be checked. Note that in the **Behavior Mgmt. List**, the policies are listed in reverse chronological order of creation, the later the policy is created, the upper the policy is listed.

11.2.2 Internet Behavior Management Policy List



ID	Address Group	Enable	Blocked Applications	Schedule	Description	Edit
1	CSD_SD	<input checked="" type="checkbox"/>	QQ, MSN, BT, Thunder, GAMEURL, STOCKURL...	worktime		Edit

Figure 11-5 Internet Behavior Management Policy List

- **Add an Internet Behavior Management Policy:** If you want to add a new Internet behavior management policy, click the **New** button or select the **Behavior Mgmt.**

Settings tab to go to the setup page, and then configure it, lastly click the **Save** button.

- **View Internet Behavior Management Policy(s):** When you have configured some Internet behavior management policies, you can view them in the **Behavior Mgmt. List**.
- **Enable an Internet Behavior Management Policy:** The **Enable** check box is used to enable or disable the corresponding Internet behavior management policy. The default value is selected, which means the policy is in effect. If you want to disable the policy temporarily instead of deleting it, please click it to remove the check mark.
- **Edit an Internet Behavior Management Policy:** If you want to modify a configured Internet behavior management policy, click its **Edit** hyperlink, the related information will be displayed in the setup page. Then modify it, and click the **Save** button.
- **Delete Internet Behavior Management Policy(s):** If you want to delete one or more Internet behavior management policies, select the leftmost check boxes of them, and then click the **Delete** button.

11.3 Policy Database

This section describes the **Restriction > Policy Database** page.



Note

In this document the policy database is called PDB for short.

11.3.1 Introduction to Policy Database

This page allows you to not only view the PDBs in the **Policy Database List**, but also upload and update PDBs. By introducing PDB, we can add a group of policies into a PDB; and we also provide PDB online update function to greatly facilitate the users. The Device currently supports four types of PDBs, which includes Route PDB, DNS PDB, Website PDB and Firewall PDB; and in the future, UTT Technologies Co., Ltd. will successively provide more types of PDBs according to actual user requirements.

The route PDBs can be referenced and configured in the **Advanced > Static Route** page. By introducing route PDB, the users don't need add static routes one by one, but instead create a large batch of static routes for each ISP connection at a time. Then the traffic destined for one ISP's servers will be forwarded through this ISP's connection, but not another ISP's connection; such as, the traffic destined for TEL servers will be forwarded to the TEL connection, the traffic destined for CNC servers will be forwarded to the CNC Internet connection, and the traffic destined for ChinaMobile servers will be forwarded to the ChinaMobile Internet connection. Thus the LAN hosts can access those servers normally. Refer **section 7.1.2 Static Route Policy Database** for more information about route PDBs.

The firewall PDBs, DNS PDBs, and Website PDBs are referenced and configured in the **Restriction > Behavior Mgmt. > Behavior Mgmt. Settings** page. By introducing firewall PDBs, you don't need add multiple access control rules one by one, but instead just click some check boxes to block or allow the LAN users to use popular IM (e.g., QQ, MSN) and P2P applications (e.g., BitComet, BitSpirit, Thunder Search).

11.3.2 Policy Database List

Policy Database List		Database Version Check	Import Policy Database
33/57	Lines/Page: 10	First	Prev Next Last
Search: <input type="text"/>			
Name	Type	Description	Referenced
<input type="checkbox"/> CNC	Route	CNC Static Route	Yes
<input type="checkbox"/> TEL	Route	TEL Static Route	No
<input type="checkbox"/> QQ	Firewall	Block QQ	No
<input type="checkbox"/> MSN	Firewall	Block MSN	No
<input type="checkbox"/> BT	Firewall	Block BT(BitSprint,BitComet)	No
<input type="checkbox"/> Thunder	Firewall	Block Thunder Search	No
<input type="checkbox"/> GAMEURL	Dns	Block Game Websites	No
<input type="checkbox"/> STOCKURL	Dns	Block Stock Websites	No
<input type="checkbox"/> FileType	Website	Block Files	No
<input type="checkbox"/> upload	Website	Block Submit	No
<input type="checkbox"/> Select All		Update All <input type="button" value="Delete"/>	

Figure 11-6 Policy Database List

- ✧ **Name:** It displays the name of the PDB.
- ✧ **Type:** It displays the type of the PDB. Now the Device provides four types of policy databases: Route, Firewall, Dns and Website.
- ✧ **Description:** It displays the description of the PDB. It is usually used to describe the purpose of the PDB.
- ✧ **Referenced:** It indicates whether the PDB is referenced or not. If the PDB is referenced, it displays **Yes**; else, it displays **No**.
- ✧ **Version:** It displays the version of the PDB. The version indicates the date on which PDB was created, for example, the version of 090805 means that the PDB was created on August 5, 2009. You can judge whether a PDB needs to be updated according to its version: the larger the value, the newer the version.
- **Update:** If you want to update a PDB, click its **Update** hyperlink to download the latest PDB from designated website and apply it automatically.
- **Update All:** If you want to update all the PDBs in the list at a time, click the **Update All** hyperlink to download all the latest PDBs from designated website and apply them automatically.
- **Delete:** If you want to delete one or more PDBs, select the leftmost check boxes of them, and then click the **Delete** button.



Note

1. You cannot delete the system default PDBs.
2. By default, the **Policy Database List** only displays the system default PDBs, which include CNC, TEL, QQ, MSN, BT, Thunder, GAMEURL, STOCKURL, FileType, and upload. It allows you to customize firewall PDBs and modify the system default firewall PDBs via CLI.
3. Only the system default PDBs can be updated. Once you have updated a firewall PDB which has been referenced, the related settings will take effect immediately; after you updated a route PDB which has been referenced, you should go to the **Advanced > Static Route** page to reference it again and perform the save operation to make the related settings take effect. Refer to **section 7.1.2.4 How to Update a System Default Static Route PDB** for detailed operation.

11.3.3 Policy Database Version Check

The screenshot shows a web interface for configuring the Policy Database Version Check. At the top, there are three tabs: 'Policy Database List', 'Database Version Check', and 'Import Policy Database'. The 'Database Version Check' tab is selected. Below the tabs, there is a configuration area with two dropdown menus. The first dropdown is labeled 'Policy Database Verison Check' and is set to 'Automatically'. The second dropdown is labeled 'Check Time' and is set to 'Everyday'. To the right of the 'Check Time' dropdown, there is a time field set to '00:00'. A 'Save' button is located at the bottom right of the configuration area.

Figure 11-7 Policy Database Version Check

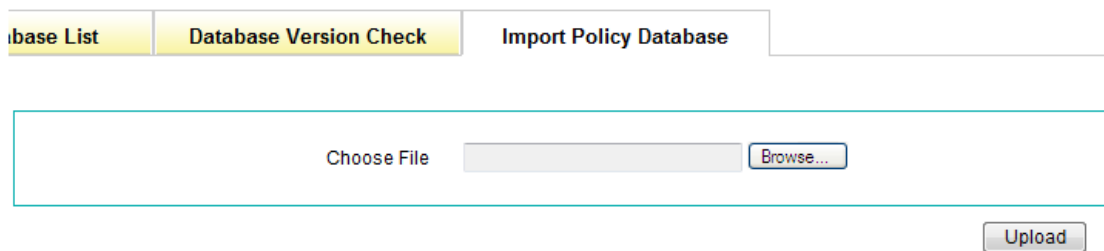
- ✧ **Policy Database Version Check:** It specifies whether the Device will automatically check the version of each PDB or not. There are two available options:
 - **Never:** It indicates that the Device will not automatically check the version of each PDB.
 - **Automatically:** It indicates that the Device will automatically check the version of each PDB at the specified time (set by **Check Time**); and log the results that mainly contain which PDBs need to be updated in the **Status > System Log** page.

- ✧ **Check Time:** It specifies a time at which PDB version check will be triggered. If you select **Automatically** from the **Policy Database Version Check** drop-down list, you should set the **Check Time** as required.
- **Save:** Click it to save the PDB version check settings.

 **Note**

If you select **Automatically** from the **Policy Database Version Check** drop-down list, you should synchronize the system clock in the **System > Time** page to ensure that the Device will automatically check the version of each PDB at the desired time.

11.3.4 Import Policy Database



The screenshot shows a web interface for importing a Policy Database. At the top, there are three tabs: 'Policy Database List', 'Database Version Check', and 'Import Policy Database'. The 'Import Policy Database' tab is selected. Below the tabs is a large text input field with the placeholder text 'Choose File'. To the right of the input field is a 'Browse...' button. Below the input field is an 'Upload' button.

Figure 11-8 Import Policy Database

- ✧ **Choose File:** Click the **Browse** button to choose a PDB file or enter the file path and name in the text box.
- **Upload:** Click it to import the selected PDB file into the Device. Once the PDB file is imported successfully, you can view it in the **Policy Database List**.

 **Note**

To avoid unexpected error, do not power off the Device during importing the PDB file.

11.4 QQ Whitelist

The Device provides QQ whitelist feature, which allows you to add some QQ numbers into the **QQ Whitelist**, then those QQ numbers will be exempt from the restriction of the Internet behavior management policies configured in the **Restriction > Behavior Mgmt. > Behavior Mgmt. Settings** page, that is, the LAN users still can use those QQ numbers to login to QQ even if you have blocked these users from using QQ by policies.

11.4.1 Enable QQ Whitelist

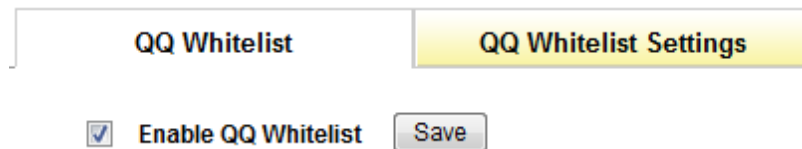


Figure 11-9 Enable QQ Whitelist

- ✧ **Enable QQ Whitelist:** It allows you enable or disable QQ whitelist. If you select the check box to enable QQ whitelist, the QQ numbers in the **QQ Whitelist** will take effect. Else, those QQ numbers will be of no effect.
- **Save:** Click it to save your settings.

11.4.2 QQ Whitelist Settings

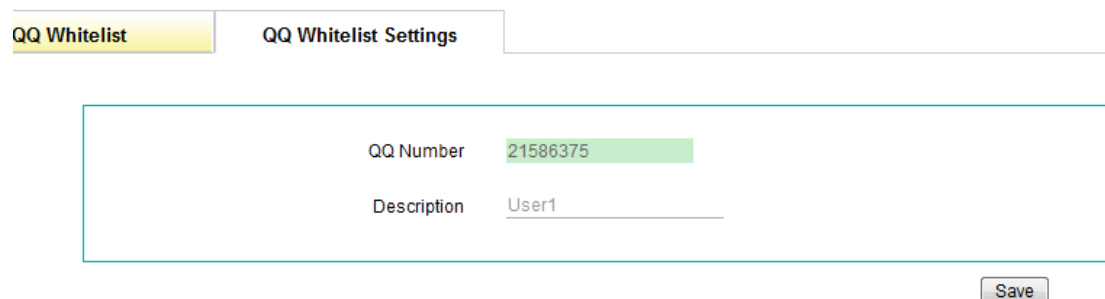


Figure 11-10 QQ Whitelist Settings

- ✧ **QQ Number:** It specifies a unique QQ number. It should be a number less than 11 digits. The QQ number will be exempt from the restriction of the Internet behavior management policies, that is, a LAN user still can use this QQ number to login to QQ even if you have blocked the user from using QQ by a policy.
- ✧ **Description:** It specifies the description of the QQ number.
- **Save:** Click it to save the QQ whitelist settings.

11.4.3 QQ Whitelist

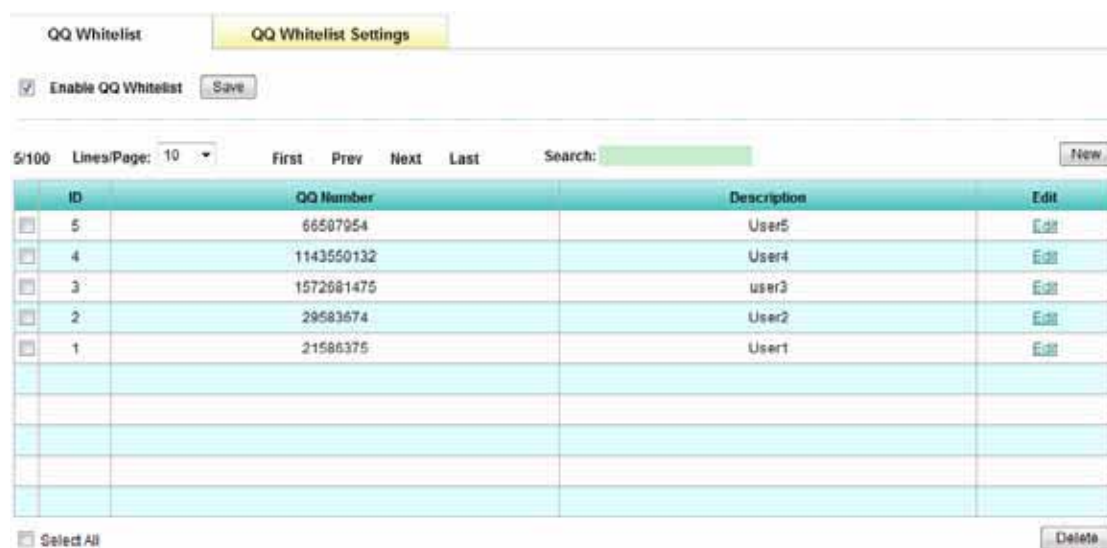


Figure 11-11 QQ Whitelist

- **Add a QQ Number:** If you want to add a new QQ number into the **QQ Whitelist**, click the **New** button or select the **QQ Whitelist Settings** tab to go to the setup page, and then configure it, lastly click the **Save** button.
- **View QQ Number(s):** When you have configured some QQ numbers, you can view them in the **QQ Whitelist**.
- **Edit a QQ Number:** If you want to modify a configured QQ number, click its **Edit** hyperlink, the related information will be displayed in the setup page. Then modify it, and click the **Save** button.
- **Delete QQ Number(s):** If you want to delete one or more QQ numbers, select the leftmost check boxes of them, and then click the **Delete** button.

11.5 Configuration Example for Internet Behavior Management

1. Requirements

In 2011, a business CEO wants to control online behavior of the employees. He wants to block all the predefined IM and P2P applications, online games, game and stock websites during working time, but allow all the Internet services during rest periods. But there are some exceptions which are as follows:

- The CEO and vice CEO can access the Internet without any restrictions. Their IP addresses are 192.168.16.4 and 192.168.16.5 respectively.
- The Customer Service and Sales Departments' employees need to use IM applications to communicate with customers during working time. Their IP address ranges are: from 192.168.16.50 to 192.168.16.70, and from 192.168.16.100 to 192.168.16.120 respectively.
- There are five employees with dynamic IP addresses, and they need to use QQ. Their QQ numbers are 21586375, 29583674, 1572681475, 1143550132 and 66587954 respectively.

The business's working time is: Monday to Friday, 9:00 to 12:00 am, and 1:00 to 6:00 pm.

2. Analysis

We need to create three Internet behavior management policies, enable QQ whitelist feature and add five QQ numbers into the **QQ Whitelist** to meet requirements.

- 1) Policy 1: It is used to block all the LAN users from using IM and P2P applications, playing online games, and accessing game and stock websites.
- 2) Policy 2: It is used to allow the Customer Service and Sales Departments' employees to use IM applications during working time. Note that as this policy has higher priority than policy 1, it should be created later than policy 1.
- 3) Policy 3: It is used to allow the CEO and vice CEO to access all the Internet services. Note that as this policy has the highest priority, it should be created at last.
- 4) Enable QQ whitelist feature and add five QQ numbers into the **QQ Whitelist**.

3. Configuration Procedure

Before creating the Internet behavior management policies, you may do the following tasks:

- Go to the **Security > Address Group** page to create two address groups, one is for the two CEOs, and it contains two IP addresses: 192.168.16.4 and 192.168.16.5; the other is for Customer Service and Sales Departments' employees, and it contains two IP address ranges: from 192.168.16.50 to 192.168.16.70, and from 192.168.16.100 to 192.168.16.120. Here we assume the first group's name is **Directors**, and the second group's name is **CSD_SD**. Refer to **section 12.6.4 How to Add the Address Groups** for detailed information about how to create them.
- Go to the **Security > Schedule** page to create one schedule for working time. Here we assume its name is **work**. Refer to **section 12.8.5 Configuration Example for Schedule** for detailed information about how to create it.

Here we only describe how to create three Internet behavior management policies, enable QQ whitelist feature and add five QQ numbers into the **QQ Whitelist**.

The configuration steps are the following:

- Step 1** Go to the **Restriction > Behavior Mgmt. > Behavior Mgmt. Settings** page.
- Step 2** Creating Policy 1: Select **Any Address** from the **Address Group** drop-down list, select **work** from the **Schedule** drop-down list, select all the check boxes in **IM, P2P, Games** and **DNS** configuration fields, and then click the **Save** button, see Figure 11-12.

B a s i c	Address Group Any Address		Schedule work	
	Select All <input checked="" type="checkbox"/>	Description _____		
I M	<input checked="" type="checkbox"/> Block QQ	<input checked="" type="checkbox"/> Block MSN	<input checked="" type="checkbox"/> Block Ali Wangwang	<input checked="" type="checkbox"/> Block Web QQ
	<input checked="" type="checkbox"/> Block Fention			
P 2 P	<input checked="" type="checkbox"/> Block BT (BitSpirit, BitComet)	<input checked="" type="checkbox"/> Block Thunder Search	<input checked="" type="checkbox"/> Block QQLive	<input checked="" type="checkbox"/> Block PPS
	<input checked="" type="checkbox"/> Block Sogou Search	<input checked="" type="checkbox"/> Block PPLive	<input checked="" type="checkbox"/> Block QVOD	
G a m e	<input checked="" type="checkbox"/> Block QQGame	<input checked="" type="checkbox"/> Block BNB	<input checked="" type="checkbox"/> Block Zhengtu	<input checked="" type="checkbox"/> Block Jade Dynasty
	<input checked="" type="checkbox"/> Block MHXY	<input checked="" type="checkbox"/> Block Audition	<input checked="" type="checkbox"/> Block CGA	<input checked="" type="checkbox"/> Block WOW
	<input checked="" type="checkbox"/> Block Aion	<input checked="" type="checkbox"/> Block Kartrider Rush		
W e b	<input type="checkbox"/> Block Files View	<input type="checkbox"/> Block Submit		
D N S	<input checked="" type="checkbox"/> Block Game Websites View	<input checked="" type="checkbox"/> Block Stock Websites View		
O t h e r s	<input type="checkbox"/> Block HTTP Proxy			
	<input type="checkbox"/> Block SOCKS4 Proxy		<input type="checkbox"/> Block SOCKS5 Proxy	
<input type="button" value="Save"/>				

Figure 11-12 Internet Management Behavior Example - Policy 1

Step 3 Creating Policy 2: Select **CSD_SD** from the **Address Group** drop-down list, select **work** from the **Schedule** drop-down list, select all the check boxes in **P2P**, **Games** and **DNS** configuration fields, and then click the **Save** button, see Figure 11-13.

B a s i c	Address Group	CSD_SD		Schedule	work
	Select All	<input checked="" type="checkbox"/>		Description	
I M	<input type="checkbox"/> Block QQ	<input type="checkbox"/> Block MSN	<input type="checkbox"/> Block Ali Wangwang	<input type="checkbox"/> Block Web QQ	
	<input type="checkbox"/> Block Fention				
P 2 P	<input checked="" type="checkbox"/> Block BT (BitSpirit, BitComet)	<input checked="" type="checkbox"/> Block Thunder Search	<input checked="" type="checkbox"/> Block QQLive	<input checked="" type="checkbox"/> Block PPS	
	<input checked="" type="checkbox"/> Block Sogou Search	<input checked="" type="checkbox"/> Block PPLive	<input checked="" type="checkbox"/> Block QVOD		
G a m e	<input checked="" type="checkbox"/> Block QQGame	<input checked="" type="checkbox"/> Block BNB	<input checked="" type="checkbox"/> Block Zhengtu	<input checked="" type="checkbox"/> Block Jade Dynasty	
	<input checked="" type="checkbox"/> Block MHXY	<input checked="" type="checkbox"/> Block Audition	<input checked="" type="checkbox"/> Block CGA	<input checked="" type="checkbox"/> Block WOW	
	<input checked="" type="checkbox"/> Block Aion	<input checked="" type="checkbox"/> Block Kartrider Rush			
W e b	<input type="checkbox"/> Block Files View		<input type="checkbox"/> Block Submit		
D N S	<input checked="" type="checkbox"/> Block Game Websites View	<input checked="" type="checkbox"/> Block Stock Websites View			
O t h e r s	<input type="checkbox"/> Block HTTP Proxy				
	<input type="checkbox"/> Block SOCKS4 Proxy	<input type="checkbox"/> Block SOCKS5 Proxy			
<input type="button" value="Save"/>					

Figure 11-13 Figure 11-9 Internet Management Behavior Example - Policy 2

Step 4 Creating Policy 3: Select **Directors** from the **Address Group** drop-down list, select **Always** from the **Schedule** drop-down list, and unselect all the check boxes in the page, and then click the **Save** button, see Figure 11-14.

B a s i c	Address Group	Directors		Schedule	Always
	Select All	<input type="checkbox"/>	Description		
I M	<input type="checkbox"/> Block QQ	<input type="checkbox"/> Block MSN	<input type="checkbox"/> Block Ali Wangwang	<input type="checkbox"/> Block Web QQ	
	<input type="checkbox"/> Block Fention				
P 2 P	<input type="checkbox"/> Block BT (BitSpirit, BitComet)	<input type="checkbox"/> Block Thunder Search	<input type="checkbox"/> Block QQLive	<input type="checkbox"/> Block PPS	
	<input type="checkbox"/> Block Sogou Search	<input type="checkbox"/> Block PPLive	<input type="checkbox"/> Block QVOD		
G a m e	<input type="checkbox"/> Block QQGame	<input type="checkbox"/> Block BNB	<input type="checkbox"/> Block Zhengtu	<input type="checkbox"/> Block Jade Dynasty	
	<input type="checkbox"/> Block MHXY	<input type="checkbox"/> Block Audition	<input type="checkbox"/> Block CGA	<input type="checkbox"/> Block WOW	
	<input type="checkbox"/> Block Aion	<input type="checkbox"/> Block Kartrider Rush			
W e b	<input type="checkbox"/> Block Files View	<input type="checkbox"/> Block Submit			
D N S	<input type="checkbox"/> Block Game Websites View	<input type="checkbox"/> Block Stock Websites View			
O t h e r s	<input type="checkbox"/> Block HTTP Proxy	<input type="checkbox"/> Block SOCKS4 Proxy	<input type="checkbox"/> Block SOCKS5 Proxy		

Figure 11-14 Internet Management Behavior Example - Policy 3

Step 5 Go to **Restriction > QQ Whitelist** page, select the **Enable QQ Whitelist** check box, and click the **Save** button, see Figure 11-15. Click the **New** button to go to the **QQ Whitelist Settings** page to add the first QQ number (i.e., 21586375) into the **QQ Whitelist**, and then add the other four QQ numbers one by one, see Figure 11-16.

QQ Whitelist	QQ Whitelist Settings
<input checked="" type="checkbox"/> Enable QQ Whitelist	<input type="button" value="Save"/>

Figure 11-15 Internet Management Behavior Example - Enable QQ Whitelist

5/100 Lines/Page: 10 First Prev Next Last Search:

ID	QQ Number	Description	Edit
<input type="checkbox"/> 5	66587954	User5	<input type="button" value="Edit"/>
<input type="checkbox"/> 4	1143550132	User4	<input type="button" value="Edit"/>
<input type="checkbox"/> 3	1572681475	user3	<input type="button" value="Edit"/>
<input type="checkbox"/> 2	29583674	User2	<input type="button" value="Edit"/>
<input type="checkbox"/> 1	21586375	User1	<input type="button" value="Edit"/>

Select All

Figure 11-16 Internet Management Behavior Example -QQ Whitelist

11.6 Notice

This section describes the **Restriction > Notice** page.

11.6.1 Introduction to Notice

The Device provides notice feature which is used to push notice messages to the specified LAN users. After you enable notice feature, if a specified LAN user accesses the Internet via a web browser (e.g., IE, Firefox), the Device will automatically push a notice message to the user.

The Device provides one-time notice and daily notice. If you enable one-time notice feature and specify a notice message, and then when a specified LAN user accesses the Internet via a web browser, the Device will automatically push the notice message to the user; in general, the one-time notice message is only pushed once. If you enable daily notice feature and specify a notice message, the Device will automatically push the notice message to the specified LAN users one time per day.

Either you use one-time notice or daily notice, it allows you to customize a notice message or just specify a notice URL. If you choose to customize a notice message, and then when a specified LAN user accesses the Internet via a web browser, the Device will automatically pop up the notice message to the user. Else, the requested web page will automatically jump to the specified URL to display the notice; in this case, you need add the notice message to that web page in advance.

Besides notice feature in this page, UTT Series Security Firewalls also provide domain blocking notice feature. Please refer to **section 12.4.2 Domain Blocking Notice** for detailed information.

11.6.2 Notice Settings

11.6.2.1 One-Time Notice Settings

When using one-time notice, the Device will push the notice message to the LAN users that belong to the specified address group. And the one-time notice message is only pushed once.

One-Time Notice **Daily Notice Settings**

Enable One-Time Notice

Address Group Any Address

Notice Mode Customized

Notice Title

Signature

Notice Content

```

Hello,
We are going to hold a party, please take time to attend.

```

Figure 11-17 One-Time Notice Settings - Customized Mode

- ✧ **Enable One-Time Notice:** It allows you to enable or disable one-time notice. If you want to enable one-time notice, please select this check box.
- ✧ **Address Group:** It specifies an address group to which the notice message will be pushed. When you enable one-time notice, the Device will directly push the notice message to the LAN users that belong to this address group. The address group is configured in the **Security > Address Group** page.
- ✧ **Notice Mode:** It specifies the mode of pushing the notice. There are two available options:
 - **Customized:** When selecting **Customized** (see Figure 11-17), it allows you to customize a notice message which consists of **Notice Title**, **Notice Content** and **Signature**, and to preview the notice message. In this case, if a specified LAN user accesses the Internet via a web browser, the Device will automatically pop up the notice message to the user.
 - **URL:** When selecting URL, it allows you specify a notice **URL**, see Figure 11-19. In his case, you need add a notice message to the specified web page in

advance; thus, if a specified LAN user accesses the Internet via a web browser, the requested web page will automatically jump to the specified URL to display the notice.

- ✧ **Notice Title:** It specifies the title of the notice message. If you select **Customized** from the **Notice Mode** check box, you need set it.
- ✧ **Signature:** It specifies the signature of the notice message. If you select **Customized** from the **Notice Mode** check box, you need set it.
- ✧ **Notice Content:** It specifies the content of the notice message. If you select **Customized** from the **Notice Mode** check box, you need set it.
- ✧ **URL:** It specifies a notice URL to which the requested web page will automatically jump. If you select **URL** from the **Notice Mode** check box, you need set it.
- **Save:** Click it to save your settings.
- **Preview:** If you select **Customized** from the **Notice Mode** check box, you may click the **Preview** button to preview the notice message you just configured. The following figure shows an example of a notice message.

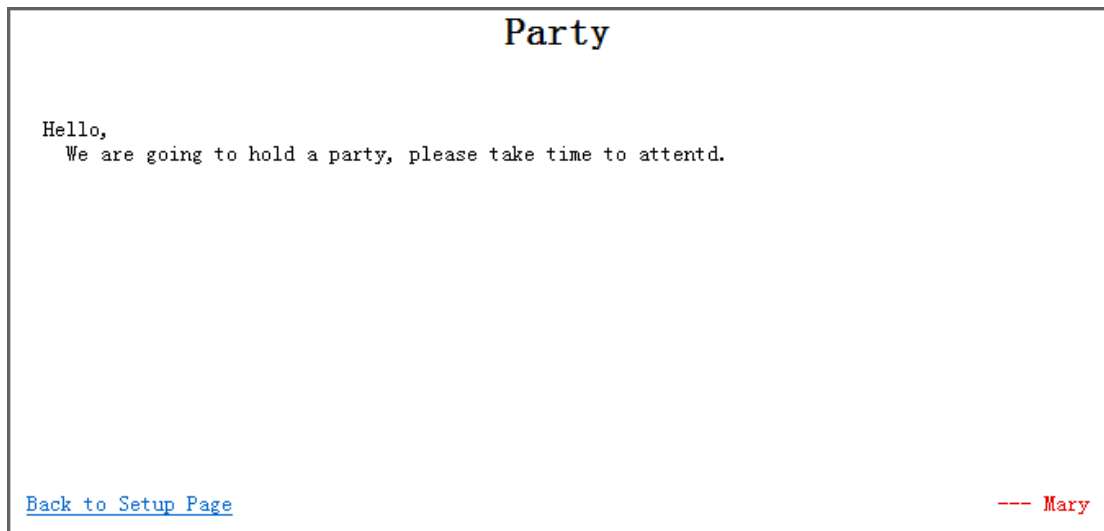


Figure 11-18 One-Time Notice Preview - Example

One-Time Notice **Daily Notice Settings**

Enable One-Time Notice

Address Group Any Address ▼

Notice Mode URL ▼

URL **http://**

Figure 11-19 One-Time Notice Settings - URL Mode

Note

1. If the Device pushes a notice message to a LAN user who hasn't launched a web browser, it will fail to push; and once the user launched the web browser and accessed an Internet domain name or IP address, he/she will receive the notice message immediately. For example, we assume that the Device will push a notice message at 8:00 am as planned, if a user hasn't launch the web browser at 8:00 am yet, the user cannot received the notice message; and if the user access the Internet via the web browser at 10:00, he/she will receive the notice message immediately.

