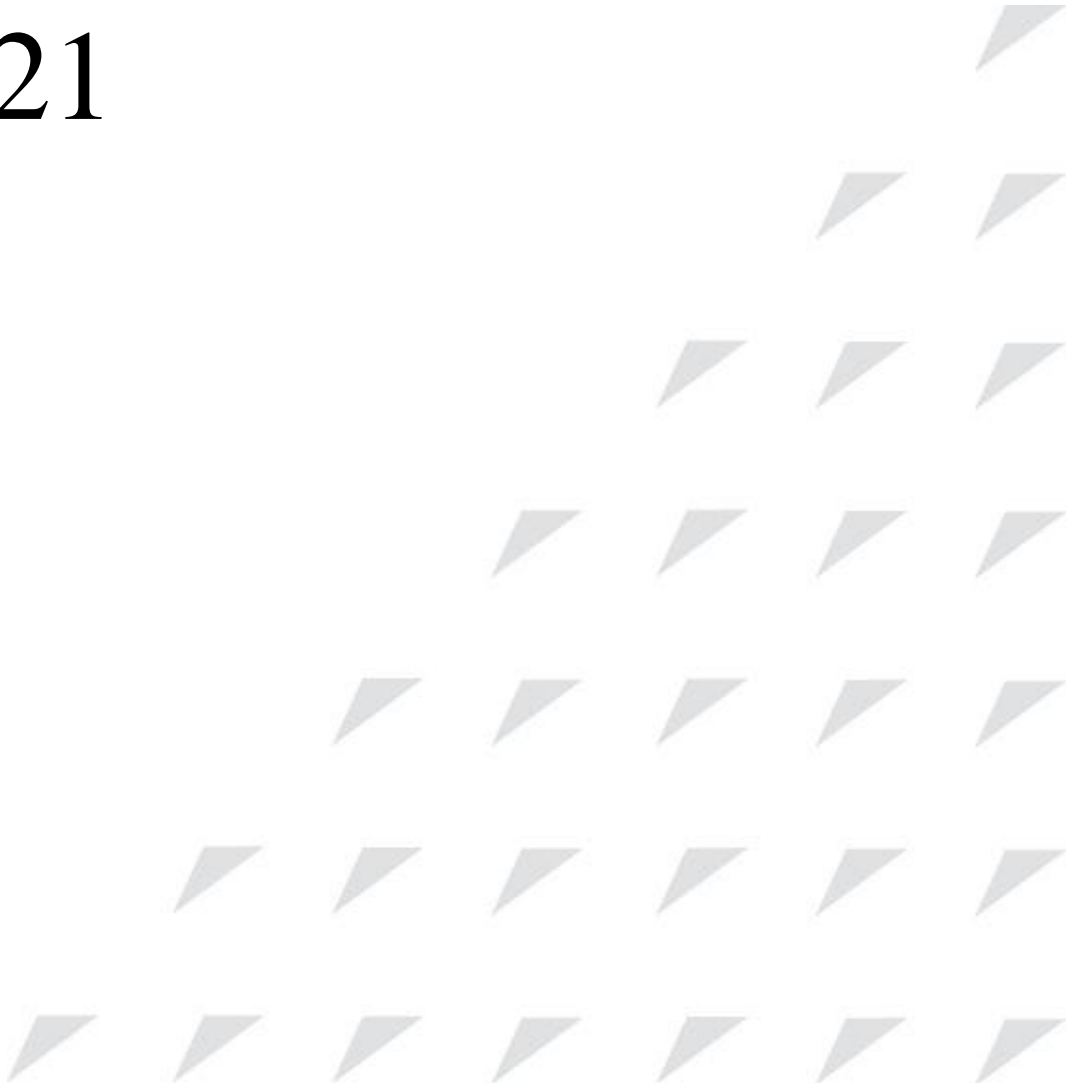


LR-2G21



Preface

Objectives

This guide describes features and Web configurations supported by the LAVA family multi-service intelligent gateway based on the RCIOS V2.10 software version. The contents include configuration preparation, overview, fast guide, basic principles and configuration procedures of interface configurations, network configurations, VPN configurations, QoS configurations, remote management configurations, user management configurations, voice configurations, security configurations, and system configurations. In addition, this guide provides typical configuration examples. The appendix lists terms and abbreviations involved in this guide.

By reading this guide, you can master the principles and configurations of the LAVA family multi-service intelligent gateway, as well as how to network with it.

Versions



The following table lists the product versions related to documents.



Product name	Hardware version	Software version
LR-2G211	A	RCIOS V2.10

Conventions

Symbol conventions

The symbols that may be found in this document are defined as follows.

Symbol	Description
 Warning	Indicates a hazard with a medium or low level of risk which, if not avoided, could result in minor or moderate injury.
 Caution	Indicates a potentially hazardous situation that, if not avoided, could cause equipment damage, data loss, and performance degradation, or unexpected results.

Symbol	Description
 Note	Provides additional information to emphasize or supplement important points of the main text.
 Tip	Indicates a tip that may help you solve a problem or save time.

General conventions

Convention	Description
Times New Roman	Normal paragraphs are in Times New Roman.
Arial	Paragraphs in Warning, Caution, Notes, and Tip are in Arial.
Boldface	Names of files, directories, folders, and users are in boldface . For example, log in as user root .
<i>Italic</i>	Book titles are in <i>italics</i> .
Lucida Console	Terminal display is in <code>Lucida Console</code> .

Interface conventions

Convention	Description
Boldface	Buttons, menus, parameters, tabs, windows, and dialog titles are in boldface . For example, click OK .
>	Multi-level menus are in boldface and separated by the ">" signs. For example, choose File > Create > Folder .

Keyboard operation

Format	Description
Key	Press the key. For example, press Enter and press Tab .
Key 1+Key 2	Press the keys concurrently. For example, pressing Ctrl+C means the two keys should be pressed concurrently.
Key 1, Key 2	Press the keys in turn. For example, pressing Alt, A means the two keys should be pressed in turn.

Mouse operation

Action	Description
Click	Select and release the primary mouse button without moving the pointer.
Double-click	Press the primary mouse button twice continuously and quickly without moving the pointer.
Drag	Press and hold the primary mouse button and move the pointer to a certain position.

Change history

Updates between document versions are cumulative. Therefore, the latest document version contains all updates made to previous versions.

Issue 01 (2013-05-28)

Initial commercial release

Contents

1 Preparing for configurations.....	19
1.1 Management modes.....	19
1.2 Web mode.....	19
1.2.1 Establishing configuration environment	19
1.2.2 Learning the Web configuration interface	21
1.3 NView NNM mode	23
2 Device information	24
2.1 Introduction to the Device interface	24
2.2 Device information.....	25
3 Quick guide.....	26
3.1 Broadband connection configuration	26
3.2 LAN configuration	27
3.3 Wireless routing configuration	28
3.4 Complete rapid configuration guide.....	29
4 Interface configurations.....	31
4.1 WAN.....	31
4.1.1 WAN0 configuration	31
4.1.2 WAN1 configuration	38
4.2 LAN	38
4.2.1 VLAN interface configuration	38
4.2.2 VLAN configuration	40
4.2.3 IPv6 configuration	41
4.2.4 ETH configuration	42
4.3 DMZ.....	43
4.3.1 DMZ.....	43
4.4 WLAN.....	43
4.4.1 Basic configuration	43
4.4.2 Advanced configuration	46
4.4.3 Wireless interface.....	48
4.4.4 WPS configuration	48
4.5 3G.....	49

4.5.1 Basic configuration	49
4.5.2 Advanced configuration	50
4.5.3 Flow warning	51
4.6 GRE.....	52
4.7 Link backup.....	54
4.8 Configuration examples	55
4.8.1 Example for configuring the WLAN interface in bridge mode.....	55
4.8.2 Example for configuring the WAN interface in router mode	57
4.8.3 Example for configuring link backup.....	59
5 Network configurations.....	62
5.1 NAT.....	63
5.1.1 ALG	63
5.1.2 Virtual server.....	63
5.1.3 Source NAT.....	64
5.1.4 One-to-one address translation.....	65
5.2 DHCP.....	66
5.2.1 DHCP service.....	66
5.2.2 DHCP address pool.....	67
5.2.3 Excluded addresses	68
5.2.4 IP/MAC binding.....	69
5.2.5 DHCP monitoring	69
5.2.6 Option60 address pool	70
5.3 DNS.....	71
5.4 Route	72
5.5 Static route	72
5.6 Policy route	73
5.7 RIP	75
5.7.1 RIP basic configuration.....	75
5.7.2 Advanced configuration	75
5.8 OSPF.....	77
5.8.1 OSPF configuration	77
5.8.2 Neighbor information.....	80
5.9 Route filter	80
5.9.1 Prefix list config.....	80
5.9.2 Interface filtering	81
5.10 Multicast.....	82
5.11 EoIP.....	83
5.11.1 EoIP configuration	83
5.12 DDNS.....	84
5.13 Page push	85
5.14 DHCPv6.....	86

5.14.1 DHCPv6 services	86
5.14.2 DHCPv6 address pool	87
5.14.3 Prefix/DUID binding.....	88
5.15 IPv6	89
5.15.1 Basic configuration	89
5.15.2 Static route	89
5.15.3 Routing table	90
5.15.4 6RD tunnel configuration.....	90
5.16 UPnP config	91
5.16.1 UPnP config	91
5.17 Configuration examples	92
5.17.1 Example for configuring static route.....	92
5.17.2 Example for configuring policy route	93
6 VPN configurations	97
6.1 L2TP VPN.....	97
6.1.1 L2TP Client.....	97
6.1.2 L2TP Server	98
6.1.3 L2TP Information.....	99
6.2 IPSec VPN	100
6.2.1 IPSec VPN	100
6.2.2 IPSec monitor.....	103
6.2.3 Binding IPSec name.....	104
6.3 PKI management	105
6.3.1 CA certificate	105
6.3.2 Local certificate	105
6.4 Configuration examples	106
6.4.1 Example for configuring L2TP VPN	106
6.4.2 Example for configuring IPSec VPN.....	107
7 QoS.....	110
7.1 Rate limit per user	110
7.2 Advanced rate limit	111
7.3 Advanced QoS config.....	113
7.4 Session counter limit	116
7.5 Connection counter management	117
7.6 Configuration examples	118
7.6.1 Example for configuring rate limit per user	118
8 Remote configuration.....	120
8.1 TR-069	120
8.2 SNMP.....	121
8.2.1 SNMP.....	121
8.2.2 USM user	122

8.3 Remote configuration	123
8.4 Syslog	124
8.4.1 Local	124
8.4.2 Remote	125
8.4.3 Mail	126
8.5 Configuration examples	127
8.5.1 Example for configuring Syslog	127
9 User management configurations	130
9.1 Um	130
9.2 WebAuth	132
9.2.1 Authentiction option	132
9.2.2 Whitelist	133
9.3 Online User	133
9.4 AuthenServer	134
9.4.1 RADIUS Authentication	134
9.4.2 LDAP Authentication	135
9.5 Configuration examples	136
9.5.1 Example for configuring user authentication	136
10 Voice configurations	139
10.1 System	139
10.2 Line	141
10.3 SIP	143
10.3.1 Server configuration	143
10.3.2 User authentication	146
10.3.3 Local number	147
10.3.4 Service configuration	148
10.3.5 Dialling rules	149
10.4 H.248	151
10.4.1 MG configuration	151
10.4.2 MGC configuration	152
10.4.3 TID configuration	153
10.4.4 Port status	154
10.5 Fax	155
10.6 Statistic	156
10.6.1 POTS call accounting	156
10.6.2 RTP call accounting	157
10.7 Configuration examples	158
10.7.1 Example for configure SIP-based VoIP phone	158
10.7.2 Example for configuring H.248-based VoIP phone	165
11 Security configurations	173
11.1 Firewall	173

11.2 Web Filter	174
11.2.2 Web Filter	175
11.2.3 Local update	177
11.3 Access control	178
11.3.1 Policy of access control	178
11.3.2 Time object	179
11.3.3 Service object	181
11.3.4 Address object	182
11.4 IPv6 AC	183
11.4.1 IPv6 policy of access control	183
11.5 MAC filter	185
11.6 ARP prevent	186
11.6.1 Prevent ARP attack	186
11.6.2 Active protection	186
11.6.3 IP-MAC bind	188
11.6.4 Custom contract	189
11.6.5 ARP table	190
11.6.6 Monitor	190
11.7 Anti-DDoS	191
11.8 Configuration examples	192
11.8.1 Example for configuring MAC filter	192
11.8.2 Example for configuring anti-ARP attack	194
11.8.3 Example for configuring anti-DDoS attack	196
12 System configurations	199
12.1 Reboot	199
12.2 Administrator	200
12.2.1 Administrator	200
12.2.2 Online administrator	201
12.3 One key recovery	202
12.4 Configuration file	202
12.4.1 Saving configurations	202
12.4.2 Importing and exporting configuration files	203
12.4.3 Uploading configuration file	203
12.5 Software Update	204
12.6 Diagnose tool	205
12.6.1 Ping	205
12.6.2 Tracert	205
12.6.3 HTTP get	206
12.6.4 DNS Query	207
12.6.5 TCP Query	207
12.7 NTP	208

12.7.1 NTP	208
12.8 Session statistics	209
12.8.1 Statistics monitor configuration	209
12.8.2 Real-time session statistics.....	209
12.8.3 Real-time traffic statistics	210
12.9 Local Log	211
12.10 SMTP server settings.....	212
13 Typical configuration examples	213
13.1 Example for configuring Internet access for wired users	213
13.2 Example for configuring Internet access for wireless users	216
13.3 Example for configuring Internet access through 3G	219
13.4 Example for configuring Web filtering	222
13.5 Example for configuring Internet access for wired users in limited period.....	224
13.6 Example for configuring EoIP	227
13.7 Example for configuring the NAT virtual server	228
13.8 Example for configuring route backup and sharing	232
14 Appendix	236
14.1 Terms	236
14.2 Acronyms and abbreviations	237

Figures

Figure 1-1 Web management mode of LAVA	20
Figure 1-2 Typical Web configuration interface	21
Figure 2-1 Device interface	24
Figure 3-1 Broadband Connection Configuration interface	27
Figure 3-2 LAN Configuration interface	28
Figure 3-3 Wireless Routing Configuration interface	29
Figure 3-4 Complete Rapid Configuration Guide interface	30
Figure 4-1 Bridge mode WAN0 interface application networking	56
Figure 4-2 Add Subinterface on WAN0 interface in bridge mode	57
Figure 4-3 Router mode WAN0 interface application networking	58
Figure 4-4 Add Subinterface on WAN0 interface in router mode	59
Figure 4-5 Link backup application networking	60
Figure 4-6 Configuring link backup	61
Figure 5-1 Static route configuration network application	92
Figure 5-2 Configuring static route	93
Figure 5-3 Static route list	93
Figure 5-4 Policy route configuration networking application	94
Figure 5-5 Configuring address	94
Figure 5-6 Address object list	95
Figure 5-7 Configuring policy route 1	95
Figure 5-8 Configuring policy route 2	96
Figure 5-9 Policy route list	96
Figure 6-1 L2TP VPN application networking	106
Figure 6-2 L2TP Server interface	107
Figure 6-3 Authenticated User-ADD interface	107
Figure 6-4 IPSec VPN application networking	108

Figure 6-5 Creating an IPSec connection	109
Figure 7-1 Rate limit per user application networking	118
Figure 7-2 Configuring rate limit per user	119
Figure 8-1 Syslog application networking	127
Figure 8-2 Syslog Local interface	128
Figure 8-3 Syslog Mail interface.....	128
Figure 9-1 Web authentication application networking.....	136
Figure 9-2 Adding a user.....	137
Figure 9-3 User management interface	137
Figure 9-4 Authentication Option interface.....	138
Figure 10-1 SIP-based VoIP phone application networking.....	158
Figure 10-2 SIP-based VoIP configuration flow.....	160
Figure 10-3 Configure system items for SIP	161
Figure 10-4 Configuring line items for SIP.....	161
Figure 10-5 Modifying line configurations for SIP	162
Figure 10-6 Adding user authentication	162
Figure 10-7 Configuring the register server	163
Figure 10-8 Configuring the proxy server.....	163
Figure 10-9 Configuring heartbeat.....	163
Figure 10-10 Modifying local SIP message listening socket	164
Figure 10-11 Modifying service configurations	164
Figure 10-12 Modifying the local number	165
Figure 10-13 H.248-based VoIP phone application networking.....	166
Figure 10-14 H.248-based VoIP configuration flow	167
Figure 10-15 Configuring system items for H.248	168
Figure 10-16 Configuring the MGC.....	168
Figure 10-17 Configuring RTP TID	169
Figure 10-18 Configuring POT TID.....	169
Figure 10-19 Configuring POTS TID in manual mode.....	169
Figure 10-20 Port State Modify interface.....	170
Figure 10-21 Line Configuration interface for H.248	170
Figure 10-22 Line Configuration Modify for H.248	171
Figure 10-23 MG Configuration interface	171

Figure 10-24 MG Register area.....	172
Figure 11-1 MAC filter application networking.....	193
Figure 11-2 Anti-ARP attack application networking	194
Figure 11-3 Configuring IP-MAC binding.....	195
Figure 11-4 Configuring active protection	195
Figure 11-5 Anti-DDoS attack application networking	197
Figure 11-6 Configuring anti-DDoS attack.....	197
Figure 13-1 Networking application for Internet access from a LAN through the LAVA	214
Figure 13-2 Configuring the WAN0 interface.....	215
Figure 13-3 Configuring the VLAN interface.....	216
Figure 13-4 Configuring DNS proxy	216
Figure 13-5 Networking with Internet access from a WLAN through the LAVA.....	217
Figure 13-6 Modifying basic WLAN configurations	218
Figure 13-7 Configuring WLAN advanced items	219
Figure 13-8 3G Internet access networking application.....	220
Figure 13-9 3G Interface Basic Configuration interface.....	221
Figure 13-10 Configuring 3G advanced items	221
Figure 13-11 Web Filter application networking	223
Figure 13-12 Firewall Configuration interface.....	223
Figure 13-13 Web Filter interface	224
Figure 13-14 Access control application networking.....	225
Figure 13-15 Configuring the time object.....	225
Figure 13-16 Configuring the address object	226
Figure 13-17 Configuring access control policies.....	226
Figure 13-18 EoIP application networking	227
Figure 13-19 Configuring EoIP on LAVA A	228
Figure 13-20 Configuring EoIP on LAVA B	228
Figure 13-21 NAT virtual server application networking	229
Figure 13-22 Adding a FTP service object.....	230
Figure 13-23 Adding a HTTP port service target	230
Figure 13-24 List of Customed Service	231
Figure 13-25 Creating a virtual server for Web service.....	231
Figure 13-26 Creating a virtual server for FTP service	232

Figure 13-27 Internal server list	232
Figure 13-28 Route backup and sharing application networking	233
Figure 13-29 Configuring default route of the WAN0 interface	234
Figure 13-30 Configuring default route of the 3G interface.....	235
Figure 13-31 Static route list	235

Tables

Table 1-1 User names and related passwords	20
Table 1-2 Common buttons on the Web configuration interface	22
Table 4-1 Configuration items in bridge mode.....	32
Table 4-2 Configuration items in router mode	33
Table 4-3 Configuration items in mixed mode.....	36
Table 4-4 Configuration items on the VLAN Interface Configuration interface.....	39
Table 4-5 Configurations items in the VLAN Add & Delete area.....	40
Table 4-6 Configuration items on the VLAN Information List area	40
Table 4-7 Configuration items on the IPv6 Configuration interface	41
Table 4-8 Configuration items on the ETH Configuration interface	42
Table 4-9 Configuration items on the DMZ interface	43
Table 4-10 Configuration items on the Modify Basic WLAN Configuration interface	44
Table 4-11 Configuration items on the Advanced Configuration interface	47
Table 4-12 Configuration items on the SSID Subset Information List area	48
Table 4-13 Configuration items on the WPS Configuration interface.....	48
Table 4-14 Configuration items in the 3G Interface Basic Configuration area	49
Table 4-15 Configuration items in the 3G Advanced Configuration area	51
Table 4-16 Configuration items on the Flow Warning interface	52
Table 4-17 Configuration items in the Create/Modify A New GRE Interface area.....	53
Table 4-18 Configuration items in the Link detect config interface.....	54
Table 5-1 Configuration items on the ALG interface	63
Table 5-2 Configuration items on the Virtual Server interface.....	64
Table 5-3 Configuration items on the Source NAT interface	64
Table 5-4 Configuration items on the One to One Address Translation interface.....	65
Table 5-5 Configuration items on the DHCP Service interface.....	66
Table 5-6 Configuration items on the DHCP Address Pool interface	67

Table 5-7 Configuration items on the Excluded Address interface	69
Table 5-8 Configuration items on the IP/MAC Binding interface	69
Table 5-9 Configuration items on the Option60 Address Pool interface	70
Table 5-10 Configuration items on the DNS interface	71
Table 5-11 Configuration items on the Static Rout List interface	73
Table 5-12 Configuration items on the Policy Route interface	74
Table 5-13 Configuration items on the RIP Basic Configuration interface	75
Table 5-14 Configuration items in the Interface RIP Version List area	76
Table 5-15 Configuration items in the Passive interface list area.....	76
Table 5-16 Configuration items in the Redistribution Setting area	77
Table 5-17 Configuration items on the Advanced Configuration interface for OSPF	78
Table 5-18 Configuration items on the Area Configuration interface for OSPF	79
Table 5-19 Configuration items on the Network Distribution interface	79
Table 5-20 Configuration items on the Interface Configuration interface.....	79
Table 5-21 Configuration items in the Passive Interface list.....	80
Table 5-22 Configuration items on the Prefix list config interface	81
Table 5-23 Configuration items on the Interface filtering config interface	82
Table 5-24 Configuration items in the Multicast area	82
Table 5-25 Configuration items on the EoIP Configuration interface	84
Table 5-26 Configuration items on the DDNS Settings interface	85
Table 5-27 Configuration items on the Page Push interface.....	86
Table 5-28 Configuration items on the DHCP Service interface.....	87
Table 5-29 Configuration items on the DHCP Address Pool interface.....	87
Table 5-30 Configuration items on the Prefix/DUID Binding interface	88
Table 5-31 Configuration items in the IPv6 Function area.....	89
Table 5-32 Configuration items on the Static Routing List interface	90
Table 5-33 Configuration items on the 6RD Tunnel Configuration interface	91
Table 5-34 Configuration items on the UPnP Config interface	92
Table 6-1 Configuration items on the L2TP Client interface	98
Table 6-2 Configuration items in the L2TP Enable area	99
Table 6-3 Basic configuration items on the Authenticated User-Add interface	99
Table 6-4 Advanced configuration items on the Authenticated User-Add interface	99
Table 6-5 Configuration items on the New IPsec interface	100