2. When using one-time notice, if you restart the Device, the Device will push the notice message once again.

11.6.2.2 Daily Notice Settings

When using daily notice, the Device will automatically push the notice message to the LAN users that belong to the specified address group one time per day.

One-Time Notice **Daily Notice Settings**

Enable Daily Notice

Address Group All Addresses ▼

Notice Mode URL ▼

URL **http://**

Figure 11-20 Daily Notice Settings

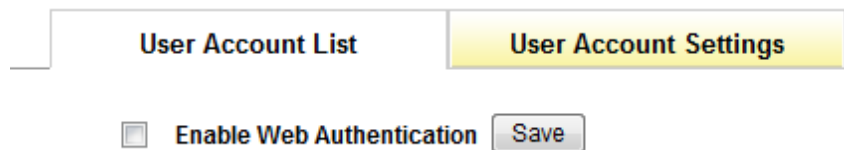
- ✧ **Enable Daily Notice:** It allows you to enable or disable daily notice. If you want to enable daily notice, please select this check box.

Please refer to **section 11.5.2.1 One-Time Notice Settings** for detailed description of the other parameters.

11.7 Web Authentication

UTT series security firewalls provide Web authentication feature. This new feature will enhance network security. If you enable the Web authentication on the Device, those non-PPPoE dial-in users cannot access the Internet through the Device unless they are authenticated successfully through Web browser.

11.7.1 Enable Web Authentication

**Figure 11-21 Enable Web Authentication**

- ✧ **Enable Web Authentication:** It allows you to enable or disable web authentication feature. By default it is disabled. If you select the check box to enable this feature, those non-PPPoE dial-in users cannot access the Internet through the Device unless they are authenticated successfully.
- **Save:** Click it to save your settings.

11.7.2 Web Authentication User Account Settings

User Account List
User Account Settings

User Name

Password

Description

Figure 11-22 Web Authentication User Account Settings

- ✧ **User Name:** It specifies a unique user name of the web authentication account. It should be between 1 and 31 characters long. The Device will use the **User Name** and **Password** to authenticate a user.
- ✧ **Password:** It specifies the password of the web authentication account.
- ✧ **Description:** It specifies the description of the web authentication account.
- **Save:** Click it to save the web authentication account settings.

11.7.3 Web Authentication User Account List

ID	User Name	User Status	IP Address	Description	Operation	Edit
<input type="checkbox"/>	1	abc	used	192.168.16.65	userA	<input type="button" value="Edit"/>

Select All

Figure 11-23 Web Authentication User Account List

- **Add a Web Authentication User Account:** If you want to add a web authentication user account, click the **New** button or select the **User Account Settings** tab to go to setup page, and then configure it, lastly click the **Save** button.
- **Edit a Web Authentication User Account:** If you want to modify a configured web authentication user account, click its **Edit** hyperlink, the related information will be displayed in the setup page. Then modify it, and click **Save** button.
- **Delete Web Authentication User Account(s):** If you want to delete one or more configured web authentication user accounts, select the leftmost check boxes of them, and then click **Delete** button.

11.7.4 How to Use Web Authentication

If you want to use web authentication for a non-PPPoE dial-in user, do the following:

- Step 1** Go to the **Restriction > Web Authentication** page, and then select the **Web User Account Settings** tab to go to setup page.
- Step 2** Configure a new web authentication user account (see figure 11-11), and then click the **Save** button to save the settings.
- Step 3** Select the **User Account List** tab, and then select the **Enable Web Authentication** check box.
- Step 4** Launch a web browser, enter an Internet domain name or IP address in the address bar, and then press **<Enter>**, the Device will automatically pop up an authentication login page, see figure 11-13.



Your device must be identified, otherwise you will not be allowed to access Internet. Please input your Identification User Name and Password.

User Name

Password

Please enable Popup from this website, or you might be not able to access Internet.

Figure 11-24 Web Authentication Login Page

- Step 5** Enter the correct user name and password in the text boxes, and then click the

Save button, the system will pop up a prompt page (see figure 11-14).

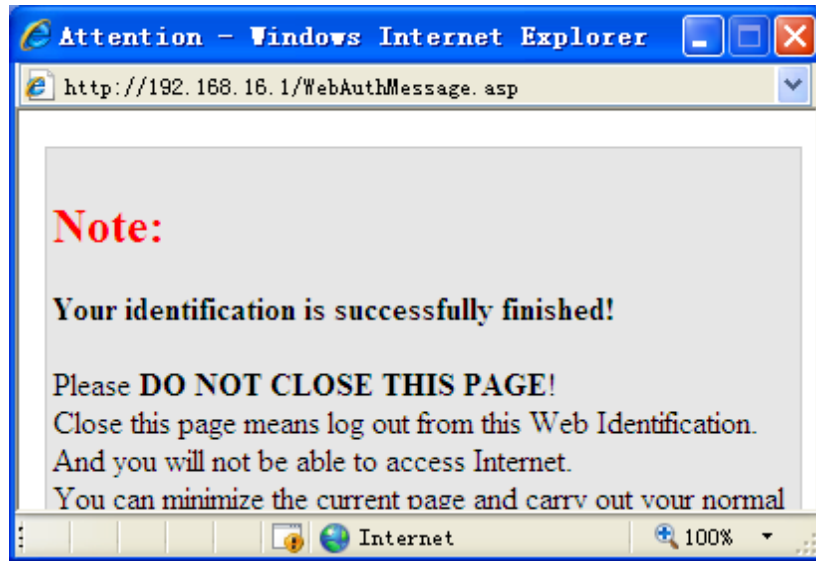


Figure 11-25 Web Authentication Prompt Page

 **Note**

Do not close the prompt page; else, the user cannot access the Internet.

Chapter 12 Security

This chapter describes how to configure security features, including attack defense, IP/MAC binding, firewall, DNS filtering, NAT session limit, address group, service group and schedule.

12.1 Attack Defense

This section describes the **Security > Attack Defense** page, which includes internal attack defense and external attack defense.

12.1.1 Internal Attack Defense

In this page, you can do basic internal attack defense settings to enhance network security. The internal attack defense includes three parts:

- **Virus Defense:** It can effectively protect the Device against popular virus attacks, such as, Anti-Blaster virus attack, UDP/ICMP/SYN flood attack, ARP spoofing attack, and so on.
- **Access Restrict:** It can effectively protect the Device against DDoS attacks by restricting LAN hosts' access to the Device.
- **Other Defense:** It can effectively protect the Device against port scanning attack.

Internal Attack Defense

External Attack Defense

V i r u s	<input type="checkbox"/> Enable Blaster Virus Defense		
	<input type="checkbox"/> Enable IP Spoofing Defense		
	<input type="checkbox"/> Enable UDP Flood Defense	Threshold	500 Packets/Second
	<input type="checkbox"/> Enable ICMP Flood Defense	Threshold	500 Packets/Second
	<input type="checkbox"/> Enable SYN Flood Defense	Threshold	500 Packets/Second
	<input type="checkbox"/> Enable ARP Spoofing Defense	ARP Broadcast Interval	100 milliseconds
R e s t r i c t	<input type="checkbox"/> Enable Device Access Restrict	Allowed IP Addresses	192.168.16.101 To 192.168.16.101
		Threshold	0 Packets/Second (0 means no limit)
O t h e r s	<input type="checkbox"/> Enable Port Scanning Defense	Threshold	100 milliseconds

Figure 12-1 Internal Attack Defense Settings

1. Virus Attacks Defense

- ✧ **Enable Blaster Virus Defense:** It allows you to enable or disable anti-blaster virus defense. If you select the check box to enable this feature, it will effectively protect the Device against blaster and sasser virus attacks. After you enable this feature, the Device will discard those TCP packets destined for port 135, 136, 137, 138, 139, 445, 1025, 5554 or 9996, so the LAN hosts cannot access the related services provided by outside hosts, e.g., windows file and printer sharing services.
- ✧ **Enable IP Spoofing Defense:** It allows you to enable or disable IP spoofing defense. If you select the check box to enable this feature, it will effectively protect the Device against IP spoofing attack. After you enable this feature, the Device will only forward the packets whose source IP address is in the same subnet as the Device LAN IP address. Note that in this case the hosts behind a L3 switch cannot access the Internet through the Device.
- ✧ **Enable UDP Flood Defense:** It allows you to enable or disable UDP flood defense. If you select this check box to enable this feature, it will effectively protect the Device against UDP flood attack. After you enable this feature, if the number of UDP packets from one source IP address (e.g., 192.168.16.66) to a single port on a remote host

exceeds the threshold, the Device will consider that the LAN host with IP address 192.168.16.66 is performing UDP flood attack, and then randomly discard the further UDP packets from that source to that destination. In most cases, leave **Threshold** the default value.

- ✧ **Enable ICMP Flood Defense:** It allows you to enable or disable ICMP flood defense. If you select this check box to enable this feature, it will effectively protect the Device against ICMP flood attack. After you enable this feature, if the number of ICMP packets from one source IP address (e.g., 192.168.16.16) to a single port on a remote host exceeds the threshold, the Device will consider that the LAN host with IP address 192.168.16.16 is performing ICMP flood attack, and then randomly discard the further ICMP packets from that source to that destination. In most cases, leave **Threshold** the default value.
- ✧ **Enable SYN Flood Defense:** It allows you to enable or disable SYN flood defense. If you select this check box to enable this feature, it will effectively protect the Device against SYN flood defense. After you enable this feature, if the number of SYN packets from one source IP address (e.g., 192.168.16.36) to a single port on a remote host exceeds the threshold, the Device will consider that the LAN host with IP address 192.168.16.36 is performing SYN flood attack, and then randomly discard the further SYN packets from that source to that destination. In most cases, leave **Threshold** the default value.
- ✧ **Enable ARP Spoofing Defense:** It allows you to enable or disable ARP spoofing defense. If you select the check box to enable this feature, and then bind all the IP/MAC address pairs of the LAN hosts (configured in the **Security > IP/MAC Binding** page), it will effectively protect the Device against ARP spoofing attack.
- ✧ **ARP Broadcast Interval:** It specifies the time interval at which the Device periodically broadcasts gratuitous ARP packets. These gratuitous ARP packets are used to inform the LAN hosts the correct MAC address of the Device's LAN interface, so the LAN hosts can effectively defense ARP spoofing attack. It should be multiple of 10 between 100 and 5000 milliseconds.

2. Access Restrict

- ✧ **Enable Device Access Restrict:** It allows you to enable or disable device access restrict. Select the check box to restrict LAN hosts' access to the Device through LAN interface, so it will protect the Device against internal DDoS attacks. The access restrict rules are as follows:
 - 1) Allow any LAN host to use ICMP to access the Device.
 - 2) Allow any LAN host to access the UDP port 53, 67 or 68 of the Device, to ensure that the Device's DNS proxy, DHCP server and DHCP client can operate properly.

- 3) Only allow the LAN hosts that belong to the range specified by **Allowed IP Addresses** to access the web or telnet service provided by the Device, but block the other hosts.
 - 4) Block LAN hosts from accessing any other services provided by the Device.
- ✧ **Allowed IP Addresses:** It specifies an address range of the allowed LAN hosts. When **Enable Device Access Restrict** is selected, only the LAN hosts that belong to this range can access the web or telnet service provided by the Device.
 - ✧ **Threshold:** It specifies the maximum number of packets passing through the Device's LAN interface per second. It should be between 0 and 20000 packets per second, and the suggested value is between 300 and 600 packets per second.

3. Other Defense

- ✧ **Enable Port Scanning Defense:** It allows you to enable or disable port scanning defense. If you select this check box to enable this feature, it will effectively protect the Device against port scanning attack. After you enable this feature, if a LAN host continuously sends the SYN packets to different ports on a remote host, and the number of ports exceeds 10 at the specified time interval (set by the **Threshold**), the Device will consider that the LAN host is performing port scanning attack, and then randomly discard the further SYN packets from it to that destination host. In most cases, leave the **Threshold** the default value.
- **Save:** Click it to save the internal attack defense settings.

12.1.2 External Attack Defense

In this page you can enable or disable WAN ping respond. As ping is often used by malicious Internet users to locate active networks or hosts, in most cases, it is recommended that you disable WAN ping respond for added security. Only in some special cases, such as network debugging, you need enable this feature.

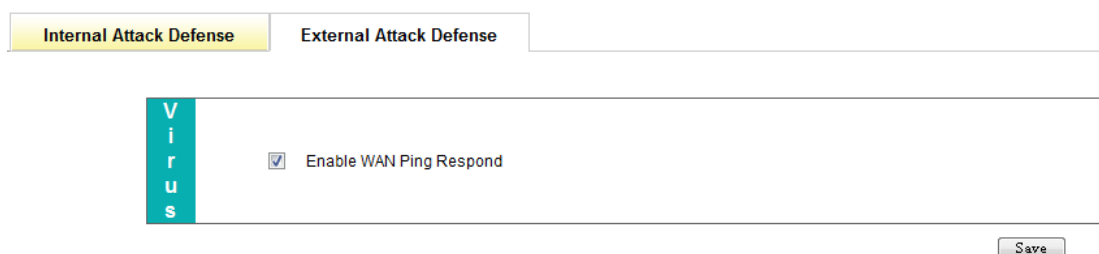


Figure 12-2 External Attack Defense Settings

- ✧ **Enable WAN Ping Respond:** It allows you to enable or disable WAN ping respond. If you select the check box to enable WAN ping respond, all the Device's WAN interfaces will respond to ping requests from the outside hosts.
- **Save:** Click it to save the external attack defense settings.

12.2 IP/MAC Binding

This section describes the **Security > IP/MAC Binding** page.

12.2.1 Introduction to IP/MAC Binding

12.2.1.1 IP/MAC Overview

To achieve network security management, you should firstly implement user identification, and then you should implement user authorization. **Section 12.3 Security > Firewall** describes how to configure and use access control rules to control the Internet behaviors of the LAN users. In this section, we will describe how to implement user identification.

The Device provides IP/MAC binding feature to implement user identification. Using the IP/MAC address pair as a unique user identity, you can protect the Device and your network against IP spoofing attacks. IP spoofing attack refers to that a host attempts to use another trusted host's IP address to connect to or pass through the Device. The host's IP address can easily be changed to a trusted address, but MAC address cannot easily be changed as it is added to the Ethernet card at the factory.

The IP/MAC binding feature allows you to add the IP and MAC address pairs of trusted LAN hosts in the **IP/MAC Binding List**. Note that in the **IP/MAC Binding List**, you can allow or block Internet access for each IP/MAC binding user. After you have added a LAN user's IP and MAC address pair into the **IP/MAC Binding List**, if its **Allow Internet Access** check box is selected (check mark \surd appears), it will allow the user to access the Device and Internet, else block the user.

12.2.1.2 The Operation Principle of IP/MAC Binding

For the sake of convenience, we firstly introduce several related terms including legal user, illegal user and undefined user.

Legal User: A legal user's IP and MAC address pair matches an IP/MAC binding whose **Allow Internet Access** check box is selected.

Illegal User: A illegal user's IP and MAC address pair matches an IP/MAC binding whose **Allow Internet Access** check box is unselected; or the IP address or MAC address is the same with an IP/MAC binding's, but not both.

Undefined User: An undefined user's IP address and MAC address both are different from any IP/MAC binding. The undefined users are all the users except legal and illegal users.

It allows the legal users to access the Device and access the Internet through the Device, and denies the illegal users. And the parameter of **Allow Undefined LAN PCs** determines whether it allows the undefined users to access the Device and access the Internet through the Device, that is, it will allow them if the **Allow Undefined LAN PCs** check box is selected, else block them.

IP/MAC binding feature can act on the packets initiated from the LAN hosts to the Device or outside hosts. When receiving a packet initiated from LAN, the Device will firstly determine the sender's identity by comparing the packet with the bindings in the **IP/MAC Binding List**, and then process the packet according to the sender's identity. The details are as follows:

1. If the sender is a legal user, the packet will be allowed to pass, and then be further processed by the firewall access control function module.
2. If the sender is an illegal user, the packet will be dropped immediately to prevent IP spoofing.
3. If the sender is an undefined user, there are two cases:
 - 1) If the **Allow Undefined LAN PCs** check box is selected, the packet will be allowed to pass, and then be further processed by the firewall access control function module.
 - 2) Else, the packet will be dropped immediately.

For example, if the IP/MAC address pair IP 192.168.16.65 and 00:15:c5:67:41:0f is added to the **IP/MAC Binding List**, and its **Allow Internet Access** check box is selected, see Figure 12-3.

ID	Description	IP Address	MAC Address	Allow Internet Access	Edit
2	test1	192.168.16.65	0015c567410f	<input checked="" type="checkbox"/>	Edit

Figure 12-3 IP/MAC Binding List - Example One

Then, when receiving a packet initiated from LAN, the Device will process it according to the following cases:

1. A packet with IP address 192.168.16.65 and MAC address 00:15:c5:67:41:0f is allowed to pass, and then it will be further processed by the firewall access control function module.
2. A packet with IP address 192.168.16.65 but with a different MAC address is dropped immediately to prevent IP spoofing.
3. A packet with a different IP address but with MAC address 00:15:c5:67:41:0f is dropped immediately to prevent IP spoofing.
4. A packet's IP address and MAC address both are not defined in the **IP/MAC Binding List**:
 - 1) If the **Allow Undefined LAN PCs** check box is selected, the packet is allowed to pass, and then it will be further processed by the firewall access control function module.
 - 2) Else, the packet is dropped.

If you want to block the user who matches the IP/MAC binding from accessing the Device and Internet, you need unselect **Allow Internet Access** check box, see Figure 12-4. Then a packet with IP address 192.168.16.65 and MAC address 00:15:c5:67:41:0f will be dropped.



ID	Description	IP Address	MAC Address	Allow Internet Access	Edit
2	test1	192.168.16.55	0015c567410f	<input checked="" type="checkbox"/>	Edit

Figure 12-4 IP/MAC Binding List - Example Two

**Note**

1. If you have added the IP and MAC address pair of a trusted LAN host in the **IP/MAC Binding List**, and later changed this host's IP address or MAC address, you must also change the corresponding binding in the **IP/MAC Binding List**; otherwise the host cannot access the Device and Internet. If the **Allow Undefined LAN PCs** check box is unselected, you must also add the IP and MAC address pair of any new host that you add to your network, and make sure that its **Allow Internet Access** check box is selected; otherwise this new host cannot access the Device and Internet.
2. IP/MAC binding feature can only act on the packets initiated from the LAN hosts to the Device or outside hosts, but cannot act on the packets within the LAN. If you change a LAN host's IP address or MAC address, this LAN host will be unable to access the Device and access the Internet through the Device, but it still can communicate with the other LAN hosts, such as, it can browse Network Neighborhood, use windows file and printer sharing services within the LAN, and so on.

12.2.2 IP/MAC Binding Settings

IP/MAC Binding Settings

Network Segment: /24

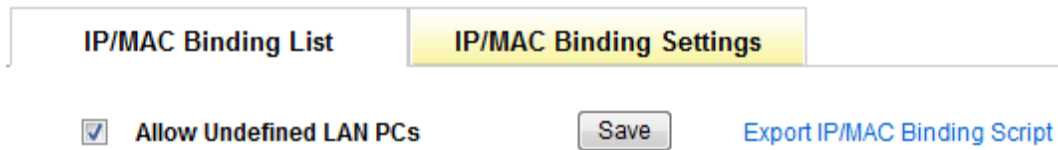
```
192.168.16.65 0015c567410f test1
192.168.16.66 0022aa112231 test2
192.168.16.99 0022aa223311 test3
```

Figure 12-5 IP/MAC Binding Settings

- **Scan:** If you click the **Scan** button, the Device will immediately scan the LAN to detect active hosts connected to the Device, learn and display dynamic ARP information (that is, IP and MAC address pairs). Note that if you have added a LAN host's IP and MAC address pair in the **IP/MAC Binding List**, this IP/MAC address pair will not be displayed here.
- **Bind:** Click it to bind all the valid IP and MAC address pairs in the list box.

Also you can manually create one or more IP/MAC bindings, the operation is as follows: Add one or more IP/MAC address pair entries in the list box, and then click the **Bind** button. The input contents are: IP Address, MAC Address and Description, one address pair entry per line; and the input format of an address pair entry is: IP Address<Space>MAC Address<Space>Description<Enter>. Note that **Description** is an optional parameter.

12.2.3 IP/MAC Binding Global Setup



The screenshot displays the 'IP/MAC Binding Global Setup' interface. At the top, there are two tabs: 'IP/MAC Binding List' and 'IP/MAC Binding Settings'. The 'IP/MAC Binding Settings' tab is selected and highlighted in yellow. Below the tabs, there is a checked checkbox labeled 'Allow Undefined LAN PCs', a 'Save' button, and a blue link labeled 'Export IP/MAC Binding Script'.

Figure 12-6 IP/MAC Binding Global Setup

- ✧ **Allow Undefined LAN PCs:** It allows or blocks the undefined LAN hosts from accessing the Device and access the Internet through the Device. If you want to allow the undefined LAN hosts to access the Device and Internet, select this check box; else unselect it. For more information about undefined LAN hosts, please refer to **section 12.2.1.2 Operation Principle of IP/MAC Binding**.
- **Save:** Click it to save the IP/MAC binding global setup.
- **Export IP/MAC Binding Script:** Click it to download the IP/MAC binding (that is, static ARP binding) script file to the local host. Then run the file and restart the host to add all the static ARP entries to the host to prevent ARP spoofing.



Note

If you want to unselect the **Allow Undefined LAN PCs** check box to block the undefined LAN hosts from accessing or passing through the Device, you should make sure that you have added the IP/MAC address pair of the host that you use to administer the Device into the **IP/MAC Binding List**.

12.2.4 IP/MAC Binding List

ID	Description	IP Address	MAC Address	Allow Internet Access	Edit
<input type="checkbox"/> 2	test1	192.168.16.65	0015c567410f	<input checked="" type="checkbox"/>	Edit
<input type="checkbox"/> 3	test2	192.168.16.66	0022aa112231	<input checked="" type="checkbox"/>	Edit
<input type="checkbox"/> 4	test3	192.168.16.99	0022aa223311	<input checked="" type="checkbox"/>	Edit

Select All

Figure 12-7 IP/MAC Binding List

- **Add an IP/MAC Binding:** If you want to add a new IP/MAC binding, click the **New** button or select the **IP/MAC Binding Settings** tab to go to the setup page, and then configure it, lastly click the **Save** button.
- **Edit an IP/MAC Binding:** If you want to modify a configured IP/MAC binding, click its **Edit** hyperlink, the related information will be displayed in the setup page. Then modify it, and click the **Save** button. The **Allow Internet Access** check box is used to allow or block a user matching an IP/MAC binding from accessing the Device and Internet. If you want to allow the user matching an IP/MAC binding to access the Device and Internet, select its check box; else unselect it.
- **Delete IP/MAC Binding(s):** If you want to delete one or more IP/MAC bindings, select the leftmost check boxes of them, and then select **Delete** from the drop-down list on the lower right corner of the **IP/MAC Binding List**, lastly click the **OK** button.
- **Delete All:** If you want to delete all the IP/MAC bindings at a time, select **Delete All** from the drop-down list on the lower right corner of the list, and then click the **OK** button.

12.2.5 How to Add the IP/MAC Bindings

If you want to add one or more IP/MAC bindings, do the following:

- Step 1** Go to the **Security > IP/MAC Binding** page, and then click the **New** button or select the **IP/MAC Binding Settings** tab to go to the setup page.

- Step 2** There are two methods to add IP/MAC bindings:
- 1) **Method One:** Click the **Scan** button to learn current dynamic ARP information (that is, IP and MAC address pairs) of the LAN hosts, and then click the **Bind** button to bind all the valid IP and MAC address pairs in the list box.
 - 2) **Method Two:** You can manually add one or more IP/MAC address pairs in the list box, and then click the **Bind** button to bind these IP/MAC address pairs. Refer to **section 12.2.2 IP/MAC Binding Settings** for more information.
- Step 3** After you have created some IP/MAC bindings, you can view them in the **IP/MAC Binding List**.
- Step 4** If you want to block the undefined LAN hosts from accessing the Device and Internet, please unselect the **Allow Undefined LAN PCs** check box; else, the undefined LAN hosts are allowed to access the Device and Internet.
- Step 5** If you want to temporarily block a user matching an IP/MAC binding from accessing the Device and Internet, please unselect its **Allow Internet Access** check box.

After you have finished configuring IP/MAC binding feature, when receiving a packet initiated from LAN, the Device will firstly compare the packet with the bindings in the **IP/MAC Binding List**, and then process the packet according to the related configuration. The packet will be allowed to pass or be dropped immediately. If it is allowed to pass, the packet will be further processed by the firewall access control function module.

12.2.6 Internet Whitelist and Blacklist

12.2.6.1 Introduction to Internet Whitelist and Blacklist Based on IP/MAC Binding

By utilizing IP/MAC binding feature, you can flexibly configure an Internet whitelist or blacklist for the LAN users.

If you want to allow only a small number of LAN users to access the Internet, you can configure an Internet whitelist for these users. Then only the users that belong to the whitelist can access the Internet, and all the other users can not access.

If you want to block only a small number of LAN users from accessing the Internet, you

can configure an Internet blacklist for these users. Then only the users that belong to the blacklist cannot access the Internet, and all the other users can access.

On the Device, a user who belongs to the whitelist is a legal user, that is, the user's IP and MAC address pair matches an IP/MAC binding whose **Allow Internet Access** check box is selected.

A user who belongs to the blacklist is an illegal user, that is, the user's IP and MAC address pair matches an IP/MAC binding whose **Allow Internet Access** check box is unselected; or the IP address or MAC address is the same with an IP/MAC binding's, but not both.

12.2.6.2 How to Configure an Internet Whitelist

If you want to configure an Internet whitelist, do the following:

Step 1 Go to the **Security > IP/MAC Binding** page, and then click the **New** button or select the **IP/MAC Binding Settings** tab to go to the setup page.

Step 2 Specify the legal users by creating the IP/MAC bindings: Add these users' IP and MAC address pairs into the **IP/MAC Binding List**. By default, an IP/MAC binding's **Allow Internet Access** check box is selected, which means that the user matching the IP/MAC binding can access the Device and Internet, so please leave it the default value. Refer to **section 12.2.2 IP/MAC Binding Settings** for detailed operation.

Step 3 Unselect the **Allow Undefined LAN PCs** check box to block all the undefined users from accessing the Device and Internet.

For example, if you want to allow a LAN user with IP address 192.168.16.68 and MAC address 0015c5674109 to access the Device and Internet, you can add an IP/MAC binding for he/her into the **IP/MAC Binding List**, see Figure 12-8. The binding's **Allow Internet Access** check box is selected by default, so please leave it the default value.

ID	Description	IP Address	MAC Address	Allow Internet Access	Edit
5	Legal1	192.168.16.68	0015c5674109	<input checked="" type="checkbox"/>	Edit

Figure 12-8 IP/MAC Binding List - Example Three

12.2.6.3 How to Configure Internet Blacklist

If you want to configure an Internet blacklist, do the following:

Step 1 Go to the **Security > IP/MAC Binding** page, and then click the **New** button or select the **IP/MAC Binding Settings** tab to go to the setup page.

Step 2 Specify the illegal users by creating the IP/MAC bindings. There are three methods:

- 1) **Method One:** Bind each illegal user's IP address to a MAC address which is different from any LAN host's in the **IP/MAC Binding List**. Refer to **section 12.2.2 IP/MAC Binding Settings** for detailed operation.
- 2) **Method Two:** Bind an IP address which is different from any LAN host's to each illegal user's MAC address in the **IP/MAC Binding List**.
- 3) **Method Three:** Add these users' IP and MAC address pairs in the **IP/MAC Binding List**. Unselect each IP/MAC binding's **Allow Internet Access** check box respectively, then the matched users can not access the Device and Internet.

Step 3 Select the **Allow Undefined LAN PCs** check box to allow all the undefined users to access the Device and Internet.

For example, if you want to block a LAN user with IP address 192.168.16.68 and MAC address 0015c5674109 from accessing the Device and Internet, you can add the corresponding IP/MAC binding in the **IP/MAC Binding List**. And then unselect the binding's **Allow Internet Access** check box to block the user's access to the Device and Internet, see Figure 12-9.

1/500 Lines/Page: 10 First Prev Next Last Search:

ID	Description	IP Address	MAC Address	Allow Internet Access	Edit
<input type="checkbox"/> 5	Legal1	192.168.10.68	0015c5674109	<input type="checkbox"/>	<input type="button" value="Edit"/>

Select All

Figure 12-9 IP/MAC Binding List - Example Four

12.3 Firewall

This section describes the **Security > Firewall** page, which includes the **Access Control List** and **ACL Settings** subpages.

The access control rules that you have created will be listed in the **Access Control List**. Note that by default the rules are listed in reverse chronological order of creation, and it allows you to manually move a rule to a different position in the list.

12.3.1 Introduction to Access Control

12.3.1.1 The Purpose of Access Control Feature

The development of Internet has brought some side effects, such as the emergence of gambling, pornography, and other illegal websites which are contrary to the state laws and regulations; broadband network provide fast surfing to the Internet users, while fast spreading worms cause great threat to the Internet users. So if an organization wants to access the Internet, it needs specific Internet access rules. Such as, a government organization wants to block the civil servants from accessing stock websites, using IM messenger applications; a business wants to block the employees from accessing game websites and other services which are unrelated to work during working time; parents want to control their children's online time; an network administrator wants to block the worms and hacker attacks.

To achieve these purposes, we develop and implement access control feature on the Device. By utilizing access control feature flexibly, you can not only assign different Internet access privileges to different LAN users, but also assign different Internet access privileges to the same users based on schedules. In practice, you can set appropriate access control rules according to the actual requirements of your organization. Such as, for a school, you can block the students to access game websites; for a family, you can only allow your children to access the Internet during the specified period of time; for a business, you can block the Financial Department's employees from accessing the Internet.

12.3.1.2 The Operation Principle of Access Control

By default, as no access control rule exists on the Device, the Device will forward all the

valid packets received by the LAN interface. After you have enabled access control, the Device will examine each packet received by the LAN interface to determine whether to forward or drop the packet, based on the criteria you specified in the access control rules.

When receiving a packet initiated from LAN, the Device will analyze the packet by extracting its source MAC address, source IP address, destination IP address, protocol type (TCP, UDP or ICMP), port number, content, and the date and time at which the packet was received, and then compare them with each rule in the order in which the rules are listed in the **Access Control List**. The first rule that matches the packet will be applied to the packet, and the Device will forward or drop it according to this rule's action. Note that after a match is found, no further rules will be checked; and if no match is found, the Device will drop the packet to ensure security.

The access control rules are applied to the packets that are received by the Device's LAN interface, that is, those packets that arrive on the LAN interface and then go through the Device. If a packet matches a rule whose **Action** is **Allow**, the packet will be allowed to pass, and then be further processed by route, NAT and other modules. Else, if the packet matches a rule whose **Action** is **Drop**, or doesn't match any rule, the packet will be dropped immediately. As these dropped packets are no longer further processed by route, NAT and other modules, it will reduce CPU load and improve the Device performance.

12.3.1.3 The Action of an Access Control Rule

The action of an access control rule is either **Allow** or **Deny**. When receiving a packet that matches a rule in the **Access Control List**, the Device will forward the packet if the rule's action is **Allow**; else the Device will drop it.

12.3.1.4 The Execution Order of Access Control Rules

The order of access control rules is very important. When receiving a packet initiated from LAN, the Device will search **Access Control List** to find out if there is a rule that matches the packet. It will check the packet against each rule in the order in which the rules are listed. After a match is found, no further rules will be checked. If no match is found, the Device will drop the packet to ensure security. Note that by default the rules are listed in reverse chronological order of creation, the later the rule is created, the upper the rule is listed; and the Device allows you to manually move a rule to a different position in the list.

Because the Device will allow or deny a packet to pass according to the first rule that matches the packet, you should arrange the rules in **Access Control List** from specific to general. For example, if you create an access control rule at the beginning that explicitly allows all packets to pass, no further rules are ever checked. Another example is that if

you only allow a LAN user to access Web service, and block any other service, then the rule that allows the user to access Web service should be listed above the rule that denies the user to access any other service.

12.3.1.5 Address Group and Service Group

On the Device, you can create the IP address groups in the **Security > Address Group** page or service groups in the **Security > Service Group** page firstly, and then reference them by name in the source or destination address group, or service group fields of access control rules.

1. Address Group

Using address groups can facilitate the configuration of access control rules. For example, if some LAN hosts' IP addresses are discontinuous, but the hosts have the same privileges of accessing the Internet, you can create an address group for these hosts. Then you only need to create one access control rule by using the address group to meet the hosts' requirements. Else you need to create multiple access control rules for these hosts. Refer to **section 12.6 Address Group** for more information about address group.

2. Service Group

The service group is used to match the source MAC address, protocol type (TCP, UDP or ICMP), port number and content of the packets that are received by the Device. Using service groups can facilitate the configuration of access control rules. For example, you can add telnet, pop3 and http services into a service group, and then create one rule by using the service group to control the access to these services. Else, you need to create multiple access control rules for the access to these services, one rule per service. Refer to **section 12.7 Service Group** for more information about service group.

12.3.1.6 System Default Access Control Rules

Besides user-defined access control rules, the Device will automatically created some system default access control rules in the **Access Control List**. The following table describes the purposes of these rules.

ID	Description
----	-------------

lan	It is used to allow the LAN users to access the Device's LAN interface. And it is the first rule, but it is implicit and not displayed in the list.
dns	It is used to allow the DNS packets to pass by default.
dhcp	It is used to allow the DHCP packets to pass by default.
pass	It is a global rule for IP packets. By default, it is used to allow all the IP packets to pass. And it is always listed and displayed at the bottom of the list.
generic	It is a global rule which is used to allow all the packets including non-IP packets to pass. And it is the last rule, but it is implicit and not displayed in the list.

Table 12-1 The System Default Access Control Rules



Note

You cannot delete the system default access control rules in the **Access Control List**, and cannot modify its parameters except **Action**.

12.3.2 Access Control Rule Settings

Before creating the access control rules, you may do the following tasks:

- Go to the **Security > Address Group** page to create the address groups that will be referenced by the rules.
- Go to the **Security > Service Group** page to create the service groups that will be referenced by the rules.
- Go to the **Security > Schedule** page to create the schedules that will be referenced by the rules.

Also, you can directly specify the source or destination IP addresses, or services of access control rules in this page. The following describes the definitions of a rule's parameters.

The screenshot displays the configuration interface for a Firewall Rule, organized into three main sections: Action, Address, and Service.

- Action:** A dropdown menu is set to "Allow".
- Schedule:** A dropdown menu is set to "Always", with a link to "Edit Schedule".
- Description:** A text input field is currently empty.
- Address:**
 - Source:** The "Addresses From" radio button is selected. It shows two input fields for IP ranges. The "Address Group" radio button is unselected, with a dropdown menu showing "Any Address" and a link to "Edit Address Group".
 - Destination:** The "Addresses From" radio button is unselected. The "Address Group" radio button is selected, with a dropdown menu showing "Any Address" and a link to "Edit Address Group".
- Service:**
 - The "Ports From" radio button is unselected, showing two input fields for port ranges.
 - The "Service Group" radio button is selected, with a dropdown menu showing "Any Service" and a link to "Edit Service Group".
 - The "Protocol" dropdown menu is set to "TCP".

A "Save" button is located at the bottom right of the configuration area.

Figure 12-10 Access Control Rule Settings

- ✧ **Action:** It determines the action of the access control rule. There are two available options:
 - **Allow:** It indicates that the Device will allow the packets that match the rule to pass, that is, the Device will forward these packets.
 - **Deny:** It indicates that the Device will deny the packets that match the rule to pass, that is, the Device will drop these packets.
- ✧ **Schedule:** It specifies a schedule to restrict when the access control rule is in effect. The default value is **Always**, which means the access control rule is in effect always. Note that after the selected schedule has expired, the rule will be in effect always.
- ✧ **Description:** It specifies the description of the access control rule. It is usually used to describe the purpose of the rule.

- ✧ **Source:** It specifies the source IP addresses of the packets to which the access control rule applies. There are two options:
 - **Addresses:** Select it to enter the start and end addresses in the associated text boxes.
 - **Address Group:** Select it to choose an address group from the associated drop-down list. By default, the **Address Group** radio button is selected, and its value is **Any Address**.

- ✧ **Destination:** It specifies the destination IP addresses of the packets to which the access control rule applies. There are two options: **Addresses** and **Address Group**.
 - **Addresses:** Select it to enter the start and end addresses in the associated text boxes.
 - **Address Group:** Select it to choose an address group from the associated drop-down list. By default, the **Address Group** radio button is selected, and its value is **Any Address**.

- ✧ **Service:** It specifies a range of ports or a service group to which the access control rule applies. There are two options:
 - **Ports:** Select it to enter the start and end port numbers in the associated text boxes, and select a protocol type from **Protocol** drop-down list. The port number is between 1 and 65535, and the protocols include **TCP**, **UDP** and **ICMP**.
 - **Service Group:** Select it to choose a service group or predefined service from the associated drop-down list. The Device provides some well-known services, such as telnet, smtp, web, pop3, and so on. By default, the **Service Group** radio button is selected, and its value is **Any Service**.

- **Edit Schedule:** Click it to go to the **Security > Schedule** page to add, view, modify or delete schedules.
- **Edit Address Group:** Click it to go to the **Security > Address Group** page to add, view, modify or delete address groups.
- **Edit Service Group:** Click it to go to the **Security > Service Group** page to add, view, modify or delete service groups.
- **Save:** Click it to save the access control rule settings.

**Note**

You can create the IP address groups in the **Security > Address Group** page or service groups in the **Security > Service Group** page firstly, and then reference them by name in the source or destination address group, or service group fields of access control rules. And if the addresses or service ports are consecutive, you also can directly specify the source or destination IP addresses, or services of rules in this page.

12.3.3 Enable Access Control

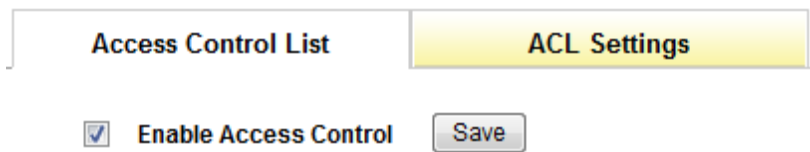


Figure 12-11 Enable Access Control

- ✧ **Enable Access Control:** It allows you to enable or disable firewall access control. If you select the check box to enable this feature, the configured access control rules will take effect. Else the rules will be of no effect.
- **Save:** Click it to save your settings.

12.3.4 Access Control List

ID	Action	Schedule	Source IP Address	Destination IP Address	Service	Description	Edit
<input type="checkbox"/> dns	Allow					dns	Edit
<input type="checkbox"/> dhcp	Allow					dhcp	Edit
<input type="checkbox"/> 1	Allow	worktime	TD_FD	Any Address	WEB_FTP	Allow TD_FD	Edit
<input type="checkbox"/> 2	Deny	worktime	TD_FD	Any Address	Any Service	Deny TD_RD	Edit
<input type="checkbox"/> pass	Allow					pass	Edit

5/298 Lines/Page: 10 First Prev Next Last Search:

Select All

Move 1 before dns

Figure 12-12 Access Control List

- **Add an Access Control Rule:** If you want to add a new access control rule, click the **New** button or select the **ACL Settings** tab to go to the setup page, and then configure it, lastly click the **Save** button.
- **View Access Control Rule(s):** When you have configured some access control rules, you can view them in the **Access Control List**.
- **Edit an Access Control Rule:** If you want to modify a configured access control rule, click its **Edit** hyperlink, the related information will be displayed in the setup page. Then modify it, and click the **Save** button.
- **Move an Access Control Rule:** The Device allows you to move an access control rule to above another rule in the list, the operation is as follows: Select the ID of a rule that you want to move from the **Move** drop-down list, and another rule's ID from the **before** drop-down list, lastly click the **OK** button. Note: Moving a rule in the list doesn't change its ID number.
- **Delete Access Control Rule(s):** If you want to delete one or more access control rules, select the leftmost check boxes of them, and then click the **Delete** button.

**Note**

1. The user-defined access control rule whose **Service** is set to **dns** will be automatically listed above the system default access control rule **dns**.
2. The system default access control rule **pass** is always listed in the bottom of the **Access Control List**, you cannot move it.
3. You cannot delete the system default access control rules in the **Access Control List**, and cannot modify its parameters except **Action**.

12.3.5 Configuration Examples for Access Control

12.3.5.1 Example One

1. Requirements

In this example, a business has four departments: Technology Department, Customer Service Department, Financial Department and Sales Department.

The IP address ranges of the departments are as follows:

- Technology Department: 192.168.16.2~192.168.16.30

- Customer Service Department: 192.168.16.31~192.168.16.60
- Financial Department: 192.168.16.61~192.168.16.70
- Sales Department: 192.168.16.71~192.168.16.100

The CEO wants to control Internet behaviors of the Technology and Financial Departments' employees:

1. Allow them to access WEB and FTP services during working time.
2. Deny them to access all other services during working time.
3. Allow them to access any service during rest periods.

Besides, he wants to allow any other employee to access any service at any time.

The working time is: Monday to Friday, 9:00 to 12:00 am, and 1:00 to 6:00 pm.

2. Analysis

We need to use two user-defined access control rules together with the default rule **pass** to meet requirements:

- User-defined rule 1: It is used to allow the Technology and Financial Departments' employees to access WEB and FTP services during working time.
- User-defined rule 2: It is used to deny any employee to access any service during working time.
- Default rule **pass**: It allows all the IP packets to pass by default.

3. Configuration Procedure

1) Configuring Access Control Rule 1

Step 1 Go to the **Security > Schedule > Schedule Settings** page to create a schedule for working time. Here we assume its name is **work**, see Figure 12-13. Refer to **section 12.8.5 Configuration Example for Schedule** for detailed operation.

Policy List | **Schedule Settings**

Schedule Name

Start Date End Date

Period	Days of the Week	Daily Start Time	Daily End Time
Period 1	<input type="text" value="Weekdays (Mon-Fri)"/>	<input type="text" value="09:00:00"/>	<input type="text" value="11:59:59"/>
Period 2	<input type="text" value="Weekdays (Mon-Fri)"/>	<input type="text" value="13:00:00"/>	<input type="text" value="17:59:59"/>
Period 3	<input type="text" value=""/>	<input type="text" value="00:00:00"/>	<input type="text" value="23:59:59"/> <input type="button" value="+"/>

Figure 12-13 The Schedule of work Settings - Example 1

Step 2 Go to the **Security > Address Group > Address Group Settings** page to create an address group for the Technology and Financial Departments' employees. It includes two address ranges: one is from 192.168.16.2 to 192.168.16.30, the other is from 192.168.16.61 to 192.168.16.70, and here we assume its name is **TD_FD**, see Figure 12-14.

Group List | **Address Group Settings**

Name

Zone

New Existing

Start Address:

End Address:

Address Members:

192.168.16.2-192.168.16.30
192.168.16.61-192.168.16.70

Figure 12-14 The Address Group of TD_FD Settings - Example 1

Step 3 Go to the **Security > Service Group > Service Group Settings** page to configure a service group which includes two services: one is web, the other is ftp, and here we assume its name is **WEB_FTP**, see Figure 12-15.

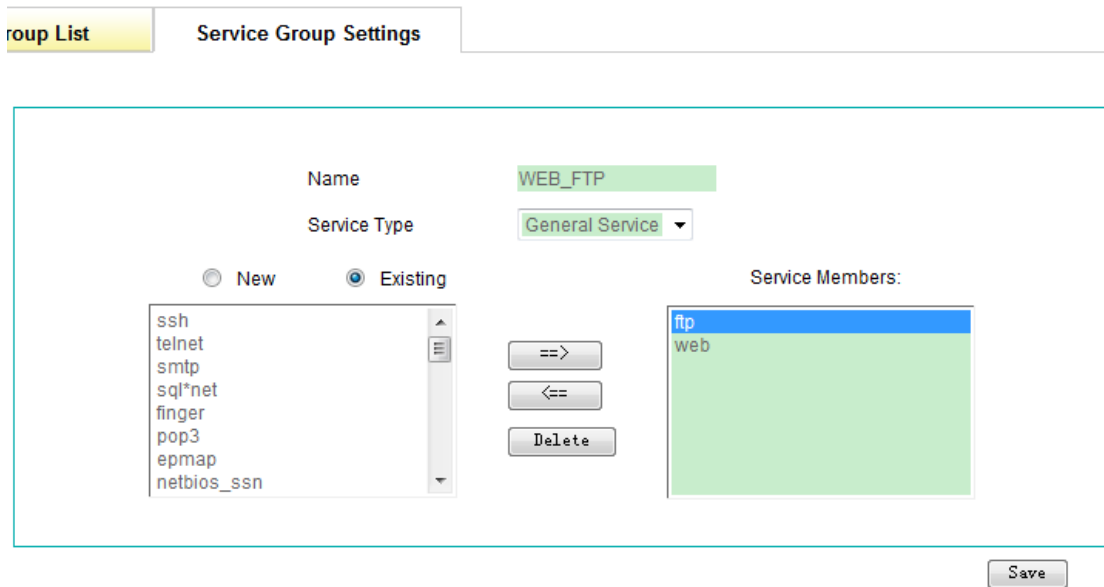


Figure 12-15 The Service Group of WEB_FTP Settings - Example 1

Step 4 Go to the **Security > Firewall > ACL Settings** page to configure rule 1, see Figure 12-16: select **Allow** from the **Action**, select **work** from the **Schedule**, select **TD_FD** from the **Source Address Group** drop-down list, select **Any Address** from the **Destination Address Group** drop-down list, and select **WEB_FTP** from the **Service Group** drop-down list, lastly click the **Save** button to save the settings.

F i r e w a l l R u l e	Action <input type="text" value="Allow"/>
	Schedule <input type="text" value="work"/> Edit Schedule
	Description <input type="text" value="Allow WEB_FTP"/>
A d d r e s s	Source <input type="radio"/> Addresses From <input type="text"/> To <input type="text"/> <input checked="" type="radio"/> Address Group <input type="text" value="TD_RD"/> Edit Address Group
	Destination <input type="radio"/> Addresses From <input type="text"/> To <input type="text"/> <input checked="" type="radio"/> Address Group <input type="text" value="Any Address"/> Edit Address Group
S e r v i c e	Service <input type="radio"/> Ports From <input type="text"/> To <input type="text"/> Protocol <input type="text" value="TCP"/> <input checked="" type="radio"/> Service Group <input type="text" value="WEB_FTP"/> Edit Service Group
	<input type="button" value="Save"/>

Figure 12-16 The Access Control Rule 1 Settings - Example 1

2) **Configuring Access Control Rule 2**

Go to the **Security > Firewall > ACL Settings** page to create rule 2, see Figure 12-17: select **Deny** from the **Action**, select **work** from the **Schedule**, select **TD_FD** from the **Source Address Group** drop-down list, select **Any Address** from the **Destination Address Group** drop-down list, and select **Any Service** from the **Service Group** drop-down list, lastly click the **Save** button to save the settings.

F i r e w a l l R u l e	Action <input type="text" value="Deny"/>
	Schedule <input type="text" value="work"/> Edit Schedule
	Description <input type="text" value="Deny Other Services"/>
A d d r e s s	Source <input type="radio"/> Addresses From <input type="text" value=""/> To <input type="text" value=""/> <input checked="" type="radio"/> Address Group <input type="text" value="TD_FD"/> Edit Address Group
	Destination <input type="radio"/> Addresses From <input type="text" value=""/> To <input type="text" value=""/> <input checked="" type="radio"/> Address Group <input type="text" value="Any Address"/> Edit Address Group
S e r v i c e	Service <input type="radio"/> Ports From <input type="text" value=""/> To <input type="text" value=""/> Protocol <input type="text" value="TCP"/> <input checked="" type="radio"/> Service Group <input type="text" value="Any Service"/> Edit Service Group
	<input type="button" value="Save"/>

Figure 12-17 The Access Control Rule 2 Settings - Example 1

3) Enabling Access Control

You should enable access control feature to let access control rules take effect, see Figure 12-18.

Access Control List	ACL Settings
<input checked="" type="checkbox"/> Enable Access Control	<input type="button" value="Save"/>

Figure 12-18 Enable Access Control - Example 1

12.3.5.2 Example Two

1. Requirements

A company uses the Device as a network access device. The requirements are as follows:

- 1) Block an outside user with IP address 202.106.11.22 from attacking a LAN user with

IP address 200.200.200.251 maliciously;

- 2) Block all the LAN users from accessing the websites which contain illegal content. Here we take pornography for example.

2. Analysis

We need to create two access control rules to meet requirements:

- Rule 1: It is used to protect the LAN user with IP address 200.20.200.251 against attack from outside IP address 202.106.11.22.
- Rule 2: It is used to block all the LAN users from accessing the websites which contain pornography.

3. Configuration Procedure

1) Configuring Access Control Rule 1

Step 1 Go to the **Security > Address Group > Address Group Settings** page to configure two address groups for the LAN user and outside user respectively, see the following two figures: One includes the single IP address 200.200.200.251, the other includes the single IP address 202.106.11.22, and here we assume their names are **Inside** and **Outside** respectively.

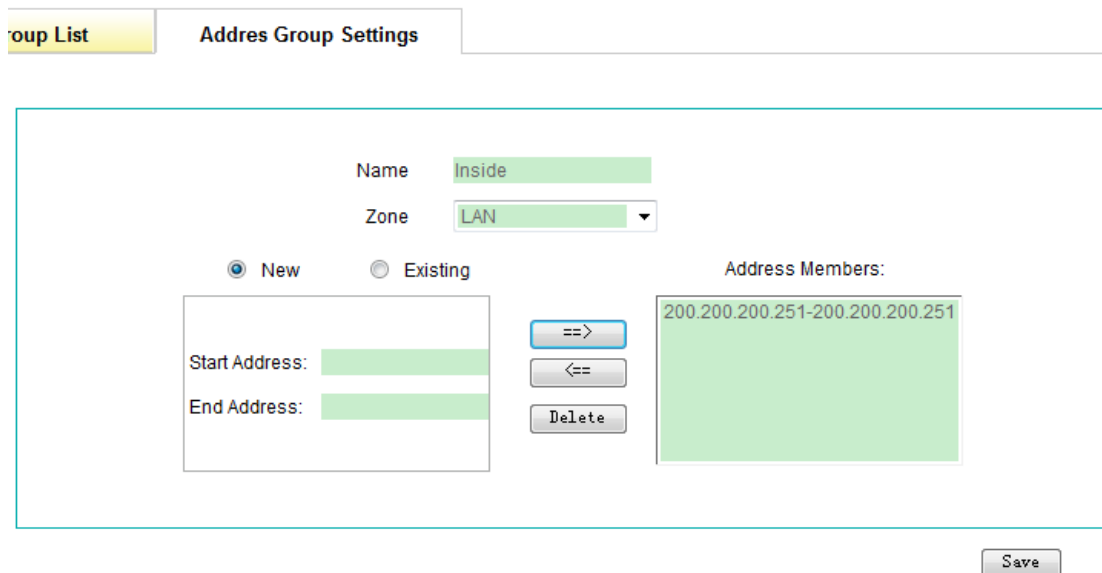


Figure 12-19 The Address Group of Inside Settings - Example 2

Group List Address Group Settings

Name:

Zone:

New Existing

Start Address:

End Address:

==>

<==

Delete

Address Members:

202.106.11.22-202.106.11.22

Figure 12-20 The Address Group of Outside Settings - Example 2

Step 2 Go to the **Security > Firewall > ACL Settings** page to configure rule 1, see Figure 12-21: select **Deny** from the **Action**, select **Always** from the **Schedule**, select **Inside** from the **Source Address Group** drop-down list, select **Outside** from the **Destination Address Group** drop-down list, and select **Any Service** from the **Service Group** drop-down list, lastly click the **Save** button to save the settings.

F i r e w a l l R u l e	Action <input type="text" value="Deny"/>
	Schedule <input type="text" value="Always"/> Edit Schedule
	Description <input type="text" value="Rule 1"/>
A d d r e s s	Source <input type="radio"/> Addresses From <input type="text"/> To <input type="text"/> <input checked="" type="radio"/> Address Group <input type="text" value="Inside"/> Edit Address Group
	Destination <input type="radio"/> Addresses From <input type="text"/> To <input type="text"/> <input checked="" type="radio"/> Address Group <input type="text" value="Outside"/> Edit Address Group
S e r v i c e	Service <input type="radio"/> Ports From <input type="text"/> To <input type="text"/> Protocol <input type="text" value="TCP"/> <input checked="" type="radio"/> Service Group <input type="text" value="Any Service"/> Edit Service Group
	<input type="button" value="Save"/>

Figure 12-21 The Access Control Rule 1 Settings - Example 2

2) Configuring Access Control Rule 2

Step 1 Go to the **Security > Service Group** page, enter **Pornography** in the **Name** text box, select **Keyword** from the **Service Type** drop-down list, select the **New** radio button, enter **pornography** in the **Keyword** text box, and then click **==>** to move the specified keyword to the **Service Members** list box, lastly click the **Save** button.

Group List | Service Group Settings

Name: Pornography

Service Type: Keyword

New Existing

Keyword:

==>

<==

Delete

Service Members:

K(pornography)

Figure 12-22 The Access Control Rule 2 Settings - Example 2

Step 2 Go to the **Security > Firewall > ACL Settings** page to create rule 2, see Figure 12-23: select **Deny** from the **Action**, select **Always** from the **Schedule**, select **Any Address** from the **Source Address Group** drop-down list, select **Any Address** from the **Destination Address Group** drop-down list, and select **Pornography** from the **Service Group** drop-down list, lastly click the **Save** button to save the settings.

F i r e w a l l R u l e	Action <input type="text" value="Deny"/>
	Schedule <input type="text" value="Always"/> Edit Schedule
	Description <input type="text" value="Rule 2"/>
A d d r e s s	Source <input type="radio"/> Addresses From <input type="text" value=""/> To <input type="text" value=""/> <input checked="" type="radio"/> Address Group <input type="text" value="Any Address"/> Edit Address Group
	Destination <input type="radio"/> Addresses From <input type="text" value=""/> To <input type="text" value=""/> <input checked="" type="radio"/> Address Group <input type="text" value="Any Address"/> Edit Address Group
S e r v i c e	Service <input type="radio"/> Ports From <input type="text" value=""/> To <input type="text" value=""/> Protocol <input type="text" value="TCP"/> <input checked="" type="radio"/> Service Group <input type="text" value="Pornography"/> Edit Service Group
	<input type="button" value="Save"/>

Figure 12-23 The Access Control Rule 2 Settings - Example 2

3) Enabling Access Control

You should enable access control feature to make the configured access control rules take effect, see Figure 12-24.

Access Control List	ACL Settings
<input checked="" type="checkbox"/> Enable Access Control	<input type="button" value="Save"/>

Figure 12-24 Enable Access Control - Example 2

12.4 Domain Filtering

This section describes the **Security > Domain Filtering** page.

12.4.1 Domain Filtering Settings

Domain Filtering Settings Domain Blocking Notice

Enable Domain Filtering

Filtering Mode Only Block Domain Names in Domain Name List
 Only Allow Domain Names in Domain Name List

Domain Name List
www.twitter.com
www.facebook.com

Save

Figure 12-25 Domain Filtering Settings

- ✧ **Enable Domain Filtering:** It allows you to enable or disable domain filtering. If you select the check box to enable domain filtering, the configured domain filtering entries will take effect. Else, the domain filtering entries will be of no effect.
- ✧ **Filtering Mode:** It specifies the mode of domain filtering. There are two available options:
 - **Only Block Domain Names in Domain Name List:** It indicates that the Device will block the LAN users from accessing the domain names in the **Domain Name list**, but allow the users to access any other domain names.
 - **Only Allow Domain Names in Domain Name List:** It indicates that the Device will allow the LAN users to access the domain names in the **Domain Name list**, but block the users from accessing any other domain names.
- ✧ **Domain Name List:** It specifies the domain names that will be blocked or allowed according to the **Filtering Mode**. You can create up to 100 domain names in the list.

- **Save:** Click it to save the domain filtering settings.

**Note**

1. The matching rule of domain filtering is whole words matching, that is, only a domain name matches the whole words of the domain name in the **Domain Name List**, the Device will block or allow it according to the **Filtering Mode**.
2. You can use the wildcard "*" in a domain name to match multiple domain names. For example, if you have created [www.163.*](#) in the **Domain Name List**, then all the domain names that begin with [www.163.](#) will be blocked or allowed according to the **Filtering Mode**.

12.4.2 Domain Blocking Notice

This section describes the **Security > Domain Filtering > Domain Blocking Notice** page.

When domain blocking notice is enabled, if a LAN user accesses a domain name which is blocked by the Device, the Device will pop up a notice message to remind the user that the website is blocked rather than network problems.