Table 6-6 Advanced configuration items on the New IPSec interface	102
Table 6-7 Configuration items on the Bind IPSec Name interface.....	104
Table 6-8 Configuration items in the Bind IPSec Name area.....	104
Table 6-9 Configuration items on the CA Certificate interface	105
Table 6-10 Configuration items on the Local Certificate interface	106
Table 7-1 Configuration items on the Rate Limit per User interface	111
Table 7-2 Configuration items on the Advanced Rate Limit interface	112
Table 7-3 Configuration items in the Matching Condition area	112
Table 7-4 Configuration items in the Global configuration area.....	113
Table 7-5 Configuration items in the Queue configuration area	114
Table 7-6 Configuration items in the Match Policy area.....	114
Table 7-7 Configuration items on the Session Counter Limit interface	116
Table 7-8 Configurations items on the Connection Counter Setting interface	117
Table 7-9 Configurations items in the Connection Counter Setting List area	117
Table 8-1 Configuration items in the ACS area.....	120
Table 8-2 Configuration items in the CPE area.....	121
Table 8-3 Configuration items on the SNMP interface	122
Table 8-4 Configuration items on the USM User interface.....	123
Table 8-5 Configuration item on the Host IP address interface.....	124
Table 8-6 Configuration items on the Local interface	125
Table 8-7 Configuration items on the Remote interface.....	125
Table 8-8 Configuration items on the Mail interface	126
Table 9-1 Configuration items in the Groups-Add area	131
Table 9-2 Configuration items in the User-Add area.....	131
Table 9-3 Configuration items on the Authentication Option interface.....	132
Table 9-4 Configuration items on the Whitelist interface	133
Table 9-5 Configuration items on the RADIUS Authentication interface.....	134
Table 9-6 Configuration items on the LDAP Authentication interface	135
Table 10-1 Configuration items in the VOIP System Configuration area	140
Table 10-2 Configuration items in the Media Configuration area.....	140
Table 10-3 Configuration items on the Line Configuration interface	142
Table 10-4 Configuration items on the Line Configuration Modify interface.....	143
Table 10-5 Configuration items in the Register Server area.....	144

Table 10-6 Configuration items in the Proxy Server area	145
Table 10-7 Configuration items in the Outbound Server area	145
Table 10-8 Configuration items in the Heartbeat area	145
Table 10-9 Configuration items in the Session Update area	146
Table 10-10 Configuration items in the Local SIP Message listening socket area	146
Table 10-11 Configuration items in the Advanced Options area	146
Table 10-12 Configuration items on the User Authentication Configuration Add interface	147
Table 10-13 Configuration items on the Local Number Modify interface	148
Table 10-14 Configuration items on the Business Configuration Modify interface	149
Table 10-15 Configuration items on the Dialling Rules Add interface	150
Table 10-16 Configuration items on the MG Configuration area	151
Table 10-17 Configuration items on the MGC Configuration interface	152
Table 10-18 Configuration items in the RTP TID Configuration area	154
Table 10-19 Configuration items in auto mode in the POTS TID Configuration area	154
Table 10-20 Configuration items in handy mode in the POTS TID manual mode configuration modification area	154
Table 10-21 Configuration items on the Port State Modify interface	155
Table 10-22 Configuration items on the Fax Configuration interface	156
Table 10-23 Configuration items on the Fax Modify interface	156
Table 11-1 Configuration items on the Firewall interface	174
Table 11-2 Configuration items on the Web Filter interface	176
Table 11-3 Configuration items on the Policy of Access Control interface	179
Table 11-4 Configuration items on the Time Object interface	180
Table 11-5 Configuration items on the Service Object interface	181
Table 11-6 Configuration items on the Address Object interface	183
Table 11-7 Configuration items on the IPv6 Policy of Access Control interface	184
Table 11-8 Configuration items on the MAC Filter interface	185
Table 11-9 Configuration items on the Prevent ARP Attack interface	186
Table 11-10 Configuration items on the Active Protection interface	187
Table 11-11 Configuration items on the IP-MAC Bind interface	188
Table 11-12 Configuration items on the Custom Contract Configuration Information interface	189
Table 11-13 Configuration items in the DDoS Attack Defence area	191
Table 11-14 Configuration items in the Abnormal Packet Attack Defence area	191
Table 11-15 Configuration items in the Scan Attack Defence area	192

Table 12-1 Configuration items in the User Configuration area	200
Table 12-2 Configuration items on the Add Administrator interface	201
Table 12-3 Configuration items on the Ping interface.....	205
Table 12-4 Configuration items on the Tracert interface.....	206
Table 12-5 Configuration items on the HTTP Get interface	206
Table 12-6 Configuration item on the DNS Query interface.....	207
Table 12-7 Configuration items on the DNS Query interface	207
Table 12-8 Configuration items on the NTP interface.....	208
Table 12-9 Configuration items on the Statistics Monitor Configuration interface	209
Table 12-10 Configuration items on the Real-time Session Statistics interface	209
Table 12-11 Configuration items on the Real-time Traffic Statistics interface	210
Table 12-12 Configuration items on the Local Log interface.....	211
Table 12-13 Configuration items on the SMTP Server Settings interface.....	212

1 Preparing for configurations

This chapter describes how to prepare for logging in to the LAVA LR-2G211 Web configuration interface and basic information about the Web configuration interface, including the following sections:

- Management modes
- Web mode
- NView NNM mode

1.1 Management modes

The device supports the following 2 management modes:

- Web mode: manage the device through the Web configuration interface.
- NView NNM mode: manage the device through the NView NNM system.

1.2 Web mode

In Web mode, the device is managed through the Web configuration interface.

1.2.1 Establishing configuration environment

By default, you can connect the client network interface and any LAN interface on LAVA to enter the configuration interface, as shown in Figure 1-1.

Figure 1-1 Web management mode of LAVA



Configuring the client

The PC must be installed with a major Web browser. Configure the IP address and LAVA device management IP address in the same network segment.

By default, the range for PC IP address is 192.168.1.2/255.255.255.0 to 192.168.1.254/255.255.255.0, such as 192.168.1.2/255.255.255.0. Ensure the interconnection between the PC and LAVA.

Configuring the LAVA device

When you log in to the LAVA for the first time, you can use default configurations as below:

- Management IP address: 192.168.1.1/255.255.255.0
- Table 1-1 lists user names and related passwords.

Table 1-1 User names and related passwords

User level	User name	Password	Authority
Super administrator	admin	admin	Have the authority to perform all operations, helping enable services and troubleshooting problems.
Common administrator	useradmin	useradmin	Be available for the enterprise administrator. Help configure and view all enabled services. However, no operation is allowed on management-level functions, such as system software upgrade, configuration file operations, VPN service, remote management configuration, and user/user group management and configuration.
Common user	user	user	Learn operation status of the device without configuring and viewing specified functions.

To log in to the Web configuration interface, follow these steps:

- Step 1 Open IE browser on a PC (take IE for example).
- Step 2 Input "http://192.168.1.1", and press **Enter** to enter the Web configuration login interface.
- Step 3 Input the user name and password.



- For the first login, please use the system default user name and password.
- After successful login, user can choose **System > Administrator** in the navigation bar to change the password. Please see section 12.2 Administrator for the specific steps.

1.2.2 Learning the Web configuration interface

Structure of the Web configuration interface

The configuration interface of LAVA Web network management client has uniform style and concise layout, as shown in Figure 1-2.

Figure 1-2 Typical Web configuration interface



1	Level 1 navigation bar	2	Level 2 navigation bar	3	Tab
4	Current location	5	Current configuration interface	—	


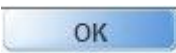


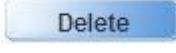


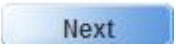

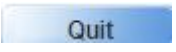


- All configuration items listed on the Web configuration interface will be described in the following chapters. Configuration item combination varies on your selection. Configure the device based on configuration items actually listed on the Web configuration interface.
- Configuration items with red "*" are required ones.
- The Web configuration interface is subject to the actual one. Screenshots in this guide are for your reference only.

Common buttons

Table 1-2 lists common buttons on the Web configuration interface.

Table 1-2 Common buttons on the Web configuration interface

Button	Description
	It is used to create an item on the current interface.
	It is used to submit the current configurations or confirm the currently displayed information.
	It is used to cancel the current configurations.
	It is used to modify a selected item on the current interface.
 or 	It is used to delete a selected item on the current interface.
	It is used to refresh the current interface.
	It is used to go to the next interface, indicating: <ul style="list-style-type: none"> • The current configuration is incomplete, and you should click it to continue. • The displayed information is incomplete, and you should click it to view more information.
	It is used to return to the previous step for reconfiguration or viewing information.
	It is used to quit the current interface.

Saving configurations

The Web configuration interface provides multiple methods to save configurations:

- Saving configuration automatically: in the navigation bar, choose **System > Configuration File > Save Configuration**. The **Save Configuration** interface is displayed. In the **Auto Save Config** area, select **ON** and the LAVA LR-2G211 will save configurations automatically.
- Saving configurations manually: click **Save Config** in the upper right corner of the current interface.

Caution

- After configurations on the current interface are saved to the memory, if the LAVA encounters power failure or is reset, configurations since the last configuration will be lost.
- After all configurations are complete, you need to save them into the configuration file. In this case, though the LAVA is powered off or reset, configurations will not be lost.


Exiting the Web configuration interface

After all configurations are complete, exit the Web configuration interface to ensure system security.

 **Caution**

Before existing from the Web configuration interface, save all configurations to avoid losing them.

You can exist from the Web configuration interface in the following two methods:

- Click the  icon of the current page on the IE, and then close the IE.
- Click the **Logout** button in the upper right corner on the Web configuration interface.

1.3 NView NNM mode

For configurations about the NView NNM mode, see related manuals about the NView NNM system.

2 Device information

This chapter describes how to learn the operating status of the LAVA on the **Device** interface, including the following sections:

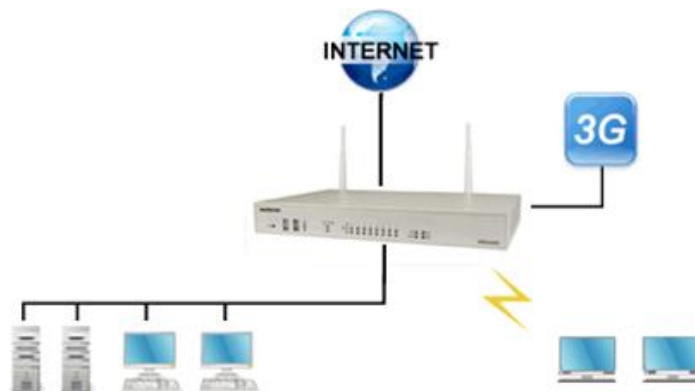
- Introduction to the Device interface
- Device information

2.1 Introduction to the Device interface

After you log in to the Web configuration interface of the LAVA, you are navigated to the **Device** interface by default. This tab displays basic information, connection status information, service interface, and system log, as shown in Figure 2-3.

Figure 2-3 Device interface

This page shows the basic information and current status of the device. Clicking the icons on the graph below will lead you to the corresponding part of information.



Note

- The different parts in Figure 2-3 are relevant to information below. When you click a part, the system switches to the corresponding part. You can click the part, the system switches to the corresponding tag.
- Click **More** to view more information.
- Click the **Refresh Period** drop-down list to configure the refresh period.

2.2 Device information

- Basic information: by view basic information of the LAVA, you can learn the operating status including:
 - Device information
 - CPU usage
 - Memory usage
- Connection status: you can view connection status information in this interface, including:
 - Broadband connection information
 - 3G Wireless LAN (WLAN) card status
 - LAN information
 - WLAN information
- Service information: you can view service information, including:
 - L2TP VPN service status
 - IPSec VPN service status
- System logs: by viewing the system log, you can learn the latest events and status of the system, which can help clear faults.



The service information is not displayed if the device does not support it.

3 Quick guide

This chapter describes how to configure basic network parameters through quick guide. You can easily complete configuring Internet access as prompted by the quick guide.

- Broadband connection configuration
- LAN configuration
- Wireless routing configuration
- Complete rapid configuration guide

3.1 Broadband connection configuration

Scenario

On the **Broadband Connection Configuration** interface, you can configure items required for the device connecting to the Internet. That is, you can configure items about the upstream WAN interface. You can configure related configuration items based on the selected accessing mode.

The gateway supports 3 common Internet connection modes:

- PPPoE: in this mode, you need to enter the user name and password provided by the Internet Service Provider (ISP).
- Obtaining the IP address automatically: in this mode, the device obtains an IP address from the ISP automatically without being configured with other items.
- Specifying the IP address manually: in this mode, you should configure the fixed IP address provided by the ISP for the device. In addition, you need to configure the IP address, subnet mask, default gateway, and primary/secondary DNS server for the WAN interface.

Configuration steps

- Step 1 In the navigation bar, choose **Quick Guide > Quick Guide**. The **Quick Guide** interface is displayed.
- Step 2 Click **Next** to enter the **Broadband Connection Configuration** interface.

- Step 3 Configure the WAN interface and Internet connection mode, enable NAT, and set the service mode binding to Internet. Configure related configuration items about the selected Internet connection mode, as shown in Figure 3-4.

Figure 3-4 Broadband Connection Configuration interface

■ Step 1: Broadband Connection Configuration

This gateway support 3 Internet connection modes.

(1) Virtual dial-up (PPPoE)

(2) Acquire IP address from IP address auto-provision service of Internet service provider (DHCP)

(3) Acquire fixed IP address from Internet service provider (Static)

WAN

Internet Connection Mode

Enable NAT NAT

Enable Sub Interface

Service Mode Binding

If you're using broadband service, the Internet service provider will provide you a fixed IP address and some other information. Please fill in the blanks below accordingly. Please contact with your service provider if you do not have this information.

IP Address *

Subnet Mask *

Default Gateway

Primary DNS Server

Secondary DNS Server



Caution

Enable NAT; otherwise, you will fail to access the Internet.

- Step 4 Click **Next** to enter the **LAN Configuration** interface.

3.2 LAN configuration

Scenario

On the **LAN Configuration** interface, you can configure basic items about the downlink LAN interface, including Virtual Local Area Network (VLAN) bound to the interface, IP address, and subnet mask. In addition, you can enable/disable DHCP. After enabling DHCP, you need to configure the range and lease time of IP addresses assigned to the downlink users.

Configuration steps

- Step 1 On the **LAN Configuration** interface, configure related items, as shown in Figure 3-5.

Figure 3-5 LAN Configuration interface

Step 2: LAN Configuration

Choose VLAN	<input type="text" value="vlan1"/>	
IP Address	<input type="text" value="192.168.1.1"/>	*(xxx.xxx.xxx.xxx)
Subnet Mask	<input type="text" value="255.255.255.0"/>	*
DHCP Service	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	
Start IP Address	<input type="text" value="192.168.1.2"/>	*(xxx.xxx.xxx.xxx)
End IP Address	<input type="text" value="192.168.1.254"/>	*(xxx.xxx.xxx.xxx)
Lease Time	<input type="text" value="2"/>	Days <input type="text" value="0"/> Hours
	<input type="text" value="0"/>	Minutes (0 minute means infinite)

Step 2 Click **Next** to enter the **Wireless Routing Configuration** interface.

3.3 Wireless routing configuration

Scenario

On the **Wireless Routing Configuration** interface, you can configure basic parameters and security authentication options for the device providing wireless network, including the wireless SSID and binding mode of the wireless address. In addition, you need to enter the key and encapsulation mode required for authentication based on the selected authentication mode.

Configuration steps

Step 1 On the **Wireless Routing Configuration** interface, configure related items, as shown in Figure 3-6.

Figure 3-6 Wireless Routing Configuration interface

The screenshot displays the 'Modify Basic WLAN Configuration' page. The left sidebar shows a navigation menu with 'WLAN' selected. The main content area contains the following configuration fields:

- Network Name(SSID): LAVA-0001 * (input length:1-31byte)
- Address Mode: VLAN Binding
- VLAN: vlan1 (Basic--> Interface--> LAN--> VLAN Configuration)
- Management Access: HTTPS PING TELNET SSH HTTP
- SSID Hide:
- WMM:
- Station Isolation:
- SSID Rate: auto
- Beacon Interval: 100 ms (value range:100-1000)
- DTIM Interval: 1 (value range:1-31)
- BSS Max Associations Limit: 0 (value range:0-32) 0 indicates the maximum number is 160.
- Authentication Mode: WPA2-PSK
- WPA Pre-Shared Key: ***** * (input length:8-63byte)
- show password:
- WPA Encryption: TKIP-AES
- MAC Filter: Enable Disable

(*) : Required



Note

Please choose **Enable Current SSID**. Otherwise, configurations are invalid.

Step 2 Click **Next** to enter the **Complete Rapid Configuration Guide** interface.

3.4 Complete rapid configuration guide

Scenario

On the **Complete Rapid Configuration Guide** interface, you can view WAN interface configurations, LAN interface configurations, and parameters about the WLAN.

Configuration steps

Step 1 On the **Complete Rapid Configuration Guide** interface, view related items, as shown in Figure 3-7.

- If the configured parameters are incorrect, click **Back** to return to the related configuration interface. Otherwise, click **Finish**.

Figure 3-7 Complete Rapid Configuration Guide interface

Complete Rapid Configuration Guide

WAN Settings	
Connection Name	WAN0
Type of Service	Internet
Internet Connection Mode	Static
IP Address	192.168.18.2
LAN Settings	
LAN	vlan1
LAN IP Address	192.168.1.1
DHCP Server	Enable
Start IP Address	192.168.1.2
End IP Address	192.168.1.254
WLAN Settings	

Congratulations! You have completed all the required network parameter settings.
The gateway should be online now.

Please click 'Finish' to end the fast configuration guide program.

Step 2 Click **Finish**. After configurations are complete, a **Modified Successfully** prompt is displayed.

Step 3 Click **Save Config** to complete quick configuration guide.



Note

For details about configuration items, see chapter 4 Interface configurations.

4 Interface configurations

The LAVA provides multiple types of interfaces to meet user's connection requirements. This chapter describes how to configure interfaces, including the following sections:

- WAN
- LAN
- DMZ
- WLAN
- 3G
- GRE
- Link backup
- Configuration examples



4.1 WAN

4.1.1 WAN0 configuration

Scenario

You can configure the WAN0 interface on this interface.

Configuration steps

- Step 1 In the navigation bar, choose **Basic > Interface > WAN**. The **WAN0 Configuration** interface is displayed.
- Step 2 View configured interface parameters.
 - To modify a configured item, click  to enter the modifying interface.
 - To add an item, click **Add** to enter the adding interface.
 - To delete an item, and click the corresponding .
- Step 3 On the modifying or adding interface, configure related items, and click **OK**.



The addition and deletion operations are available for the WAN sub-interface.

Step 4 After configurations are complete, click **Save Config** to save configurations.

Configuration items

The WAN interface has three connection modes as below:

- Bridge mode: Table 4-3 lists configuration items in the bridge mode.
- Router mode: Table 4-4 lists configuration items in the router mode.
- Mixed mode: Table 4-5 lists configuration items in the mixed mode.

Table 4-3 Configuration items in bridge mode

Configuration item	Description
Connection Name	Name of a connection
Connection Mode	Used in bridge mode
IP Address	Management IP address
Subnet Mask	Subnet mask of the management IP address
Subinterface ID	VLAN ID of the corresponding connection, ranging from 1 to 4095, where 4095 indicates that no VLAN is configured.
802.1p Priority	802.1p priority, ranging from 0 to 7
MAC Address	MAC address of the sub-interface
Belongs to Bridge	Name of the bridge interface to which the interface belongs, automatically added by the system
Interface List	List of interfaces which belong to the same bridge. Click the interface or VLAN to add it to this list.
Interface List	List of interfaces that belong to the same bridge



Configuration item	Description
Service Type	<p>Type of service that is bound with the connection, including</p> <ul style="list-style-type: none"> • Management_Internet: management and Internet channel • Management: management channel • Internet: internet channel • Management_Voice: management and voice channel • Management_Voice_Internet: management, voice, and Internet channel • Voice: voice channel • Voice_Internet: voice and Internet channel • Other: other channels <p> Note</p> <p>Default routes are generated for the Management or Internet channel rather than other channels. The Management_Internet WAN interface can generate the default route automatically and can generate a 32-bit management route. The Management WAN interface can generate the 32-bit management route automatically. The Internet WAN interface can only generate the default route automatically. The Management_Voice, Management_Voice_Internet, Voice, and Voice_Internet WAN interfaces are available on the device that supports the voice feature. In addition, they generate the policy route automatically. The Other WAN interface does not generate the route automatically.</p>

Table 4-4 Configuration items in router mode

Configuration item	Description
Connection Name	Name of a connection
Connection Mode	<p>Used in route mode.</p> <p>It is the mode to connect to the Internet. You can choose the modes provided by the Internet Service Provider (ISP), including:</p> <ul style="list-style-type: none"> • DHCP: the LAVA obtains an IP address from the ISP. • Static: the LAVA obtains a static IP address from the ISP. • PPPoE: the LAVA obtains a user name and its password from the ISP.
Username	User name in PPPoE mode, provided by ISP
Password	Password in PPPoE mode, provided by ISP
PPPoE dial-mode	<p>Select a PPPoE dial-mode, including:</p> <ul style="list-style-type: none"> • now • demand

Configuration item	Description
idle time	<p>Enter the idle time when the PPPoE dial-mode is set to demand. It is an integer ranging from 10 to 65535, in unit of second. By default, it is set to 0s, which means no timeout.</p> <p> Note</p> <p>The idle time refers to the period when no service is available for users. When the idle time exceeds the configured value, the LAVA LR-2G211 will block the network automatically to save traffic. When a service is available, the LAVA LR-2G211 will automatically resume the network.</p>
IP Address	IP address of the WAN0 interface in static mode
Subnet Mask	Subnet mask of the IP address of the WAN0 interface in static mode
Default Gateway	Default gateway of subnet of the WAN0 interface in static mode
Primary DNS server	IP address of the primary DNS server of the WAN0 interface in static mode
Secondary DNS server	IP address of the secondary DNS server in static mode
Access Control	Enable/Disable HTTPS, PING, Telnet, SSH and/or HTTP server. If you select one, it is enabled.
Enable NAT	Enable/Disable NAT. If you select it, it is enabled.
NAT Log	After NAT is enabled, you can choose whether to record the NAT log. If you select it, it is enabled.
Enable NAT Address Pool	After NAT is enabled, you need to enable the NAT address pool as required. In addition, you need to configure the IP address range of the NAT address pool. It is used to configure the WAN interface allowing multiple IP addresses to connect to the Internet.
Subinterface ID	VLAN ID of the corresponding connection, ranging from 1 to 4095, where 4095 indicates that no VLAN is configured.
802.1p Priority	802.1p priority, ranging from 0 to 7
MAC Address	MAC address of the sub-interface




Configuration item	Description
Service Type	<p>Type of service that is bound with the connection, including</p> <ul style="list-style-type: none"> • Management_Internet: management and Internet channel • Management: management channel • Internet: internet channel • Management_Voice: management and voice channel • Management_Voice_Internet: management, voice, and Internet channel • Voice: voice channel • Voice_Internet: voice and Internet channel • Other: other channels <p> Note</p> <p>Default routes are generated for the Management or Internet channel rather than other channels. The Management_Internet WAN interface can generate the default route automatically and can generate a 32-bit management route. The Management WAN interface can generate the 32-bit management route automatically. The Internet WAN interface can only generate the default route automatically. The Management_Voice, Management_Voice_Internet, Voice, and Voice_Internet WAN interfaces are available on the device that supports the voice feature. In addition, they generate the policy route automatically. The Other WAN interface does not generate the route automatically.</p>
IPv6 Setting	<p>Configure IPv6 on the WAN0 interface on the following</p> <ul style="list-style-type: none"> • DHCPv6-PD: an IPv6 address automatically obtained from the ISP through DHCPv6 • Static: a static IPv6 address configured by the ISP • Stateless: address and DNS automatically obtained through automatic configuration.
IPv6 Address	<p>IPv6 address of the WAN0 interface in static mode, in colon hexadecimal notation, such as 3001::3</p>
IPv6 Prefix Length	<p>Length of IPv6 prefix of the WAN0 interface in static mode. It is an integer ranging from 1 to 128.</p>
IPv6 Default Gateway	<p>Default IPv6 gateway of the WAN0 interface in static mode, in colon hexadecimal notation, such as 3001::3</p>
IPv6 Primary DNS	<p>IPv6 address of primary DNS server of the WAN0 interface in static mode, in colon hexadecimal notation, such as 3001::3</p>
IPv6 Secondary DNS	<p>IPv6 address of secondary DNS server of the WAN0 interface in static mode, in colon hexadecimal notation, such as 3001::3</p>
Obtain Subnet Prefix	<p>IPv6 address prefix obtained through ND-RA</p>

Table 4-5 Configuration items in mixed mode

Configuration item	Description
Connection Name	Name of a connection
Connection mode	Used in mixed mode. It is the mode to connect to the Internet. You can choose the modes provided by the Internet Service Provider (ISP), including: <ul style="list-style-type: none"> • DHCP: the LAVA obtains an IP address from the ISP. • Static: the LAVA obtains a static IP address from the ISP. • PPPoE: the LAVA obtains a user name and its password from the ISP.
Username	User name in PPPoE mode
Password	Password in PPPoE mode
PPPoE dial-mode	Select a PPPoE dial-mode, including: <ul style="list-style-type: none"> • now • demand
idle time	Enter the idle time when the PPPoE dial-mode is set to demand. It is an integer ranging from 10s to 65535s. By default, it is set to 0s, which means no timeout.  Note The idle time refers to the period when no service is available for users. When the idle time exceeds the configured value, the LAVA LR-2G211 will block the network automatically to save traffic. When a service is available, the LAVA LR-2G211 will automatically connect to the network again.
IP Address	IP address of the WAN0 interface in static mode
Subnet Mask	Subnet mask of the IP address of the WAN0 interface in static mode
Default Gateway	Default gateway of subnet of the WAN0 interface in static mode
Primary DNS	IP address of the primary DNS server of the WAN0 interface in static mode
Secondary DNS	IP address of the secondary DNS server in static mode
Access control	Enable/Disable HTTPS, PING, Telnet, SSH and/or HTTP server. If you select one, it is enabled.
Enable NAT	Enable/Disable NAT. If you select it, it is enabled.
NAT Log	After NAT is enabled, you can choose whether to record the NAT log. If you select it, it is enabled.