Domain Filtering | **Domain Blocking Notice**

Enable Domain Blocking Notice

Notice Title

Redirecting Time s

Signature

Redirecting URL

Notice Content

Hello,
The website that you want to access is blocked by the Device. Please try to access another website.
If you have any questions, please contact the administrator.

Figure 12-26 Domain Blocking Notice

- ✧ **Enable Domain Blocking Notice:** It allows you to enable or disable domain blocking notice. If you want to enable domain blocking notice, please select this check box. In this case, if a LAN user accesses a domain name which is blocked by the Device, the Device will pop up a notice message to remind the user. And the requested web page will automatically jump to the specified web page (set by the **Redirecting URL**) after the specified time interval (set by the **Redirecting Time**).
- ✧ **Notice Title:** It specifies the title of the notice message.
- ✧ **Redirecting Time:** It specifies the time interval after which the requested web page will jump to the specified web page. 0 means that the requested web page will immediately jump to the specified web page. Leave it blank if you don't want the requested web page to jump to any other web page.
- ✧ **Signature:** It specifies the signature of the notice message.
- ✧ **Redirecting URL:** It specifies the redirecting URL to which the requested web page will jump. Leave it blank if you don't want the requested web page to jump to any other web page.
- ✧ **Notice Content:** It specifies the content of the notice message.

- **Save:** Click it to save domain blocking notice settings.
- **Preview:** Click it to preview the notice message you just configured. The following figure shows an example of a notice message.



Figure 12-27 Domain Name Blocking Notice Preview

 **Note**

Only after you have enabled domain filtering and chosen the **Only Block Domain Names in Domain Name List** as the filtering mode, the Device will pop up the domain blocking notice messages to the LAN users.

12.5 NAT Session Limit

This section describes the **Security > NAT Session Limit** page.

The NAT session limit feature allows you to limit the maximum number of concurrent NAT sessions based on the LAN hosts. And it allows you to specify different maximum NAT sessions for different LAN hosts. Furthermore, it allows you to limit the maximum number of concurrent TCP sessions, UDP sessions and ICMP sessions respectively.

12.5.1 NAT Session Limit Rule Settings

Limit List	Session Limit Settings
IP Addresses	192.168.16.100 To 192.168.16.150
Max. Sessions	500
Max. TCP Sessions	500
Max. UDP Sessions	50
Max. ICMP Sessions	50
Description	SD
<input type="button" value="Save"/>	

Figure 12-28 NAT Session Limit Rule Settings

- ✧ **IP Addresses** and **To**: They specify the start IP address and end IP address of the LAN hosts to which the NAT session limit rule applies. Please enter the start IP address in the first text box, and the end IP address in the second text box. The Device provides a default NAT session limit rule. Its start IP address and end IP address both are 0.0.0.0, which means that the default rule applies to all the IP addresses. You can modify its parameters except **IP Addresses**, but cannot delete it.
- ✧ **Max. Sessions**: It specifies the maximum number of concurrent sessions per restricted host.
- ✧ **Max. TCP Sessions**: It specifies the maximum number of concurrent TCP sessions per restricted host.
- ✧ **Max. UDP Sessions**: It specifies the maximum number of concurrent UDP sessions per restricted host.
- ✧ **Max. ICMP Sessions**: It specifies the maximum number of concurrent ICMP sessions per restricted host.
- ✧ **Description**: It specifies the description of the NAT session limit rule.
- **Save**: Click it to save the NAT session limit rule settings.



Note

1. When using NAT session limit function, the Device will search the **Session Limit List** to find out if there is a rule that matches a LAN host. It will check the host's IP address against each rule in the order in which the rules are listed. After a match is found, no further rules will be checked. Note that the rules are listed in reverse chronological order of creation, the later the rule is created, and the upper the rule is listed.
2. The start IP address should be less than or equal to the end IP address. The address ranges of different NAT session limit rules can overlap.
3. If some applications (such as online games) performance is degraded due to the maximum NAT sessions limit, you can increase the **Max. Sessions** and **Max. TCP sessions** (or **Max. UDP sessions**) properly. Note that if they are too large, it will lower or lose the Device's ability to prevent DDoS attacks.
4. In most cases, to ensure that the LAN users surf the Internet normally, the maximum NAT sessions cannot be too small. It is suggested that both the **Max. Sessions** and **Max. TCP sessions** should be larger than or equal to 100, the **Max. UDP sessions** should be larger than or equal to 50, and **Max. ICMP sessions** should be larger than or equal to 10.

12.5.2 NAT Session Limit Rule List

ID	Start Src.IP	End Src.IP	Enable	Max. Sessions	Max. TCP Sessions	Max. UDP Sessions	Max. ICMP Sessions	Description	Edit
2	192.168.16.100	192.168.16.150	<input checked="" type="checkbox"/>	500	500	50	50	SD	Edit
1	0.0.0.0	0.0.0.0	<input checked="" type="checkbox"/>	2500	2200	2200	100	Default Session Limit	Edit

Figure 12-29 NAT Session Limit Rule List

- **Add a NAT Session Limit Rule:** If you want to add a new NAT session limit rule, click the **New** button or select the **Session Limit Settings** tab to go to the setup page, and then configure it, lastly click the **Save** button.

- **Enable a NAT Session Limit Rule:** The **Enable** check box is used to enable or disable the corresponding NAT session limit rule. The default value is selected, which means the NAT session limit rule is in effect. If you want to disable the NAT session limit rule temporarily instead of deleting it, please click it to remove the check mark.
- **View NAT Session Limit Rule(s):** When you have configured some NAT session limit rules, you can view them in the **Session Limit List**.
- **Edit a NAT Session Limit Rule:** If you want to modify a configured NAT session limit rule, click its **Edit** hyperlink, the related information will be displayed in the setup page. Then modify it, and click the **Save** button.
- **Delete NAT Session Limit Rule(s):** If you want to delete one or more NAT session limit rules, select the leftmost check boxes of them, and then click the **Delete** button.

12.6 Address Group

This section describes the **Security > Address Group** page.

12.6.1 Introduction to Address Group

An address group can contain up to ten address members. A member may be an address range or address group. And an address group may contain address ranges only, or address groups only, or both.

If you want to create an access control rule (in the **Security > Firewall** page) whose destination or source IP addresses are discontinuous, you can create an address group for them in this page firstly, and then reference it in the access control rule. When receiving a packet, if the packet's destination or source IP address belongs to the address group, the Device will consider that its IP address matches the access control rule. And if the packet also matches other criteria (protocol type, destination ports, schedule, etc.) of the access control rule, the Device will consider that the packet matches the access control rule.

Using address groups can facilitate the configuration of access control rules. For example, if some LAN hosts' IP addresses are discontinuous, but the hosts have the same privileges of accessing the Internet, you can create an address group for these hosts. Then you only need to create one access control rule by using the address group to meet the hosts' requirements. Else you need to create multiple access control rules for these hosts.

Similarly, you also can reference an address group in a rule limit rule in the **QoS > Rate Limit Rule** page.

12.6.2 Address Group Settings

The screenshot shows the 'Address Group Settings' configuration page. At the top, there are two tabs: 'Group List' and 'Address Group Settings'. The 'Address Group Settings' tab is active. The form contains the following elements:

- Name:** A text input field containing 'TD_LD'.
- Zone:** A dropdown menu showing 'LAN'.
- Radio Buttons:** Two radio buttons labeled 'New' (which is selected) and 'Existing'.
- Address Range:** Two text input fields: 'Start Address' with '192.168.16.61' and 'End Address' with '192.168.16.70'.
- Buttons:** Three buttons: '==>' (move right), '<==', and 'Delete'.
- Address Members:** A list box containing the address range '192.168.16.2-192.168.16.30'.
- Save:** A 'Save' button located at the bottom right of the form area.

Figure 12-30 Address Group Settings

- ✧ **Name:** It specifies a unique name of the address group. It should be between 1 and 11 characters long.
- ✧ **Zone:** It specifies a network zone to which the address group belongs.
- ✧ **New:** Select it to add a new address range to the group.
- ✧ **Existing:** Select it to display the configured address groups.
- ✧ **Address Members:** It displays the members of the address group. A member may be an address range or address group.
- **==>:** Click it to move the new address range or selected address group(s) to the **Address Members** list.
- **<==:** Click it to move the selected address member from the **Address Members** list box to the left editable list.
- **Delete:** Click it to delete the selected address member from the **Address Members** list box.
- **Save:** Click it to save the address group settings.



Note

the **Security > Firewall** page or rate limit rule in the **QoS > Rate Limit Rule** page. If you actually want to delete it, please remove all the references firstly.

12.6.4 How to Add the Address Groups

If you want to add one or more address groups, do the following:

- Step 1** Go to the **Security > Address Group** page, and then click the **New** button or select the **Address Group Settings** tab to go to the setup page.
- Step 2** Specify the **Name** of the address group.
- Step 3** Select the network zone from the **Zone** drop-down list.
- Step 4** Add IP addresses to the group. There are two methods to add them.
 - 1) Method One: Select the **New** radio button, enter the start and end IP addresses in the **Start Address** and **End Address** text boxes, and then click **=>** to move the new address range to the **Address Members** list box. You can continue to add another address ranges if needed.
 - 2) Method Two: Select the **Existing** radio button, select one or more configured address groups, and then click **=>** to move the selected address groups to the **Address Members** list box.
- Step 5** Click the **Save** button to save the settings. You can view the address group in the **Address Group List**.
- Step 6** If you want to add another new address group, please repeat the above steps.

12.6.5 How to Edit an Address Group

If you want to modify a configured address group, do the following:

- Step 1** Go to the **Security > Address Group** page.
- Step 2** Click the **Edit** hyperlink of the address group in the **Address Group List** to go to the setup page.
- Step 3** Modify the address members as required. There are two cases:
 - 1) If you want to modify an address range, select the address range in the **Address Members** list, click **<=>** to move it from the **Address Members**

list box to the left editable list, and then modify the **Start Address** and/or **End Address**, lastly click ==> to move the modified address range to the **Address Members** list box again.

- 2) If you want to delete an address member, select the member in the **Address Members** list box, and then click the **Delete** button.

Step 4 Click the **Save** button to save the changes to make them take effect.

12.7 Service Group

This section describes **Security > Service Group** page.

12.7.1 Introduction to Service Group

The Device provides five service types including general service, URL, Keyword, DNS and MAC address for the service group. Then the service groups can be used to match the protocol type (TCP, UDP or ICMP), port number, content, source MAC address of packets that are received by the Device. For each service type, it allows you to define new services, or select existing services or service groups, and then add them to the service group. A service group can contain up to ten service members. A member may be a service or service group. And a service group may contain services only, or service groups only, or both.

If you want to create an access control rule in the **Security > Firewall** page, you can create a service group in this page firstly, and then reference it in the access control rule. Using service groups can facilitate the configuration of access control rules. For example, you can add telnet, pop3 and http services into a service group, and then create one rule by using the service group to control the access to these services. Else, you need to create multiple access control rules for the access to these services, one rule per service.

Similarly, you also can reference a service group whose **Service Type** is **General Service** in a rule limit rule in the **QoS > Rate Limit Rule** page.

12.7.2 Service Group Settings

The screenshot displays the 'Service Group Settings' configuration window. At the top, there are two tabs: 'Group List' and 'Service Group Settings'. The 'Service Group Settings' tab is active. The configuration fields are as follows:

- Name:** WEB_FTP
- Service Type:** General Service (dropdown menu)
- Radio Buttons:** New, Existing
- Service List:** A list of service types including ipinip, gre, esp, ah, ospf, igrp, rsvp, and web. The 'web' service is currently selected.
- Buttons:** ==>, <==, and Delete.
- Service Members:** A box containing the service 'ftp'.
- Save:** A button at the bottom right of the configuration area.

Figure 12-32 Service Group Settings

- ✧ **Name:** It specifies a unique name of the service group. It should be between 1 and 11 characters long.
- ✧ **Service Type:** It specifies the service type of the service group. The Device provides five service types, which include **General Service**, **URL**, **Keyword**, **DNS** and **MAC**.
 - **General Service:** It is used to match the source port, destination port and protocol type of the packets.
 - **URL:** It is used for URL filtering to control the LAN users' access to the specified URLs or web sites.
 - **Keyword:** It is used for keyword filtering to block the web sites which contain the specified keywords.
 - **DNS:** It is used for DNS request filtering to allow or block the DNS requests for the specified domain names.
 - **MAC:** It is used for source MAC address filtering to allow or block the packets with the specified source MAC address.

- ✧ **New:** Select it to add a new service to the group. For different **Service Types**, you need configure different parameters.
- ✧ **Existing:** Select it to display the service groups that you have configured. If you select **General Service** from the **Service Type** drop-down list, it will also display the system predefined services here. The Device provides 38 predefined services.
- ✧ **Service Members:** It displays the members of the service group. A member may be a user-defined service, predefined service or a service group.
- **==>:** Click it to move the new user-defined service or selected existing service(s) to the **Service Members** list box.
- **<==:** Click it to move the selected service member from the **Service Members** list box to the left editable list.
- **Delete:** Click it to delete the selected service member from the **Service Members** list box.
- **Save:** Click it to save the service group settings.

**Note**

1. A service group can contain up to ten service members.
2. The **Name** of a service group is case insensitive. For example, the service group **test** or **TEST** is the same group. You must pay attention to it when creating a service group.
3. If a service group (e.g., group A) has already included another service group (e.g., group B), then the service group A cannot be added to any other service group.

12.7.3 Service Group List

Name	Service Type	Service Members	Edit
<input type="checkbox"/> WEB_FTP	General Service	ftp, web;	Edit
<input type="checkbox"/> Pornography	Keyword	{K(pornography)};	Edit
<input type="checkbox"/> Test	MAC	{M(0022aa112233)};	Edit

Figure 12-33 Service Group List

- **Add a Service Group:** If you want to add a new service group, click the **New** button or select the **Service Group Settings** tab to go to the setup page, and then configure it, lastly click the **Save** button.
- **View Service Group(s):** When you have configured some service groups, you can view them in the **Service Group List**.
- **Edit a Service Group:** If you want to modify a configured service group, click its **Edit** hyperlink, the related information will be displayed in the setup page. Then modify it, and click the **Save** button.
- **Delete Service Group(s):** If you want to delete one or more service groups, select the leftmost check boxes of them, and then click the **Delete** button.



Note

You cannot delete a service group which is referenced by the access control rule in the **Security > Firewall** page or rate limit rule in the **QoS > Rate Limit Rule** page. If you actually want to delete it, please remove all the references firstly.

12.7.4 How to Add the Service Groups

If you want to add one or more service groups, do the following:

- Step 1** Go to the **Security > Service Group** page, and then click the **New** button or select the **Service Group Settings** tab to go to the setup page.
- Step 2** Specify the **Name** of the service group.
- Step 3** Select the type from the **Service Type** drop-down list.
- Step 4** Add services to the group. There are two methods to add them.
- 1) Method One: Select the **New** radio button, add a new service as required, and then click **==>** to move the new service to the **Service Members** list box. You can continue to add another services if needed.
 - 2) Method Two: Select the **Existing** radio button, select one or more existing services, and then click **==>** to move the selected services to the **Service Members** list box.
- Step 5** Click the **Save** button to save the settings. You can view the service group in the **Service Group List**.
- Step 6** If you want to add another new service group, please repeat the above steps.

12.7.5 How to Edit an Service Group

If you want to modify a configured service group, do the following:

- Step 1** Go to the **Security > Service Group** page.
- Step 2** Click the **Edit** hyperlink of the group in the **Service Group List** to go to the setup page.
- Step 3** Modify the service members as required. There are two cases:
- 1) If you want to modify a user-defined service, select the service in the **Service Members** list, click **<==** to move it from the **Service Members** list to the left editable list box, and then modify it, lastly click **==>** to move the modified service to the **Service Members** list box again.
 - 2) If you want to delete a service member, select the member in the **Service Members** list box, and then click the **Delete** button.
- Step 4** Click the **Save** button to save the changes to make them take effect.

12.8 Schedule

This section describes the **Security > Schedule** page.

12.8.1 Introduction to Schedule

The schedule feature lets you define schedules that can be applied to various time-related features, e.g., dial schedule, rate limit rule, access control rule, etc. The schedule is identified by a name and then referenced by a function, so that those time restrictions are imposed on the function itself.

A schedule consists of a start date, an end date, and optional time periods (up to eight). The **Start Date** and **End Date** specify when the schedule begins and ends. If exceed the specified range, the schedule will be of no effect. If both of them are set to **1990-1-1**, the schedule will be in effect forever. The time periods (**Period 1-8**) specify further constraints of active time by the days of the week, daily start time and daily end time.



Note

To ensure that the schedules take effect at the desired time, you should synchronize the system clock in the **System > Time** page.

12.8.2 Schedule Settings

Schedule Name

Start Date End Date

Year	Month							
SUN	MON	TUE	WED	THU	FRI	SAT		
26	27	28	29	30	1	2		
3	4	5	6	7	8	9		
10	11	12	13	14	15	16		
17	18	19	20	21	22	23		
24	25	26	27	28	29	30		
31	1	2	3	4	5	6		

Today is: [2011-7-24](#)

Period	Days of the Week	Daily End Time
Period 1	<input type="text" value="Everyday"/>	<input type="text" value="23:59:59"/>
Period 2	<input type="text"/>	<input type="text" value="23:59:59"/>
Period 3	<input type="text"/>	<input type="text" value="23:59:59"/> <input style="float: right;" type="button" value="+"/>

Figure 12-34 Schedule Settings

- ✧ **Schedule Name:** It specifies a unique name of the schedule. It should be between 1 and 11 characters long.
- ✧ **Start Date** and **End Date:** They specify when the schedule begins and ends. If exceed the specified range, the schedule will be of no effect. The date is in the range of 1989-1-1 through 2050-12-31. If you want the schedule to be in effect for ever, set both of **Start Date** and **End Date** to **1990-1-1**. There are two methods to set them.
 - **Directly enter a date:** You can directly enter a date in the **Start Date** or **End Date** text box. The date should be entered in the format YYYY-MM-DD, for example, 2011-03-23 (or 2011-3-23). Therein, YYYY indicates a four-digit year, MM indicates a month of the year, and DD indicates a day of that month.
 - **Select a Date from the Drop-down Calendar:** You also can select a date from the drop-down calendar, see figure 12-34. Click the **<Year** and **Year>** to select the year, click the **<Month** and **Month>** to select the month, and select a date directly from the calendar.
- ✧ **Period 1 to Period 8:** They specify further constraints of active time within the specified date range. It allows you to configure up to eight time periods for each schedule.
- ✧ **Days of the Week:** It specifies the day(s) of the week on which the schedule is active. The available options are **Everyday**, **Monday**, **Tuesday** ... **Sunday**, **Weekdays**

(Mon-Fri) and Weekends (Sat-Sun).

- ✧ **Daily Start Time** and **Daily End Time:** They specify a daily start time and end time during which the schedule is active. The default values of them are 00:00:00 and 23:59:59 respectively. Note that the time should be entered in the format HH:MM:SS and it is expressed in 24-hour clock. For example, 06:30:00 is 06:30:00 am and 18:30:00 is 06:30:00 pm.
- **Save:** Click it to save the schedule settings.

**Note**

A schedule that spans two days should be divided into two consecutive time periods. E.g., for a schedule from 8:00 p.m. to 5:00 a.m. next day, you need configure two time periods, one is 20:00:00~23:59:59, and the other is 00:00:00 ~ 05:00:00.

12.8.3 Schedule List

Schedule List		Schedule Settings		
2/10	Lines/Page: 10	First	Prev Next Last	
Search:			New	
Schedule Name	Start Date and Time	End Date and Time	Edit	Details
<input type="checkbox"/> test	2010-12-12 00:00:00	2010-12-24 23:59:59	Edit	Details
<input type="checkbox"/> work	2011-1-1 00:00:00	2011-12-31 23:59:59	Edit	Details
<input type="checkbox"/> Select All				
				Delete

Figure 12-35 Schedule List

- **Add a Schedule:** If you want to add a new schedule, click the **New** button or select the **Schedule Settings** tab to go to the setup page, and then configure it, lastly click the **Save** button.
- **View Schedule(s):** When you have configured some schedules, you can view them in the **Schedule List**.
- **Edit a Schedule:** If you want to modify a configured schedule, click its **Edit** hyperlink, the related information will be displayed in the setup page. Then modify it, and click

the **Save** button.

- **Delete Schedule(s):** If you want to delete one or more schedules, select the leftmost check boxes of them, and then click the **Delete** button.
- **View a Schedule's Details:** If you want to view the details of a configured schedule, click its **Details** hyperlink, then the schedule details page will be displayed (see Figure 12-36). Furthermore, if the schedule is referenced, the related information will be displayed too.

The screenshot shows a web interface for viewing schedule details. It includes the following elements:

- Current System Time:** 2011-7-31 10:44:20
- Schedule Name:** work
- Start Date and Time:** 2011-1-1 00:00:00
- End Date and Time:** 2011-12-31 23:59:59
- Table:**

Period	Type	Start Time	End Time
Period 1	Weekdays	09:00:00	17:59:59
Period 2	Weekdays	13:00:00	17:59:59
- Referenced By:** A text area with a scroll bar, currently empty.

Figure 12-36 Schedule Details

12.8.4 How to Add the Schedules

If you want to add one or more schedules, do the following:

- Step 1** Go to the **Security > Schedule** page, and then click the **New** button or select the **Schedule Settings** tab to go to the setup page.
- Step 2** Specify the **Schedule Name** of the schedule.
- Step 3** Specify the **Start Date** and **End Date** as required.
- Step 4** Specify one or more periods as required.
- Step 5** Click the **Save** button to save the settings. You can view the schedule in the **Schedule List**.
- Step 6** If you want to add another new schedule, please repeat the above steps.



Note

If you want to delete one or more schedules, select the leftmost check boxes of them

in the **Schedule List**, and then click the **Delete** button.

12.8.5 Configuration Example for Schedule

1. Requirements

In 2011, a business CEO wants to control online behavior of the sales department's employees. He only allows them to access WEB service during working time, but allows them to access all the Internet services during rest periods. The working time is: Monday to Friday, 9:00 to 12:00 am, and 1:00 to 6:00 pm.

2. Analysis

As the sales department's employees can only access the WEB service during working time, we need to create a schedule during which only the WEB service is accessible.

The details of the schedule are as follows:

- **Schedule Name:** Here we assume its name is **work**.
- **Start Date:** 2011-1-1
- **End Date:** 2011-12-31
- **Period 1:** Monday to Friday, 9:00:00 to 11:59:59
- **Period 2:** Monday to Friday, 13:00:00 to 17:59:59

3. Configuration Procedure

The configuration steps are the following:

- Step 1** Go to the **Security > Schedule** page, and then click the **New** button or select the **Schedule Settings** tab to go to the setup page, see the following figure.

le List Schedule Settings

Schedule Name

Start Date End Date

Period	Days of the Week	Daily Start Time	Daily End Time
Period 1	<input type="text" value="Weekdays (Mon-Fri)"/>	<input type="text" value="09:00:00"/>	<input type="text" value="11:59:59"/>
Period 2	<input type="text" value="Weekdays (Mon-Fri)"/>	<input type="text" value="13:00:00"/>	<input type="text" value="17:59:59"/>
Period 3	<input type="text" value=""/>	<input type="text" value="00:00:00"/>	<input type="text" value="23:59:59"/> <input type="button" value="+"/>

Figure 12-37 Schedule Settings Example

- Step 2** Enter **work** in the **Schedule Name** text box.
- Step 3** Enter **2011-1-1** in the **Start Date**, and enter **2011-12-31** in the **End Date**.
- Step 4** Configuring the two periods of the schedule respectively.
- 1) Configuring **Period 1**: Select **Weekdays (Mon-Fri)** from the **Days of the Week** drop-down list, enter **09:00:00** in the **Daily Start Time**, and enter **11:59:59** in the **Daily End Time**.
 - 2) Configuring **Period 2**: Select **Weekdays (Mon-Fri)** from the **Days of the Week** drop-down list, enter **13:00:00** in the **Daily Start Time**, and enter **17:59:59** in the **Daily End Time**.
- Step 5** Click the **Save** button to save the settings. Till now you have finished configuring the schedule of **work**, and then you can reference it in an access control rule. Please refer to **section 12.3.5.1** for detailed operation.

Chapter 13 System

This chapter describes how to manage the Device, including how to configure administrator accounts, system time, remote admin, Web server, and how to upgrade firmware, backup and restore configuration, and restart the Device.

13.1 Administrator

In the **System > Administrator** page, you can add, view, modify and delete the administrator accounts.

13.1.1 Administrator Settings

The screenshot shows a web interface with two tabs: "Administrator List" and "Administrator Settings". The "Administrator Settings" tab is active. The form contains the following fields:

- User Name: Test
- Password: [masked]
- Confirm Password: [masked]
- Privilege Group: Read (dropdown menu)

A "Save" button is located at the bottom right of the form.

Figure 13-1 Administrator Settings

- ✧ **User Name:** It specifies a unique login name of the administrator. It should be between 1 and 31 characters long.
- ✧ **Password:** It specifies a login password of the administrator.
- ✧ **Confirm Password:** You should re-enter the password.
- ✧ **Privilege Group:** It allows you to select the privilege group you want the administrator to have. Each type of privilege group has different privileges.
 - **Read:** It gives the administrator the ability to view the Device's settings and status via the Web UI, except the **Status > Session Monitor** page. Note: This page will only display the current login administrator's information, and only the

password can be modified.

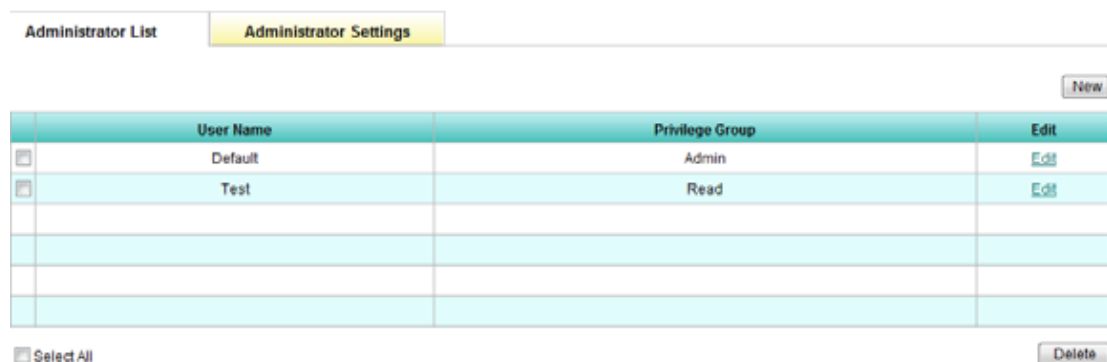
- **Execute:** It gives the administrator the ability to view and configure the Device via the Web UI, except the **Status > Session Monitor** page. Note: This page will only display the current login administrator’s information, and only the password can be modified.
- **Admin:** It gives the administrator the full administrative privileges to view and configure the Device via the Web UI.

➤ **Save:** Click it to save the administrator account settings.

 **Note**

1. It allows you to login to the Device from multiple IP addresses concurrently with the same administrator user name. To avoid configuration conflict, it is suggested that each time you configure the Device from one IP address only.
2. The default administrator user name is **Default** (case sensitive) with a blank password. To ensure security, it is strongly recommended that you change the default password and remember it.
3. Only the administrator who has **Admin** privileges can telnet the Device.

13.1.2 Administrator List



Administrator List		Administrator Settings	
<input type="button" value="New"/>			
<input type="checkbox"/>	User Name	Privilege Group	Edit
<input type="checkbox"/>	Default	Admin	Edit
<input type="checkbox"/>	Test	Read	Edit
<input type="checkbox"/> Select All		<input type="button" value="Delete"/>	

Figure 13-2 Administrator List

- **Add an Administrator Account:** If you want to add a new administrator account, click the **New** button or select the **Administrator Settings** tab to go to the setup page, and then configure it, lastly click the **Save** button.
- **View Administrator Account(s):** When you have configured some administrator accounts, you can view them in the **Administrator List**.
- **Edit an Administrator Account:** If you want to modify a configured administrator account, click its **Edit** hyperlink, the related information will be displayed in the setup page. Then modify it, and click the **Save** button.
- **Delete Administrator Account(s):** If you want to delete one or more administrator accounts, select the leftmost check boxes of them, and then click the **Delete** button.

**Note**

You cannot delete the default administrator account.

13.1.3 How to Add the Administrator Accounts

If you want to add one or more administrator accounts, do the following:

- Step 1** Go to the **System > Administrator** page.
- Step 2** Click the **New** button or select the **Administrator Settings** tab to go to the setup page, and then specify the **User Name**, **Password**, **Confirm Password** and **Privilege Group** as required.
- Step 3** Specify the **Privilege Group** as required. If you choose **Admin** as the **Privilege Group**, you can use this administrator account to telnet the Device.
- Step 4** Click the **Save** button to save the settings. You can view the administrator account in the **Administrator List**.
- Step 5** If you want to add another new administrator account, please repeat the above steps.