Configuration item	Description
Enable NAT Address Pool	After NAT is enabled, you need to enable the NAT address pool as required. In addition, you need to configure the IP address range of the NAT address pool. It is used to configure the WAN interface allowing multiple IP addresses to connect to the Internet.
Subinterface ID	VLAN ID of the corresponding connection, ranging from 1 to 4095, where 4095 indicates that no VLAN is configured.
802.1p Priority	802.1p priority, ranging from 0 to 7
MAC Address	MAC address of the interface
Belongs to Bridge	Name of the bridging interface to which the interface belongs, automatically added by the system
Interface List	List of available interfaces or VLANs in the current system
Interface List	List of interfaces which belong to the same bridge. In the Interface List , double click the interface or VLAN to add it to this list.
Service Type	<p>Type of service that is bound with the connection, including</p> <ul style="list-style-type: none"> • Management_Internet: management and Internet channel • Management: management channel • Internet: internet channel • Management_Voice: management and voice channel • Management_Voice_Internet: management, voice, and Internet channel • Voice: voice channel • Voice_Internet: voice and Internet channel • Other: other channels <p> Note</p> <p>Default routes are generated for the Management or Internet channel rather than other channels. The Management_Internet WAN interface can generate the default route automatically and can generate a 32-bit management route. The Management WAN interface can generate the 32-bit management route automatically. The Internet WAN interface can only generate the default route automatically. The Management_Voice, Management_Voice_Internet, Voice, and Voice_Internet WAN interfaces are available on the device that supports the voice feature. In addition, they generate the policy route automatically. The Other WAN interface does not generate the route automatically.</p>
Obtain Subnet Prefix	IPv6 address prefix obtained through ND-RA

4.1.2 WAN1 configuration

Scenario

You can switch the LAN interface to the WAN interface on this interface. Therefore, users can access to the Internet more flexibly.

Configuration steps

- Step 1 In the navigation bar, choose **Basic > Interface > WAN > WAN1 Configuration**. The **WAN1 Configuration** interface is displayed.
- Step 2 To switch the LAN interface to the WAN interface, select **LAN4 switch the GE** radio button in the **switch LAN4/WAN1** area and then click **OK**. A **Modified Successfully** prompt is displayed. Click **OK**. An item is listed in the **WAN Interface Configuration** area.
- Step 3 Configuration steps are the same as those in section 4.1.1 WAN0 configuration.

Configuration items

Configuration steps are the same as those in section 4.1.1 WAN0 configuration.

4.2 LAN

4.2.1 VLAN interface configuration

Scenario

You can configure the VLAN interface of the LAVA on this interface.

As a virtual interface, the VLAN interface is mainly used to configure the IP address and subnet mask of the VLAN, protocols allowed to be managed and accessed, and DHCP. After configuring the VLAN interface, you can bind the LAN interface to the VLAN interface to realize the forwarding feature of the LAN interface.

Configuration steps

- Step 1 In the navigation bar, choose **Basic > Interface > LAN > VLAN Interface Configuration**. The **VLAN Interface Configuration** interface is displayed.
- Step 2 On the VLAN Interface Configuration interface,
 - In **VLAN Interface Configuration** area, select a configured VLAN, and configure related items.
 - In the **DHCP Service List**, information about the VLANs enabled with DHCP service is enabled. To delete a VLAN, click **Delete**.
- Step 3 After configurations are complete, click **Save Config** to save configurations.

Configuration items

Table 4-6 Configuration items on the VLAN Interface Configuration interface

Configuration item		Description
VLAN		You can choose a VLAN in the drop-down list.
IP Address		IP address of the VLAN interface
Net mask		Subnet mask of the VLAN interface
Management Access		Enable or enable HTTPS, PING, Telnet, SSH, and/or HTTP. When you check one, it is enabled.
Server	Enable	Enable DHCP on the VLAN interface.
	Disable	Disable DHCP on the VLAN interface.
	Subnet	IP address of the DHCP subnet, in dotted decimal notation, such as 192.168.1.1
	Netmask	Subnet mask of the DHCP subnet, in dotted decimal notation, such as 255.255.255.0
	Start IP	Start IP address of the address pool of the DHCP server, in dotted decimal notation, such as 192.168.1.1
	End IP	End IP address of the address pool of the DHCP server, in dotted decimal notation, such as 192.168.1.254
	Gateway Address	Default gateway of the subnet that the interface is connected to, in dotted decimal notation, such as 192.168.1.1
	Primary DNS	IP address of the primary DNS server, in dotted decimal notation, such as 192.168.101.1
	Secondary DNS	IP address of the secondary DNS server, in dotted decimal notation, such as 192.168.101.2
	Reserved IP	IP addresses that are kept from automatical assignment in the address pool of the DHCP server. You can fill in up to 8 IP addresses which should be separated by a comma (.).
	Lease Time	After a PC applies for an IP address successfully, it can use the IP address for 5 minutes to 100 days. The value 0 indicates that the period is infinite.

4.2.2 VLAN configuration

Scenario

You can create VLANs and add LAN interfaces to a VLAN on this interface.

VLAN is a protocol proposed to resolve the Ethernet broadcast problem and enhance the Ethernet security. It is a Layer 2 isolation technology used to partition devices in a LAN into different broadcast domains logically instead of physically. Therefore, multiple virtual working groups can work independently.

VLAN interface modes of the LAVA are divided into Access mode and Trunk mode. The Access interface is mainly used to connect with the host while the Trunk interface is mainly used to connect with other network devices.

Configuration steps

- Step 1 In the navigation bar, choose **Basic > Interface > LAN > VLAN Configuration**. The **VLAN Configuration** window is displayed.
- Step 2 In the **VLAN Create & Delete** area,
- To create a VLAN, click **Create**, enter a VLAN ID, and click **OK**. In the **VLAN Information List** area, all successfully created VLANs will be displayed.
 - To delete a VLAN, click **Delete**, enter a VLAN ID, and click **OK**. In the **VLAN Information List** area, deleted VLANs will not be displayed.
- Step 3 In the **VLAN Information List** area, you can select LAN interfaces and add them into a VLAN. Then, configure the mode and PVID of the VLAN interface.
- Step 4 After configurations are complete, click **Save Config** to save configurations.

Configuration items

Table 4-7 Configurations items in the VLAN Add & Delete area

Configuration item	Description
VLAN Create & Delete	<ul style="list-style-type: none"> • To create a VLAN, click Create. • To delete a VLAN, click Delete.
VLAN ID	ID of the VLAN to be created or deleted, ranging from 1 to 4093

Table 4-8 Configuration items on the VLAN Information List area

Configuration item	Description
LAN	Display all LAN interfaces provided by the LAVA LR-2G211.
Mode	Each LAN interface has two VLAN modes: <ul style="list-style-type: none"> • Access • Trunk

Configuration item	Description
PVID	Default VLAN ID for the LAN interface. This VLAN ID must be created.
vlanID	A Created VLAN. Select the radio button corresponding to a LAN interface to add the LAN interface to the VLAN.

4.2.3 IPv6 configuration

Scenario

By configuring IPv6 items, you can make the VLAN support IPv6 features.

Configuration steps

- Step 1 In the navigation bar, choose **Basic > Interface > LAN > IPv6 Configuration**. The **IPv6 Configuration** interface is displayed.
- Step 2 Select a created VLAN, configure related items, and click **OK**.
- Step 3 After configurations are complete, click **Save Config** to save configurations.

Configuration items

Table 4-9 Configuration items on the IPv6 Configuration interface

Configuration item	Description
VLAN	Select a VLAN interface from the drop-down list.
IPv6 address	IPv6 address of the selected interface, in colon hexadecimal notation, such as 3001::3
Prefix Length	Number of bits of the IPv6 prefix, ranging from 0 to 128
Send RA	Send or not send Router Advertisement (RA).
Send Interval	Interval for sending RA, in unit of second, ranging from 3 to 1800, being 600 by default
Router Lifetime	Valid Keepalive time for default route, in unit of second, ranging from 0 to 9000, being 1800 by default
Reachable Time	Time for judge whether the neighbor is reachable, in unit of second, in unit of millisecond, ranging from 0 to 3 600 000, being 0 by default
Set Management Flag	Configure the management flat or not.
Set Other Flag	Configure the other flat or not.
Prefix Information	Prefix of the IPv6 address sent in the RA, in colon hexadecimal notation, such as 3001::3/64

Configuration item	Description
Prefix Lifetime	You can choose finite or infinite for the lifetime of RA prefix
Valid Lifetime	Leased period of the IPv6 prefix. It is an integer ranging from 1s to 4294967295s. By default, it is set to 2592000s.
Preferred Lifetime	In this period, the prefix keeps being selected with high priority. The preferred lifetime should not be greater than the valid lifetime. It is an integer ranging from 1s to 4294967295s. By default, it is set to 604800s.

4.2.4 ETH configuration

Scenario

You can configure physical features and loopback detection of LAVA Ethernet interfaces.

Configuration steps

- Step 1 In the navigation bar, choose **Basic > Interface > LAN > ETH Configuration**. The **ETH Configuration** interface is displayed.
- Step 2 Configure related items and then click **Set**.

Configuration items

Table 4-10 Configuration items on the ETH Configuration interface

Configuration item	Description
Loopback Detect	Enable/Disable loopback detection.
Eth Exist	Display whether a loopback is generated. It is displayed based on the real situation without being configured.
Link Status	Display current link status of LAN interfaces. It is displayed based on the real situation without being configured.
Shutdown Status	Open/Shut down the current LAN interface. <ul style="list-style-type: none"> • NO SHUT: open the current LAN interface. • SHUT: shut down the current LAN interface.
Auto Negotiation	Configure auto-negotiation of LAN interfaces, including: <ul style="list-style-type: none"> • ON: enable auto-negotiation. • OFF: disable auto-negotiation.
Eth Speed	Configure the speed of LAN interfaces. This item is available when auto-negotiation is disabled.
Eth Duplex	Configure the duplex mode of LAN interfaces. This item is available when auto-negotiation is disabled.

4.3 DMZ

4.3.1 DMZ

Scenario


You can configure the DMZ interface of the LAVA LR-2G211.

Configuration steps

- Step 1 In the navigation bar, choose **Basic > Interface > DMZ**. The **DMZ** interface is displayed.
- Step 2 Configure related items and then click **OK**.
- Step 3 After configurations are complete, click **Save Config** to save configurations.

Configuration items

Table 4-11 Configuration items on the DMZ interface

Configuration item		Description
OFF		Disable DMZ of the interface.
ON	–	Enable DMZ of the interface.
	Attach to DMZ	Select interfaces to be added to DMZ, including the WAN interface and LAN interface.  Note Select interfaces based on the configuration items listed on the Web configuration interface. The WAN interface and LAN interface cannot be added to DMZ simultaneously.
	IP Address	IP address of the DMZ subnet. This IP address should not be at the same network segment with the one of the intranet.
	Subnet Mask	Subnet Mask of the DMZ subnet


4.4 WLAN

4.4.1 Basic configuration

Scenario

You can configure the WLAN access function to connect wireless devices to a LAN.

Configuration steps

- Step 1 In the navigation bar, choose **Basic > Interface > WLAN > Basic Configuration**. The **Basic Configuration** interface is displayed.
- Step 2 View wireless server, data encryption, and service status.
- To disable a wireless service, select it, and click **OFF**.
 - To enable a wireless service, select it, and click **ON**.
 - To modify a wireless service, click the corresponding  to enter the modifying interface. After configurations are complete, click **OK**.
- Step 3 After configurations are complete, click **Save Config** to save configurations.

Configuration items

Table 4-12 Configuration items on the Modify Basic WLAN Configuration interface

Configuration item		Description	
Network Name (SSID)		Name of a wireless connection, in 1–31 characters. The LAVA supports up to 4 wireless connections.	
Address Mode		There are three address modes: <ul style="list-style-type: none"> • Static: manually specifying IP addresses • VLAN binding • BVI binding 	
Static	IP Address	Subnet mask of a wireless network (the same SSID)	
	Subnet Mask	IP address of a subnet of a wireless network (the same SSID)	
	Management Access	Enable/Disable HTTPS, PING, Telnet, SSH, and/or HTTP. If you check one, it is enabled.	
	DHCP	Enable/Disable	Enable/Disable the DHCP server functions on the interface.
		DHCP Starting IP Address	Start IP address of the address pool of the interface
		DHCP Ending IP Address	End IP address of the address pool of the interface
		Default Gateway	Default IP address of the gateway of the subnet connected with the interface
DNS Server1		IP address of the primary DNS server of the subnet connected with the interface	
DNS Server2	IP address of the secondary DNS server of the subnet connected with the interface		

Configuration item		Description
	Lease Time	After a PC applies for an IP address successfully, it can use the IP address for 5 minutes to 100 days. The value 0 indicates that the period is infinite.
VLAN binding	VLAN	Bind with an existing VLAN interface.
BVI binding	–	Bind with an existing bridge interface. The prerequisite is that the WAN interface is configured to bridge mode.
SSID Hide		Hide/Unhide wireless network name.
WMM		Enable Wi-Fi MultiMedia (WMM) to grant video/audio data higher priority than common data. The client must support WMM as well.
AP Isolation		Users under the same SSID network cannot communicate with each other after the option is selected.
SSID Rate		Wireless RX/TX rate. The value Auto indicates the self-adaptive rate in the current network environment.
Beacon Interval		Interval for sending Beacon frames, in unit of millisecond, being 100 by default, and ranging from 40 to 1000
DTIM Interval		Interval for sending Delivery Traffic Indication Message (DTIM), ranging from 1 to 31, being 1 by default
BSS Max Associations Limit		Upper limit to the number of users concurrently connected to the network, ranging from 2 to 32 being 32 by default
Authentication Mode		<p>Authentication mode for the user to connect to the LAVA, including:</p> <ul style="list-style-type: none"> • Disabled: no encryption • Open Mode: use open authentication and WEP encryption and need to configure the key, key length, and key index. • Share Mode: use shared authentication and WEP encryption and need to configure the key, key length, and key index. • WPA-PSK: use WPA-PSK authentication to encrypt data and need to configure the WPA Pre-Shared key and WPA encryption algorithm. • WPA2-PSK: use WPA2-PSK authentication to encrypt data and need to configure the WPA Pre-Shared key and WPA encryption algorithm.

Configuration item		Description
WPA Pre-Shared Key		Configure the key used for authentication. <ul style="list-style-type: none"> • 128-bit key corresponds to 26-bit hexadecimal or 13-bit ASCII code. • 64-bit key corresponds to 10-bit hexadecimal or 5-bit ASCII code.
Key length		Length of the WEP pre-shared key <ul style="list-style-type: none"> • 128-bit key • 64-bit key
Key		Key index, varying with networks, ranging from 1 to 4
WPA Pre-Shared Key		WPA key, in a character string form ranging from 8 to 63
WPA Encryption		WAP encryption algorithms, including: <ul style="list-style-type: none"> • Advanced Encryption Standard (AES) • Temporal Key Integrity Protocol (TKIP)
MAC Filter	–	Enable/Disable MAC address filtering.
	Filter Rule	Two filtering rules are available: <ul style="list-style-type: none"> • Allow MAC on Table to Access • Deny MAC on Table to Access
	Add MAC	Enter a MAC address in the text box and then click Add to add the MAC address to the MAC Filter Table. This MAC address is matched based on the filtering rules. Double-click the MAC address to delete it from the MAC Filter Table.



Note

By default, the wireless network SSID-0001 is enabled; the WPA2-PSK security mode is adopted; the connection password is set to a5d82ec6b3.

4.4.2 Advanced configuration

Scenario


You can configure advanced WLAN items on this interface.

Configuration steps

- Step 1 In the navigation bar, choose **Basic > Interface > WLAN > Advanced Configuration**. The **Advanced Configuration** interface is displayed.
- Step 2 Configure related items, and click **OK**.
- Step 3 After configurations are complete, click **Save Config** to save configurations.

Configuration items

Table 4-13 Configuration items on the Advanced Configuration interface

Configuration item	Description
Country Code	<p>The country code is used to identify the counter of the Radio Frequency (RF). It is mapped with RF features, such as power and the total number of channels for transmitting frames. Before configuring the Access Point (AP), you must configure valid country code or region code.</p> <ul style="list-style-type: none"> • The LAVA supports the following country codes: • Australia • China • Canada • Israel • Japan • United States
Working Mode	<ul style="list-style-type: none"> • auto: automatically select working mode. • 802.11b: support a maximum sending rate of 11 Mbit/s. • 802.11g: support a maximum sending rate of 54 Mbit/s. • 11nht20: support a maximum sending rate of 130 Mbit/s. • 11nht40minus: support a maximum sending rate of 300 Mbit/s. • 11nht40plus: : support a maximum sending rate of 300 Mbit/s.
Working Channel	<p>WLAN working channel. Working channels 1–13 or Auto is available. If you choose auto, the LAVA will automatically selects working channel according to current network environment.</p> <p> Note</p> <p>The working channel ID varies on the country code. When the country code is set to Australia, China, or Japan, working channels 1–13 or auto is available. When the country code is set to Canada or United States, working channels 1–11 or auto is available. When the country code is set to Israel, working channels 1–9 or auto is available.</p>
Power	<p>RX power of radio wave. Following options are available:</p> <ul style="list-style-type: none"> • 20%: 20% of the maximum power • 40%: 40% of the maximum power • 60%: 60% of the maximum power • 80%: 80% of the maximum power • 100%: the maximum power
Service Status	<p>Enable/Disable the wireless module. Therefore, you can enable/disable WLAN through hardware.</p>

4.4.3 Wireless interface

Scenario

You can view wireless terminals connected to the WLAN.

Configuration steps

- Step 1 In the navigation bar, choose **Basic > Interface > WLAN > Wireless Interface**. The **Wireless Interface** interface is displayed.
- Step 2 Choose a WLAN, click **View**. Information about wireless terminals connected to the WLAN is displayed.

Configuration items

Table 4-14 Configuration items on the SSID Subset Information List area

Configuration item	Description
Wireless Interface	Parameters of the devices connected to the wireless interface, including interface ID, MAC address, channel, speed, IP address, and connection time.

4.4.4 WPS configuration

Scenario

Wi-Fi Protected Setup (WPS) is an authentication created by Wi-Fi Alliance. It is mainly used to simplify the security encryption setting of wireless network. Just by pressing the WPS button on the wireless client/entering the PIN at the WPS management tool of the client and performing simple operations, users can complete the wireless encryption configurations. In addition, a secure connection between the wireless client and LAVA is established.

Configuration steps

- Step 1 In the navigation bar, choose **Basic > Interface > WLAN > WPS Configuration**. The **WPS Configuration** interface is displayed.
- Step 2 Configure related items, and click **OK**.

Configuration items

Table 4-15 Configuration items on the WPS Configuration interface

Configuration item	Description
WPS	Enable/Disable WPS of the LAVA LR-2G211. If it is enabled, you can configure more features about WPS.

Configuration item	Description
Local PIN	Local PIN of the LAVA LR-2G211, consisting of 8 digits. Click Refresh to get a random PIN for WPS encryption.
Add Device	If the Add Device radio button is selected, you can configure the encryption mode further and add clients to the wireless network.
Input client PIN	Add a client to the wireless network by entering the PIN generated by the wireless client. You need to enter the client PIN in the Device text box.
Client input local PIN	Add a client to the wireless network by entering the local PIN at the configuration tool of the client.
Push client button	Add a client to the wireless network by pressing the WPS button on the client. You need to press the WPS button in 120s after WPS is enabled.

4.5 3G

4.5.1 Basic configuration

Scenario

You can configure basic configurations of the 3G interface on this interface.

The LAVA can be connected to a USB 3G Modem through its USB interface. The USB 3G Modem is embedded with a UIM card of an ISP for 3G wireless communication.

Configuration steps

- Step 1 In the navigation bar, choose **Basic > Interface > 3G > Basic Configuration**. The **Basic Configuration** interface is displayed.
- Step 2 Configure related items, and click **OK**.
- Step 3 After configurations are complete, click **Save Config** to save configurations.

Configuration items

Table 4-16 Configuration items in the 3G Interface Basic Configuration area

Configuration item	Description
Interface Name	3gppp, read-only

Configuration item		Description
Dial Network		3G access mode, including: <ul style="list-style-type: none"> • VPDN: use the VPDN server purchased from the carrier, and still use the 3G network. • 3G: used to access the Internet
Username		User name registered to the carrier's network, used for network authentication, in a character string form ranging from 1 to 80
Password		Matching the user name, used for network authentication, in a character string form ranging from 1 to 48
Dial-string		Used to initiate a call connection to the network, provided by the carrier, in a character string form ranging from 1 to 48
Online Mode	–	Online mode of 3G network status
	All the time	After the dialling is successful, the 3G WLAN card keeps being connected to the network until it is changed. <ul style="list-style-type: none"> • Interval-time: it is the interval between the first failed dialling and the next attempted dialling. It is in unit of second, ranges from 1 to 65535, and is 15 by default. • Idle-time: after the connection is manually released, the LAVA waits for an idle interval, and then automatically performs dialling. It is in unit of second, ranges from 1 to 65535, and is 120 by default.
	Disconnect automatically after a period of time	When there is traffic need, the 3G module will automatically dial the number to connect to the network. When there is no traffic need, the 3G module will automatically release the connection from the network and waits for the next traffic need. It is in unit of second, ranges from 1 to 65535, and is 60 by default.
	Manual	Connect to /Disconnect from the network manually.

4.5.2 Advanced configuration

Scenario

You can configure more items of the 3G interface on this interface.

Configuration steps

- Step 1 In the navigation bar, choose **Basic > Interface > 3G > Advanced Configuration**. The **Advanced Configuration** interface is displayed.
- Step 2 Configure related items, and click **OK**.
- Step 3 After configurations are complete, click **Save Config** to save configurations.

Configuration items

Table 4-17 Configuration items in the 3G Advanced Configuration area

Configuration item	Description
Authentication methods	It is the PPP authentication mode. It is the network authentication mode obtained during dialling, including 3 modes: <ul style="list-style-type: none"> • Challenge Handshake Authentication Protocol (CHAP) (default) • Password Authentication Protocol (PAP) • AUTO
DNS	IP address of the DNS server
TCP-MSS	It is the length of the maximum block data that is transmitted to the peer through TCP, can be set to an integer between 128 and 2048. It is 1460 by default.
MTU	It is the maximum transmission unit. If a packet exceeds this size, it is fragmented. It is set to an integer between 128 and 1500. It is 1500 by default.
Enable NAT	Enable/Disable Network Address Translation (NAT).
APN	It is the Access Point Name (APN) of the leased network, and obtained from the carrier together with the user name and password. It is 1–30 characters.



Note

In general, you do not need to modify configuration items on the **Advanced Configuration** interface. Default configurations are permitted.

4.5.3 Flow warning

Scenario


When the 3G flow reaches the preset threshold, the LAVA reminds you of warning information.

Configuration steps

- Step 1 In the navigation bar, choose **Basic > Interface > 3G > Flow Warning**. The **Flow Warning** window is displayed.
- Step 2 Configure related items, and then click **OK**.
- Step 3 After configurations are complete, click **Save Config** to save configurations.

Configuration items

Table 4-18 Configuration items on the Flow Warning interface

Configuration item	Description
Plan warning percentage	When the used amount of package reaches a specified percentage of the entire packet, the LAVA sends a warning SMS. It ranges from 1 to 100, which indicates occupying 1%–100% entire packet. The default value is 90%.
Type of monthly plan	It is the type of the monthly package. <ul style="list-style-type: none"> • Flow package: it is charged by flow, in unit of G/month. It ranges from 1 to 15. The default value is 1G/month. • Time packet: it is charged by time, in unit of hour/month. It ranges from 1 to 744. The default value is 150h/month.
Warning mode	When the 3G flow or time used by the user reaches the configured threshold, the LAVA will alert the user in three methods: <ul style="list-style-type: none"> • Log: displaying warning information in the system log. • SMS: notifying the user of warning information in a SMS. You should input the cell phone number and SMS center number to receive the SMS in advance. • Email: notifying the user of warning information in an Email. You should input the Email to receive warning information in advance. <div style="margin-top: 10px;">  Note The SMS warning feature may result surcharge. Therefore, please pay enough telephone charge in advance. When you choose the Email mode, configure the Simple Network Management Protocol (SNMP) mail server in advance. For details, see section 12.10 SMTP server settings. </div>



4.6 GRE

Scenario

You can configure the GRE interface and establish GRE tunnels on this interface.

Configuration steps

- Step 1 In the navigation bar, choose **Basic > Interface > GRE > GRE Configuration**. The **GRE Configuration** window is displayed.
- Step 2 View configured GRE interfaces.

- To modify a configured item, click  to enter the modifying interface.
- To add an item, click **Add** to enter the adding interface.
- To delete an item, and click the corresponding .

Step 3 On the modifying or adding interface, configure related items, and click **OK**.

Step 4 After configurations are complete, click **Save Config** to save configurations.

Configuration items

Table 4-19 Configuration items in the Create/Modify A New GRE Interface area

Configuration item		Description
Name		Name of a GRE tunnel
IP Address		Local IP address of the GRE tunnel, in dotted decimal notation, such as 192.168.1.1
IP Subnet mask		Mask of the local IP address of the GRE tunnel, in dotted decimal notation, such as 255.255.255.0
Tunnel source	Source interface	Name of the interface used by the tunnel <ul style="list-style-type: none"> • 3gppp • WAN0
	Source IP address	IP address of the source of the GRE tunnel, namely, the external source IP address of GRE encapsulation
Tunnel destination	Destination IP Address	Peer IP address of the GRE tunnel
	Dynamic	Set the GRE tunnel to dynamically obtain the peer IP address. Set the peer IP address of the GRE tunnel to dynamic IP addresses; the peer IP address is the source IP address of packets sent from the peer upon GRE negotiation.
KeepAlive Tunnel ID		Key of the GRE tunnel, ranging from 1 to 9999. This key is for security sake during GRE data exchange. By default, no key is used.
KeepAlive interval		KeepAlive interval for the GRE tunnel, in unit of second, and ranging from 1 to 86400
KeepAlive Retries		Number of KeepAlive retry times for the GRE tunnel, ranging from 1 to 1000.
TTL		TTL of packets encapsulated by the GRE tunnel, ranging from 1 to 255
Calculate Checksum		Check checksum upon GRE capsulation and decapsulation
Access Control		Enable/Disable HTTPS, PING, Telnet, and/or HTTP. If you check one, the service is enabled; otherwise, it is disabled.

4.7 Link backup

Scenario

You can configure link backup on this interface.

Configuration steps




Note


Link backup is available for the WAN interface, WAN sub-interface, and 3G interface. In this section, the WAN interface link is taken as the primary link while the 3G interface link is taken as the backup link.

- Step 1 In the navigation bar, choose **Basic > Interface > WAN**. Set the WAN interface connection mode to Router mode and set the service type to Management_internet/Internet. If the interface IP type is set to static, you must configure a default gateway for it.
- Step 2 Configure the 3G interface of the LAVA LR-2G211 and establish the 3G connection. For details, see section 4.5 3G.
- Step 3 In the navigation bar, choose **Basic > Network > Route**. Confirm that there are 2 default routes in the routing table. For one route, the egress interface is set to WAN0/WAN1 interface. For the other router, the egress interface is set to 3G interface. Therefore, link backup preparation is finished and then you can perform link backup.
- Step 4 In the navigation bar, choose **Basic > Interface > LINK_DETECT**. The **Link detect config** interface is displayed.
- Step 5 Configure related items, and click **OK**.
- Step 6 After configurations are complete, click **Save Config** to save configurations.

Configuration items

Table 4-20 Configuration items in the Link detect config interface

Configuration item	Description
Enable	Enable link backup
Main link	Interface that is set to the main link, including: <ul style="list-style-type: none"> • WAN0 • WAN1 • 3gppp  Note The type of interfaces varies with device models.
ICMP message detect server	IP address of the peer on the main link
ICMP message detect interval	Interval to send ICMP packets, in unit of second, and ranging from 3 to 120

Configuration item	Description
Max retry times	Number of times that the LAVA resends ICMP packets upon link failure. After retries of the number, the LAVA switches to the backup link. The number ranges from 1 to 10.
Backup link	<p>Choose the link to back up the main link, including the following configuration items:</p> <ul style="list-style-type: none">• WANO• WAN1• 3gppp <p> Note</p> <p>The type of interfaces varies with device models. The backup link and the main link cannot use the same interface.</p>

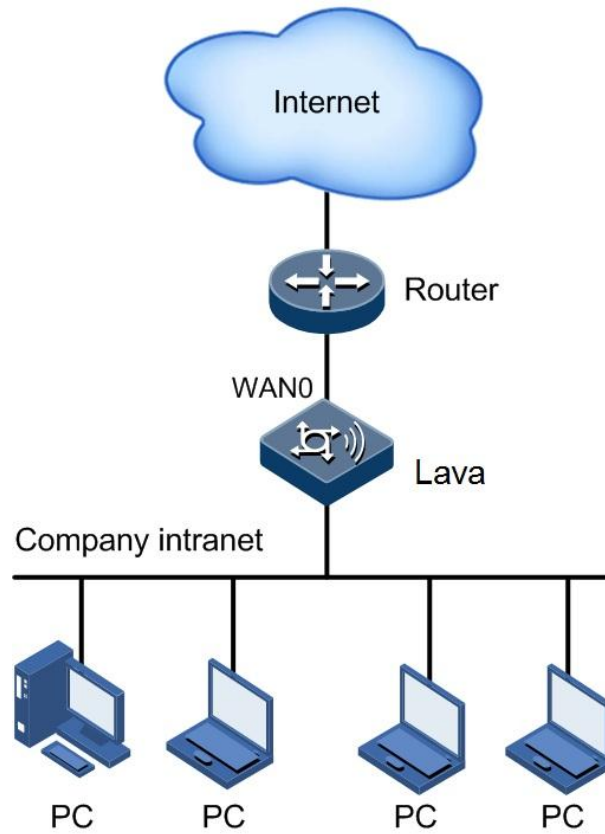
4.8 Configuration examples

4.8.1 Example for configuring the WLAN interface in bridge mode

Networking requirements

An enterprise uses a router to connect internal users to the Internet. Now the LAVA is added to the network to enhance security without changing its structure, as shown in Figure 4-8.

Figure 4-8 Bridge mode WAN0 interface application networking



Configuration steps

- Step 1 In the navigation bar, choose **Basic > Interface > WAN**. The **WAN0 Configuration** interface is displayed.
- Step 2 Click **Add** to enter the adding interface.
- Step 3 Select bridge mode, configure related items, and click **OK**, as shown in Figure 4-9.
- Step 4 After configurations are complete, click **Save Config** to save configurations.

Figure 4-9 Add Subinterface on WAN0 interface in bridge mode

Add Subinterface on WAN0					
Connection Name:	<input type="text" value="Create a new uplink cor"/>				
Connection Mode:	<input type="text" value="Bridge Mode"/>				
IP Address:	<input type="text"/> (e.g. "10.12.1.2")				
Subnet Mask:	<input type="text"/> (e.g. "255.255.255.0")				
Subinterface ID:	<input type="text" value="1"/> *[1-4095]				
802.1p Priority:	<input type="text"/> [0-7]				
MAC Address:	<input type="text" value="(XXXXXXXXXXXX)"/>				
Belongs to Bridge:	<input type="text" value="Create a new bridge"/>				
<table border="1"> <thead> <tr> <th>Interface List(Physical Interface, Vlan)</th> <th>Group Interface List(Physical Interface, Vlan)</th> </tr> </thead> <tbody> <tr> <td>vlan1 ath2 ath3</td> <td></td> </tr> </tbody> </table>		Interface List(Physical Interface, Vlan)	Group Interface List(Physical Interface, Vlan)	vlan1 ath2 ath3	
Interface List(Physical Interface, Vlan)	Group Interface List(Physical Interface, Vlan)				
vlan1 ath2 ath3					
Service Type	<input type="text" value="Management_Internet"/>				
* Required Field					

Checking configurations

You can access the Internet and use security functions of the LAVA on this interface.

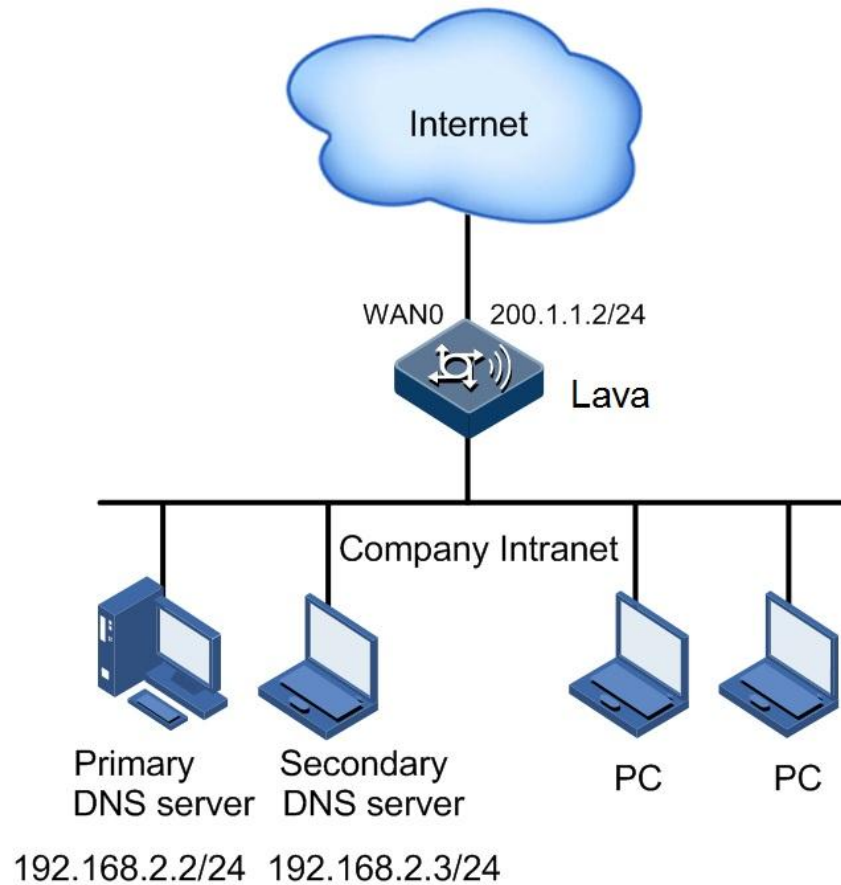
4.8.2 Example for configuring the WAN interface in router mode

Networking requirements

Internal users of an enterprise access the Internet through the LAVA, as shown in Figure 4-10, with the following configurations:

- Set the IP address of the WAN0 interface to 200.1.1.2/255.255.255.0.
- Set the IP address of the default gateway to 200.1.1.2/255.255.255.0.
- Set the IP address of the primary DNS server to 192.168.2.2/255.255.255.0.
- Set the IP address of the secondary DNS server to 192.168.2.3/255.255.255.0.
- Enable NAT and all types of access.

Figure 4-10 Router mode WAN0 interface application networking



Configuration steps

- Step 1 In the navigation bar, choose **Basic > Interface > WAN**. The **WAN0 Configuration** interface is displayed.
- Step 2 Click **Add** to enter the adding interface.
- Step 3 Select router mode, configure related items, and click **OK**, as shown in Figure 4-11.
- Step 4 After configurations are complete, click **Save Config** to save configurations.

Figure 4-11 Add Subinterface on WAN0 interface in router mode

WAN0 Modify	
Connection Name:	<input type="text" value="1_Internet_R_"/>
Connection Mode:	<input type="button" value="Router Mode"/>
<input type="radio"/> DHCP	Choose this option to obtain an IP address automatically from your ISP.
<input checked="" type="radio"/> Static	Choose this option to set an static IP address provided by your ISP.
<input type="radio"/> PPPoE	Choose this option if your ISP use PPPoE(For most DSL users).
IP Address:	<input type="text" value="200.1.1.2"/> *(e.g. "10.12.1.2")
Subnet Mask:	<input type="text" value="255.255.255.0"/> *(e.g. "255.255.255.0")
Default Gateway:	<input type="text" value="200.1.1.1"/>
Primary DNS:	<input type="text" value="192.168.2.2"/>
Secondary DNS:	<input type="text" value="192.168.2.3"/>
Access Control:	<input checked="" type="checkbox"/> HTTPS <input checked="" type="checkbox"/> PING <input checked="" type="checkbox"/> TELNET <input checked="" type="checkbox"/> SSH <input checked="" type="checkbox"/> HTTP
Enable NAT	<input checked="" type="checkbox"/> NAT
NAT Log	<input type="checkbox"/> NAT LOG
Enable NAT Address Pool	<input type="checkbox"/> NAT POOL
Service Type	<input type="button" value="Internet"/>
* Required Field	

Checking configurations

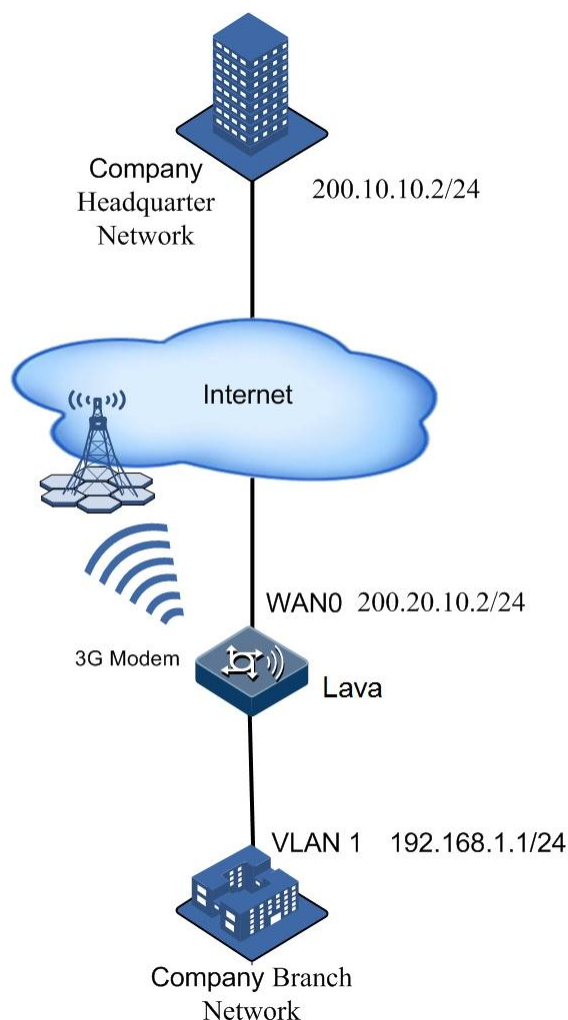
You can access the Internet through the WAN0 interface, access the LAVA through HTTPS, Telnet, SSH, and HTTP, and ping through the LAVA.

4.8.3 Example for configuring link backup

Networking requirements

The branch of an enterprise is connected to the Headquarter through the Internet. The enterprise now uses 3G connection. If the main link fails, the LAVA can fast switch to the 3G backup link to resume key services. When the main link recovers, the LAVA switches back to it, as shown in Figure 4-12.

Figure 4-12 Link backup application networking



Configuration steps

- Step 1 Configure the IP address of the WAN interface on the LAVA (for details, see related configuration examples).
- Step 2 Configure the IP address of the VLAN1 interface on the LAVA (for details, see related configuration examples).
- Step 3 Configure the IP address of the 3G interface on the LAVA (for details, see related configuration examples).
- Step 4 Configure the VPN connection between the branch and the Headquarter (for details, see related configuration examples).
- Step 5 Configure link backup.
 1. In the navigation bar, choose **Basic > Interface > LINK_DETECT**. The **Link detect config** interface is displayed.
 2. Configure related items, and click **OK**, as shown in Figure 4-13.

Figure 4-13 Configuring link backup

Link detect config	
Enable :	<input checked="" type="checkbox"/>
Main link :	WANO <input type="button" value="v"/>
ICMP message detect server :	200.10.10.2 *
ICMP message detect interval :	30 (3-120Seconds)
Max retry times :	3 (1-10times)
Backup link :	3gppp <input type="button" value="v"/>

Step 6 After configurations are complete, click **Save Config** to save configurations.

5 Network configurations

This chapter describes how to configure network items on the **Network** interface, including the following sections:

- NAT
- DHCP
- DNS
- Route
- Static route
- Policy route
- RIP
- OSPF
- Route filter
- Multicast
- EoIP
- DDNS
- Page push
- DHCPv6
- IPv6
- UPnP config
- Configuration examples

5.1 NAT

5.1.1 ALG

Scenario

You can configure application layer gateways on this interface to support some special application layer protocols, such as Generic Routing Encapsulation (GRE), Layer 2 Tunneling Protocol (L2TP), and Real Time Streaming Protocol (RTSP).

Configuration steps

- Step 1 In the navigation bar, choose **Basic > Network > NAT > ALG**. The **ALG** interface is displayed.
- Step 2 Configure related items, and then click **OK**.
- Step 3 After configurations are complete, click **Save Config** to save configurations.

Configuration items

Table 5-21 Configuration items on the ALG interface

Configuration item	Description
GRE	Enable Application Layer Gateway (ALG) of GRE.
SIP	Enable ALG of Session Initiation Protocol (SIP).
H.323	Enable ALG on the H.323 protocol.
RTSP	Enable ALG of RTSP.
IPSEC	Enable ALG of IP Security (IPSec).
L2TP	Enable ALG of L2TP.

5.1.2 Virtual server

Scenario

You can configure NAT virtual servers on this interface.

Configuration steps

- Step 1 In the navigation bar, choose **Basic > Network > NAT > Virtual Server**. The **Virtual Server** interface is displayed.
- Step 2 In the **Create Virtual Servers** area, configure related items, and click **Add** to create virtual servers.
- Step 3 In the **Select the internal servers you want to delete** area, select a virtual server, and click **Delete** to delete it.

Step 4 After configurations are complete, click **Save Config** to save configurations.

Configuration items

Table 5-22 Configuration items on the Virtual Server interface

Configuration item	Description
Interface	Ingress interface matching NAT rules
Type of protocol	Protocol type matching NAT rules
External IP address	Destination IP address matching NAT rules, an IP address of an ingress interface or a manually configured IP address
Internal IP address	IP address after translation, a single IP address or a range of IP addresses
Internal port	Port after translation. The default port is used. Configure this by selecting the Customer-defined port and inputting the port number only when you configure port mapping. The port ID ranges from 1 to 65535.

5.1.3 Source NAT

Scenario

You can configure source NAT rules on this interface.

Configuration steps

- Step 1 In the navigation bar, choose **Basic > Network > NAT > Source NAT**. The **Source NAT** interface is displayed.
- Step 2 In the first **Create Source NAT rules** area, configure related items, and click **Add** to create a source NAT rule.
- Step 3 In the second **Create Source NAT rules** area, you can select a rule and click **Delete** to delete it.
- Step 4 After configurations are complete, click **Save Config** to save configurations.

Configuration items

Table 5-23 Configuration items on the Source NAT interface

Configuration item	Description
Source Address	Source address matching NAT rules. The any parameter indicates matching all addresses.

Configuration item	Description
Destination Address	Destination address matching NAT rules. The any parameter indicates matching all addresses.
Service	Service name matching NAT rules
Converted Source Address	Source address after translation, an address of the egress interface, or customer-defined address object, or address pool
Egress	Egress interface matching NAT rules
Syslog	Source NAT system log switch, recording NAT information

5.1.4 One-to-one address translation

Scenario

You can create global static translation rules on this interface.

Configuration steps

- Step 1 In the navigation bar, choose **Basic > Network > NAT > One to One Address Translation**. The **One to One Address Translation** interface is displayed.
- Step 2 In **Create global static conversion rules** area, configure required items, and click **Add** to create global static translation rules.
- Step 3 In **Select the rules that you want to delete** area, select a rule and click **Delete** to delete it.
- Step 4 After configurations are complete, click **Save Config** to save configurations.

Configuration items

Table 5-24 Configuration items on the One to One Address Translation interface

Configuration item	Description
Internal IP Address	Internal IP address to be translated
External IP Address	External IP address after translation
External port	Name of the port connected to the external network


5.2 DHCP

5.2.1 DHCP service

Scenario

You can configure the type of DHCP service on each interface on the LAVA.

Configuration steps

- Step 1 In the navigation bar, choose **Basic > Network > DHCP > DHCP Service**. The **DHCP Service** interface is displayed.
- Step 2 View the type of DHCP server on each interface.
- To configure an interface, click  to enter the modifying interface.
- Step 3 Configure related items, and then click **OK**.
- Step 4 After configurations are complete, click **Save Config** to save configurations.