**Note**

If you want to delete one or more administrator accounts, select the leftmost check boxes of them in the **Administrator List**, and then click the **Delete** button.

13.2 System Time

In the **System > Time** page, you can view and configure the system time.

To ensure that the time-related functions (e.g., DDNS, Schedule) work well, you should set the right time on the Device.

You can manually configure the system time or enable SNTP (Synchronize with SNTP Server) to automatically synchronize time from a designated SNTP server on the Internet.

Some models cannot keep clock running if powered off, that is, it will reset the time to the default value. In this case, you need to choose **SNTP** to automatically synchronize the system time.

The screenshot shows the 'System Time' configuration page. It is divided into two main sections: 'System Time' and 'Date and Time Settings'.

System Time

Current System Time	2011-7-1 12:09:26
---------------------	-------------------

Date and Time Settings

Mode	SNTP
Time Zone	UTC-0500(Eastern Time, United States, Canada)
SNTP Server 1 IP Address	192.43.244.18
SNTP Server 2 IP Address	129.6.15.28
SNTP Server 3 IP Address	0.0.0.0

At the bottom right of the settings section, there is a 'Save' button.

Figure 13-3 System Time - Enable SNTP

- ✧ **Current System Time:** It displays the Device's current date (YYYY-MM-DD) and time (HH:MM:SS).
- ✧ **Mode:** It specifies the mode by which you set the system clock. The available options are **SNTP** and **Manual**.
 - **SNTP:** If you want the Device to automatically synchronize the system clock from designated SNTP server on the Internet, select this option (see Figure 13-3).
 - **Manual:** If you want to set the date (YYYY-MM-DD) and time (HH:MM:SS) for the Device manually, select this option (see Figure 13-4).
- ✧ **Time Zone:** It specifies the time zone for your local time.
- ✧ **SNTP Server 1 IP Address ~ SNTP Server 3 IP Address:** It allows you to configure up to three SNTP servers on the Device. The Server 1 is the primary server (the

default value is 192.43.244.18), and the Server 2 is the first backup server (the default value is 129.6.15.28), and the Server 3 is the second backup server (the default value is 0.0.0.0).

System Time

Current System Time 2011-7-1 12:08:53

Date and Time Settings

Mode

Year Month Day

Figure 13-4 System Time - Set Time Manually

- **Save:** Click it to save the system time settings.

 **Note**

To find an NTP server with which you can synchronize your Device, please refer to the Website: <http://www.ntp.org/>.

13.3 Firmware Upgrade

In the **System > Upgrade** page, you can view the current firmware version information and upgrade the firmware.

13.3.1 Save Firmware

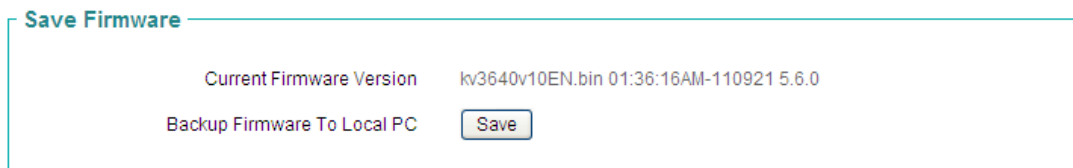


Figure 13-5 Save Firmware to Local PC

The following figure describes the firmware version details:

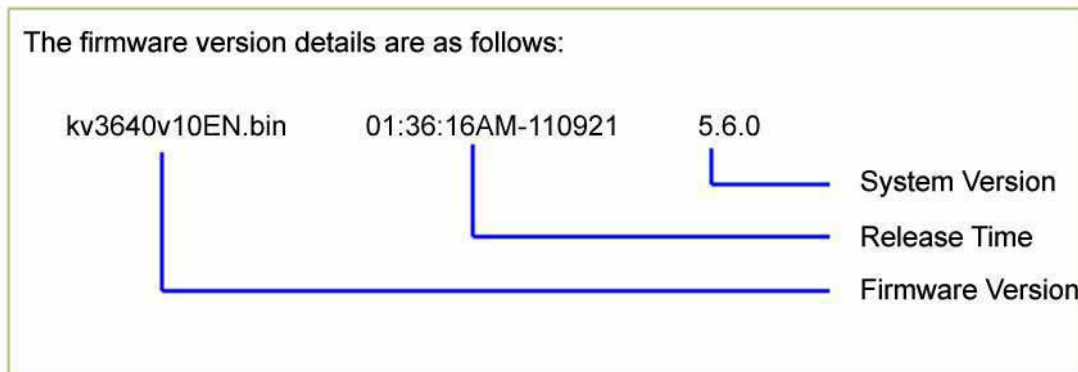


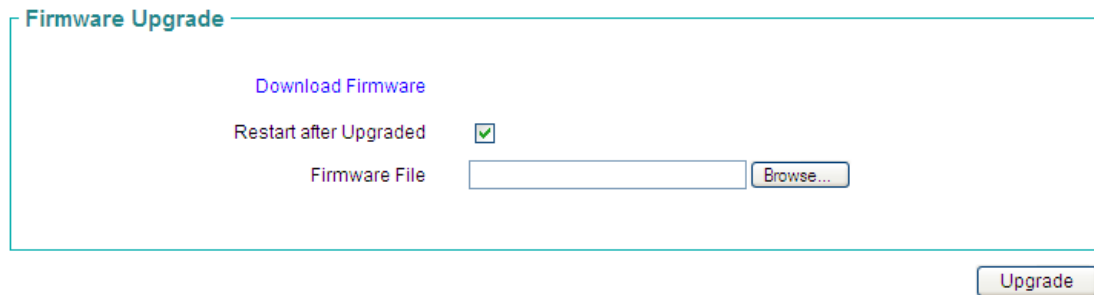
Figure 13-6 Firmware Version Details

- **Backup Firmware to Local PC:** Click the **Save** button to save the current running firmware to your local PC.

 **Note**

The operation will save the Device’s current running firmware only, but it won’t save the current configuration file.

13.3.2 Firmware Upgrade



The screenshot shows a web interface for firmware upgrade. At the top left, the title 'Firmware Upgrade' is displayed. Below it, there is a blue hyperlink 'Download Firmware'. Underneath, the text 'Restart after Upgraded' is followed by a checked checkbox. Below that, the text 'Firmware File' is followed by an empty text input box and a 'Browse...' button. At the bottom right of the main content area, there is an 'Upgrade' button.

Figure 13-7 Upgrade Firmware

To upgrade the Device's firmware, do the following:

Step 1 Download the Latest Firmware

Click the **Download Firmware** hyperlink to download the latest firmware from the website of UTT Technologies Co., Ltd.

Note

1. Please select the proper firmware that must accord with your product hardware platform.
2. It is recommended that you go to the **System > Configuration** to back up the Device's current configuration before upgrading.

Step 2 Choose the Firmware

Click **Browse** button to choose the firmware file you want to upgrade or enter the file path and name in the **Firmware File** text box.

- ✧ **Restart after Upgraded:** After upgraded, you have two options to apply this new firmware: select the **Restart after Upgraded** check box to let the Device restart itself automatically once upgraded, or manually restart the Device.

Step 3 Renew Firmware

Click the **Upgrade** button to renew the Device's firmware.

 **Note**

1. It is strongly recommended that you upgrade firmware when the Device is under light load.
2. If you upgrade firmware timely, the Device will have more functionality and better performance. The right upgrade will not change the Device's current settings.
3. The Device will take several minutes to upgrade its firmware. During this process, do not power off the Device and perform any other operation to avoid damaging it.

13.4 Configuration

In the **System > Configuration** page, you can back up and restore configuration, and reset the Device to factory default settings.

13.4.1 Backup Configuration



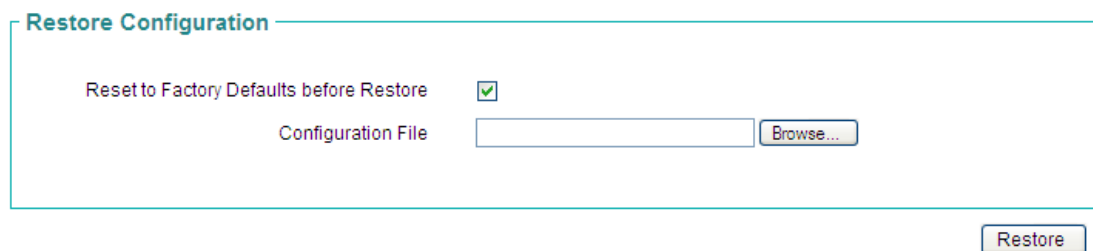
Backup Configuration

Backup configuration to local PC

Figure 13-8 Backup Configuration

- **Backup:** Click it to save the current configuration file to the local PC.

13.4.2 Restore Configuration



Restore Configuration

Reset to Factory Defaults before Restore

Configuration File

Figure 13-9 Restore Configuration

- ✧ **Reset to Factory Defaults before Restore:** If you select this check box, it will reset the Device to factory default settings before importing the configuration file; else import the file directly.
- ✧ **Configuration File:** Click the **Browse** button to choose an appropriate configuration file or enter the file path and name in the text box.
- **Restore:** Click it to import the selected configuration file. It will overwrite the current configuration on the Device with the new configuration.

**Note**

To avoid unexpected error, do not power off the Device during importing the configuration file.

13.4.3 Restore Defaults

**Figure 13-10 Restore Default**

- **Reset:** Click it to reset the Device to factory default settings.

**Note**

1. This operation will clear all of the Device's custom settings. It is strongly recommended that you backup the current configuration before resetting.
2. The default administrator user name is **Default** (case sensitive) with a blank password. The default LAN interface IP address is 192.168.16.1, and subnet mask is 255.255.255.0.

13.5 Remote Admin

This section describes **System > Remote Admin** page.

As the Device has built-in firewall function, it will block all requests initiated from the Internet by default. To remotely configure and manage the Device via Internet, you should enable the HTTP remote management.

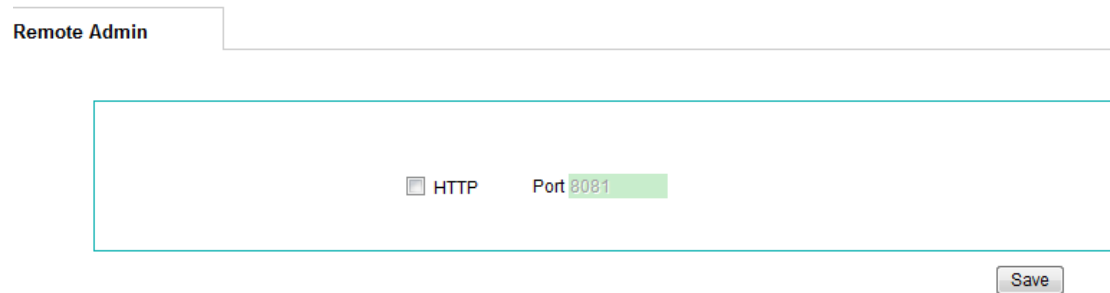


Figure 13-11 Remote Admin Settings

- ✧ **HTTP:** It allows you to enable or disable HTTP remote management. Select this check box to enable HTTP remote management via Internet. When accessing the Device from Internet, you will enter **http://** and enter the Device's WAN IP address, followed by a colon (:) and the port number. For example, if the WAN IP address is 218.21.31.3 and port number is 8081, enter <http://218.21.31.3:8081> in your browser URL field.
- ✧ **Port:** It specifies the port number for HTTP remote management. The default value is 8081. Note: If the port value is changed to 80, the system will automatically create one port forwarding rule: protocol is TCP and port is 80; and you can go to the **NAT > Port Forwarding** page to view it in the **Port Forwarding List**. In this case, it will cause conflict if you add a new port forwarding rule for a LAN Web server.
- **Save:** Click it to save the remote admin settings.



Note

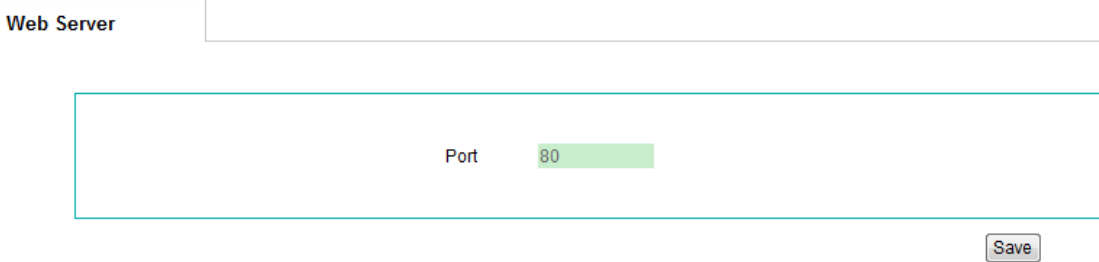
1. You can find the Device's WAN IP address from the **WAN List** in **Basic > WAN** page.
2. To ensure security, it is strongly recommended that you don't enable HTTP remote management unless necessary. If you are sure to enable it, you had better go to the **System > Administrator** page to change the default password.
3. If the Internet connection has a dynamic IP address, you had better enable DDNS in the **Advanced > DDNS** page, so you may use a fixed domain name to manage the

Device via Internet.

4. Once you enable the HTTP remote management, the system will automatically create two port forwarding rules: their IDs are http and telnet respectively. You can go to the **NAT > Port Forwarding** page to view them in the **Port Forwarding List**.
5. Please enable the HTTP remote management before asking a UTT customer engineer for the technical support.

13.6 WEB Server

In the **System > WEB Server** page, you can specify the port number that the Device Web service uses to listen for HTTP requests from the LAN hosts.



The screenshot shows a configuration page titled "Web Server". A large rectangular area contains a "Port" label followed by a text input field containing the number "80". The input field has a light green background. Below the input field, on the right side, is a "Save" button.

Figure 13-12 WEB Server

- ✧ **Port:** The port number that the Web server uses to listen for HTTP requests from the LAN hosts. The default port number is 80. If it has been changed, you should enter **http://Device's LAN IP address: port number** (e.g., `http://192.168.16.1:88`) to access the Device.
- **Save:** Click it to save your settings.

13.7 Restart

The **System > Restart** page lets you restart the Device.

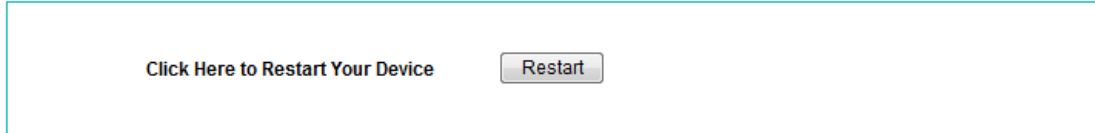


Figure 13-13 Restart the Device

- **Restart:** Click it to restart the Device.

If you click the **Restart** button, the system will pop up a prompt dialog box (see Figure 13-19). Then you can click **OK** to restart the Device, and the system will jump to a countdown page (see Figure 13-20). Or click **Cancel** to cancel the operation.

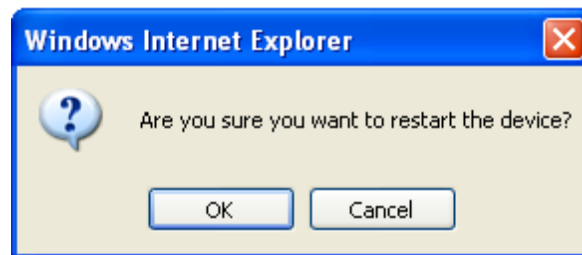


Figure 13-14 Prompt Dialog Box - Restart the Device

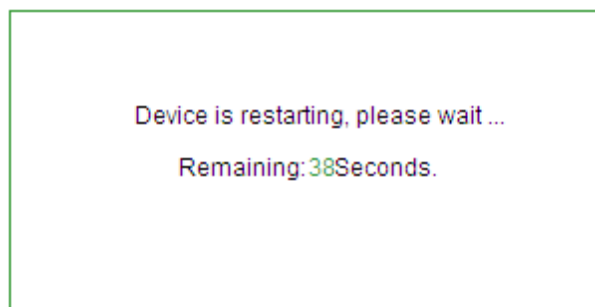


Figure 13-15 Restarting.....

 **Note**

Because restarting the Device will disconnect all the sessions, please do it with

caution. The Device will return to the **Status > System Info** page after restarted.

Appendix A How to configure your PC

This appendix describes how to install and configure TCP/IP properties for Windows 95 and Windows 98.

Step 1: Installing TCP/IP components

To install TCP/IP component, do the following:

1. On the Windows taskbar, click **Start > Settings > Control Panel**.
2. Double-click the **Network** icon, and select the **Configuration** tab. In **The following network components are installed** box, you must make sure that your network card driver and TCP/IP are installed. To do this, please check that **TCP/IP -> (your Ethernet adapter)** option exist.
3. If your network card driver and TCP/IP are not installed, at first you should install the network card driver properly.
4. After installing the network card driver, you should install TCP/IP. Do the following: At first, open the **Network** dialog box (refer to the previous step), and then click **Add** button on the **Configuration** tab, this will bring up the **Select Network Component Type** window. Select **Protocol** and click the **Add** button, this will bring up the **Select Network Protocol** window. Select **Microsoft** in the **Manufacturers** box, and select **TCP/IP** in the **Network Protocols** box, lastly click **OK** to reboot the server PC. Your computer will prompt you to restart, and then TCP/IP will be installed.

Step 2: Configuring TCP/IP properties

Once the proper Ethernet card and TCP/IP protocol are installed, you should configure the TCP/IP properties. There are two methods of configuring TCP/IP properties: one is to manually configure TCP/IP properties, the other is to automatically configure TCP/IP properties with DHCP. The following describes the configuration procedure of these two methods respectively.

➤ Method One: Manually Configuring TCP/IP

To configure the TCP/IP protocol manually, do the following:

1. On the Windows taskbar, click **Start > Settings > Control Panel**.
2. Double-click the **Network** icon, and select the **Configuration** tab. In **The following network components are installed** box, select **TCP/IP -> (your Ethernet adapter)**, and then click **Properties**.

3. In the **TCP/IP properties** dialog box, select the **IP address** tab, and then select the **Specify an IP address** radio button. Enter 192.168.16.x (x is between 2 and 254, including 2 and 254) in the **IP Address** box, and enter 255.255.255.0 in the **Subnet Mask** box.
4. Select the **Gateway** tab, enter the IP address of the Device's LAN interface (default value is 192.168.16.1) in the **New gateway** box, and then click **Add** button.
5. Select the **DNS Configuration** tab, enter a host name in the **Host** box, and enter a domain name in the **Domain** box optionally. In the **DNS Server Search Order** box, enter the IP address of the primary DNS server provided by your ISP. Then click **Add** button to add the IP address to the list. Add the secondary DNS server IP address in the same manner as the first. Leave the **domain suffix search order** blank.
6. Click **OK** in the **TCP/IP properties** window, this will return you to the **Network** window. Click **OK** again. Till now you have finished configuring the TCP/IP properties. Restart your PC for the changes to take effect.

➤ **Method Two: Automatically Configuring TCP/IP with DHCP**

1. To ensure that the host can obtain an IP address and other TCP/IP parameters automatically from the Device, you should enable the Device's DHCP server function in **Basic > DHCP & DNS** page.
2. On the Windows taskbar, click **Start > Settings > Control Panel**.
3. Double-click the **Network** icon, and select the **Configuration** tab. In **The following network components are installed** box, select **TCP/IP ->** (your Ethernet adapter), and then click **Properties**.
4. In the **TCP/IP properties** dialog box, select the **IP address** tab, and then select **Obtain an IP address automatically**.
5. Select the **Gateway** tab, and then make sure that the Installed gateway box is left blank. If any gateways are shown, remove them.
6. Click the **DNS Configuration** tab, and then make sure that the **Disable DNS** is selected.
7. Click **OK** in the **TCP/IP properties** window, this will return you to the **Network** window. Click **OK** again. Till now you have finished configuring the TCP/IP properties. Restart your PC for the changes to take effect.

Step 3: Selecting Windows' Internet Access Method

1. On the Windows taskbar, click **Start > Programs > accessories > communications > Internet Connection Wizard**.
2. Select the third option **I want to set up my Internet connection manually, or I want**

to connect through a Local Area Network (LAN), and click the **Next** button.

3. Select **I want to connect through a Local Area Network** radio button, and click the **Next** button.
4. Uncheck all boxes in the **LAN Internet Configuration** screen, and click the **Next** button.
5. In the **Set Up Your Internet Mail Account** screen, select **No** and click the **Next** button.
6. In the **Internet Connection Wizard** screen, Click **Finish** button to complete the wizard.

Till now you have finished configuring the TCP/IP properties, then you can use the web browser, FTP client, or other Internet client programs normally.

Appendix B FAQ

1. How to connect the Device to the Internet using PPPoE

- Step 1** Set your ADSL Modem to bridge mode (RFC 1483 bridged mode).
- Step 2** Please make sure that your PPPoE Internet connection use standard dial-type. You may use Windows XP built-in PPPoE dial-in client to test.
- Step 3** Connect a network cable from the ADSL modem to a WAN port of the Device, and connect your telephone line to the ADSL modem's line port.
- Step 4** Configure the PPPoE Internet connection related parameters in the **Basic > WAN** page or through the **Quick Wizard**. Refer to **section 6.2.2.1 PPPoE Internet Connection Settings** for more information.
- Step 5** If you pay monthly for the Internet connection, you can choose **Always On** as the **Dial Type**; else, you can choose **On Demand** or **Manual** as the **Dial Type**, and specify the **Idle Timeout** to avoid wasting online time due to that you forget to hang up the connection in time.
- Step 6** If you choose **Manual** as the **Dial Type**, you need go to the **Basic > WAN > WAN List** page to dial up manually. Refer to **section 6.2.1.3 How to Dial and Hang up a PPPoE Connection** for more information.
- Step 6** After the PPPoE connection is established successfully, you can view its configuration and status information in the **Basic > WAN > WAN List** page, such as **Status** (**Connected** means the connection is established successfully), the connection's **IP address** and **Gateway** provided by your ISP, and so on, see Figure B-0-1.

Interface	Type	Status	IP Address	Gateway	Rx Rate(bps)	Tx Rate(bps)	Operation	Edit
WAN1	PPPoE(ad21589756 [Normal Mode])	Connected(Up time: 00:00:01:02)	10.0.0.1	10.0.0.1	397	1k	Dial Hang Up Delete Edit	

Figure B-0-1 Viewing PPPoE Internet Connection Status in WAN List

- Step 7** You may go to the **Status > System Log** page to view the system logs related

to the PPPoE connection, see Table B-0-1.

Call Syslog	Call Result
<p>Session Up [x]</p> <p>PPPoE Up 00:0c:f8:f9:66:c6</p> <p>Call Connected, on Line1, on Channel 0</p> <p>Outgoing Call @51:1-1</p>	<p>PPPoE session has been established successfully.</p>
<p>Call Terminated @clearSession: 1</p> <p>Outgoing Call @51:1-1</p>	<p>Failed to establish the physical connection, please check whether the Internet connection is normal. You may use Windows XP built-in PPPoE dial-in client to test.</p>
<p>Call Terminated @clearSession: 1</p> <p>Call Connected, on Line1, on Channel 0</p> <p>Outgoing Call @51:1-1</p>	<p>The physical connection has been established, but failed to authenticate. Please go to the Basic > WAN page to check whether the user name and password are correct. If they are correct, please change the PPP Authentication to CHAP or NONE (see Figure B-0-2) and then click the Save button, lastly restart the Device.</p>

Table B-0-1 PPPoE Dial-up System Logs

Connection Type

 Tx Bandwidth Kbit/s

 Rx Bandwidth Kbit/s

 ISP

 User Name

 Password

 Dial Mode

 DNS Server

Advanced Options (Service Name, Priority, Proxy ARP, Mode, MAC Address etc.)

 PPP Authentication

Figure B-0-2 PPPoE Connection Settings (Part)

Step 8 You may go to the **Status > Route Stats** page to view the related route information in the **Routing Table**, such as the **Gateway IP Address** provided by your ISP, **Flag** (**N** should appear, which means NAT is enabled on the route), and so on, see Figure B-0-3.

Destination IP/Mask	Gateway IP	Interface	Flag	Priority	Metric	Count	Age
0.0.0.0/0	10.0.0.1	ptb2	lupaN	60	1	134	45

Figure B-0-3 Routing Table - Example 1

Step 9 Configure the LAN hosts according to the steps described in **Appendix A How to configure your PC**.

2. How to connect the Device to the Internet using Static IP

- Step 1** Please make sure the Internet connection is normal. You may use your PC to test.
- Step 2** Connect a network cable from the network device provided by your ISP to a WAN port of the Device.
- Step 3** Configure the static IP Internet connection related parameters in the **Basic > WAN** page or through the **Quick Wizard**. Refer to **section 6.2.2.2 Static IP Internet Connection Settings** for more information.
- Step 4** After you finish configuring the static IP Internet connection, you may go to the **Status > Route Stats** page to view the related route information in the **Routing Table**, such as the **Gateway IP Address** provided by your ISP, **Flag** (**N** should appear, which means NAT is enabled on the route), and so on, see Figure B-0-4

Destination IP/Mask	Gateway IP	Interface	Flag	Priority	Metric	Count	Age
0.0.0.0	200.200.202.254	le1	luppaNF	60	1	179	54

Figure B-0-4 Routing Table - Example 2

- Step 5** Configure the LAN hosts according to the steps described in **Appendix A How to configure your PC**.

3. How to connect the Device to the Internet using DHCP

- Step 1** Please make sure the Internet connection is normal. You may use your PC to test.
- Step 2** Connect a network cable from the Cable modem to a WAN port of the Device.
- Step 3** Configure the DHCP Internet connection related parameters in the **Basic > WAN** page or through the **Quick Wizard**. Refer to **section 6.2.2.3 DHCP Internet Connection Settings** for more information.



Note

For DHCP Internet connection, the Cable Modem may record the old connected network device's MAC address, and only allows the network device with the recorded MAC address to connect to it. Thus you should set the new Device's MAC address to the recorded MAC address, the operation is as follows: Go to the **Basic > WAN** page to select **DHCP** from the **Connection Type**, enter the recorded MAC address in the **MAC Address** text box, and then click **Save** to save the change, lastly restart the Device to make the change take effect.

- Step 4** After the DHCP Internet connection is established successfully, you can view its configuration and status information in the **Basic > WAN > WAN List** page, such as **Status (Connected** means the connection is established successfully, and in this case, it will also display the left time before the lease expires for the current IP address), the connection's **IP address** and **Gateway** provided by your ISP, and so on, see Figure B-0-5.

Interface	Type	Status	IP Address	Gateway	Rx Rate(bps)	Tx Rate(bps)	Operation	Edit
WAN1	DHCP	Connected(Left:00:00:58:54)	58.26.245.10	58.26.245.3	694	2k	Renew Release Delete	Edit

Figure B-0-5 View DHCP Internet Connection Status Information

- Step 5** You may go to the **Status > Route Stats** page to view the related route information in the **Routing Table**, such as the **Gateway IP Address** provided by your ISP, **Flag (N** should appear, which means NAT is enabled on the route), and so on, see Figure B-0-6.

Destination IP:Mask	Gateway IP	Interface	Flag	Priority	Metric	Count	Age
0.0.0.0/0	58.26.245.3	ie1	luppaN	60	1	331	97

Figure B-0-6 Routing Table - Example 3

Step 6 Configure the LAN hosts according to the steps described in **Appendix A How to configure your PC**.

4. How to reset the Device to factory default settings

The following describes how to reset the Device to factory default settings. There are two cases depending on whether you remember the administrator password or not.



Note

- 1) The reset operation will clear all the custom settings on the Device, so do it with caution.
- 2) Here we take Windows XP for example.

4-1 Case One: Remember the administrator password

When you remember the administrator password, you can use the following two ways to reset the Device to factory default settings. Note that only when the Device has a terminal port, you can use the second way.

➤ **The first way: Reset the Device to factory default settings via Web UI.**

The operation is as follows: Go to the **System > Configuration > Restore Default** page, and then click **Reset** button to reset the Device to factory default settings.

➤ **The second way: Reset the Device to factory default settings via HyperTerminal.**

The operation steps are the following:

Step 1 Connect the RJ-45 connector of the supplied serial cable to the terminal port on the Device, and the DB9 connector of the cable to an open COM port on your PC.

Step 2 Click **Start > Programs > Accessories > Communications > HyperTerminal**, the first screen that appears is the **New Connection** dialog box, see Figure B-0-7; enter a name (**Term9600** in this example) in the **Name** text box, and then click **OK** button.

Note that if HyperTerminal is not installed, click **Start > Settings > Control Panel > Add or Remove Programs > Add/Remove Windows Components > Accessories and Utilities > Details > Communications > Details**, select the

HyperTerminal check box, and then click **OK**.