Configuration items

Table 5-25 Configuration items on the DHCP Service interface

Configuration item	Description
Server Name	On this interface, the DHCP server is enabled.
DHCP Service Type	The interface may use the following DHCP service types: <ul style="list-style-type: none"> • Disable • DHCP Client • DHCP Relay • DHCP Server
Enable Option60	This item is available when the DHCP Service Type is set to DHCP Client. Select the radio button to enable Option60 field. The DHCP server assigns configurations, such as specified IP address to the DHCP client based on the Option60 filed in the DHCP packet sent by the DHCP client.
Address Pool Name in DHCP Server	Address pool name in DHCP server. It is in a character string form, ranging from 1 to 64 and including letters, digits, and underlines. Match this name with the Option60 address pool name configured on the DHCP server. If they are matched, the DHCP server will apply host configurations.



Configuration item	Description
Enable DHCP Option125	This item is available when the DHCP Service Type is set to DHCP Client/DHCP Server. Select the radio button to enable Option125 field. The DHCP client receives packets sent by the specified DHCP server based on the Option125 filed in the DHCP packet sent by the DHCP server.
Option125 Match String	Option125 string ranging from 1 to 64 characters and including letters, digits, and underlines. Match this string with the one configured on the DHCP client. If they are matched, the DHCP client will receive host configurations sent by the DHCP server.
DHCP Server IP	This item is available when the DHCP Service Type is set to DHCP Relay. Enter the IP address of the DHCP server.

5.2.2 DHCP address pool

Scenario

You can configure the address pool of the DHCP server on the LAVA.

Configuration steps

- Step 1 In the navigation bar, choose **Basic > Network > DHCP > DHCP Address Pool**. The **DHCP Address Pool** interface is displayed.
- Step 2 View information about the configured DHCP address pool.
 - To modify a configured item, click  to enter the modifying interface.
 - To add an item, click **Add** to enter the adding interface.
 - To delete an item, and click the corresponding .
- Step 3 On the modifying or adding interface, configure related items, and click **OK**.
- Step 4 After configurations are complete, click **Save Config** to save configurations.

Configuration items

Table 5-26 Configuration items on the DHCP Address Pool interface

Configuration item	Description
Interface	Interface on which DHCP is enabled
Start IP Address	Start IP address in the address pool of the DHCP server, smaller than the end IP address
End IP Address	End IP address in the address pool of the DHCP server



Configuration item	Description
Subnet	Subnet corresponding to each interface
Subnet Mask	Subnet mask of the subnet IP address
Gateway	Gateway of the network segment of the subnet
Lease Period	Period that a PC can use an IP address after successfully applied it
Lease time	When you choose Finite , specify the time for the PC to use the IP address.
IP/MAC Binding	Enable IP/MAC binding.
Primary DNS Servers	IP address of the primary DNS server required for domain name resolution
Secondary DNS Server	IP address of the secondary DNS server required for domain name resolution
Primary WINS Servers	IP address of the primary WINS server, which is used to dynamically register and query mappings between IP addresses and NetBIOS names
Secondary WINS Server	IP address of the Secondary WINS server, which is used to dynamically register and query mappings between IP addresses and NetBIOS names.
Domain Name	Configure the domain name of the PC.

5.2.3 Excluded addresses

Scenario

You can exclude some DHCP addresses on this interface.

Configuration steps

- Step 1 In the navigation bar, choose **Basic > Network > DHCP > Excluded Address**. The **Excluded Address** interface is displayed.
- Step 2 View the **Excluded Address List** interface.
 - To modify a configured item, click  to enter the modifying interface.
 - To add an item, click **Add** to enter the adding interface.
 - To delete an item, and click the corresponding .
- Step 3 On the modifying or adding interface, configure related items, and click **OK**.
- Step 4 After configurations are complete, click **Save Config** to save configurations.

Configuration items

Table 5-27 Configuration items on the Excluded Address interface



Configuration item	Description
Start IP	Start IP address that the DHCP server excluded to assign to PCs
End IP	End IP address that the DHCP server excluded to assign to PCs

5.2.4 IP/MAC binding

Scenario

You can configure IP/MAC address binding on this interface.

Configuration steps

- Step 1 In the navigation bar, choose **Basic > Network > DHCP > IP/MAC Binding**. The **IP/MAC Binding** interface is displayed.
- Step 2 View the **IP/MAC Binding List** interface.
- To modify a configured item, click  to enter the modifying interface.
 - To add an item, click **Add** to enter the adding interface.
 - To delete an item, and click the corresponding .
- Step 3 On the modifying or adding interface, configure related items, and click **OK**.
- Step 4 After configurations are complete, click **Save Config** to save configurations.

Configuration items

Table 5-28 Configuration items on the IP/MAC Binding interface

Configuration item	Description
Name	Name of an IP/MAC binding
IP address	Static IP address bound with a MAC address
MAC address	MAC address bound with a static IP address

5.2.5 DHCP monitoring

Scenario

You can view configured DHCP items, such as IP/MAC binding and lease time, after DHCP is enabled.

Configuration steps

- Step 1 In the navigation bar, choose **Basic > Network > DHCP > DHCP Monitoring**. The **DHCP Monitoring** interface is displayed.
- Step 2 View configured DHCP items.

Configuration items



N/A

5.2.6 Option60 address pool

Scenario

You can configure the DHCP Option60 specified address pool of the LAVA on this interface.


Configuration steps

- Step 1 In the navigation bar, choose **Basic > Network > DHCP > Option60 Address Pool**. The **Option60 Address Pool** interface is displayed.
- Step 2 On the **Option60 Address Pool** interface, you can view information about configured DHCP address pools.
- To modify a configured item, click  to enter the modifying interface.
 - To add an item, click **Add** to enter the adding interface.
 - To delete an item, and click the corresponding .
- Step 3 On the modifying or adding interface, configure related items, and click **OK**.
- Step 4 After configurations are complete, click **Save Config** to save configurations.

Configuration items

Table 5-29 Configuration items on the Option60 Address Pool interface

Configuration item	Description
Interface	Interface where DHCP service is enabled
Address Pool Name	Name of the Option60 address pool, in a character string form, ranging from 1 to 64, and including letters, digits, and underlines. If the DHCP client uses the address pool, it needs to enable Option60 and configure the Address Pool Name in DHCP server and the address pool name to be identical.
Start IP Address	Start IP address of the DHCP server address pool. In general, it is smaller than the end IP address.



Configuration item	Description
End IP Address	End IP address of the DHCP server address pool  Note The start and end IP addresses of Option60 address pool should be co-included with the ones of the common DHCP address pool.
Lease Period	Period that a PC can use an IP address after successfully applied it, including: <ul style="list-style-type: none"> • Infinite • Finite
Lease time	When you choose Finite , specify the time for the PC to use the IP address.
IP/MAC Binding	Enable IP/MAC binding.

5.3 DNS

Scenario

You can configure DNS on this interface.

Configuration steps

- Step 1 In the navigation bar, choose **Basic** > **Network** > **DNS**. The **DNS** interface is displayed.
- Step 2 Enable DNS Proxy.
- Step 3 View static DNS information.
 - To modify a configured item, click  to enter the modifying interface.
 - To add an item, click **Add** to enter the adding interface.
 - To delete an item, and click the corresponding .
- Step 4 On the modifying or adding interface, configure related items, and click **OK**.
- Step 5 After configurations are complete, click **Save Config** to save configurations.

Configuration items

Table 5-30 Configuration items on the DNS interface

Configuration item	Description
DNS Proxy	Enable/Disable DNS Proxy.

Configuration item	Description
Host Name	Configured static domain name, in a character string form ranging from 1 to 255
Host IP Address	IP address corresponding to the static domain name

5.4 Route

Scenario

You can view information about the routing table on this interface.

Configuration steps

- Step 1 In the navigation bar, choose **Basic > Network > Route**. The **Routing Table** interface is displayed.
- Step 2 View routing information.

Configuration items



N/A

5.5 Static route

Scenario

You can configure static routes on this interface.

Configuration steps

- Step 1 In the navigation bar, choose **Basic > Network > Static Route**. The **Static Rout List** interface is displayed.
- Step 2 View the static route list.
 - To modify a configured item, click  to enter the modifying interface.
 - To add an item, click **Add** to enter the adding interface.
 - To delete an item, and click the corresponding .
- Step 3 On the modifying or adding interface, configure related items, and click **OK**.
- Step 4 After configurations are complete, click **Save Config** to save configurations.

Configuration items

Table 5-31 Configuration items on the Static Rout List interface

Configuration item	Description
Network Destination	Destination network address that the static route reaches
Subnet mask	Subnet mask of the network that the static route reaches
Next Hop	IP address of the interface of the next hop router for the static route
Interface	Egress interface of the static route. The static route of the egress interface is valid only when the egress interface is in PPPoE mode.
Weight	Route cost, integer, and ranging from 1 to 100
Distance	Route priority, integer, and ranging from 1 to 255
Monitor Address	Reference address of the static route. It believes that the static route is valid if the monitor address can be ping through on the LAVA LR-2G211. Otherwise, the static route is invalid.
Send Interval	If the Monitor Address check box is select, this sending interval is the interval for monitoring. It is in unit of second, ranging from 1 to 300, and being 3 by default.
The number of packets	Number of ICMP packets to be send upon monitoring, ranging from 1 to 10, being 3 by default


5.6 Policy route

Scenario

You can configure policy route on this interface.

Policy route is a packet forwarding mechanism more flexible than destination network route. By configuring policy route, you can specify packets of a network to be forwarded to the specified interface or specify the route for some routes.

Configuration steps

- Step 1 In the navigation bar, choose **Basic > Network > Policy Route**. The **Policy Route** interface is displayed.
- Step 2 View the policy route list.
 - To modify a configured item, click  to enter the modifying interface.
 - To add an item, click **Add** to enter the adding interface.

- To delete a static route, click .

Step 3 On the modifying or adding interface, configure related items, and click **OK**.

Step 4 After configurations are complete, click **Save Config** to save configurations.

Configuration items

Table 5-32 Configuration items on the Policy Route interface

Configuration item	Description
Policy Route ID	Identify a policy route, ranging from 1 to 100.
Source Interface/Security Domain	Source interface or security domain of a flow. It is one of policy matching rules.
Source Address	Source address target name, a set of various addresses, including MAC address, host address, and range of IP addresses. It is one of policy matching rules.
Destination Address	Destination address target name, a set of various addresses, including MAC address, host address, and range of IP addresses. It is one of policy matching rules.
Service	Service target name, a set of protocols and port number, such as TCP, UDP, and range of port numbers. It is one of policy matching rules.
Schedule	Time target name, indicating that the policy takes effect in a specified period. It is one of policy matching rules.
Next Hop Mode	Address or interface
Next Hop Address	Next hop IP address. Configure it when you choose Address in the Next Hop Mode area.
Next Hop Interface	Next hop interface, virtual interface with the interface type as NO ARP, such as 3gppp and GRE. Configure it when you choose Interface in the Next Hop Mode area.
Reference Policy ID	You can adjust the priorities of policy routes to grant the ahead policy with higher priority, ranging from 1 to 100.
Before/After	Configure this policy with higher or lower priority than the reference policy. <ul style="list-style-type: none"> • Before: higher priority • After: lower priority


5.7 RIP

5.7.1 RIP basic configuration

Scenario

You can configure basic RIP items on this interface.

Configuration steps

- Step 1 In the navigation bar, choose **Basic > Network > RIP > RIP Basic Configuration**. The **RIP Basic Configuration** interface is displayed.
- Step 2 Configure related items in the **Version Selection** and **Set up Timer** areas.
- Step 3 View the RIP network list.
- To add an item, enter the IP address of the subnet, and click **Add**.
 - To delete an item, and click the corresponding .
- Step 4 On the modifying or adding interface, configure related items, and click **OK**.
- Step 5 After configurations are complete, click **Save Config** to save configurations.

Configuration items

Table 5-33 Configuration items on the RIP Basic Configuration interface



Configuration item	Description
Version	RIP version: v1 or v2
Set up Timer	<ul style="list-style-type: none"> • Update: period to send route update packets, in unit of second, ranging from 5 to 3600, and being 30 by default • Timeout: expiration time, used to count time before routing information expires, in unit of second, ranging from 5 to 3600, and being 180 by default. When the update message of the same route is received, it is reset. • Garbage: garbage timer, in unit of second, ranging from 5 to 3600, and being 120 by default. After the timer expires, invalid routing information will be deleted.
Add Subnet	Add a subnet to broadcast routing information.

5.7.2 Advanced configuration

Scenario

You can configure advanced RIP items on this interface.

Configuration steps

- Step 1 In the navigation bar, choose **Basic > Network > RIP > Advanced Configuration**. The **Advanced Configuration** interface is displayed.
- Step 2 View the RIP network list.
- To modify a configured item, click  to enter the modifying interface.
 - To add an item, enter the IP address of the subnet, and click **Add**.
 - To delete an item, and click the corresponding .
- Step 3 On the modifying or adding interface, configure related items, and click **OK**.
- Step 4 In the **Passive Interface List** area, click **OK** to enter the **Passive Interface** interface.
- Step 5 Configure related items, and click **OK**.
- Step 6 After configurations are complete, click **Save Config** to save configurations.

Configuration items

Table 5-34 Configuration items in the Interface RIP Version List area

Configuration item	Description
Interface	Interface enabled with RIP
Sending Version	<ul style="list-style-type: none"> • V1: sending RIPv1 packets in broadcast mode. The broadcast address is set to 255.255.255.255. • V2: sending RIPv2 packets in multicast mode. The multicast is set to 224.0.0.9. • Compatible: sending RIPv2 packets in broadcast mode. The broadcast address is set to 255.255.255.255.
Receiving Version	<ul style="list-style-type: none"> • V1: receiving RIPv1 packets • V2: receiving RIPv2 packets • Compatible: receiving both packets, which are processed based on the packet version.
Authentication Type	Support password and MD5 authentication. If you choose V1 for both sending version and receiving version, you must choose No authentication here.
Authentication Password	If you choose password or MD5 authentication, you must fill in the authentication code, in a character string form ranging from 1 to 16.

Table 5-35 Configuration items in the Passive interface list area

Configuration item	Description
Passive Interface	The interface does not send routing information.

Table 5-36 Configuration items in the Redistribution Setting area

Configuration item	Description
Redistribution filtering	Enable redistribution filtering or not.
Prefix list config	Configured address list, used to filter IP addresses, in a character string form ranging from 1 to 20. For details, see section 5.9.1 Prefix list config.
Default Metric Distribution	Configure the default metric value, integer, ranging from 1 to 16.
Redistribution Type	There are three redistribution types. After you select a type, you can configure the distribution value. The value is 1 by default and configurable to 1 to 16.
Default-information Originate	Set the device to the default gateway of the internal network or not.



5.8 OSPF

5.8.1 OSPF configuration

Scenario

You can configure OSPF on this interface.


Configuration steps



- Step 1 In the navigation bar, choose **Basic > Network > OSPF > OSPF Configuration**. The **OSPF Configuration** interface is displayed.
- Step 2 In the **Advanced Options** area, configure related items, and click **OK**.
- Step 3 In the **Network Configuration** area, view configured networks.
- To modify a configured item, click  to enter the modifying interface.
 - To add an item, enter the IP address of the subnet, and click **Add**.
 - To delete an item, and click the corresponding .



Note

The domain is also added when you add network configurations. Therefore, domain configurations cannot be deleted but can be modified only. When you delete the current network configurations, the domain is deleted too.

- Step 4 In the **Interface Configuration** area, view configured networks.
- To modify a configured item, click  to enter the modifying interface.
 - To add an item, enter the IP address of the subnet, and click **Add**.

- To delete an item, and click the corresponding .
- Step 5 In the **Passive Interface List** area, view configured networks.
- To add an item, enter the IP address of the subnet, and click **Add**.
 - To delete an item, and click the corresponding .
- Step 6 On the modifying or adding interface, configure related items, and click **OK**.
- Step 7 After configurations are complete, click **Save Config** to save configurations.

Configuration items

Table 5-37 Configuration items on the Advanced Configuration interface for OSPF

Configuration item	Description
Router_ID	A 32-bit non-symbol integer, identifying a router, manually configured. If it is not manually configured, the system automatically selects a maximum IP address from IP addresses of all interfaces as the router ID.
Default Routing Information	You can choose three options: <ul style="list-style-type: none"> • No Default-Information Originate: the LAVA does not distribute route redistribution information. • Default-Information Originate: check whether there is route redistribution information. If yes, the LAVA distributes it as Class 5 LSA; otherwise, no distribution. • Default-Information Originate: no matter there is route redistribution information or not, the LAVA distributes it as Class 5 LSA.
Redistribute filtering	Filter redistribution or not.
Prefix list configure	Configured address list, used to filter IP addresses, in a character string form ranging from 1 to 20. For details, see section 5.9.1 Prefix list config.
Routing Redistribution	Configure route distribution information, such as type and weight. There are 3 distribution modes. You cannot choose the weight unless you choose a distribution mode. By default, it is set to 1. It ranges from 1 to 16777214.
Connect route	Route information when the route redistribution type is set to directly-connected route.
Static route	Route information when the route redistribution type is set to manually-configured static route.
RIP	Route information when the route redistribution type is set to route generated by RIP.

Table 5-38 Configuration items on the Area Configuration interface for OSPF

Configuration item	Description
Area	Domain to be configured, read-only
Authentication Type	Configure the authentication type of the domain: <ul style="list-style-type: none"> • No Authentication • Password Authentication • MD5

Table 5-39 Configuration items on the Network Distribution interface

Configuration item	Description
IP Address/Mask	Subnet address/mask to be distributed
Area	32-bit integer, starting from 0. Different areas use ABR to transmit routing information.

Table 5-40 Configuration items on the Interface Configuration interface

Configuration item	Description
Interface	Currently the VLAN and WAN interfaces support OSPF.
Priority	Integer, ranging from 0 to 255
Cost	OSPF link cost, integer, ranging from 0 to 65535
Network Type	<ul style="list-style-type: none"> • Broadcast • Point to Point
Authentication Type	When you select Password Authentication , you need to type the password. The content in Authentication Type must be consistent with that in the Password box.
Key ID	When you select MD5 in the Authentication Type drop-down list, you need to type the key ID.
MD5 Key	When you select MD5 in the Authentication Type drop-down list, you need to type the MD5 key.
Hello Interval	Interval for sending Hello packets, in unit of second, range from 1 to 65535
Dead Interval	In unit of second, ranging from 1 to 65535. If the router stops responding for such a time, its neighboring router takes it faulty.
Retransmission interval	Retransmission interval for link status, in unit of second, ranging from 3 to 65535
Send delay	Sending interval for link status, in unit of second, ranging from 1 to 65535

Table 5-41 Configuration items in the Passive Interface list

Configuration item	Description
Interface	This interface does not broadcast routing information.

5.8.2 Neighbor information

Scenario

You can view OSPF neighbor information on this interface.

Configuration steps

- Step 1 In the navigation bar, choose **Basic > Network > OSPF > Neighbor Information**. The **Neighbor Information** interface is displayed.
- Step 2 View OSPF neighbor information.
- Step 3 To refresh the list, click **Refresh**.

Configuration items

N/A

5.9 Route filter

5.9.1 Prefix list config


Scenario


You can configure the address prefix list on this interface.

The address prefix list is sorted by the name, and contains multiple entries. Each entry can be independently specified to a matching range of the network prefix and identified by an index ID. The index ID specifies the sequence of matching check.

During matching, the LAVA checks each entry identified by the index number in ascending order. Once an index matches rules, the address prefix list is filtered.

Configuration steps

- Step 1 In the navigation bar, choose **Basic > Network > Routing Filter > Prefix list config**. The **Prefix list config** interface is displayed.
- Step 2 View the prefix address list.
 - To modify an address prefix, click  to enter the modifying interface.

- To add a address prefix, click **Add** to enter the **Prefix list add** interface.
- To delete an address prefix, and click the corresponding .

Step 3 On the **Prefix list add** interface, configure related items, and click **OK**.

Step 4 After configurations are complete, click **Save Config** to save configurations.

Configuration items

Table 5-42 Configuration items on the Prefix list config interface

Configuration item	Description
Name	Name of the address prefix list
Mode	Action taken over matching packets: <ul style="list-style-type: none"> • PERMIT: permit matching packets to pass. • DENY: deny matching packets of passing.
Prefix list source IP	Subnet address to match rules for route filtering
Prefix list source mask	Subnet mask
Seq	Priority for matching check. The smaller the sequence number is, the higher the priority is. It is a positive integer and is smaller than 1000000.
Min mask	Minimum number of matching bits of subnet mask, greater than the number of source mask, smaller than the maximum number of matching bits of subnet mask
Max mask	Maximum number of matching bits of subnet mask, greater than the minimum number of matching bits of subnet mask, smaller than 32

5.9.2 Interface filtering

Scenario

You can configure interface filtering on this interface; namely, filter RIP routing information sent by an interface.

Configuration steps

Step 1 In the navigation bar, choose **Basic > Network > Routing Filter > Interface filtering**. The **Interface filtering** interface is displayed.

Step 2 View the prefix address list.

To add a new address prefix, click **Add** to enter the **Interface filtering config** interface.

Step 3 On the **Interface filtering config** interface, configure related items, and click **OK**.

Step 4 After configurations are complete, click **Save Config** to save configurations.

Configuration items

Table 5-43 Configuration items on the Interface filtering config interface

Configuration item	Description
Protocol	Being RIP by default, unchangeable
Prefix list config	Configured address list, used to filter IP addresses , in a character string form ranging from 1 to 20. It supports letter form only. For details, see section 5.9.1 Prefix list config.
Interface	Interface to be filtered on
Interface direction	Ingress or egress direction

5.10 Multicast

Scenario

You can configure working mode and multicast protocols of LAVA multicast.

Configuration steps

- Step 1 In the navigation bar, choose **Basic > Network > Multicast**. The **Multicast** interface is displayed.
- Step 2 Configure related items, and click **OK**.
- Step 3 After configurations are complete, click **Save Config** to save configurations.

Configuration items

Table 5-44 Configuration items in the Multicast area

Configuration item	Description	
Work_mode	Multicast can work in the following mode: <ul style="list-style-type: none"> • Router Mode: Layer 3 multicast • Bridge Mode: Layer 2 multicast 	
IGMP Protocol	disable	Disable multicast protocols.
	IGMP Proxy	Enable Layer 3 multicast Proxy.
	IGMP L2-Proxy	Enable Layer 2 multicast Proxy.
	IGMP Snooping	Enable Layer 2 multicast Snooping. This configuration item is unavailable for the route mode.

Configuration item	Description
bridge option	Select a bridge interface.
Upstream interface	Uplink interfaces required to enable IGMP Proxy
Interface list	A list of interfaces/VLANs available for the current system. By double-clicking an interface/VLAN, add it to downlink interfaces enabled with IGMP Proxy.
Downstream interface	Select a downlink interface required to enable IGMP Proxy.
Subinterface list	A list of interfaces available for the current system. By double-clicking an interface, add it to the multicast VLAN.
Multicast VLAN interface list	Add a multicast VLAN ID.
fast leave	This configuration item is available for the bridge mode. When there are a great number of users and users enter/leave the group frequently, you can enable this function. Therefore, the related multicast forwarding entry will be deleted quickly.


5.11 EoIP

5.11.1 EoIP configuration

Scenario

You can configure EoIP on this interface.