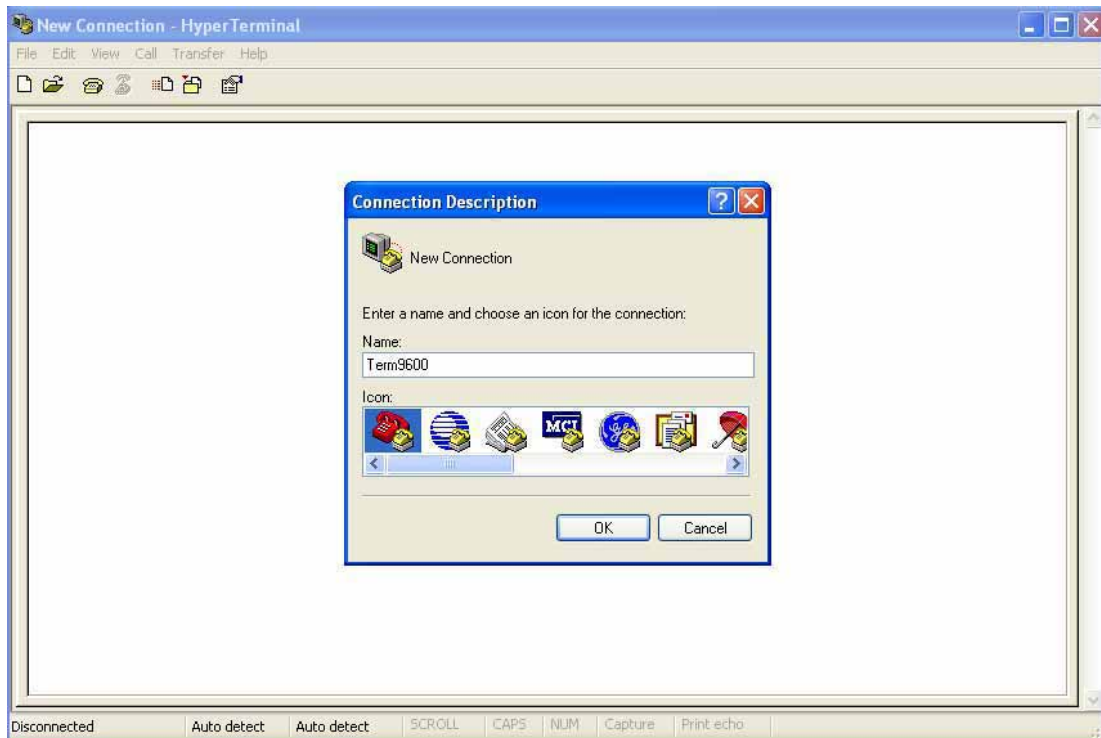


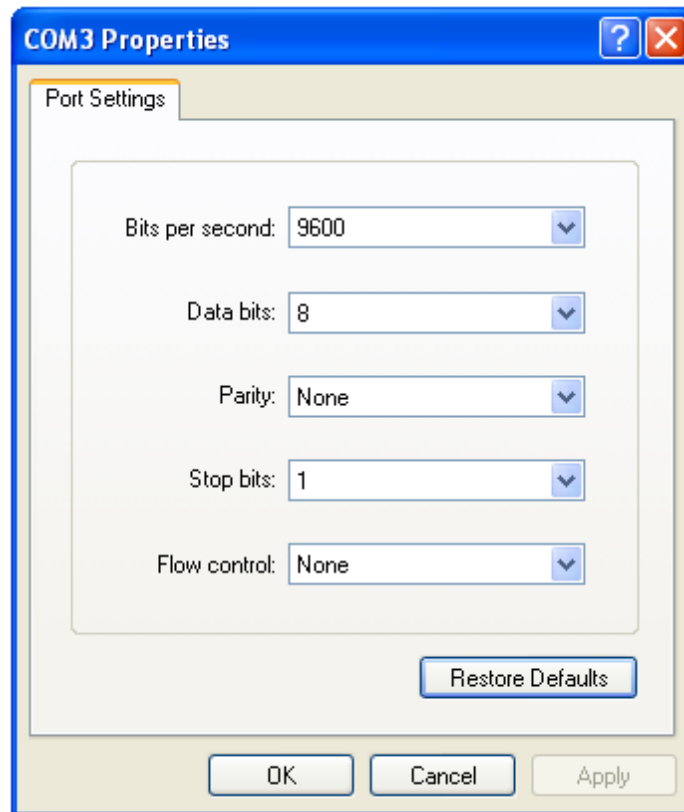
Figure B-0-7 New Connection - Term9600

Step 3 The **Connect To** dialog box appears, see Figure B-0-8. From the **Connect using** drop-down list, select the COM port that links your PC to the Device (**COM3** in this example), and then click **OK** button.



Figure B-0-8 Choose a COM Port - Term9600

- Step 4** The COM port properties dialog box appears (see Figure B-0-9). Select **9600** from **Bits per second**, **8** from **Data bits**, **None** from **Parity**, **1** from **Stop bits**, **None** from **Flow control**, and then click **OK** button.

**Figure B-0-9 COM Port Properties - Term9600**

- Step 5** Now the HyperTerminal is started and ready for use, see Figure B-0-10.

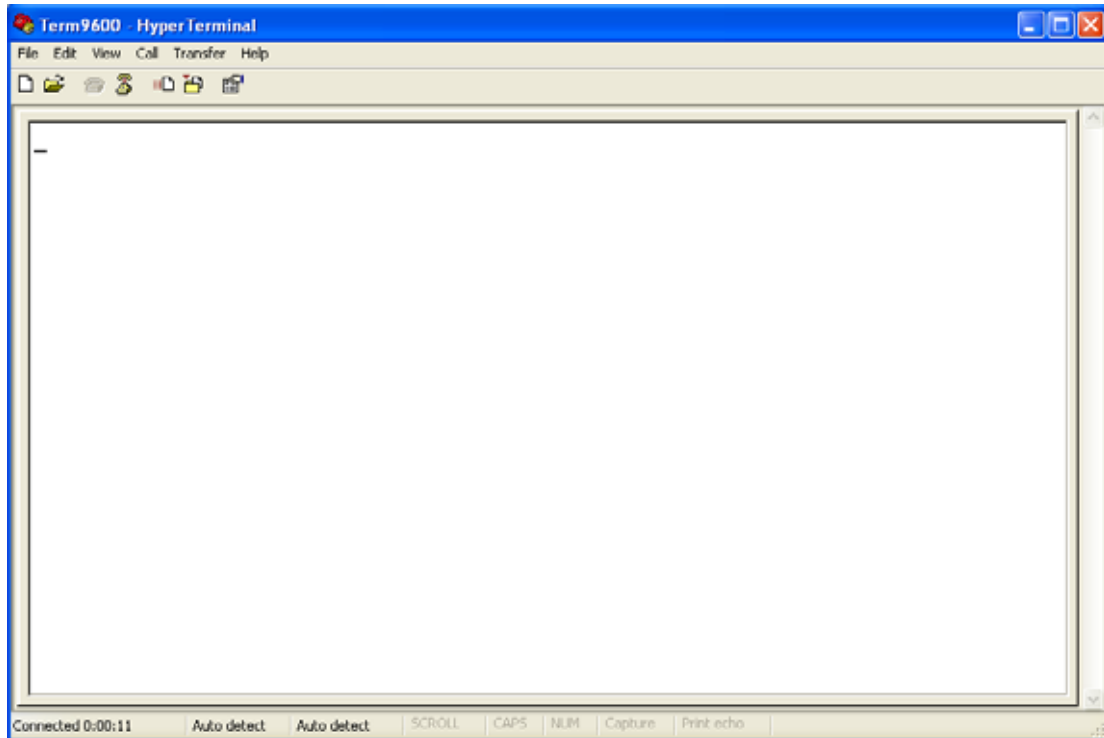


Figure B-0-10 HyperTerminal Window - Term9600

Step 6 Directly press **<Enter>** key, the Device will acknowledge active connection with the **“Login”** prompt, see Figure B-0-11. Enter the administrator user name (**Default** in this example) at the prompt and press **<Enter>** key. Then the **“Password”** prompt appears; enter the password (**test** in this example) at the prompt and press **<Enter>** key. Then the **“hiper%”** prompt appears, which means that you have logged in to the Device successfully, and the Device is ready to receive a command.

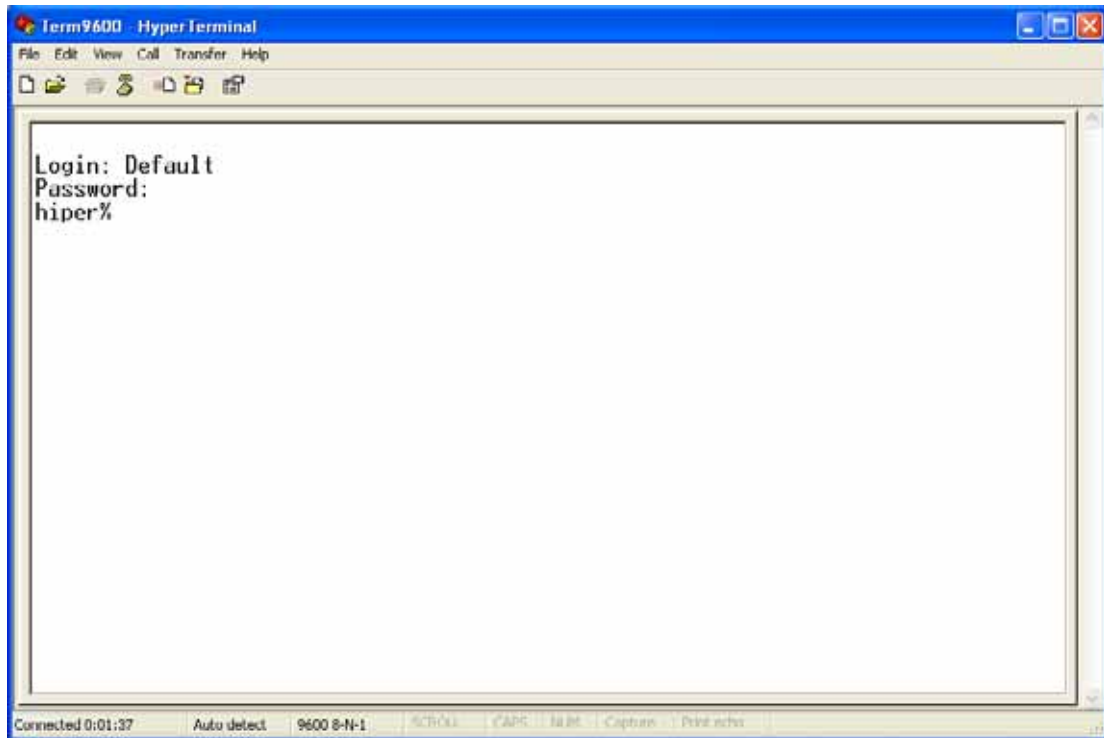


Figure B-0-11 Login to the Device - Term9600

- Step 7** Enter **nvranc** at the prompt and press **<Enter>** key (see Figure 8-12); the Device will immediately restore to factory default settings and restart itself. Once restarted, you can use the system default administrator account to login to the Device via Web UI.

Note that by default, the LAN interface IP address is **192.168.16.1**, and the administrator user name is **Default** (case sensitive) with a blank password.

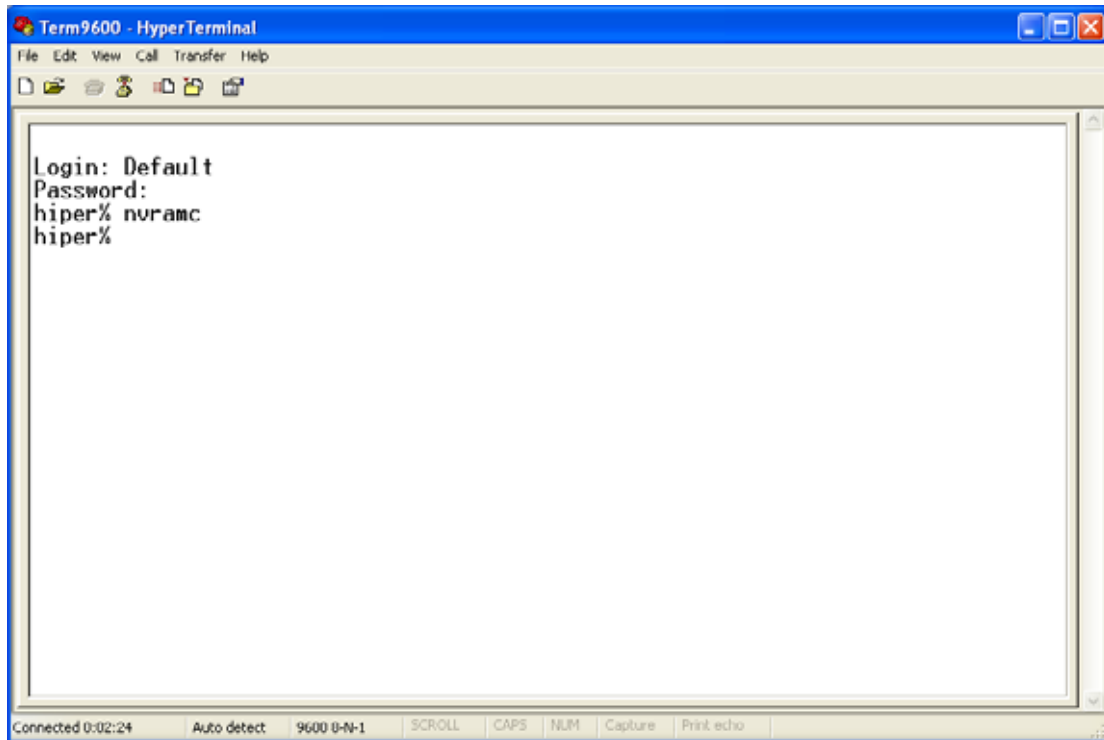


Figure B-0-12 Reset to Factory Default Settings - Term9600

4-2 Case Two: Forget the administrator password

If you forget the administrator password, you can use the following two ways to reset the Device to factory default settings. Note that only when the Device has a reset button, you can use the first way; and only when the Device has a terminal port, you can use the second way.

➤ **The first way: Reset the Device to factory default settings via Reset Button.**

The operation is as follows: While the Device is powered on, use a pin or paper clip to press and hold the Reset button for more than 5 seconds, and then release the button. After that, the Device will restart with factory default settings.

➤ **The second way: Reset the Device to factory default settings via Hyper Terminal.**

The operation steps are the following:

Step 1 Connect the RJ-45 connector of the supplied serial cable to the terminal port on the Device, and the DB9 connector of the cable to an open COM port on your PC.

Step 2 Click **Start > Programs > Accessories > Communications > HyperTerminal**, the first screen that appears is the **New Connection** dialog box, see Figure B-0-13; enter a name (**Term115200** in this example) in the **Name** text box, and then click **OK** button.

Note that if HyperTerminal is not installed, click **Start > Settings > Control Panel > Add or Remove Programs > Add/Remove Windows Components > Accessories and Utilities > Details > Communications > Details**, select the **HyperTerminal** check box, and then click **OK**.

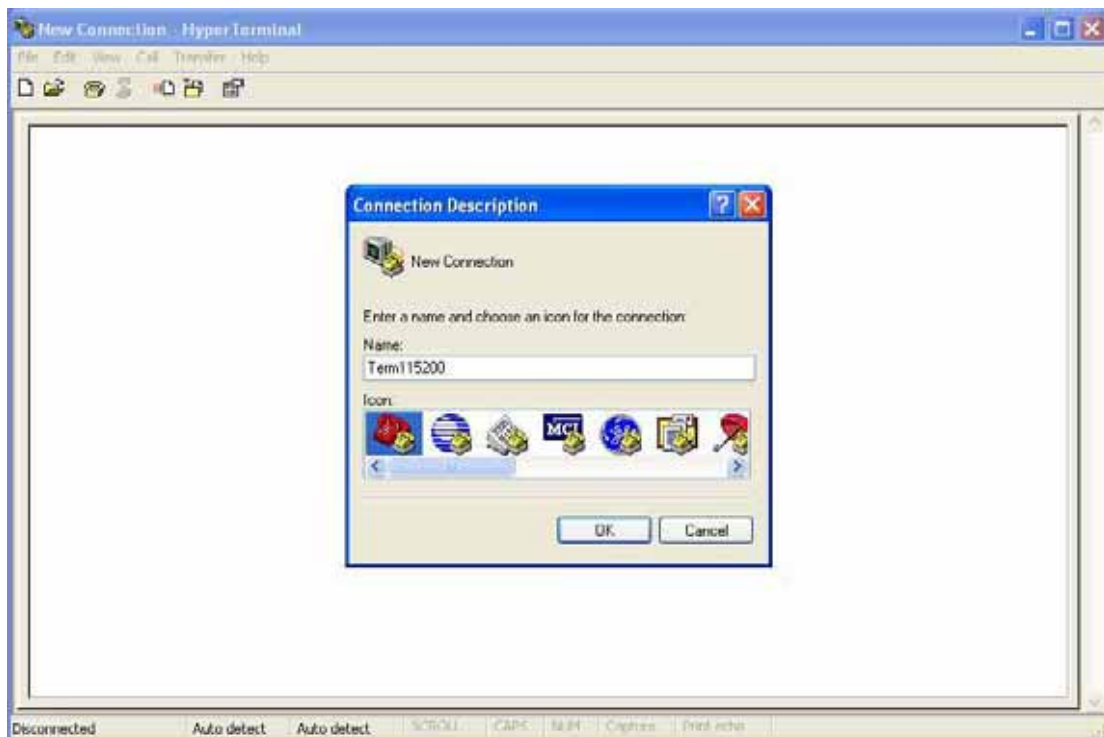


Figure B-0-13 New Connection - Term115200

Step 3 The **Connect To** dialog box appears, see Figure B-0-14. From the **Connect using** drop-down list, select the COM port that links your PC to the Device (**COM3** in this example), and then click **OK** button.



Figure B-0-14 Choose a COM Port - Term115200

Step 4 The COM port properties dialog box appears (see Figure B-0-15). Select **115200** from **Bits per second**, **8** from **Data bits**, **None** from **Parity**, **1** from **Stop bits**, **None** from **Flow control**, and then click **OK** button.

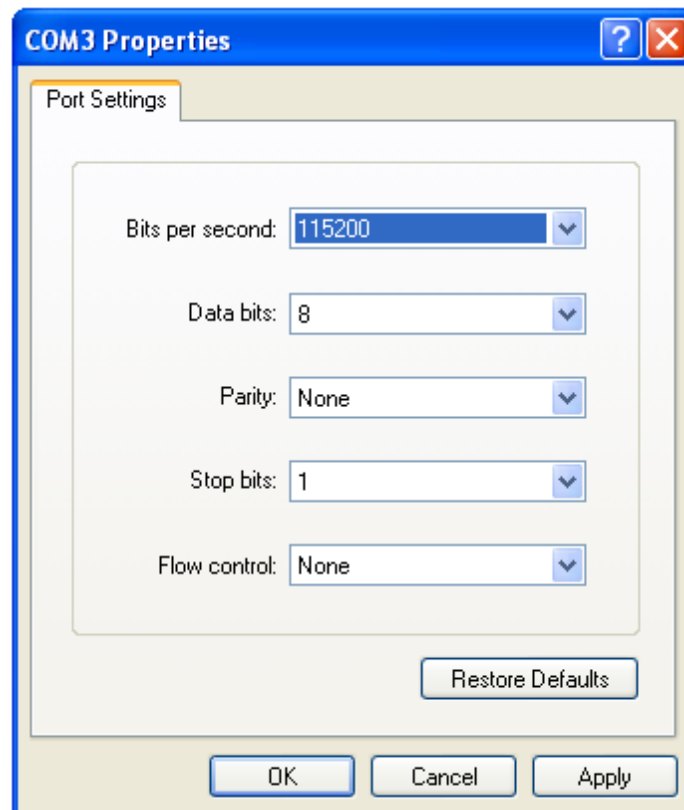
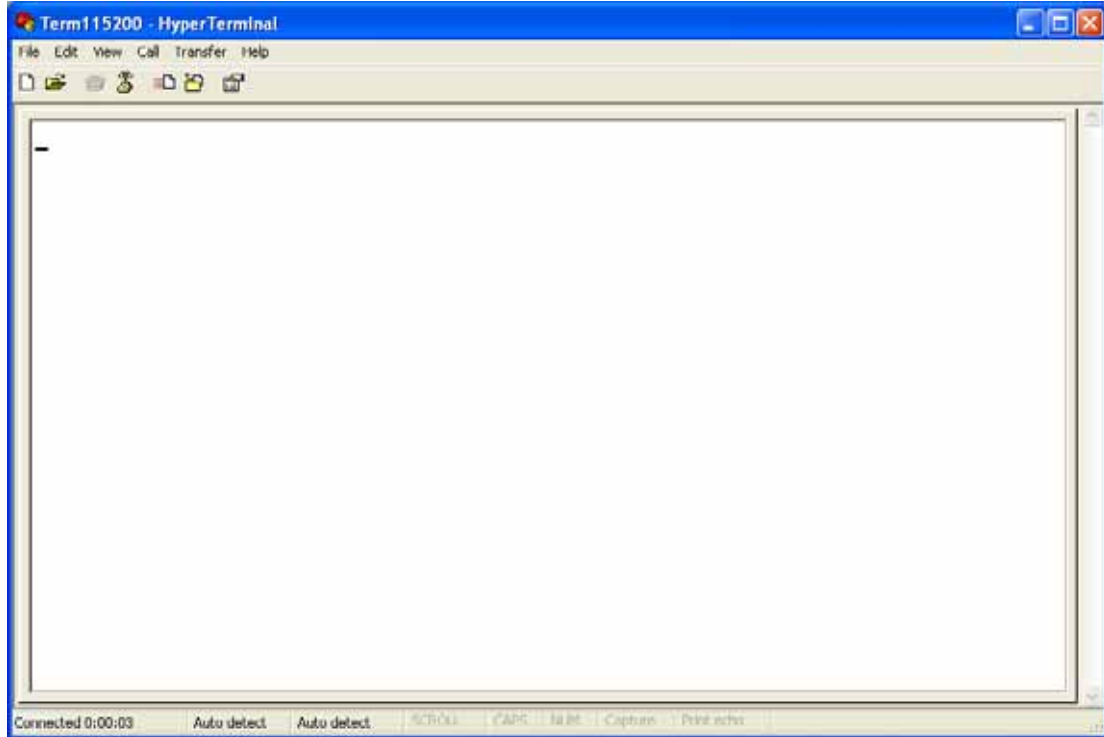


Figure B-0-15 COM Port Properties - Term115200

Step 5 Now the HyperTerminal is started and ready for use, see Figure B-0-16.

**Figure B-0-16 The HyperTerminal Window - Term115200**

Step 6 Restart the Device and immediately enter **ast** (lower case) in three seconds, then the **"Ast>"** prompt appears, see Figure B-0-17. Note that if failed to appear, please try several times until the **"Ast>"** prompt appears.

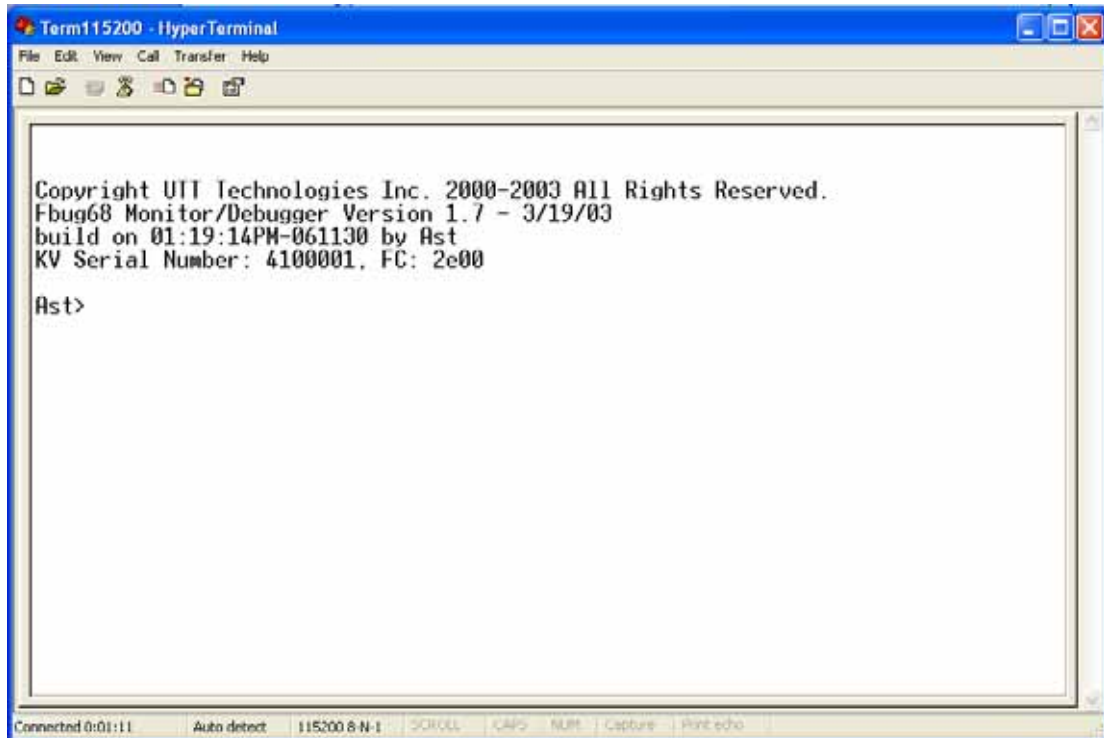
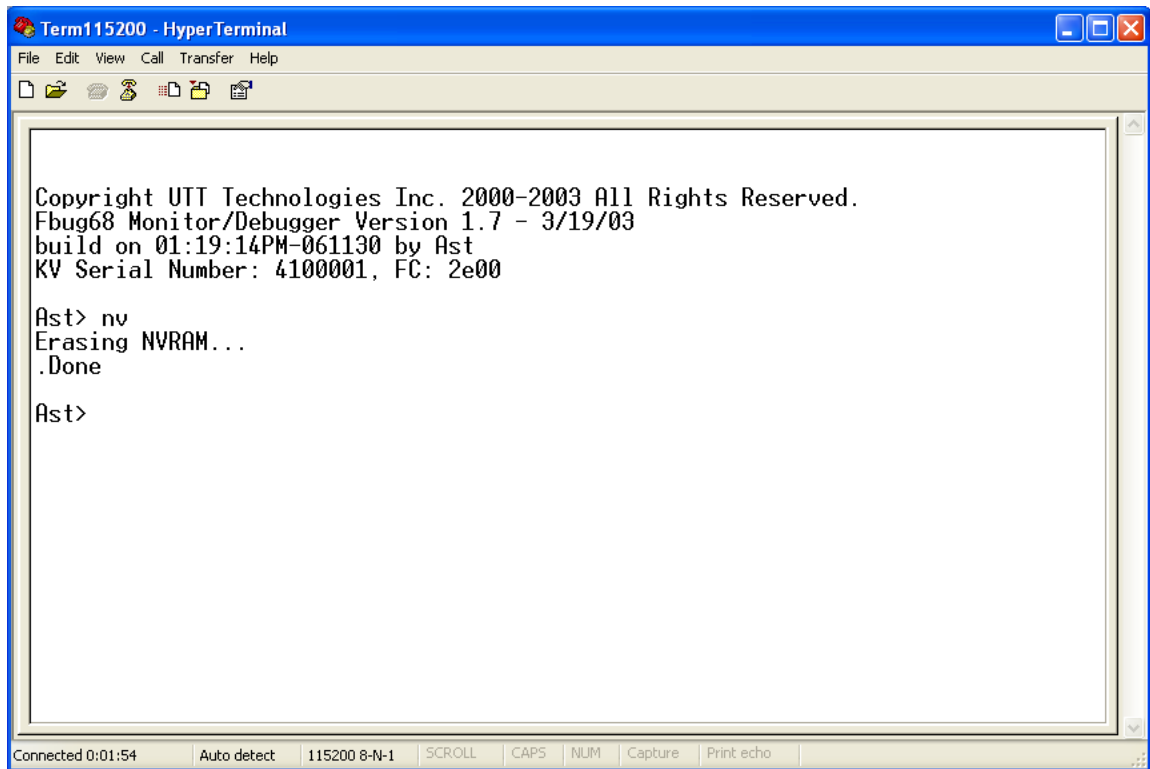


Figure B-0-17 Login to the Device - Term115200

- Step 7** Enter **nv** at the prompt and press **<Enter>** key (see Figure B-0-18), the Device will immediately restore to the factory default settings. The appearance of **“Erasing NVRAM.....Done”** means that the Device has restored to the factory default settings successfully. Once you have restarted the Device, you can use the system default administrator to login to the Device via Web UI.

Note that by default, the LAN interface IP address is **192.168.16.1**, and the administrator user name is **Default** (case sensitive) with a blank password.



```
Term115200 - HyperTerminal
File Edit View Call Transfer Help
Copyright UTT Technologies Inc. 2000-2003 All Rights Reserved.
Fbug68 Monitor/Debugger Version 1.7 - 3/19/03
build on 01:19:14PM-061130 by Ast
KV Serial Number: 4100001, FC: 2e00

Ast> nv
Erasing NVRAM...
.Done

Ast>
```

Connected 0:01:54 Auto detect 115200 8-N-1 SCROLL CAPS NUM Capture Print echo

Figure B-0-18 Reset to Factory Default Settings - Term115200

5. How to use CLI Rescue Mode

In most cases, the Device can normally boot or reboot in **Normal Startup Mode**. However, sometimes you are unable to start the Device in **Normal Startup Mode** due to configuration errors, forgetting the administrator password or other reasons. To solve this problem, we provide **Rescue Mode** in the Device with ReOS 5.0 or a latter version.

After boot into **Rescue Mode**, the Device will run with factory default settings without custom settings, so it will like a new device that hasn't been configured. In **Rescue Mode**, it allows you to use any CLI command to perform any operation.



Note

Only the Device having a serial port supports **Rescue Mode**.

Here we take Windows XP for example to describe how to start the Device in **Rescue Mode**. The operation steps are the following:

- Step 1** Connect the RJ-45 connector of the supplied serial cable to the terminal port on the Device, and the DB9 connector of the cable to an open COM port on your PC.
- Step 2** Click **Start > Programs > Accessories > Communications > HyperTerminal**, the first screen that appears is the **New Connection** dialog box, see Figure B-0-19; enter a name (**rescue** in this example) in the **Name** text box, and then click **OK** button.

Note that if HyperTerminal is not installed, click **Start > Settings > Control Panel > Add or Remove Programs > Add/Remove Windows Components > Accessories and Utilities > Details > Communications > Details**, select the **HyperTerminal** check box, and then click **OK**.

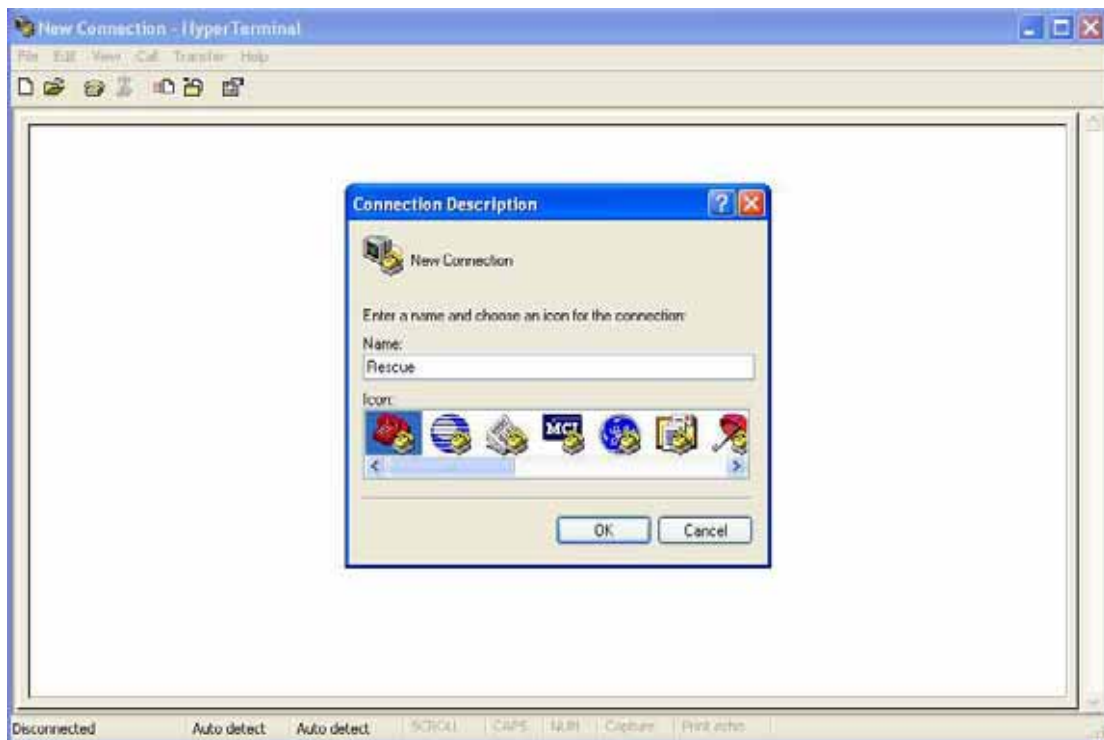


Figure B-0-19 New Connection - Rescue

Step 3 The **Connect To** dialog box appears, see Figure B-0-20. From the **Connect using** drop-down list, select the COM port that links your PC to the Device (**COM3** in this example), and then click **OK** button.



Figure B-0-20 Choose a COM port - Rescue

- Step 4** The COM port properties dialog box appears (see Figure B-0-21). Select **9600** from **Bits per second**, **8** from **Data bits**, **None** from **Parity**, **1** from **Stop bits**, **None** from **Flow control**, and then click **OK** button.

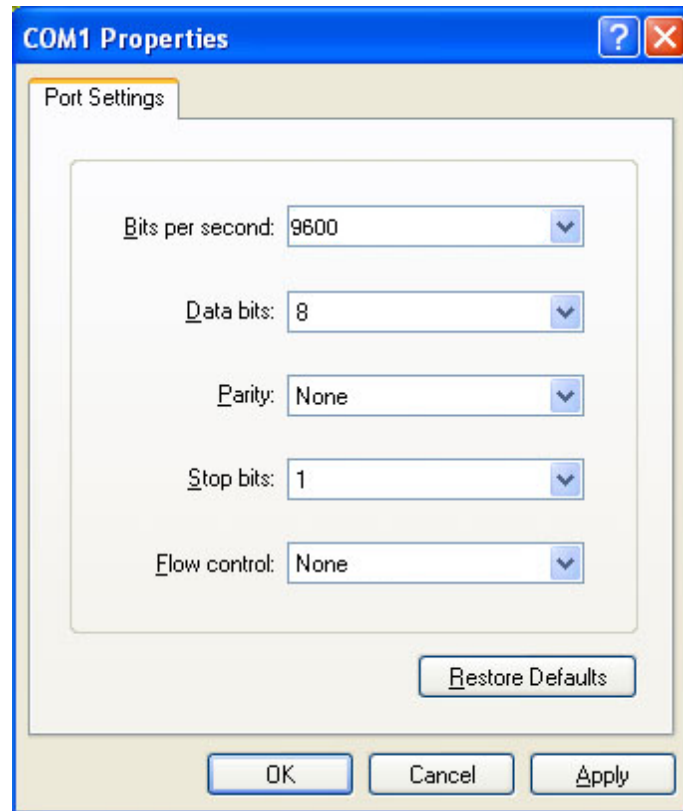


Figure B-0-21 COM Port Properties - Rescue

- Step 5** Now the HyperTerminal is started and ready for use, see Figure B-0-22.

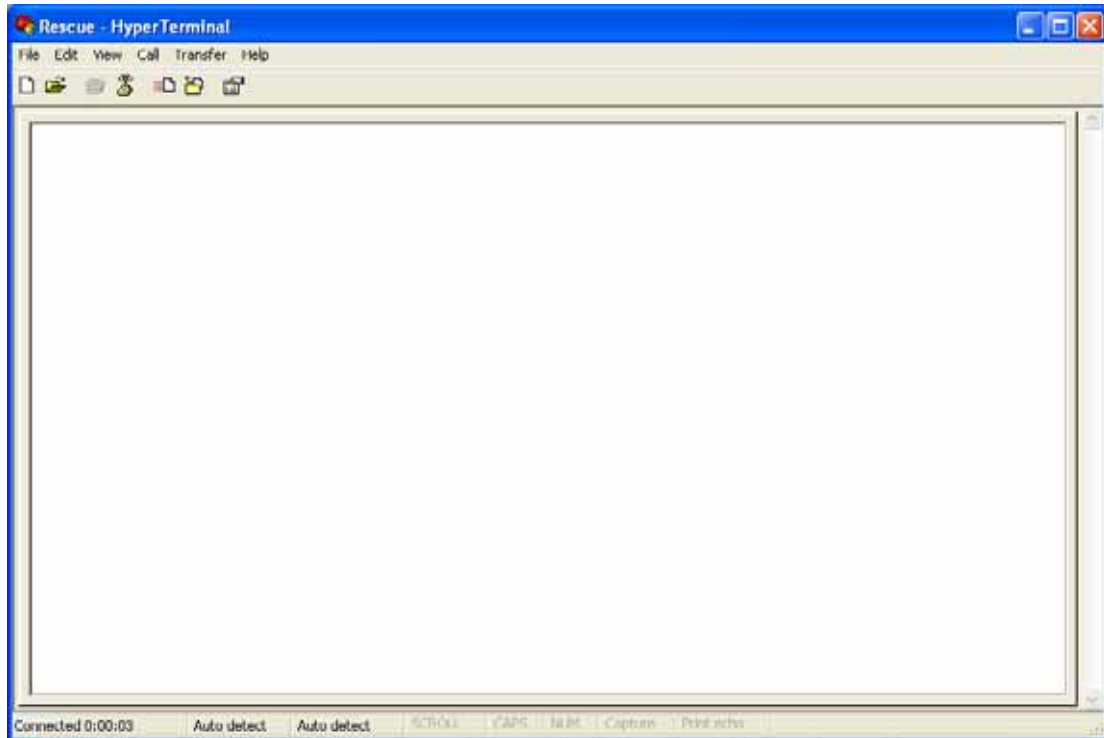
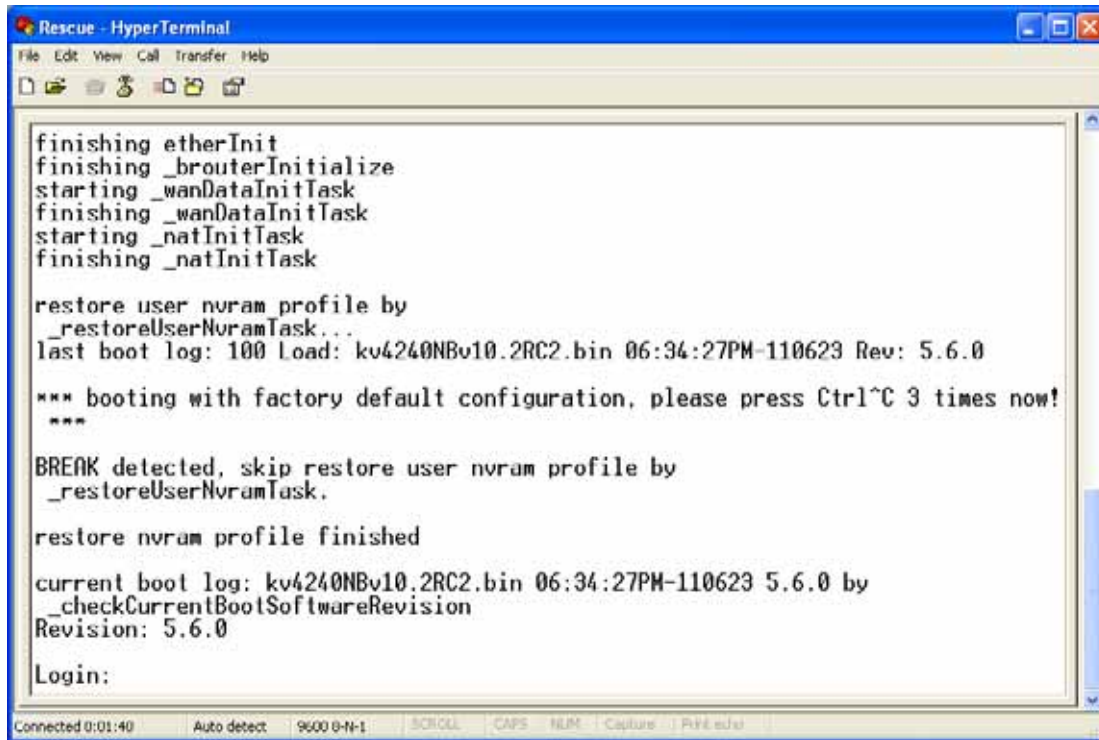


Figure B-0-22 The HyperTerminal Window - Rescue

- Step 6** Restart the Device; and during restarting, once the **“***booting with factory default configuration, please press Ctrl~C 3 times now!***”** prompt appears, please immediately press **<Ctrl + C>** keys three consecutive times within three seconds. Then the appearance of **“BREAK detected, skip restore user nvram profile by _restoreUserNvramTask.”** prompt means that the system has booted into **Rescue Mode** successfully.



```
Rescue - HyperTerminal
File Edit View Call Transfer Help
finishing etherInit
finishing _brouterInitialize
starting _wanDataInitTask
finishing _wanDataInitTask
starting _natInitTask
finishing _natInitTask

restore user nvram profile by
_restoreUserNvramTask...
last boot log: kv4240NBv10.2RC2.bin 06:34:27PM-110623 Rev: 5.6.0

*** booting with factory default configuration, please press Ctrl^C 3 times now!
***

BREAK detected, skip restore user nvram profile by
_restoreUserNvramTask.

restore nvram profile finished

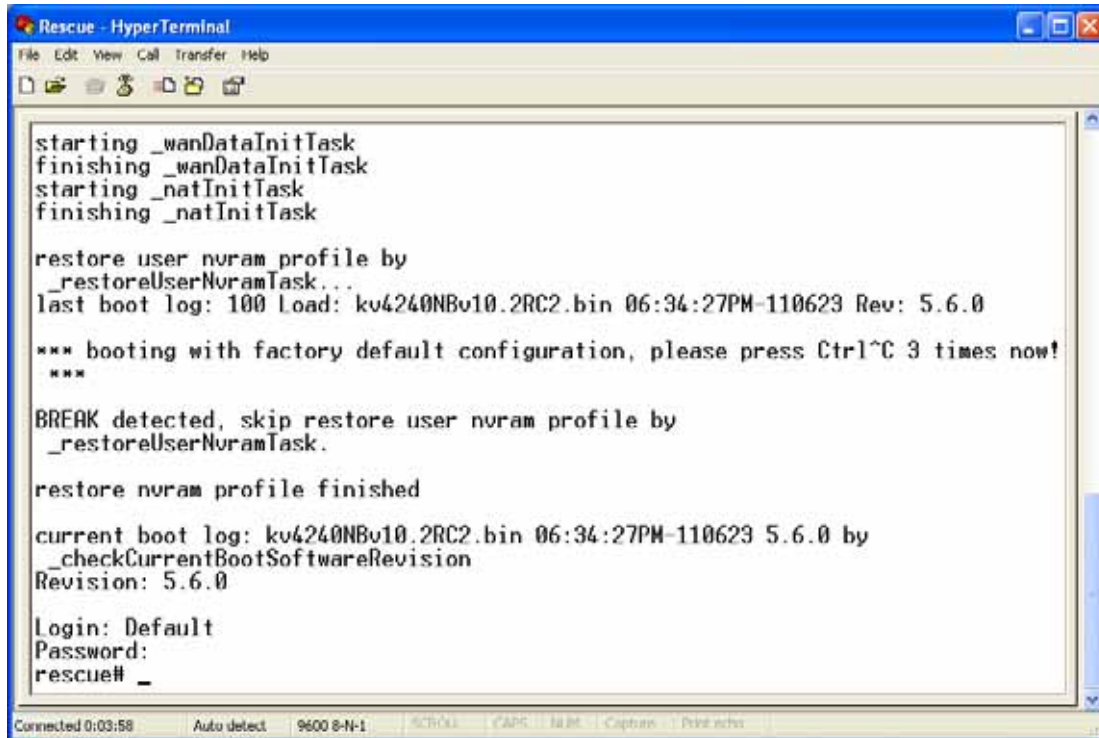
current boot log: kv4240NBv10.2RC2.bin 06:34:27PM-110623 5.6.0 by
_checkCurrentBootSoftwareRevision
Revision: 5.6.0

Login:

Connected 0:01:40 Auto detect 9600 0-N-1 SCROLL CAPS NEM Capture Print echo
```

Figure B-0-23 Boot into Rescue Mode - Rescue

Step 7 After the Device has booted into **Rescue Mode**, you can use the system default administrator account to login to the Device. Enter **Default** at the “**Login**” prompt and press **<Enter>** key, see Figure 8-24 Then the “**Password**” prompt appears; directly press **<Enter>** key. Then the “**rescue#**” prompt appears, which means that you have logged in to **Rescue Mode** configuration interface successfully, and the Device is ready to receive a command. Now you can perform any operation.



```
Rescue - HyperTerminal
File Edit View Call Transfer Help
starting _wanDataInitTask
finishing _wanDataInitTask
starting _natInitTask
finishing _natInitTask

restore user nvram profile by
_restoreUserNvramTask...
last boot log: 100 Load: kv4240NBv10.2RC2.bin 06:34:27PM-110623 Rev: 5.6.0

*** booting with factory default configuration, please press Ctrl^C 3 times now!
***

BREAK detected, skip restore user nvram profile by
_restoreUserNvramTask.

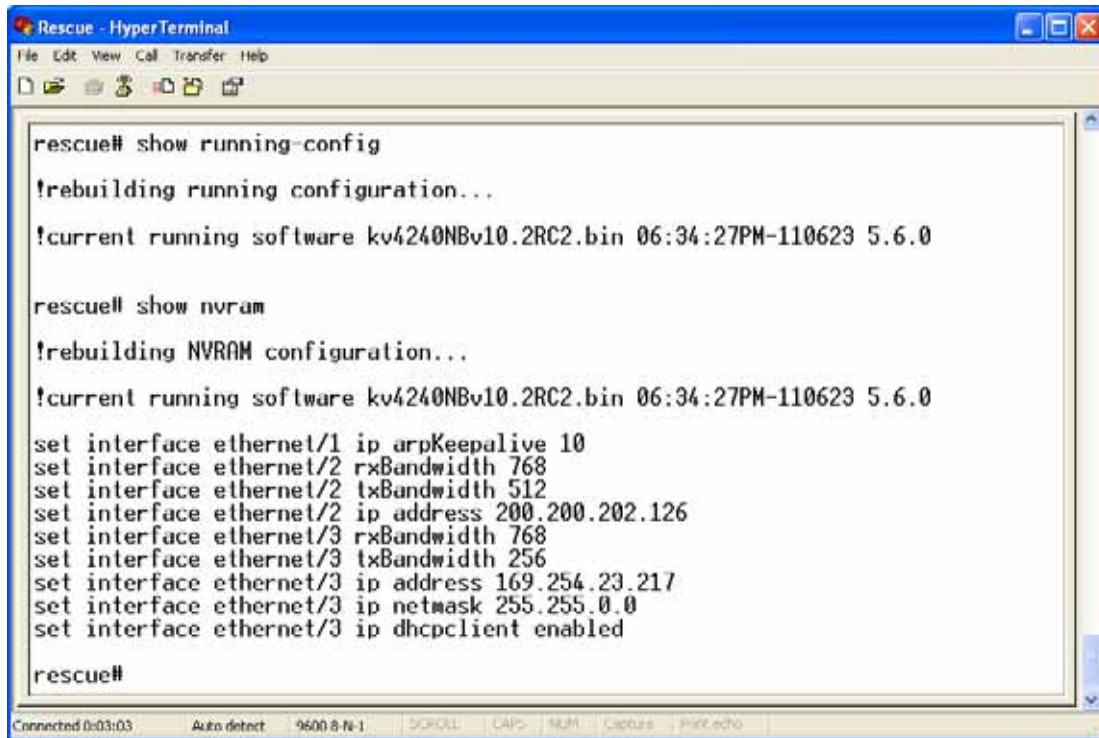
restore nvram profile finished

current boot log: kv4240NBv10.2RC2.bin 06:34:27PM-110623 5.6.0 by
_checkCurrentBootSoftwareRevision
Revision: 5.6.0

Login: Default
Password:
rescue# _
```

Figure B-0-24 Login to Rescue Mode Configuration Interface - Rescue

- Step 8** In **Rescue Mode** configuration interface, see Figure B-0-25, if you enter **show running-config** at the prompt and press **<Enter>** key, it will only output firmware version information, but not output any custom settings, which means that the system is running with the factory default settings; if you enter **show nvram** at the prompt and press **<Enter>** key, it will output not only firmware version information but also your custom settings.



```
rescue# show running-config
!rebuilding running configuration...
!current running software kv4240NBv10.2RC2.bin 06:34:27PM-110623 5.6.0

rescue# show nvram
!rebuilding NVRAM configuration...
!current running software kv4240NBv10.2RC2.bin 06:34:27PM-110623 5.6.0

set interface ethernet/1 ip arpKeepalive 10
set interface ethernet/2 rxBandwidth 768
set interface ethernet/2 txBandwidth 512
set interface ethernet/2 ip address 200.200.202.126
set interface ethernet/3 rxBandwidth 768
set interface ethernet/3 txBandwidth 256
set interface ethernet/3 ip address 169.254.23.217
set interface ethernet/3 ip netmask 255.255.0.0
set interface ethernet/3 ip dhcpclient enabled

rescue#
```

Figure B-0-25 View Settings - Rescue

**Note**

In **Rescue Mode**, it will only save the settings you have made in **Rescue Mode** configuration interface by **write** command, and all of your original custom settings will be lost. Thus if you want to save the original custom settings, please do the following: Perform **show nvram** command to display all the original custom settings firstly, and then re-enter the settings that you need by copy and paste function, lastly perform **write** command to save those settings; or save the settings that you need as a text file, and then perform **write** command, lastly re-enter the settings in **Normal Startup Mode** configuration interface.

Step 9 Finally, you need restart the Device to exit **Rescue Mode** configuration interface.

6. IP/MAC Binding and Access Control

This section mainly describes the characteristics of the IP/MAC binding and access control functions, and the relationship between them. Its purpose is to help you better understand them, and use them to flexibly control and manage the Internet behaviors of the LAN users to enhance network security.

To achieve network security management, you should firstly implement user identification, and then you should implement user authorization. On the Device, you can use IP/MAC binding feature to implement user identification, and use access control feature to use access control rules to control the Internet behaviors of the LAN users.

Refer to **section 12.2 IP/MAC Binding** for more information about IP/MAC binding; refer to **section 12.3 Firewall** for more information about access control.

A. IP/MAC Binding

The Device provides IP/MAC binding feature to implement user identification. Using the IP/MAC address pair as a unique user identity, you can protect the Device and your network against IP address theft, MAC address theft, IP spoofing attack, and MAC spoofing attack.

For those non-IP/MAC binding users (i.e., the users whose IP address and MAC address both are different from any IP/MAC binding's.), the Device allows them to access the Device and Internet by default. If you want to block them from accessing, please unselect the **Allow Undefined LAN PCs** check box in the **Security > IP/MAC Binding > IP/MAC Binding List** page.

IP/MAC binding feature can only act on the packets initiated from the LAN hosts to the Device or outside hosts, but cannot act on the packets within the LAN. If you change a LAN host's IP address or MAC address, this LAN host will be unable to access the Device and access the Internet through the Device, but it still can communicate with the other LAN hosts, such as, it can browse Network Neighborhood, use windows file and printer sharing services within the LAN, and so on.

B. Access Control

The Device allows you to create access control rules by referencing address groups, service groups and schedules. By default, as no access control rule exists on the Device, the Device will forward all the valid packets received by the LAN interface. After you have enabled access control, the Device will examine each packet received by the LAN interface to determine whether to forward or drop the packet, based on the criteria you specified in the access control rules.

C. The Relationship between Them

- 1) Using IP/MAC binding feature can only implement user identification, but cannot

control and manage the Internet behaviors of the LAN users. The latter is implemented by access control function module.

- 2) In most cases, you can create an access control rule for a group of users. If some users have the privileges of accessing the Internet, you can create an address group for these hosts even their IP addresses are discontinuous. Then you only need to create one access control rule by using the address group to meet the hosts' requirements, instead of creating a rule for each user respectively. Of course, you can create access control rules for individual users if needed.
- 3) On the Device, at first you can use IP/MAC binding feature to implement user identification, and then divide the LAN users into several address groups (the users with the same Internet access privileges are divided into the same group), lastly create different access control rules for different address groups. Thus, you can implement not only user identification, but also Internet behavior management of LAN users to ensure network security and efficient use of network resources.

D. Operation Process

When receiving a packet initiated from LAN to the Device or outside host, the Device will process the packet in the following order:

- 1) **User identification** (i.e., the packet is processed by the IP/MAC binding function module)
 - a) If the sender is a legal user, the packet will be allowed to pass, and then be further processed by the firewall access control function module.
 - b) If the sender is an illegal user, the packet will be dropped immediately
 - c) If the sender is an undefined user, there are two cases:
 - i. If the **Allow Undefined LAN PCs** check box is selected, the packet will be allowed to pass, and then be further processed by the firewall access control function module.
 - ii. Else, the packet will be dropped immediately.



Note

The definitions of legal user, illegal user and undefined user are as follows:

- **Legal User:** A legal user's IP and MAC address pair matches an IP/MAC binding whose **Allow Internet Access** check box is selected.
- **Illegal User:** A illegal user's IP and MAC address pair matches an IP/MAC binding whose **Allow Internet Access** check box is unselected; or the IP address or MAC address is the same with an IP/MAC binding's, but not both.

- **Undefined User:** An undefined user's IP address and MAC address both are different from any IP/MAC binding. The undefined users are all the users except legal and illegal users.

2) **User authorization** (i.e., the packet is processed by the firewall access control function module)

When receiving a packet initiated from LAN, the Device will analyze the packet by extracting its source MAC address, source IP address, destination IP address, protocol type (TCP, UDP or ICMP), port number, content, and the date and time at which the packet was received, and then compare them with each rule in the order in which the rules are listed in the **Access Control List**. The first rule that matches the packet will be applied to the packet, and the Device will forward or drop it according to this rule's action. Note that after a match is found, no further rules will be checked; and if no match is found, the Device will drop the packet to ensure security.

Note that if a schedule is referenced in an access control rule, you need judge whether the schedule is in effect or not at first. If the schedule has expired, it will be of no effect. In this case, if the access control rule still needs a time restriction, you should reconfigure the schedule.

E. Configuration Procedure

From the above analysis, we can see that if you want to configure the network access privileges for the LAN users, you need follow these steps:

- 1) At first, you need assign network access privileges to each LAN user: determine whether a user can access and pass through the Device, and assign specific Internet access privileges to the user.
- 2) Divide the LAN users into several address groups: the users with the same Internet access privileges are divided into the same address group.
- 3) Configure TCP/IP properties for each LAN user's host, and record each host's MAC address.
- 4) Go to the **Security > IP/MAC Binding** page to create IP/MAC bindings. Note that if you want to block the undefined LAN users from accessing the Device and Internet, you should unselect the **Allow Undefined LAN PCs** check box.
- 5) Go to the **Security > Address Group** page to create address groups.
- 6) Go to the **Security > Service Group** page to create service groups.
- 7) Go to the **System > Time** page to synchronize the system clock.
- 8) If you want to create the access control rules based on schedules, go to the **Security > Schedule** page to create schedules.

- 9) Go to the **Security > Firewall** page to create access control rules for each address group respectively.

7. How to find out who uses the most bandwidth?

By viewing the **NAT Statistics** list in the **Status > NAT Stats** page, you can find out the LAN user who uses the most bandwidth.

A. How to find out who has downloaded the most packets?

Query the **Rx Packets** in the **NAT Statistics** list: the larger value means the more downloaded packets. The most **Rx Packets** means the corresponding LAN user has downloaded the most packets from the Internet.

B. How to find out who has uploaded the most packets?

Query the **Tx Packets** in the **NAT Statistics** list: the larger value means the more uploaded packets. The most **Tx Packets** means the corresponding LAN user has uploaded the most packets to the Internet.

C. How to find out who is most active in the LAN?

Query the **Active Sessions** in the **NAT Statistics** list: the larger value means the user is more active. The most **Active Sessions** means the corresponding user is the most active in the LAN.

8. How to troubleshoot faults caused by worm viruses or hacker attacks on the Device?



Note

Each of the following points can only be used as a reference for network troubleshooting, but cannot be used as a basis for finding a network virus or attack.

A. How to find out who is using an IP/Port Scanner

When using an **IP/Port Scanner**, a host sends a larger number of ICMP/UDP/TCP packets to the target host in a very short time to detect whether the target IP address exists or there are open ports on the target host. The host using an **IP/Port Scanner** can generate a large amount of traffic, and too much traffic (i.e., too heavy network load) will cause network congestion, thus the other users may be unable to surf the Internet normally.

On the Device, you can find out who is using an **IP/Port Scanner** through the following three ways.

- 1) You can view the **NAT Statistics** list in the **Status > NAT Stats** page to find out if there is a LAN host whose **Overflow** is larger than 100. If a host's concurrent NAT sessions has reached the maximum value (configured in the **Security > NAT Session Limit** page), any further request for creating a new session will be discarded, and the **Overflow** will be updated synchronously; so if a host's **Overflow** is larger than 100, the host is suspicious of using an **IP/Port Scanner**.
- 2) You can view the **NAT Statistics** list in the **Status > NAT Stats** page to find out if there is a LAN host whose **Tx Packets** is far larger than **Rx Packets**. An **IP/Port Scanner** often uses a forged source IP address to send out packets, this will cause that the response packets cannot arrive at the sender; so if a host's **Tx Packets** is far larger than **Rx Packets**, the host is suspicious of using an **IP/Port Scanner**.
- 3) You can view system logs in the **Status > System Log** page to find out if there is a NAT exceeded log message. For example, the log message of "*NAT exceeded 192.168.16.221*" means that the host with IP address 192.168.16.221 has exceeded the maximum concurrent NAT sessions limited by the Device (configured in the **Security > NAT Session Limit** page), and this host is suspicious of an **IP/Port Scanner**.