Configuration steps

- Step 1 In the navigation bar, choose **Basic > Network > EoIP**. The **EoIP Configuration** interface is displayed.
- Step 2 View the EoIP tunnel list.
 - To add an item, click **Add** to enter the adding interface.
 - To delete an item, and click the corresponding .
- Step 3 On the modifying or adding interface, configure related items, and click **OK**.
- Step 4 After configurations are complete, click **Save Config** to save configurations.

Configuration items

There are three modes to establish tunnels:

- Configure the tunnel ID and the peer IP address on both the server and client.

- On the client, configure the tunnel ID and the IP address of the server. On the server, configure the tunnel ID the same as that of the client, and you do not need to configure the IP address of the client.
- Configure the remote IP address on both the server and client.

Table 5-45 Configuration items on the EoIP Configuration interface



Configuration item	Description
Tunnel ID	Used to identify a tunnel, ranging from 1 to 127
Interface	Interface bound with the EoIP tunnel, usually being a VLAN
Remote Address	IP address of the peer device
keep alive	Enable/Disable KeepAlive.
Master/Backup	Master/Backup tunnel
Monitor IP	When you configure the tunnel as backup, input the remote IP address of the main link.

5.12 DDNS

Scenario

You can configure Dynamic Domain Name Server (DDNS) on this interface to transmit IP address information of the corresponding interface to the DDNS service provider and parse feedback response packets.

Configuration steps

- Step 1 In the navigation bar, choose **Basic > Network > DDNS**. The **DDNS Settings** interface is displayed.
- Step 2 View information about configured DDNS.
- To modify a configured item, click  to enter the modifying interface.
 - To add an item, click **Add** to enter the adding interface.
 - To delete an item, and click the corresponding .
- Step 3 On the modifying or adding interface, configure related items, and click **OK**.
- Step 4 After configurations are complete, click **Save Config** to save configurations.

Configuration items

Table 5-46 Configuration items on the DDNS Settings interface



Configuration item		Description
Host Name		Host name registered at the ISP, in a character string form, ranging from 1 to 80
Server Configuration	ISP	Internet Service Provider (ISP) providing domain name service. At present, the following items are available: <ul style="list-style-type: none"> • 3322.org • no-ip.com • oray.net • dyndns.org • tzo.com
	Server IP	Address of the server providing domain name service, automatically generated based on the selected ISP, and read-only
Account configuration	Username	User name used for registering a domain name, in a character string form, ranging from 1 to 38
	Password	Password used for registering a domain name, in a character string form, ranging from 1 to 38
Other Configuration	Binding interface	Bind DDNS to an interface.
	DDNS	<ul style="list-style-type: none"> • ON: enable DDNS on the bound interface. • OFF: disable DDNS on the bound interface. By default, DDNS is enabled on the bound interface.

5.13 Page push

Scenario

You can configure page push on this interface.


Configuration steps

- Step 1 In the navigation bar, choose **Basic > Network > Page Push**. The **Page Push** interface is displayed.
- Step 2 View configured information about page push.
 - To modify a configured item, click  to enter the modifying interface.
 - To add an item, click **Add** to enter the adding interface.
 - To delete an item, and click the corresponding .
- Step 3 On the modifying or adding interface, configure related items, and click **OK**.

Step 4 After configurations are complete, click **Save Config** to save configurations.

Configuration items

Table 5-47 Configuration items on the Page Push interface

Configuration item	Description
Interface Name	Internal network interface enabled for page push.  Note The push interface should be a created VLAN interface in the system. Global page push can be configured by selecting the global parameters of the interface.
State	Enable/Disable page push.
Push Interval	Interval for executing page push for each IP address, ranging from 60 to 86400, in unit of second, being 86400 by default
Push site	Uniform Resource Locator (URL) of the page to be pushed


5.14 DHCPv6

5.14.1 DHCPv6 services

Scenario

You can configure DHCPv6 service type on this interface.

Configuration steps

- Step 1 In the navigation bar, choose **Basic > Network > DHCPv6 > DHCPv6 Service**. The **DHCPv6 Service** interface is displayed.
- Step 2 View configured DHCPv6 services.
- Step 3 To configure an item, click .
- Step 4 Configure related items, and click **OK**.
- Step 5 After configurations are complete, click **Save Config** to save configurations.

Configuration items

Table 5-48 Configuration items on the DHCP Service interface



Configuration item	Description
Server Name	On this interface, the DHCPv6 server is enabled.
DHCP Service Type	Type of the DHCPv6 server, including <ul style="list-style-type: none"> • Disable • DHCPv6 relay • DHCPv6 server
DHCPv6 Server IP	This configuration item is available only when the DHCPv6 server type is set to DHCPv6 relay. Enter the IP address of the DHCP server.

5.14.2 DHCPv6 address pool

Scenario

You can configure DHCPv6 address pool on this interface.

Configuration steps

- Step 1 In the navigation bar, choose **Basic > Network > DHCPv6 > DHCP Address Pool**. The **DHCP Address Pool** interface is displayed.
- Step 2 View configured DHCPv6 servers.
 - To modify a configured item, click  to enter the modifying interface.
 - To add an item, click **Add** to enter the adding interface.
 - To delete an item, and click the corresponding .
- Step 3 On the modifying or adding interface, configure related items, and click **OK**.
- Step 4 After configurations are complete, click **Save Config** to save configurations.

Configuration items

Table 5-49 Configuration items on the DHCP Address Pool interface

Configuration item	Description
Interface	Interface enabled with DHCPv6 server
Start IPv6 Address	Start IPv6 Address assigned by the DHCPv6 server to PCs
End IPv6 Address	End IPv6 Address assigned by the DHCPv6 server to PCs

Configuration item	Description
Lease Period	Period for using the IPv6 address after successfully applying for it, including: <ul style="list-style-type: none"> • Infinite • Finite
Primary DNS Servers	Address 1 of the DNS server assigned to the DHCP Unique Identifier (DUID)
Secondary DNS Server	Address 2 of the DNS server assigned to the DUID
Domain Name	Domain of the prefix

5.14.3 Prefix/DUID binding



Scenario

You can assign IPv6 address prefixes to various DHCPv6 Clients.

Configuration steps

Step 1 In the navigation bar, choose **Basic > Network > DHCPv6 > Prefix/DUID Binding**. The **Prefix/DUID Binding** interface is displayed.

Step 2 View configured information.

- To modify a configured item, click  to enter the modifying interface.
- To add an item, click **Add** to enter the adding interface.
- To delete an item, and click the corresponding .

Step 3 On the modifying or adding interface, configure related items, and click **OK**.

Step 4 After configurations are complete, click **Save Config** to save configurations.

Configuration items

Table 5-50 Configuration items on the Prefix/DUID Binding interface

Configuration item	Description
Interface	Interface enabled with DHCPv6 server
Client Duid	Configure the DUID of the DHCP Client.
Prefix	IPv6 prefix assigned to the DUID.
Lease Period	Period for using the IPv6 address after successfully applying for it, including: <ul style="list-style-type: none"> • Infinite • Finite
Primary DNS Servers	Address 1 of the DNS server assigned to the DUID

Configuration item	Description
Secondary DNS Server	Address 2 of the DNS server assigned to the DUID
Domain Name	Domain of the prefix

5.15 IPv6

5.15.1 Basic configuration

Scenario

You can configure whether to enable IPv6 functions on this interface.

Configuration steps

- Step 1 In the navigation bar, choose **Basic > Network > IPv6 > Basic Configuration**. The **Basic Configuration** interface is displayed.
- Step 2 Configure related items, and click **OK**.
- Step 3 After configurations are complete, click **Save Config** to save configurations.

Configuration items

Table 5-51 Configuration items in the IPv6 Function area


Configuration item	Description
IPv6 enable	Enable/Disable IPv6 protocol stack.
IPv4 enable	Enable/Disable IPv4 protocol stack.


5.15.2 Static route

Scenario

You can configure IPv6 static route on this interface.

Configuration steps

- Step 1 In the navigation bar, choose **Basic > Network > IPv6 > Static Routing List**. The **Static Routing List** interface is displayed.
- Step 2 View the static route list.
 - To modify a configured item, click  to enter the modifying interface.

- To add an item, click **Add** to enter the adding interface.
- To delete an item, and click the corresponding .

Step 3 On the modifying or adding interface, configure related items, and click **OK**.

Step 4 After configurations are complete, click **Save Config** to save configurations.

Configuration items

Table 5-52 Configuration items on the Static Routing List interface

Configuration item	Description
Destination Address	Destination IPv6 address
Prefix length	Length of the IPv6 address prefix, ranging from 0 to 128
Next Hop Address	Gateway of the next route
Next Hop Interface	Egress interface for forwarding data
Weight	Route priority, integer, and ranging from 1 to 100
Distance	Number of route hops, integer, and ranging from 1 to 255

5.15.3 Routing table

Scenario

You can view information about the IPv6 routing table on this interface.

Configuration steps

Step 1 In the navigation bar, choose **Basic > Network > IPv6 > System Routing Table**. The **System Routing Table** interface is displayed.

Step 2 View routing information.

Configuration items

N/A

5.15.4 6RD tunnel configuration

Scenario

You can configure 6RD tunnel on this interface. IPv6 Rapid Deployment (6RD) is a mechanism to transmit encrypted IPv6 packets over IPv4 backbone network.

Configuration steps

- Step 1 In the navigation bar, choose **Basic > Network > IPv6 > 6RD Tunnel Configuration**. The **6RD Tunnel Configuration** interface is displayed.
- Step 2 Configure related items, and click **OK**.
- Step 3 After configurations are complete, click **Save Config** to save configurations.

Configuration items

Table 5-53 Configuration items on the 6RD Tunnel Configuration interface

Configuration item	Description
Tunnel Local Address	IPv6 address of the local end of the tunnel
Tunnel Prefix	Provided by the ISP, used to distinguish the IPv6 address from the IPv6 tunnel
Tunnel Relay Prefix	IPv6 address of the remote end of the tunnel

5.16 UPnP config

5.16.1 UPnP config

Scenario

You can configure UPnP on this interface.

A PC connects to the Internet through the gateway. When the PC uses the P2P software to download contents, the gateway, which is enabled with UPnP, will automatically add the port mapping of some P2P software and add a DNAT to make the PC exposed to the Internet, providing its resources.

Based on the P2P software algorithm, the PC, which provides more resources, will receive more resources. Therefore, the PC can have a greater download speed. At this section, the gateway only provides port mapping service for UPnP device. However, the PC is the UPnP control point, controlling the gateway to add/delete port mapping.

Configuration steps

- Step 1 In the navigation bar, choose **Basic > Network > UPnP Config**. The **UPnP Config** interface is displayed.
- Step 2 Configure related items, and click **OK**.
- Step 3 After configurations are complete, click **Save Config** to save configurations.

Configuration items

Table 5-54 Configuration items on the UPnP Config interface

Configuration item	Description
UPnP Port Mapping	Enable/Disable port mapping.

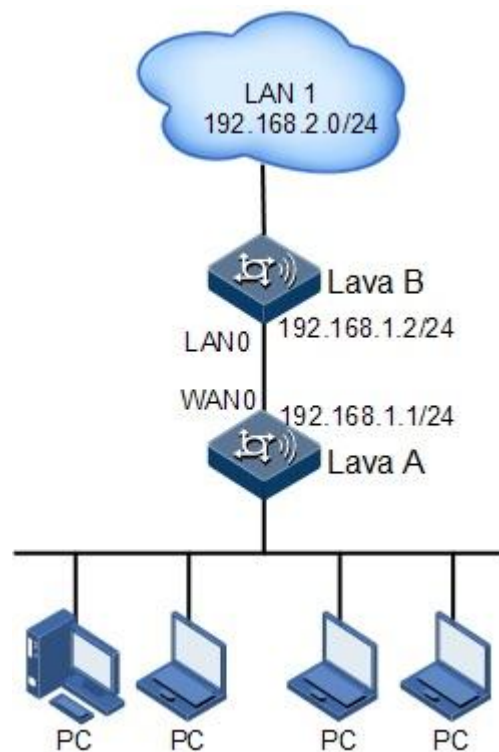
5.17 Configuration examples

5.17.1 Example for configuring static route

Networking requirements

An enterprise needs to configure a static route on LAVA A so that PC users can access LAN 1, as shown in Figure 5-14.

Figure 5-14 Static route configuration network application



Configuration steps

- Step 1 In the navigation bar, choose **Basic > Network > Static Route**. The **Static Rout List** interface is displayed.
- Step 2 Click **Add** to enter the adding interface.

Step 3 On the adding interface, configure related items, and click **OK**, as shown in Figure 5-15.

Figure 5-15 Configuring static route

Static Route	
Network Destination	192.168.2.0 *
Subnet Mask	255.255.255.0 *
<input checked="" type="radio"/> Next Hop	192.168.1.2
<input type="radio"/> Interface	WAN0
Weight	1 (1-100)
Distance	2 (1-255)
<input checked="" type="checkbox"/> Monitor Address	192.168.2.0
Send Interval (seconds)	60 (1-300)
The number of packets	3 (1-10)

Step 4 After configurations are complete, click **Save Config** to save configurations.

Checking configurations

PC users in the enterprise network can access the Internet. You can see the added static route in the static route list, Figure 5-16.

Figure 5-16 Static route list

Static Route						
Static Route List						
<input type="checkbox"/>	Network Destination	Subnet Mask	Next Hop/Interface	Distance	Weight	Operation
<input type="checkbox"/>	0.0.0.0	0.0.0.0	192.168.27.1	1	1	
<input type="checkbox"/>	192.168.2.0	255.255.255.0	192.168.1.2	2	1	

Total 2 records, current is the 1 page, total 1 pages

[First](#)
[Previous](#)
[Next](#)
[Last](#)
 Jump to page [Jump](#)

[Add](#)
[Delete](#)

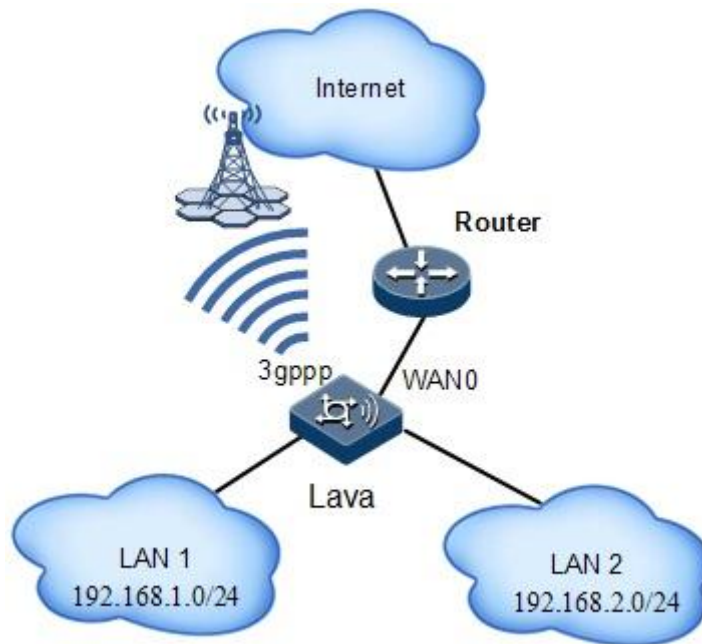
5.17.2 Example for configuring policy route

Networking requirements

An enterprise has two LANs: LAN 1 and LAN 2, as shown in Figure 5-17. The requirements are as below:

- LAN 1 users access the Internet in 3G mode.
- LAN 2 users access the Internet through the Router.

Figure 5-17 Policy route configuration networking application



Configuration steps

Step 1 Configure access control, and configure two address objects src1 and src2.

1. In the navigation bar, choose **Security > Security > Access Control > Address Object**. The **Address Object** interface is displayed.
2. Click **Add** to enter the adding interface.
3. On the adding interface, configure related items, and click **OK**, as shown in Figure 5-18.

Figure 5-18 Configuring address

The screenshot shows the 'Address Object' configuration page. The navigation bar at the top includes 'Policy of Access Control', 'Time Object', 'Service Object', and 'Address Object'. The 'Name' field is filled with 'src1' and the 'Description' field is filled with 'aa'. Below these fields, there is a section for defining the address object: 'Type of Node' is set to 'Subnet/mask' and 'Subnet/mask' is filled with '192.168.1.0/24'. An 'Add>>' button is located to the right of the 'Subnet/mask' field. A list box on the right side of the page contains the address '192.168.1.0/24'. At the bottom of the page, there are 'Submit' and 'Back' buttons.

4. Repeat the previous three sub-steps to create address object src2, as shown in Figure 5-19.

Figure 5-19 Address object list

Policy of Access Control				
Time Object		Service Object		
Address Object				
List of Address				
Name	Content of Node	Cited Times	Description	Operation
any	Subnet0.0.0.0/0;	1		
src1	Subnet192.168.1.0/24;	0	aa	 

Total 2 records, current is the 1 page, total 1 pages

Jump to page

Step 2 Configure policy route.

1. In the navigation bar, choose **Basic > Network > Policy Route**. The **Policy Rout List** interface is displayed.
2. Click **Add** to enter the adding interface.
3. On the adding interface, configure related items, and click **OK**, as shown in Figure 5-20.

Figure 5-20 Configuring policy route 1

Policy Route

Policy Route ID: (1-100)

Source Interface/Security Domain: 

Source Address: 

Destination Address: 

Service: 

Schedule: 

Next Hop Mode: Address Interface

Next Hop Address:

Reference Policy ID: (1-100)

Before/After: 

4. Repeat previous three sub-steps to configure policy route 2, as shown in Figure 5-21.

Figure 5-21 Configuring policy route 2

Policy Route	
Policy Route ID	<input type="text" value="2"/> (1-100)
Source Interface/Security Domain	<input type="text" value="any"/> ▼
Source Address	<input type="text" value="src1"/> ▼
Destination Address	<input type="text" value="any"/> ▼
Service	<input type="text" value="any"/> ▼
Schedule	<input type="text" value="always"/> ▼
Next Hop Mode	<input checked="" type="radio"/> Address <input type="radio"/> Interface
Next Hop Address	<input type="text" value="10.1.1.2"/>
Reference Policy ID	<input type="text"/> (1-100)
Before/After	<input type="text" value="Before"/> ▼

5. View configured policy routes, as shown in Figure 5-22.

Figure 5-22 Policy route list

Policy Route							
Policy Route List							
Policy Route ID	Source Interface/Security Domain	Source Address	Destination Address	Service	Schedule	Next Hop	Basic Operation
2	any	src2	any	any	always	10.1.1.2	
1	any	src1	any	any	always	10.1.1.2	

Total 2 records, current is the 1 page, total 1 pages

Jump to page

Step 3 After configurations are complete, click **Save Config** to save configurations.

Checking configurations

LAN 1 users access the Internet in 3G mode and LAN 2 users access the Internet through the Router.

6 VPN configurations

This chapter describes how to configure VPN items on the **VPN** interface, including the following sections:

- L2TP VPN
- IPSec VPN
- PKI management
- Configuration examples

6.1 L2TP VPN

6.1.1 L2TP Client

Scenario

You can configure L2TP client on this interface, namely, the L2TP Access Concentrator (LAC).

If you configure the L2Tp client after configuring the L2TP server, configurations of the L2TP server will be lost; vice versa.

Configuration steps

- Step 1 In the navigation bar, choose **Basic > VPN > L2TP VPN > L2TP Client**. The **L2TP Client** interface is displayed.
- Step 2 Configure related items, and click **OK**.
- Step 3 In the **L2TP Status** area, click **Connect** or **Disconnect** to connect or disconnect the L2TP client and L2TP server respectively.
- Step 4 After configurations are complete, click **Save Config** to save configurations.

Configuration items

Table 6-55 Configuration items on the L2TP Client interface

Configuration item	Description
L2TP LAC Enable	Enable/Disable L2TP client.
L2TP Server Address	IP address of the L2TP Server
L2TP Username	User name used to connect to the L2TP server
L2TP Password	User password
Peer Intranet IP	Intranet IP address of the L2TP server
Peer Intranet Mask	Intranet subnet mask of the L2TP server
Enable Auto-Dial	The Tunnel is automatically created after the LAVA is powered on.
Connect	Click it to send a request to establish the L2TP connection.
Disconnect	Click it to release current L2TP connection.



6.1.2 L2TP Server

Scenario

You can configure L2TP client on this interface, namely, the L2TP Network Server (LNS).

If you configure the L2TP server after configuring the L2TP client, configurations of the L2TP client will be lost.

Configuration steps

- Step 1 In the navigation bar, choose **Basic > VPN > L2TP VPN > L2TP Server**. The **L2TP Server** interface is displayed.
- Step 2 Configure related items, and click **OK**.
- Step 3 In the **Authenticated User List Information** area,
 - To modify a configured item, click  to enter the modifying interface.
 - To add an item, click **Add** to enter the adding interface.
 - To delete an item, and click the corresponding .
- Step 4 On the adding interface, configure related items, and click **OK**.
- Step 5 After configurations are complete, click **Save Config** to save configurations.

Configuration items

Table 6-56 Configuration items in the L2TP Enable area

Configuration item	Description
L2TP Enable	Enable/Disable L2TP server.
Start IP Address	Start IP address of the address pool for L2TP access users
End IP Address	End IP address of the address pool for L2TP access users
Mask	Subnet mask of the subnet

Table 6-57 Basic configuration items on the Authenticated User-Add interface

Configuration item	Description
Username	Name of the User who is permitted to access the L2TP server
User Type	Configure the authentication type of the user: <ul style="list-style-type: none"> • Local User • Radius User
Password	When you select Local User, configure the password for the user.
Password Confirm	When you select Local User, confirm the password for the user. It is in a character string form, ranging from 3 to 38.
RADIUS server	When you select Radius User, configure the RADIUS server.
User status	Enable/Disable configurations of the current user.

Table 6-58 Advanced configuration items on the Authenticated User-Add interface

Configuration item	Description
User IP	Bind the user and the IP address of the user's access device.
Temporary Account	Configure the keep-alive time for the user account, choosing the start time and end time.

6.1.3 L2TP Information

Scenario

You can view information about established L2TP tunnels on this interface.

Configuration steps

- Step 1 In the navigation bar, choose **Basic > VPN > L2TP VPN > L2TP Information**. The **L2TP Information** interface is displayed.
- Step 2 View tunnel information.

Configuration items

N/A



6.2 IPsec VPN

6.2.1 IPsec VPN

Scenario

You can configure IPsec VPN connection on this interface.

Configuration steps

- Step 1 In the navigation bar, choose **Basic > VPN > IPsec VPN > IPsec VPN**. The **IPsec VPN** interface is displayed.
- Step 2 View configured IPsec VPN connections.
- To enable a configured item, click **ON**.
 - To disable a configured item, click **OFF**.
 - To modify a configured item, click  to enter the modifying interface.
 - To add an item, click **Add** to enter the adding interface.
 - To delete an item, click the corresponding .
- Step 3 On the modifying or adding interface, configure related items, and click **OK**.
- Step 4 To enable/disable a connection, choose the related item from the list and then click **ON/OFF**. The system will perform the related operation. After configurations, a dialog box is displayed and then click **OK**.
- Step 5 After configurations are complete, click **Save Config** to save configurations.

Configuration items

Table 6-59 Configuration items on the New IPsec interface

Configuration item	Description
IPsec Name	Name of a IPsec connection, in a character string form, 1–31 letters, digits, and/or underlines
Enabled	Enable/Disable IPsec connection. By default it is enabled.

Configuration item		Description
Interface		Egress interface of the IPSec connection
Network Mode		Support two network modes: <ul style="list-style-type: none"> • Site-to-Site: in this mode, you need to configure the address of the peer gateway. • Remote-Access: used as a central site, without configuring the IP address of the peer gateway, being 0.0.0.0 by default, namely, accepting the access from all addresses
Peer IP/Host Name		Address of the peer gateway of an IPSec connection, supporting IP address and domain name as the address
Local IP		Local IP address used by the local device to initiate an IPSec connection, usually being the IP address of the egress interface of the gateway
Authentication	Pre-shared Key	String of the Pre-shared key for authentication between the two ends of the IPSec connection, no more than 39 characters
	Certificate	Local certificate to identify the local device to the peer
Gateway ID		ID used by IKE in phase 1 negotiation: <ul style="list-style-type: none"> • Local IP type: IP address or gateway name. If you choose Gateway Name, you need to input the gateway name accordingly. It is in a character string form, ranging from 1 to 31. • Peer IP type: IP address or gateway name. If you choose Gateway Name, you need to input the gateway name accordingly. It is in a character string form, ranging from 1 to 31.
Filter Method		Filter the data flow to be protected by IPSec, and support Flow Characteristics only.
Source IP/Mask		<ul style="list-style-type: none"> • Sub Net: range of the local subnet to be protected, supporting multiple network segments • Interface Addr: protecting local interface address only • Any: protecting any subnet, namely, 0.0.0.0/0
Destination IP/Mask		<ul style="list-style-type: none"> • Sub Net: range of the peer subnet to be protected, supporting multiple network segments • Peer IP: protecting peer gateway address only • Any: protecting any subnet, namely, 0.0.0.0/0


Configuration item	Description
Policy Protocol	<p>Choose the protocol type of the specified protected data flow. The value <i>any</i> indicates that any protocol data is protected.</p> <p> Note</p> <p>The sender and receiver must follow the policies as below: Sender: a specified protocol; receiver: the same protocol Sender: a specified protocol; receiver: any Sender: any; receiver: any</p>

Table 6-60 Advanced configuration items on the New IPSec interface

Configuration item	Description	
Phase 1	Mode	<p>Support main or aggressive mode. It is the main mode by default.</p> <ul style="list-style-type: none"> • Main: this mode has three phases during IKE negotiation: SA exchange, Key exchange, and IP exchange and authentication. • Aggressive: this mode has only two phases: SA exchange and key generation, ID exchange and authentication.
	Authentication Algorithm	Support MD5 or SHA algorithm. By default, the SHA algorithm is used.
	Encryption Algorithm	Support 3DES, DES, AES-128, AES-192, AES-256, BLOWFISH, TWOFISH algorithms. By default, the 3DES algorithm is used.
	DH	Diffie-Hellman (DH, switching and key allocation) group. By default, Diffie-Hellman Group2 is used.
	Phase 1 SA Lifetime	Lifetime of IKE security league in phase 1, integer, ranging from 1200 to 86400, in unit of second, being 10800 by default
	DPD	<p>Enable Dead Peer Detection (DPD).</p> <p>By default, it is disabled.</p> <p>The DPD interval ranges from 1 to 120, integer, in unit of second, and being 10 by default. The number of DPD retry times is an integer, ranges from 1 to 30, and is 3 by default.</p>
Phase 2	Encapsulation Protocol	Negotiate the proposed parameter used by the IPSec security league; namely, choose ESP encryption, authentication algorithm, and AH authentication algorithm. By default, it is ESP.

Configuration item		Description
	ESP Encapsulation	It is valid only when you choose ESP or AH-ESP in the Encapsulation Protocol drop-down list. By default, it is esp-3des-sha1.
	AH encapsulation	It is valid only when you choose AH or AH-ESP in the Encapsulation Protocol drop-down list. By default, it is ah-md5-hmac.
	Encapsulation Mode	Support tunnel and transport modes. By default, the tunnel mode is used.
	PFS (Perfect Forward Secrecy)	DH switching group used by the IPsec security league in negotiation. By default, it is None.
	Phase 2 SA Lifetime	Lifetime of the IPsec security league in phase 2, supporting two lifetime period management modes: <ul style="list-style-type: none"> • Time-based lifetime: ranging from 600 to 86400, in unit of second, being 3600 by default • Flow-based lifetime: ranging from 2560 to 56 870 912, in unit of KByte, being 1 843 200 by default
	Limit the Minimum Length of Access	By limiting the minimum length of access, one end of an IPsec connection can reject IPsec negotiation from the other end which has a smaller subnet length (source address/mask). By default, it is OFF.

6.2.2 IPsec monitor



Scenario

You can monitor connection status of the IPsec VPN on this interface.

Configuration steps

Step 1 In the navigation bar, choose **Basic > VPN > IPsec VPN > IPsec Monitor**. The **IPsec Monitor** interface is displayed.

Step 2 View Security Association (SA) information.

- To delete a tunnel, click the corresponding .
- To view detailed SA information about a single Tunnel, click  corresponding to the record.
- To delete all tunnels, click **Delete All**.

Configuration items



N/A

6.2.3 Binding IPsec name

Scenario

You can configure IPsec name so that you can search IPsec monitor for an IPsec connection.

Configuration steps

- Step 1 In the navigation bar, choose **Basic > VPN > IPsec VPN > Bind IPsec Name**. The **Bind IPsec Name** interface is displayed.
- Step 2 Input local IPsec gateway name in the **Local Gateway Name** input box, and click **OK**.
- Step 3 In the **Bind IPsec Name** area,
 - To modify a configured item, click  to enter the modifying interface.
 - To add an item, click **Add** to enter the adding interface.
 - To delete an item, click the corresponding .
- Step 4 On the modifying or adding interface, configure related items, and click **OK**.
- Step 5 After configurations are complete, click **Save Config** to save configurations.

Configuration items

Table 6-61 Configuration items on the Bind IPsec Name interface

Configuration item	Description
Local Gateway Name	Global name to identify IPsec connection of the local device, in a character string form, ranging from 0 to 31

Table 6-62 Configuration items in the Bind IPsec Name area

Configuration item	Description
Bind Name	Name of the IPsec connection of a subnet, in a character string form, ranging from 1 to 31
Bind Net	IP address and subnet mask of the subnet to be bound with

Note

- The priority of the local IPsec gateway name is higher than the name bounded with the subnet. Namely, when the peer user configures the local IPsec gateway name, the name bound with the subnet does not take effect.
- The local IPsec gateway name is used to notify the peer of the name. The peer user can fast find with whom it is in IPsec connection.
- Binding name is to bind the name and the subnet. The local user can fast find with whom it is in IPsec connection.


6.3 PKI management

6.3.1 CA certificate

Scenario

You can configure the CA certificate in PKI management on this interface.

Configuration steps

- Step 1 In the navigation bar, choose **Basic > VPN > PKI > CA Certificate**. The **CA Certificate** interface is displayed.
- Step 2 Click the button left to **Upload** to choose a CA certificate, and then click **Upload**.
You will see the uploaded CA certificate displayed in the **CA Certificate List** area.
To delete an item, click .
- Step 3 After configurations are complete, click **Save Config** to save configurations.

Configuration items

Table 6-63 Configuration items on the CA Certificate interface


Configuration item	Description
CA Certificate	CA certificate used by the CA certificate center, supporting DER or PEM format

6.3.2 Local certificate

Scenario

You can configure the local certificate in PKI management on this interface.

Configuration steps

- Step 1 In the navigation bar, choose **Basic > VPN > PKI > Local Certificate**. The **Local Certificate** interface is displayed.
- Step 2 Click the button above **Upload** to choose a local certificate, and then click **Upload**.
You will see the uploaded local certificate displayed in the **CA Certificate List** area.
To delete an item, click .
- Step 3 After configurations are complete, click **Save Config** to save configurations.

Configuration items

Table 6-64 Configuration items on the Local Certificate interface

Configuration item	Description
Local Certificate	Specify the local location of the local certificate, supporting the P12 format only
Certificate Password	Password to decrypt the P12 certificate

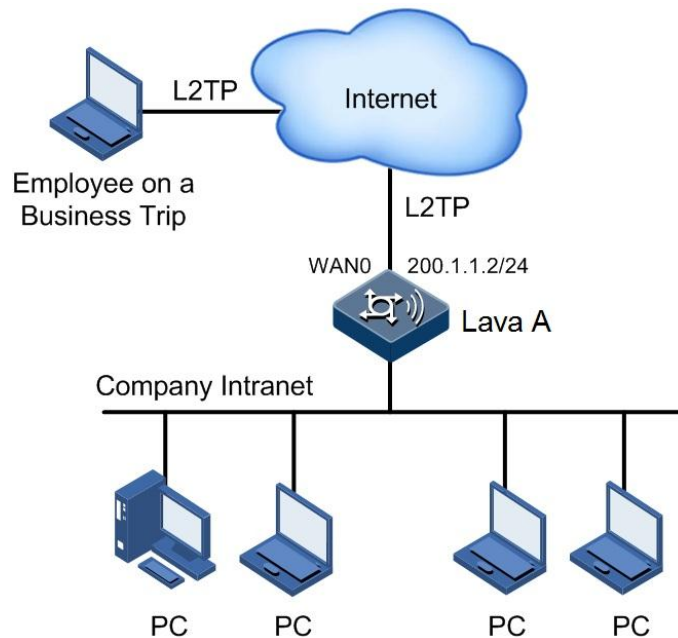
6.4 Configuration examples

6.4.1 Example for configuring L2TP VPN

Networking requirements

An enterprise needs employees on a business trip to access the enterprise internal network through L2TP VPN without authentication, as shown in Figure 6-23. The LAVA works as a LNS.

Figure 6-23 L2TP VPN application networking



Configuration steps

- Step 1 In the navigation bar, choose **Basic > VPN > V2TP VPN > L2TP Server**. The **L2TP Server** interface is displayed.
- Step 2 Configure related items, and click **OK**, as shown in Figure 6-24.

Figure 6-24 L2TP Server interface

L2TP Client	L2TP Server	L2TP Information
L2TP Enable	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	
Start IP Address	<input type="text" value="192.168.1.5"/> *	(xxx.xxx.xxx.xxx)
End IP Address	<input type="text" value="192.168.1.30"/> *	(xxx.xxx.xxx.xxx)
Mask	<input type="text" value="255.255.255.0"/> *	(xxx.xxx.xxx.xxx)

Step 3 In the **Authenticated User List Information** area, add user information. Configure related items and then click **OK**, as shown in Figure 6-25.

Figure 6-25 Authenticated User-ADD interface

L2TP Client	L2TP Server	L2TP Information
Authenticated User -Modify		
Basic Configuration		
Username	<input type="text" value="user"/> *	
User Type	<input type="text" value="Local User"/> ▼	
Password	<input type="password" value="....."/> *(3~38)	
Password Confirm	<input type="password" value="....."/> *(3~38)	
User Status	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	
Advanced Options ▾		

Step 4 After configurations are complete, click **Save Config** to save configurations.

Checking configurations

After configuring L2TP terminal on a PC, the employee on a business trip can access the enterprise internal network through L2TP client after entering the user name and the password.

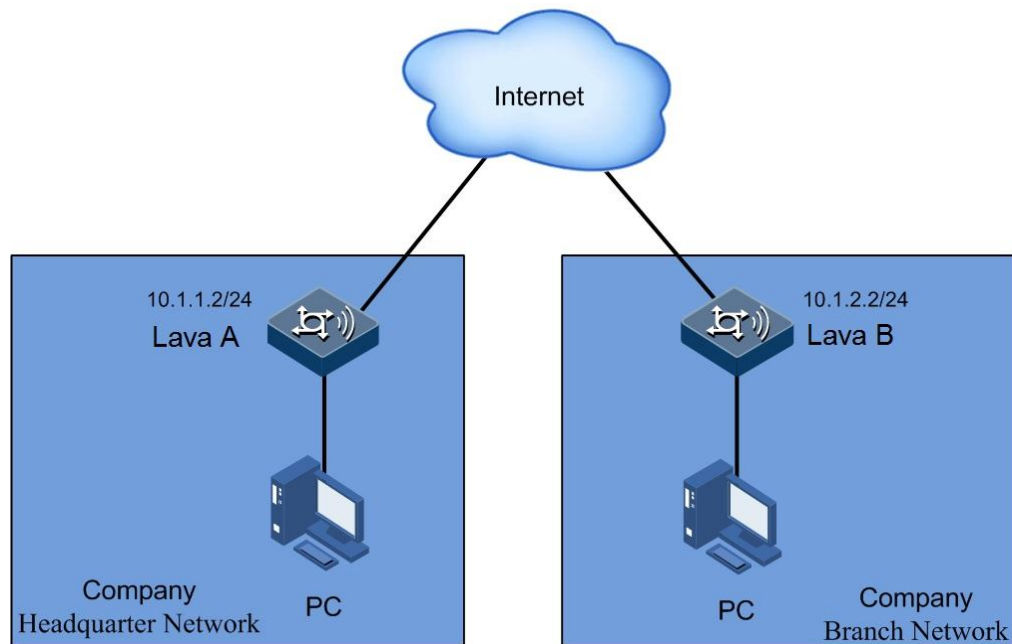
6.4.2 Example for configuring IPsec VPN

Networking requirements

The headquarter and branch of an enterprise use a LAVA respectively. PC A in the headquarter needs to access PC B in the branch, so an IPsec VPN connection needs to be established between them, as shown in Figure 6-26. Detailed requirements are as below:

- The network mode is site-to-site.
- The authentication mode is pre-shared.
- The WAN0 interface is used.
- Advanced options use default configurations.

Figure 6-26 IPsec VPN application networking



Configuration steps

Step 1 On LAVA A.

- In the navigation bar, select **Basic > VPN > IPsec VPN > IPsec VPN**. The **IPsec VPN** interface is displayed.
- Click **Add** to enter the adding interface.
- Configure related items, and click **OK**, as shown in Figure 6-27.

Figure 6-27 Creating an IPsec connection

The screenshot shows the 'New IPsec' configuration page. It has three tabs: 'New IPsec' (active), 'IPsec Monitor', and 'Bind IPsec Name'. The configuration is organized into several sections:

- General Settings:**
 - IPsec Name: * characters (1-31)
 - Enabled: ON OFF
- Gateway Information:**
 - Interface: (dropdown)
 - Network Mode: Site-to-Site Remote-Access
 - Gateway IP Address: (empty)
 - Peer IP/Host Name: *
 - Local IP:
- Authentication:**
 - Authentication: Pre-shared Key * characters (1-39) Certificate (dropdown)
 - Gateway ID:
 - Peer ID Type: IP Address Gateway Name
 - Local ID Type: IP Address Gateway Name
- Filter:**
 - Filtering Method: (dropdown)
 - Source IP/Mask: Sub Net Interface Addr Any
 -
 - Source IP/Mask List:
 - Destination IP/Mask: Sub Net Peer IP Any
 -
 - Destination IP/Mask List:
 - Policy Protocol: (dropdown)
- Advanced Options:** (collapsed)

- After configurations are complete, click **Save Config** to save configurations.

Step 2 Configure LAVA B.

Configurations are similar to the ones of LAVA A. the IPsec connection name can be customized. The interface is the uplink interface of the gateway. The peer gateway address, local gateway address, source address/mask, and destination address/mask of LAVA B are opposite to the ones of LAVA A. Other configuration items keep consistent.

Checking configurations

After configurations are successful, the configured connection will be displayed in the **IPsec Connection** area and the connection status will be displayed on the **IPsec Monitor** interface.

7 QoS

This chapter describes how to configure QoS on the **QoS** interface, including the following sections:



- Rate limit per user
- Advanced rate limit
- Advanced QoS config
- Session counter limit
- Connection counter management
- Configuration examples

7.1 Rate limit per user

Scenario

You can configure rate limiting per user by source/destination IP address on this interface. When the flow complies with the defined rules, packets are allowed to pass; otherwise, packets are discarded. This protects network resources.

Configuration steps

- Step 1 In the navigation bar, choose **Basic > QoS > Rate Limit per User**. The **Rate Limit per User** interface is displayed.
- Step 2 View the rate limit per user list.
 - To modify a configured item, click  to enter the modifying interface.
 - To add an item, click **Add** to enter the adding interface.
 - To delete an item, click the corresponding .
- Step 3 On the modifying or adding interface, configure related items, and click **OK**.
- Step 4 After configurations are complete, click **Save Config** to save configurations.

Configuration items

Table 7-65 Configuration items on the Rate Limit per User interface



Configuration item	Description
Start IP	Start IP address of the range for rate limit
End IP	End IP address of the range for rate limit
Interface	Egress interface for rate limit
Total Rate	Average rate after rate limiting, in unit of Kbit/s, ranging from 10 to 100000
Dynamic Bandwidth Adjustment	Enable dynamic bandwidth adjustment.
Type	<ul style="list-style-type: none"> • Share: all IP addresses in the range share the bandwidth. • Exclusive: exclusive bandwidth is provided for each IP address.
Direction	Support three types: <ul style="list-style-type: none"> • Upload • Download • Bidirection

7.2 Advanced rate limit

Scenario

You can configure advanced rate limit to monitor flows by interface on the IP layer in different modes on this interface. When the flow complies with the defined rules, packets are allowed to pass; otherwise, packets are discarded. This protects network resources.

Configuration steps

- Step 1 In the navigation bar, choose **Basic > QoS > Advanced Rate Limit**. The **Advanced Rate Limit** interface is displayed.
- Step 2 View the advanced rate limit list.
 - To modify a configured item, click  to enter the modifying interface.
 - To add an item, click **Add** to enter the adding interface.
 - To delete an item, click the corresponding .
- Step 3 On the modifying or adding interface, configure related items, and click **OK**.
- Step 4 After configurations are complete, click **Save Config** to save configurations.

Configuration items

Table 7-66 Configuration items on the Advanced Rate Limit interface

Configuration item	Description
Description	Describe the rate limit rule. It is in a character string form, ranging from 1 to 32.
Interface	Egress interface of the flow
Direction	Support three types: <ul style="list-style-type: none"> • Upload • Download • Bidirection
Rate	Average rate after rate limiting, in unit of Kbit/s, ranging from 10 to 100000
Type of Flag	Support 3 types: <ul style="list-style-type: none"> • NULL • 802.1p • Differentiated Services Code Point (DSCP)
new flag value	It is available when the flag type is set to 802.1p. It ranges from 0 to 7.
CFI	It is available when the flag type is set to 802.1p. It is set to 0 or 7. By default, it is set to 0.
value of source direction	It is available when the flag type is set to DSCP. It ranges from 0 to 63. By default, it is set to 0.
value of reverse direction	It is available when the flag type is set to DSCP. It ranges from 0 to 63. By default, it is set to 0.

Table 7-67 Configuration items in the Matching Condition area

Configuration item	Description
Way of Limit	Rate Limit by IP Add the source IP address for rate limit in dotted decimal notation and subnet mask. Click Add to enter the IP address list interface. The Any parameter indicates performing rate limit on all IP addresses.
	Rate Limit by User Choose the user for rate limit.
	Rate Limit by User Group Choose the user group for rate limit.
Ingress	Ingress of the flow



Configuration item		Description
Time		Specify the start time and end time for rate limit. The value NULL indicates that rate limit is permanent.
Rate Limit Type: Protocol	Protocol Name	Choose the protocol for rate limit.
	Self-defined protocol type	Support UDP or TCP.
	Source port	Port number for receiving data with rate limit, ranging from 1 to 65535
	Destination port	Port number for sending data with rate limit, ranging from 1 to 65535

7.3 Advanced QoS config

Scenario

You can modify the DSCP, 802.1p, MAC address, source/destination IP address, source/destination interface, ToS value, and protocol types of data flow and then use them as the matching rules of the policy.

Configuration steps

- Step 1 In the navigation bar, choose **Basic > QoS > advanced qos config**. The **advanced qos config** interface is displayed.
- Step 2 Configure global QoS policy in the **Global configuration** area and configure the weight and priority of queues in the **Queue configuration** area. And then click **OK**.
- Step 3 View the created QoS policies in the **Match policy** area.
 - To modify a configured item, click  to enter the modifying interface.
 - To add an item, click **Add** to enter the adding interface.
 - To delete an item, click the corresponding .
- Step 4 On the modifying or adding interface, configure related items, and click **OK**.
- Step 5 After configurations are complete, click **Save Config** to save configurations.

Configuration items

Table 7-68 Configuration items in the Global configuration area

Configuration item	Description
Advanced QoS	Enable/Disable advanced QoS.


Configuration item	Description
Description	Configure descriptions about advanced QoS. In addition, advanced QoS is used for service flow, such as VoIP and TR069. It is in a character string form, ranges from 1 to 16.
Egress rate	Configure the rising bandwidth value of the egress interface, in unit of Kbit/s and ranging from 10 to 100000.
Enforce weight	If it is selected, it is set to forced bandwidth. Forced bandwidth is used for weighted QoS mechanism, forcibly setting the upload bandwidth for all queues. The configured bandwidth cannot be exceeded even there is no other queue to upload data. By default, it is disabled.
Enable DSCP rewrite	If it is selected, DSCP re-writing is enabled. DSCP re-writing is used to rewrite DSCP values of data packets on the egress interface. By default, it is disabled.
Enable 802.1p rewrite	If it is selected, 802.1P re-writing is enabled. 802.1P re-writing is used to rewrite 802.1P values of data packets on the egress interface. By default, it is disabled.
Queue type	Configure QoS queue mechanism: <ul style="list-style-type: none"> • Priority • Weight By default, it is set to Priority
Outinterface	Select the egress interface where advanced QoS is applied.  Note This configuration item may be different based on real configurations.

Table 7-69 Configuration items in the Queue configuration area

Configuration item	Description
Weight	Configure the weight value of the queue. This configuration item takes effect only when the Queue type is set to weight.
Priority	Configure the priority of the queue. This configuration item takes effect only when the Queue type is set to priority.

Table 7-70 Configuration items in the Match Policy area

Configuration item	Description
Enable	Enable/Disable the matching policy.

Configuration item	Description
Matched Queue	Configure the ID of ingress queue that is applied with the matching policy. The system matches data packets based on the matching policy and sends packets to the specified queue based on policy configurations.
Matched Mode	Configure the mode of the matching policy: <ul style="list-style-type: none"> • Service model: need to configure pre-defined service type. • Policy model: need to configure the DSCP value, 802.1P value, MAC address, source/destination IP address, source/destination port ID, and ToS value.
Service type	Select a service type of the policy when the Matched Mode is set to Service model.
Set DSCP Value	Set the value of DSCP field in the data packet that matches the policy. It is an integer ranging from 0 to 63.
Set 802.1P Value	Set the value of 802.1P field in the data packet that matches the policy. It is an integer ranging from 0 to 7.
Source MAC	Set the MAC address range of the data packet that matches the policy. Packets in the MAC address range can be applied with this policy.
802.1P Value	Set the 802.1P range of the data packet that matches the policy and select the protocol of the policy service. Packets in the 802.1P range can be applied with this policy.
Source IP	Set the source IP address range of the data packet that matches the policy and select the protocol of the policy service. Packets in the source IP address range can be applied with this policy.
Destination IP	Set the destination IP address range of the data packet that matches the policy and select the protocol of the policy service. Packets in the destination IP address range can be applied with this policy.
Source port	Set the source interface range of the data packet that matches the policy and select the protocol of the policy service. Packets in the source interface range can be applied with this policy.
Destination port	Set the destination interface range of the data packet that matches the policy and select the protocol of the policy service. Packets in the destination interface range can be applied with this policy.
ToS	Set the ToS range of the data packet that matches the policy and select the protocol of the policy service. Packets in the ToS range can be applied with this policy.
DSCP Value	Set the DSCP range of the data packet that matches the policy and select the protocol of the policy service. Packets in the DSCP range can be applied with this policy.