Note

Recommended solution: It is recommended that you stop all the running

applications on that suspicious host, and then run an effective antivirus software, lastly restart or reinstall the operating system.

B. How to find out who is attacking an Internet host with DoS/DDoS

A **DoS** attack (denial-of-service attack) or **DDoS** attack (distributed denial-of-service attack) is an attempt to make a host resource unavailable to its intended users. When performing a **DoS/DDoS** attack, a host sends a larger number of packets to the target host (typically it is a web server) in a very short time to cause too heavy load on the host, thus the host is unable to provide normal services. The host performing **DoS/DDoS** attacks can generate a large amount of traffic, and too much traffic (i.e., too heavy network load) will cause network congestion, thus the other users may be unable to surf the Internet normally.

On the Device, you can find out who is performing a **DoS/DDoS** attack through the following three ways.

- 1) You can view the **NAT Statistics** list in the **Status > NAT Stats** page to find out if there is a LAN host whose **Tx Packets** is far larger than the other hosts', but its **Rx Packets** is very small or zero. When a LAN host attacks an Internet host with DoS/DDoS, it sends a large number of packets to the Internet host; so if a LAN host meets the above conditions, it is suspicious of performing a **DoS/DDoS** attack.

Note that the user who is uploading files via HTTP/FTP should be excluded.

- 2) You can view the **NAT Statistics** list in the **Status > NAT Stats** page to find out if there is a LAN host whose **Tx Packets** is far larger than **Rx Packets**. A DoS/DDoS attack program often uses a forged source IP address to send out packets, this will cause that the response packets cannot arrive at the sender; so if a host's **Tx Packets** is far larger than **Rx Packets**, the host is suspicious of performing a **DoS/DDoS** attack.
- 3) You can view system logs in the **Status > System Log** page to find out if there is a NAT exceeded log message. For example, the log message of "NAT exceeded 192.168.16.221" means that the host with IP address 192.168.16.221 has exceeded the maximum concurrent NAT sessions limited by the Device (configured in the **Security > NAT Session Limit** page), and this host is suspicious of performing a **DoS/DDoS** attack.



Note

Recommended solution: It is recommended that you stop all the running applications on that suspicious host, and then run an effective antivirus software, lastly restart or reinstall the operating system.

C. How to find out a host infected with Code Red worm virus?

You can view the **NAT Statistics** list in the **Status > NAT Stats** page to find out if there is a LAN host whose **Tx Packets** is very large but **Rx Packets** is very small or zero. If a host meets the above conditions and hasn't used any LAN server, the host is likely to be infected with **Code Red** worm virus.

D. How to find out a host performing a TCP SYN Flood, UDP Flood or ICMP Flood attack?

You can view the **NAT Statistics** list in the **Status > NAT Stats** page to find out if there is a LAN host whose **Tx Packets** is very large but **Rx Packets** is very small. If a host meets the above conditions, the host is likely to perform a **TCP SYN Flood, UDP Flood or ICMP Flood** attack.



Note

The user who is uploading files via HTTP/FTP should be excluded.

E. How to find out a host performing an ARP Spoofing attack?

You can view system logs in the **Status > System Log** page to find out if there is a LAN host whose MAC address is changing constantly, for example, the following log message means that the host with IP address 192.168.1.1 is likely to perform an ARP Spoofing attack.

MAC New 00:22:aa:00:22:bb

MAC Old 00:22:aa:00:22:aa

ARP SPOOF 192.168.1.1

F. How to find out a host infected with Blaster/Sasser virus

The host infected with **Blaster/Sasser** virus randomly sends out a large number of ICMP packets and broadcasts a large number of packets whose destination port is 135, 137, 139 or 445, thus it causes network congestion even the whole internal and external networks paralysis.

Go to the **Status > Session Monitor** page, select **All** from the **Filter Option** drop-down list, and then click **Query** button to view all the active NAT sessions in the **NAT Session List**. If there are many sessions whose **Protocol** is ICMP, and many sessions whose **Dest Port** is 135, 137, 139 or 445, the corresponding LAN host is likely to be infected with **Blaster/Sasser** virus.

If a host has been infected with **Blaster** virus, it has the following symptoms: inexplicably crashes or restarts itself; links in IE cannot be opened properly; copy and paste operation cannot be performed; sometimes there are certain applications running abnormally, such as Word; network grows slowly; there is a process named **msblast.exe** in Task Manager.

If a host has been infected with **Sasser** virus, it has the following symptoms: inexplicably

crashes or restarts itself; there is a process named **avserve.exe**, **avserve2.exe** or **skynetave.exe** in Task Manager; there is a virus file named **avserve.exe**, **avserve2.exe** or **skynetave.exe** in the system directory; system is running extremely slow, and CPU usage is 100%.

9. How to enable WAN ping respond?

To facilitate debugging and testing your Internet connections, the Device provides **Enable WAN Ping Respond** feature; that is, it allows you to ping each WAN interface's IP address to detect whether each Internet connection is normal. The operation is as follows: Go to the **Security > Attack Defense > External Defense** page, select the **Enable WAN Ping Respond** check box, and then click the **Save** button.

After you have enabled WAN ping respond, you can test each Internet connection by using **ping** command on an outside host. When you ping the IP address of a WAN interface, correct responses from the WAN interface means that the corresponding Internet connection is normal; else, the connection itself is abnormal, ping response is disabled on a device between your PC and Device, or there is a configuration error in the Device.

Appendix C Common IP Protocols

Protocol Name	Protocol Number	Full Name
IP	0	Internet Protocol
ICMP	1	Internet Protocol Message Protocol
IGMP	2	Internet Group Management
GGP	3	Gateway-Gateway Protocol
IPINIP	4	IP in IP Tunnel Driver
TCP	6	Transmission Control Protocol
EGP	8	Exterior Gateway Protocol
IGP	9	Interior Gateway Protocol
PUP	12	PARC Universal Packet Protocol
UDP	17	User Datagram Protocol
HMP	20	Host Monitoring Protocol
XNS-IDP	22	Xerox NS IDP
RDP	27	Reliable Datagram Protocol
GRE	47	General Routing Encapsulation
ESP	50	Encap Security Payload
AH	51	Authentication Header
RVD	66	MIT Remote Virtual Disk
EIGRP	88	Enhanced Interior Gateway Routing Protocol
OSPF	89	Open Shortest Path First

Appendix D Common Service Ports

Service Name	Port	Protocol	Description
echo	7	tcp	
echo	7	udp	
discard	9	tcp	
discard	9	udp	
systat	11	tcp	Active users
systat	11	udp	Active users
daytime	13	tcp	
daytime	13	udp	
qotd	17	tcp	Quote of the day
qotd	17	udp	Quote of the day
chargen	19	tcp	Character generator
chargen	19	udp	Character generator
ftp-data	20	tcp	FTP, data
ftp	21	tcp	FTP, control
telnet	23	tcp	
smtp	25	tcp	Simple Mail Transfer Protocol
time	37	tcp	timserver
time	37	udp	timserver
rlp	39	udp	Resource Location Protocol
nameserver	42	tcp	Host Name Server
nameserver	42	udp	Host Name Server
nicname	43	tcp	whois
domain	53	tcp	Domain Name Server
domain	53	udp	Domain Name Server
bootps	67	udp	Bootstrap Protocol Server
bootpc	68	udp	Bootstrap Protocol Client

tftp	69	udp	Trivial File Transfer
gopher	70	tcp	
finger	79	tcp	
http	80	tcp	World Wide Web
kerberos	88	tcp	Kerberos
kerberos	88	udp	Kerberos
hostname	101	tcp	NIC Host Name Server
iso-tsap	102	tcp	ISO-TSAP Class 0
rtnet	107	tcp	Remote Telnet Service
pop2	109	tcp	Post Office Protocol - Version 2
pop3	110	tcp	Post Office Protocol - Version 3
sunrpc	111	tcp	SUN Remote Procedure Call
sunrpc	111	udp	SUN Remote Procedure Call
auth	113	tcp	Identification Protocol
uucp-path	117	tcp	
nntp	119	tcp	Network News Transfer Protocol
ntp	123	udp	Network Time Protocol
epmap	135	tcp	DCE endpoint resolution
epmap	135	udp	DCE endpoint resolution
netbios-ns	137	tcp	NETBIOS Name Service
netbios-ns	137	udp	NETBIOS Name Service
netbios-dgm	138	udp	NETBIOS Datagram Service
netbios-ssn	139	tcp	NETBIOS Session Service
imap	143	tcp	Internet Message Access Protocol
pcmail-srv	158	tcp	PCMail Server
snmp	161	udp	
snmptrap	162	udp	SNMP trap
print-srv	170	tcp	Network PostScript
bgp	179	tcp	Border Gateway Protocol

irc	194	tcp	Internet Relay Chat Protocol
ipx	213	udp	IPX over IP
ldap	389	tcp	Lightweight Directory Access Protocol
https	443	tcp	MCom
https	443	udp	MCom
microsoft-ds	445	tcp	
microsoft-ds	445	udp	
kpasswd	464	tcp	Kerberos (v5)
kpasswd	464	udp	Kerberos (v5)
isakmp	500	udp	Internet Key Exchange
exec	512	tcp	Remote Process Execution
biff	512	udp	
login	513	tcp	Remote Login
who	513	udp	
cmd	514	tcp	
syslog	514	udp	
printer	515	tcp	
talk	517	udp	
ntalk	518	udp	
efs	520	tcp	Extended File Name Server
router	520	udp	route routed
timed	525	udp	
tempo	526	tcp	
courier	530	tcp	
conference	531	tcp	
netnews	532	tcp	
netwall	533	udp	For emergency broadcasts
uucp	540	tcp	
klogin	543	tcp	Kerberos login

kshell	544	tcp	Kerberos remote shell
new-rwho	550	udp	
remotefs	556	tcp	
rmonitor	560	udp	
monitor	561	udp	
ldaps	636	tcp	LDAP over TLS/SSL
doom	666	tcp	Doom Id Software
doom	666	udp	Doom Id Software
kerberos-adm	749	tcp	Kerberos administration
kerberos-adm	749	udp	Kerberos administration
kerberos-iv	750	udp	Kerberos version IV
kpop	1109	tcp	Kerberos POP
phone	1167	udp	Conference calling
ms-sql-s	1433	tcp	Microsoft-SQL-Server
ms-sql-s	1433	udp	Microsoft-SQL-Server
ms-sql-m	1434	tcp	Microsoft-SQL-Monitor
ms-sql-m	1434	udp	Microsoft-SQL-Monitor
wins	1512	tcp	Microsoft Windows Internet Name Service
wins	1512	udp	Microsoft Windows Internet Name Service
ingreslock	1524	tcp	
l2tp	1701	udp	Layer Two Tunneling Protocol
pptp	1723	tcp	Point-to-point tunnelling protocol
radius	1812	udp	RADIUS authentication protocol
radacct	1813	udp	RADIUS accounting protocol
nfsd	2049	udp	NFS server
knetd	2053	tcp	Kerberos de-multiplexor
man	9535	tcp	Remote Man Server

Appendix E Figure Index

Figure 0-1 IP/MAC Binding List	2
Figure 0-2 NAT Statistics	4
Figure 0-3 Enable DNS Proxy	5
Figure 2-1 Connecting the UTT 2512 to the LAN and Internet.....	24
Figure 2-2 LEDs on the UTT 2512	25
Figure 2-3 Install the U2000 in a Rack	27
Figure 2-4 Connecting the U2000 to the LAN and Internet.....	28
Figure 2-5 LEDs on the U2000.....	29
Figure 3-1 Entering IP address in the Address Bar	34
Figure 3-2 Login Screen	34
Figure 3-3 Homepage - System Info Page.....	35
Figure 3-4 Shortcut Icons	35
Figure 4-1 Running the Quick Wizard	37
Figure 4-2 LAN Settings	38
Figure 4-3 Choosing an Internet Connection Type.....	39
Figure 4-4 Choose PPPoE as the Connection Type	41
Figure 4-5 PPPoE Internet Connection Settings	41
Figure 4-6 Choosing Static IP as the Connection Type.....	42
Figure 4-7 Static IP Internet Connection Settings	42
Figure 4-8 Choosing DHCP as the Connection Type.....	44
Figure 4-9 Viewing and Saving the Settings Made in the Quick Wizard	45
Figure 5-1 System Up Time.....	46
Figure 5-2 System Resource Usage Information	47
Figure 5-3 System Version	48
Figure 5-4 Port Status.....	48
Figure 5-5 Interface Rate Chart.....	49
Figure 5-6 NAT Statistics List	51
Figure 5-7 DHCP Pool Statistics List.....	53
Figure 5-8 DHCP Server Statistics List	55
Figure 5-9 DHCP Conflict Statistics List	56
Figure 5-10 DHCP Client Statistics List.....	57
Figure 5-11 DHCP Relay Statistics List.....	58
Figure 5-12 Interface Statistics List	60

Figure 5-13 Routing Table	62
Figure 5-14 Session Monitor Settings	65
Figure 5-15 NAT Session List.....	67
Figure 5-16 Session Monitor Settings - Example1	68
Figure 5-17 NAT Session List - Example1.....	69
Figure 5-18 Session Monitor Settings - Example2	70
Figure 5-19 NAT Session List - Example2.....	70
Figure 5-20 Session Monitor Settings - Example3	71
Figure 5-21 NAT Session List - Example3.....	71
Figure 5-22 Session Monitor Settings - Example3	72
Figure 5-23 NAT Session List - Example4.....	73
Figure 5-24 System Log Settings	74
Figure 5-25 System Logs	75
Figure 5-26 Enable Web Log.....	78
Figure 5-27 View Web Logs	79
Figure 5-28 Enable Application Traffic Statistics	80
Figure 5-29 Application Traffic Statistics List	80
Figure 5-30 User Traffic Statistics List.....	81
Figure 5-31 WAN Traffic Statistics List	83
Figure 6-1 LAN Interface Settings	84
Figure 6-2 WAN Internet Connection List.....	86
Figure 6-3 WAN List - PPPoE Internet Connection	89
Figure 6-4 WAN List DHCP Internet Connection.....	90
Figure 6-5 PPPoE Internet Connection Settings	92
Figure 6-6 Static IP Internet Connection Settings	96
Figure 6-7 DHCP Internet Connection Settings	98
Figure 6-8 Delete the Internet Connection	99
Figure 6-9 Prompt Dialog Box - Delete an Internet Connection.....	100
Figure 6-10 Enable ID Binding	107
Figure 6-11 Global Settings - Full Load Balancing	108
Figure 6-12 Global Settings - Partial Load Balancing	109
Figure 6-13 Detection and Weight Settings.....	111
Figure 6-14 Load Balancing List.....	112
Figure 6-15 DHCP Server Settings	115
Figure 6-16 DHCP Auto Binding.....	117
Figure 6-17 Enable DNS Proxy	117

Figure 7-1 Static Route Settings.....	121
Figure 7-2 Static Route List.....	123
Figure 7-3 Static Route Settings - Example One	124
Figure 7-4 Static Route Settings - Example Two.....	125
Figure 7-5 Static Route PDB Settings	127
Figure 7-6 Static Route PDB Settings - Example One	128
Figure 7-7 Static Route PDB Settings - Example Two	129
Figure 7-8 Policy-Based Routing Settings.....	131
Figure 7-9 Enable Policy-Based Routing.....	133
Figure 7-10 PBR List	134
Figure 7-11 Enable DNS Redirection	135
Figure 7-12 DNS Redirection List.....	136
Figure 7-13 DNS Redirection Settings	137
Figure 7-14 Enable Plug and Play.....	139
Figure 7-15 SNMP Settings	141
Figure 7-16 SYSLOG Settings	143
Figure 7-17 Apply for a DDNS Account from IPLink.com.cn	146
Figure 7-18 DDNS Settings Related to iplink.com.cn.....	147
Figure 7-19 Apply for a DDNS Account from 3322.org.....	148
Figure 7-20 DDNS Settings Related to 3322.org	149
Figure 7-21 Requesting for an IP Address from a DHCP Server	153
Figure 7-22 Select DHCP Client.....	161
Figure 7-23 DHCP Client Settings.....	161
Figure 7-24 DHCP Client List	163
Figure 7-25 Select DHCP Server	164
Figure 7-26 DHCP Server Global Settings	165
Figure 7-27 DHCP Manual Binding List.....	165
Figure 7-28 DHCP Manual Binding Settings	166
Figure 7-29 DHCP Address Pool List	168
Figure 7-30 DHCP Address Pool Settings.....	170
Figure 7-31 Select DHCP Relay Agent.....	173
Figure 7-32 DHCP Relay Agent Settings.....	174
Figure 7-33 DHCP Relay Agent List	176
Figure 7-34 Select Raw Option	177
Figure 7-35 Raw Option Settings	177
Figure 7-36 Raw Option List.....	178

Figure 7-37 Network Topology where DHCP Server and Clients on Same Subnet.....	180
Figure 7-38 DHCP Server Global Settings - Example.....	181
Figure 7-39 DHCP Address Pool Settings - Example (pool1)	182
Figure 7-40 DHCP Address Pool Settings - Example (pool2)	183
Figure 7-41 DHCP Manual Binding Settings - Example.....	184
Figure 7-42 Network Topology Where DHCP Client is Applied on WAN Interface.....	185
Figure 7-43 DHCP Client Settings - Example.....	185
Figure 7-44 Network Topology Where the Device Acting as a DHCP Relay Agent	186
Figure 7-45 DHCP Relay Agent Settings - Example	187
Figure 7-46 Raw Option Settings - Example	188
Figure 7-47 Network Topology for DHCP Comprehensive Example.....	191
Figure 7-48 DHCP Server Global Settings - Comprehensive Example	192
Figure 7-49 DHCP Address Pool Settings - Comprehensive Example (pool1).....	193
Figure 7-50 DHCP Relay Agent Settings - Comprehensive Example (DHCP Relay1).....	194
Figure 7-51 Port Mirroring Settings	196
Figure 7-52 Port-Based VLAN Setup	197
Figure 7-53 Miscellaneous	198
Figure 7-54 Scheduled Task Settings.....	199
Figure 8-1 Port Forwarding Settings.....	202
Figure 8-2 Port Forwarding List.....	203
Figure 8-3 Port Forwarding Settings - Example One	205
Figure 8-4 Port Forwarding Settings - Example Two.....	205
Figure 8-5 Port Forwarding Settings - Example Three.....	206
Figure 8-6 Global DMZ Host Settings.....	208
Figure 8-7 Interface DMZ Host Settings	208
Figure 8-8 EasyIP NAT Rule Settings.....	215
Figure 8-9 One2One NAT Rule Settings	216
Figure 8-10 Passthrough NAT Rule Settings.....	217
Figure 8-11 NAT Rule List.....	218
Figure 8-12 EasyIP NAT Rule Settings - Example	221
Figure 8-13 Network Topology for One2One NAT Rule Configuration Example.....	222
Figure 8-14 One2One NAT Rule Settings - Example.....	223
Figure 8-15 Network Topology for Passthrough NAT Rule Configuration Example	224
Figure 8-16 Passthrough NAT Rule Settings - Example	225
Figure 8-17 Enable UPnP.....	226
Figure 8-18 UPnP Port Forwarding List.....	227

Figure 9-1 PPPoE Discovery Stage Flows	228
Figure 9-2 PPPoE Server Global Settings.....	230
Figure 9-3 Internet Access Control Settings	231
Figure 9-4 PPPoE Account Settings.....	233
Figure 9-5 PPPoE Account List	236
Figure 9-6 PPPoE Accounts Import.....	237
Figure 9-7 PPPoE Account Billing mechanism.....	238
Figure 9-8 PPPoE Account Billing By Date	239
Figure 9-9 PPPoE Account Billing By Hour	240
Figure 9-10 PPPoE Account Billing By Traffic	240
Figure 9-11 PPPoE IP/MAC Binding Settings	241
Figure 9-12 PPPoE IP/MAC Binding List.....	242
Figure 9-13 PPPoE Status List.....	244
Figure 9-14 PPPoE Server Global Settings - Example	246
Figure 9-15 Internet Control Settings - Example	247
Figure 9-16 Configuring the Universal PPPoE Account - Example	248
Figure 9-17 Configuring the Advanced PPPoE Account - Example	249
Figure 9-18 Configuring a PPPoE IP/MAC Binding – Example	249
Figure 9-19 PPPoE Account Expiration Notice by Date	251
Figure 9-20 PPPoE Account Expiration Notice Preview – Example 1	252
Figure 9-21 PPPoE Account Expiration Notice by Hours	253
Figure 9-22 PPPoE Account Expiration Notice Preview – Example 2	254
Figure 9-23 PPPoE Account Expiration Notice by Traffic.....	255
Figure 9-24 PPPoE Account Expiration Notice Preview – Example 3	256
Figure 10-1 Rate Limit Global Settings.....	260
Figure 10-2 Rate Limit Rule Settings.....	262
Figure 10-3 Rate Limit Rule List	264
Figure 10-4 P2P Rate Limit Settings	266
Figure 10-5 Preferential Forwarding for Some Applications Traffic	268
Figure 10-6 Rate Limit Global Settings - Example One	270
Figure 10-7 Rate Limit Rule Settings - Example One	271
Figure 10-8 P2P Rate Limit Settings - Example One	271
Figure 10-9 Rate Limit Rule 1 Settings - Example Two.....	273
Figure 10-10 Rate Limit Rule 2 Settings - Example Two.....	274
Figure 10-11 Rate Limit Rule 3 Settings - Example Two.....	275
Figure 10-12 Enable Preferential Forwarding for Web Traffic- Example Two	275

Figure 11-1 User Status List	277
Figure 11-2 Personal Rate Limit Settings	279
Figure 11-3 Personal Internet Behavior Management Settings.....	280
Figure 11-4 Internet Behavior Management Policy Settings	282
Figure 11-5 Internet Behavior Management Policy List.....	286
Figure 11-6 Policy Database List	289
Figure 11-7 Policy Database Version Check	290
Figure 11-8 Import Policy Database	291
Figure 11-9 Enable QQ Whitelist	292
Figure 11-10 QQ Whitelist Settings	292
Figure 11-11 QQ Whitelist.....	293
Figure 11-12 Internet Management Behavior Example - Policy 1	296
Figure 11-13 Figure 11-9 Internet Management Behavior Example - Policy 2.....	297
Figure 11-14 Internet Management Behavior Example - Policy 3	298
Figure 11-15 Internet Management Behavior Example - Enable QQ Whitelist	298
Figure 11-16 Internet Management Behavior Example -QQ Whitelist	299
Figure 11-17 One-Time Notice Settings - Customized Mode	301
Figure 11-18 One-Time Notice Preview - Example	302
Figure 11-19 One-Time Notice Settings - URL Mode	303
Figure 11-20 Daily Notice Settings	304
Figure 11-21 Enable Web Authentication	304
Figure 11-22 Web Authentication User Account Settings	305
Figure 11-23 Web Authentication User Account List	305
Figure 11-24 Web Authentication Login Page	306
Figure 11-25 Web Authentication Prompt Page	307
Figure 12-1 Internal Attack Defense Settings	309
Figure 12-2 External Attack Defense Settings.....	311
Figure 12-3 IP/MAC Binding List - Example One	315
Figure 12-4 IP/MAC Binding List - Example Two	316
Figure 12-5 IP/MAC Binding Settings.....	317
Figure 12-6 IP/MAC Binding Global Setup	318
Figure 12-7 IP/MAC Binding List	319
Figure 12-8 IP/MAC Binding List - Example Three	322
Figure 12-9 IP/MAC Binding List - Example Four	323
Figure 12-10 Access Control Rule Settings.....	328
Figure 12-11 Enable Access Control	330

Figure 12-12 Access Control List.....	330
Figure 12-13 The Schedule of work Settings - Example 1	333
Figure 12-14 The Address Group of TD_FD Settings - Example 1	333
Figure 12-15 The Service Group of WEB_FTP Settings - Example 1.....	334
Figure 12-16 The Access Control Rule 1 Settings - Example 1	335
Figure 12-17 The Access Control Rule 2 Settings - Example 1	336
Figure 12-18 Enable Access Control - Example 1.....	336
Figure 12-19 The Address Group of Inside Settings - Example 2.....	337
Figure 12-20 The Address Group of Outside Settings - Example 2	338
Figure 12-21 The Access Control Rule 1 Settings - Example 2	339
Figure 12-22 The Access Control Rule 2 Settings - Example 2	340
Figure 12-23 The Access Control Rule 2 Settings - Example 2.....	341
Figure 12-24 Enable Access Control - Example 2.....	341
Figure 12-25 Domain Filtering Settings.....	342
Figure 12-26 Domain Blocking Notice.....	344
Figure 12-27 Domain Name Blocking Notice Preview	345
Figure 12-28 NAT Session Limit Rule Settings	346
Figure 12-29 NAT Session Limit Rule List.....	347
Figure 12-30 Address Group Settings	350
Figure 12-31 Address Group List.....	351
Figure 12-32 Service Group Settings	355
Figure 12-33 Service Group List.....	357
Figure 12-34 Schedule Settings	360
Figure 12-35 Schedule List.....	361
Figure 12-36 Schedule Details	362
Figure 12-37 Schedule Settings Example	364
Figure 13-1 Administrator Settings	365
Figure 13-2 Administrator List.....	366
Figure 13-3 System Time - Enable SNTP	368
Figure 13-4 System Time - Set Time Manually	369
Figure 13-5 Save Firmware to Local PC	370
Figure 13-6 Firmware Version Details	370
Figure 13-7 Upgrade Firmware	371
Figure 13-8 Backup Configuration	372
Figure 13-9 Restore Configuration	373
Figure 13-10 Restore Default	373

Figure 13-11 Remote Admin Settings.....	374
Figure 13-12 WEB Server	376
Figure 13-13 Restart the Device.....	378
Figure 13-14 Prompt Dialog Box - Restart the Device	378
Figure 13-15 Restarting.....	378
Figure B-0-1 Viewing PPPoE Internet Connection Status in WAN List.....	383
Figure B-0-2 PPPoE Connection Settings (Part).....	385
Figure B-0-3 Routing Table - Example 1	385
Figure B-0-4 Routing Table - Example 2	386
Figure B-0-5 View DHCP Internet Connection Status Information.....	387
Figure B-0-6 Routing Table - Example 3	388
Figure B-0-7 New Connection - Term9600	390
Figure B-0-8 Choose a COM Port - Term9600.....	391
Figure B-0-9 COM Port Properties - Term9600.....	391
Figure B-0-10 HyperTerminal Window - Term9600	392
Figure B-0-11 Login to the Device - Term9600.....	393
Figure B-0-12 Reset to Factory Default Settings - Term9600	394
Figure B-0-13 New Connection - Term115200	395
Figure B-0-14 Choose a COM Port - Term115200	396
Figure B-0-15 COM Port Properties - Term115200	397
Figure B-0-16 The HyperTerminal Window - Term115200.....	397
Figure B-0-17 Login to the Device - Term115200.....	398
Figure B-0-18 Reset to Factory Default Settings - Term115200.....	399
Figure B-0-19 New Connection - Rescue.....	401
Figure B-0-20 Choose a COM port - Rescue	401
Figure B-0-21 COM Port Properties - Rescue.....	402
Figure B-0-22 The HyperTerminal Window - Rescue	403
Figure B-0-23 Boot into Rescue Mode - Rescue.....	404
Figure B-0-24 Login to Rescue Mode Configuration Interface - Rescue	405
Figure B-0-25 View Settings - Rescue	406

Appendix F Table Index

Table 0-1 Factory Default Settings of Interfaces	6
Table 0-2 Document Organization	13
Table 1-1 Detailed Specifications	22
Table 2-1 Description of the System LEDs on the UTT 2512	26
Table 2-2 Description of the Port LEDs on the UTT 2512	26
Table 2-3 Description of the System LEDs on the U2000	29
Table 2-4 Description of the Port LEDs on the U2000.....	30
Table 3-1 Detailed Description of Shortcut Icons	36
Table 5-1 System Logs List	78
Table 6-1 Description of PPPoE Connection Status.....	87
Table 6-2 Description of Static IP Connection Status.....	88
Table 6-3 Description of DHCP Connection Status	88
Table 6-4 Detection Method and Detection Target IP.....	104
Table 7-1 Reserved Detection Route Name	121
Table 7-2 DHCP Message Types.....	155
Table 7-3 DHCP Relay Agent Forwarding Policies.....	160
Table 7-4 DHCP Relay Agent IP Addresses and IDs - Comprehensive Example.....	189
Table 12-1 The System Default Access Control Rules	327
Table B-0-1 PPPoE Dial-up System Logs	384