Configuration item	Description
WAN interface	Set the uplink interface range of the data packet that matches the policy and select the protocol of the policy service. Packets in the uplink interface range can be applied with this policy.
LAN interface	Set the downlink interface range of the data packet that matches the policy and select the protocol of the policy service. Packets in the downlink interface range can be applied with this policy.

7.4 Session counter limit

Scenario

You can configure session counter limit on this interface.

Configuration steps

- Step 1 In the navigation bar, choose **Basic > QoS > Session Counter Limit**. The **Session Counter Limit** interface is displayed.
- Step 2 Configure related items, and click **OK**.
- Step 3 After configurations are complete, click **Save Config** to save configurations.

Configuration items

Table 7-71 Configuration items on the Session Counter Limit interface


Configuration item	Description	
Session Counter Switch	Enable/Disable session counter switch.	
Session Limit by IP	–	Limit session counter on each IP address in a range.
	Max Session Per IP	Number of maximum sessions for each IP address with rate limit, ranging from 1 to 65535
	IP Range	Range of the IP addresses for session rate limit
Total Session Counter Limit	Limit the total number of sessions, ranging from 10 to 2000000	

7.5 Connection counter management

Scenario

You can configure the threshold of number of sessions. If the threshold is exceeded, no new session is established.

Configuration steps

- Step 1 In the navigation bar, choose **Basic > QoS > Connection Counter Management**. The **Connection Counter Management** interface is displayed.
- Step 2 The Connection Counter Setting List is displayed. To configure the threshold of sessions, click  to enter **Connection Counter Setting** interface.
- Step 3 Configure related items, and click **OK**.
- Step 4 After configurations are complete, click **Save Config** to save configurations.

Configuration items

Table 7-72 Configurations items on the Connection Counter Setting interface

Configuration item		Description
Total Connection	Threshold	Enable/Disable session counter switch.
Half Connection	Max	Number of incomplete sessions, being 2000000 by default
	Min	Number of incomplete sessions, being 40000 by default
new connection per minute	Max	Number of newly-created sessions every minute, being 2000000 by default
	Min	Number of newly-created sessions every minute, being 40000 by default

Table 7-73 Configurations items in the Connection Counter Setting List area

Configuration item	Description
system	Number of sessions sent to the extranet through the LAVA LR-2G211
TCP	Number of TCP sessions forwarded through the LAVA LR-2G211
UDP	Number of UDP sessions forwarded through the LAVA LR-2G211
ICMP	Number of ICMP sessions forwarded through the LAVA LR-2G211

Configuration item	Description
other	Number of other sessions (except for the above 4 types) forwarded through the LAVA LR-2G211

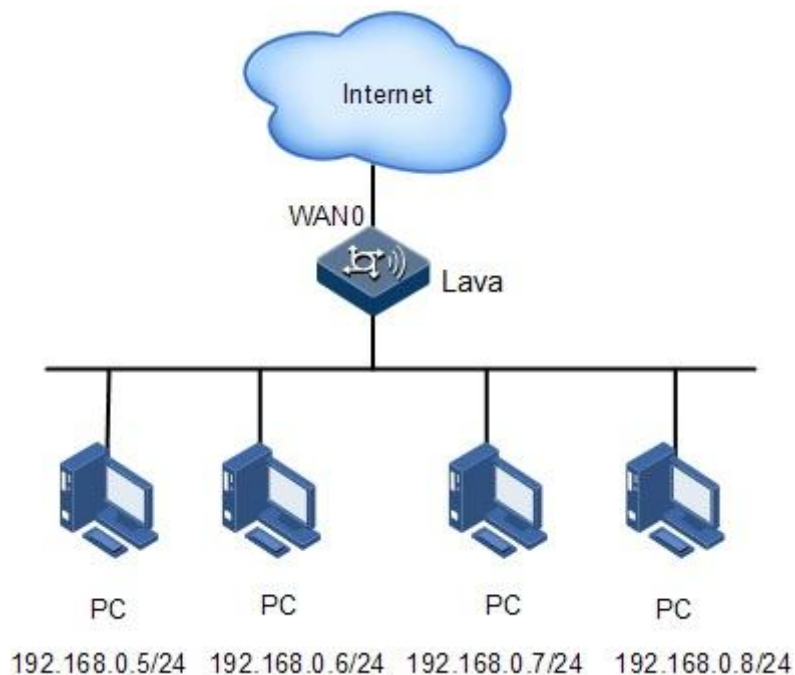
7.6 Configuration examples

7.6.1 Example for configuring rate limit per user

Networking requirements

An enterprise needs to limit rate per internal user to 1 Mbit/s, as shown in Figure 7-28.

Figure 7-28 Rate limit per user application networking



Configuration steps

- Step 1 In the navigation bar, choose **Basic > VPN > QoS > Rate Limit per User**. The **Rate Limit per User** interface is displayed.

Figure 7-29 Configuring rate limit per user

Rate Limit per User	Advanced Rate Limit	Session Counter Limit	Connection Counter Management
Rate Limit per User Settings			
Start IP	<input type="text"/>	*	
End IP	<input type="text"/>	*	
Interface	<input type="text" value="3gppp"/>		
Rate	<input type="text"/>	kbps(10-100000)*	<input type="checkbox"/> Dynamic Bandwidth Adjustment
Type	<input checked="" type="radio"/> Share(All IP addresses share the bandwidth.)		<input type="radio"/> Exclusive(Exclusive bandwidth is provided for each IP address.)
Direction	<input checked="" type="radio"/> download	<input type="radio"/> upload	<input type="radio"/> bidirection

Step 2 Configure related items, and click **OK**.

Step 3 After configurations are complete, click **Save Config** to save configurations.

Checking configurations

The actual download rate per user is at most 1 Mbit/s.

8 Remote configuration

This chapter describes how to configure remote management and configurations on the **Remote** interface, including the following sections:

- TR-069
- SNMP
- Remote configuration
- Syslog
- Configuration examples

8.1 TR-069

Scenario

You can configure the TR-069 protocol on this interface.

Configuration steps

- Step 1 In the navigation bar, choose **Basic > Remote > TR-069**. The **Rate Limit per User** interface is displayed.
- Step 2 Configure related items, and click **OK**.
- Step 3 After configurations are complete, click **Save Config** to save configurations.

Configuration items

Table 8-74 Configuration items in the ACS area

Configuration item	Description
URL	Valid HTTP or HTTPS URL of ACS, such as <code>http://192.168.2.4:7547/ACS</code>
Username	When the CPE is connected to the ACS through CWMP, the ACS authenticates the CPE by using this user name. It is used for HTTP authentication only.

Configuration item	Description
Password	When the CPE is connected to the ACS through CWMP, the ACS authenticates the CPE by using this password. It is used for HTTP authentication only.

Table 8-75 Configuration items in the CPE area

Configuration item	Description
URL	HTTP URL through which the ACS can be connected to the CPE, in format of http://host:port/path. Wherein, the "host" may be the IP address of the management interface on the CPE, such as http://192.168.1.1:7547/cpe.
User name	When the ACS is connected to the CPE, the CPE authenticates the ACS by using this user name.
Password	When the ACS is connected to the CPE, the CPE authenticates the ACS by using this password. When the password is read, the system returns a null string regardless of the value of password.
CPE Interface	The ACS is connected to the CPE through this interface. The host part of the URL in CPE configurations will be the IP address of this interface.
Send Period	Reporting period by CPE, in unit of second, being 600 by default, and ranging from 1 to 2000000000
CPE enable	Enable/Disable CWMP on the CPE.
Enable LOID Certification	Enable/Disable logic authentication.
LOID Authentication Timeout	Timeout time for logic authentication, in unit of second, and ranging from 1 to 300

8.2 SNMP

8.2.1 SNMP

Scenario

You can configure SNMP on this interface.

Configuration steps

- Step 1 In the navigation bar, choose **Basic > Remote > SNMP > SNMP**. The **SNMP** interface is displayed.

Step 2 Configure the required item, and click **OK**.

Step 3 After configurations are complete, click **Save Config** to save configurations.

Configuration items

Table 8-76 Configuration items on the SNMP interface

Configuration item	Description
Equipment Position	Location of the agent, in a character string form, and ranging from 0 to 63 characters
SNMP Read Community	Password for the NMS (Network Management System) to query agents
SNMP Set Community	Password for the NMS to set agents
SNMP Trust Host	Host address of the NMS. Up to 3 addresses are available.
Trap Receiving Host	IP address of the destination host for SNMP Trap messages
SNMP listen port	SNMP listening port number, being 161 by default, and ranging from 1024 to 65535
SNMP Trap Port	Trap port number, being 162 by default, and ranging from 1024 to 65535
SNMP Agent Register Cycle	Period for the LAVA to send Trap messages, integer, ranging from 1 to 3600, in unit of second, and being 10 by default
SNMP Agent Register Enable	After it is enabled, Trap messages can be sent to the NMS and the NMS can add devices automatically.
SNMP Version	Choose the SNMP version. <ul style="list-style-type: none"> • v1 • v2c • v3
SNMP Agent	Enable/Disable SNMP on the device.

8.2.2 USM user



Scenario

You can configure users' SNMP v3 User-based Security Model (USM) on this interface.

Configuration steps

Step 1 In the navigation bar, choose **Basic > Remote > SNMP > USM User**. The **USM User** interface is displayed.

Step 2 View the SNMPv3 user-based configuration list.

- To modify a configured item, click  to enter the modifying interface.
- To add an item, click **Add** to enter the adding interface.
- To delete an item, click the corresponding .

Step 3 Configure the required item, and click **OK**.

Step 4 After configurations are complete, click **Save Config** to save configurations.

Configuration items

Table 8-77 Configuration items on the USM User interface


Configuration item	Description
Name	Name of the USM user
Authentication Mode	Support the following authentication modes: <ul style="list-style-type: none"> • none • MD5 • SHA
Authentication Password	Authentication password for MD5 or SHA mode
Encryption Mode	Support the following encryption modes: <ul style="list-style-type: none"> • none • AES • DES
Encrypted password	Authentication password for AES or DES mode

8.3 Remote configuration

Scenario

You can configure the remote trusted host for the LAVA. Only the trusted host with its IP address can access specified services, such as HTTP and HTTPS.

Configuration steps

- Step 1 In the navigation bar, choose **Basic > Remote > Remote**. The **Remote** interface is displayed.
- Step 2 Configure the HTTPS and HTTP ports in the **Web Server Port** area and then click **OK**.
- Step 3 Configure the IP address of the host in the **Host IP address** area and then click **Add**.
- Step 4 The configured item will be displayed in the **Remote trust host IP list** area. To delete an item, click the corresponding .
- Step 5 After configurations are complete, click **Save Config** to save configurations.

Configuration items

Table 8-78 Configuration item on the Host IP address interface

Configuration item	Description
HTTPS	Configure the port of HTTPS server. It ranges from 1024 to 65535 and is set to 443 by default.
HTTP	Configure the port of HTTP server. It ranges from 1024 to 65535 and is set to 80 by default.
Host IP address	IP address of the host allowed accessing the LAVA. If it is null, all hosts can access the LAVA.

8.4 Syslog

8.4.1 Local

Scenario

You can manage local Syslog on this interface.

Configuration steps

- Step 1 In the navigation bar, choose **Basic > Remote > Syslog > Local**. The **Local** interface is displayed.
- Step 2 Configure the required item, and click **OK**.
- Step 3 After configurations are complete, click **Save Config** to save configurations.

Configuration items

Local logs are classified into 7 types. Each type has 8 levels as below:

- Emergency
- Alert
- Critical
- Error
- Warning
- Notice
- Informational
- Debug

These levels are in descending order in terms of severity. The lower level you configure logs with, the more logs are reported. For example, if you set the level of logs to Critical, then Emergency, Alert, and Critical logs are reported; if you set the level of logs to Error, then Emergency, Alert, Critical, and Error logs are reported.

Table 8-79 Configuration items on the Local interface

Configuration item	Description
Local Log (State/Level)	Enable/Disable the log server.
All Logs	Enable/Disable uniform configurations for alarm level of all logs.
Equipment Alarm Log	Enable/Disable alarm logs.
Login Log	Enable/Disable login logs.
Operation Log	Enable/Disable operation logs.
ARP Attack Log	Enable/Disable ARP attack logs.
DDoS Log	Enable/Disable DDoS logs.
URL Filtering Hit	Enable/Disable URL filtering hit logs.
Flow Log	Enable/Disable flow logs.

8.4.2 Remote

Scenario

You can manage remote syslog on this interface.

Configuration steps

- Step 1 In the navigation bar, choose **Basic > Remote > Syslog > Remote**. The **Remote** interface is displayed.
- Step 2 Configure the required item, and click **OK**.
- Step 3 After configurations are complete, click **Save Config** to save configurations.

Configuration items

Remote logs are logs which are sent to the syslog server of the remote device. The address or domain name is the IP address for the remote server, which is input in the text box.

Table 8-80 Configuration items on the Remote interface

Configuration item	Description
Log Server Status	Enable/Disable the log server.
Address or Hostname	IP address or domain name of the log server
Server Port	Service port of the log server, ranging from 0 to 65535, and being 514 by default
All Logs	Enable/Disable uniform configurations for alarm level of all logs.

Configuration item	Description
Equipment Alarm Log	Enable/Disable alarm logs.
Login Log	Enable/Disable login logs.
Operation Log	Enable/Disable operation logs.
ARP Attack Log	Enable/Disable ARP attack logs.
DDoS Log	Enable/Disable DDoS logs.
URL Filtering Hit	Enable/Disable URL filtering hit logs.
Flow Log	Enable/Disable flow logs.

8.4.3 Mail

Scenario

You can configure the mail server and fault code level on this interface so that the LAVA sends an alarm mail to the users and is added with the method of receiving alarms for users.

Configuration steps

- Step 1 In the navigation bar, choose **Basic > Remote > Syslog > Mail**. The **Mail** interface is displayed.
- Step 2 Configure the required item, and click **OK**.
- Step 3 After configurations are complete, click **Save Config** to save configurations.

Configuration items

Table 8-81 Configuration items on the Mail interface

Configuration item	Description
Log Alarm	Enable/Disable mail log alarm.
Shortest Send Interval	Shortest interval for sending alarm mails, in unit of minute, ranging from 1 to 100, and being 5 minutes by default
Recipient's E-mail	E-mail of the recipient. Up to 255 characters are available.
All Logs	Enable/Disable uniform configurations for alarm level of all logs.
Equipment Alarm Log	Enable/Disable alarm logs.
Login Log	Enable/Disable login logs.
Operation Log	Enable/Disable operation logs.
ARP Attack Log	Enable/Disable ARP attack logs.

Configuration item	Description
DDoS Log	Enable/Disable DDoS logs.
URL Filtering Hit	Enable/Disable URL filtering hit logs.
Flow Log	Enable/Disable flow logs.

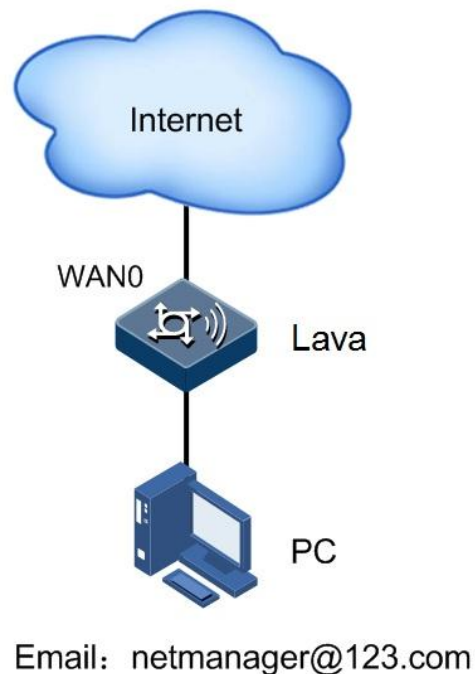
8.5 Configuration examples

8.5.1 Example for configuring Syslog

Networking requirements

An enterprise needs to learn the operating status of the LAVA through system logs and send mails to the NMS administrator, as shown in Figure 8-30.

Figure 8-30 Syslog application networking



Configuration steps

Step 1 Configure local Syslog management.

- In the navigation bar, choose **Basic > Remote > Syslog > Local**. The **Local** interface is displayed.

Figure 8-31 Syslog Local interface

Local Log Code Level Set	
Local Log (State/Level)	<input checked="" type="checkbox"/> Enable
All Logs	<input checked="" type="checkbox"/> Emergency
Equipment Alarm Log	<input checked="" type="checkbox"/> Emergency
Login Log	<input type="checkbox"/> Emergency
Operation Log	<input checked="" type="checkbox"/> Emergency
ARP Attack Log	<input type="checkbox"/> Emergency
DDos Log	<input checked="" type="checkbox"/> Emergency
URL Filtering Hit	<input checked="" type="checkbox"/> Emergency
Flow Log	<input checked="" type="checkbox"/> Emergency

- Configure the required item, and click **OK**.

Step 2 Configure the E-mail mode of Syslog management.

- In the navigation bar, choose **Basic > Remote > Syslog > Mail**. The **Mail** interface is displayed.

Figure 8-32 Syslog Mail interface

The mail server configuration and fault code level set	
Log Alarm	<input checked="" type="checkbox"/> Enable
Shortest Send Interval	<input type="text" value="5"/> (1-100) Minutes
Recipient's E-Mail	<input type="text" value="netmanager@123.com"/> *(Enter up to 255 characters!)
All Logs	<input checked="" type="checkbox"/> Emergency
Equipment Alarm Log	<input checked="" type="checkbox"/> Emergency
Login Log	<input type="checkbox"/> Emergency
Operation Log	<input checked="" type="checkbox"/> Emergency
ARP Attack Log	<input checked="" type="checkbox"/> Emergency
DDos Log	<input checked="" type="checkbox"/> Emergency
URL Filtering Hit	<input checked="" type="checkbox"/> Emergency
Flow Log	<input checked="" type="checkbox"/> Emergency

- Configure the required item, and click **OK**

Step 3 After configurations are complete, click **Save Config** to save configurations.



Note

Before configuring the system to send system logs, configure the mail server in **System > SNMP Server**.
If you set all log levels to Emergency, no logs will be generated.

Checking configurations

You can view system logs by choosing **Device > Information > Recent System Logs**. You can also receive system log mails.

9 User management configurations

This chapter describes how to configure user management on the **Manage Users** interface, including the following sections:



- Um
- WebAuth
- Online User
- AuthenServer
- Configuration examples

9.1 Um

Scenario

You can create and manage users and user groups on this interface.

Configuration steps

- Step 1 In the navigation bar, choose **Basic > Manage Users > Um**. The **User Management** interface is displayed.
- Step 2 In the **User Management** area,
- Click **Open All** or **Close All** to view user group structure.
 - Click a user group to view the user group in the **User/Groups List** area.
- Step 3 In the **User/Groups List** area,
- To add a user group, click **Add** in the **Group** area.
 - To add a user, click **Add** in the **Username** area.
 - To modify a configured item, click  to enter the modifying interface.
 - To delete an item, and click the corresponding .
- Step 4 After configurations are complete, click **Save Config** to save configurations.

Configuration items

Table 9-82 Configuration items in the Groups-Add area

Configuration item	Description
Group	Name of the group to be created
Parent Group	An upper-level user group for the group to be created, being Company by default
Description	Describe the user group. It is in a character string form ranging from 1 to 128.

Table 9-83 Configuration items in the User-Add area

Configuration item	Description
Username	Name of the user to be created
Auth Mode	– Please choose the type.
Local Authenticate	<ul style="list-style-type: none"> • Password: password for local authentication • Password: confirmed password for local authentication • Prohibiting multi-pc-login: enable/disable the user to log in from multiple PCs. • IP Address Binding: enable/disable binding the user and IP address. • MAC Address Binding: enable/disable binding the user and MAC address.
RADIUS Authenticate	<ul style="list-style-type: none"> • RADIUS server: choose a RADIUS server. To choose a RADIUS Server, configure the RADIUS server in advance. For details, see section 9.4 AuthenServer. • Prohibiting multi-pc-login: enable/disable the user to log in from multiple PCs. • IP Address Binding: enable/disable binding the user and IP address. • MAC Address Binding: enable/disable binding the user and MAC address.
LDAP Authenticate	<ul style="list-style-type: none"> • LDAP Server: IP address of the LDAP server • Prohibiting multi-pc-login: enable/disable the user to log in from multiple PCs. • IP Address Binding: enable/disable binding the user and IP address. • MAC Address Binding: enable/disable binding the user and MAC address.
IP Authenticate	User IP: IP address of the user for authentication
MAC Authenticate	User MAC: MAC address of the user for authentication
User State	Enable/Disable the user.
Groups belong to	Add the user to a user group.

Configuration item	Description
Affiliated Information	Other user information, including: <ul style="list-style-type: none"> • Real Name • Phone • Email Address • Description

9.2 WebAuth

9.2.1 Authentiction option

Scenario

The authentication function is to authenticate the users desiring of accessing the Internet. After you configure authentication, the HTTP request is redirected to the Web authentication login page on which the user is required to provide current user name and password. After the user is successfully authenticated, the system assigns a role for user by configured policies to implement access control over different users.

Configuration steps

- Step 1 In the navigation bar, choose **Basic > Manage Users > WebAuth > Authentication Option**. The **Authentication Option** interface is displayed.
- Step 2 Configure related items, and click **OK**.
- Step 3 After configurations are complete, click **Save Config** to save configurations.

Configuration items

Table 9-84 Configuration items on the Authentication Option interface

Configuration item	Description
Webauth Global Switch	Enable/Disable global web authentication.
User Logout Method	<ul style="list-style-type: none"> • Session Timeout Logout: when the user does not have a session for this period, the user is logged out. It is in unit of minute, ranges from 1 to 1440 and is set to 1440 by default. Web Manual Logout: manually log out the user.
Interface Configuration	<p>You can switch interfaces between authenticated interface and unauthenticated interface:</p> <ul style="list-style-type: none"> • Unauthenticated Interface: interfaces that need not to be authenticated. Double-click it to add it to the authenticated interface. • Authenticated Interface: interfaces that need to be authenticated. Double-click it to make it return to the authenticated interface.

9.2.2 Whitelist

Scenario

You can configure the whitelist on this interface so that the users complying with whitelist rules can directly access the Internet without user name and password.

Configuration steps

- Step 1 In the navigation bar, choose **Basic > Manage Users > WebAuth > Whitelist**. The **Whitelist** interface is displayed.
- Step 2 View the whitelist.
- To add a user, input the IP address, and click **Add**.
 - To delete an IP address, select one, and click **Delete**.
 - To delete all IP addresses, click **Select All**, and click **Delete**.
- Step 3 After configurations are complete, click **Save Config** to save configurations.

Configuration items

Table 9-85 Configuration items on the Whitelist interface


Configuration item	Description
IP address	IP address of the user in the whitelist

9.3 Online User

Scenario

You can view current online users on this interface.

Configuration steps

- Step 1 View information about online users.
- In the navigation bar, choose **Basic > Manage Users > OnlineUser**. The **OnlineUser** interface is displayed
 - Information about all online users is displayed, including the user name, user group, IP address, and online period (min).
- Step 2 Delete Web-authenticated users.
- In the navigation bar, choose **Basic > Manage Users > OnlineUser**. The **OnlineUser** interface is displayed
 - Click the online user to be deleted and then click the corresponding . A dialog box is displayed and then click **OK**.

Step 3 After configurations are complete, click **Save Config** to save configurations.

Configuration items

N/A

9.4 AuthenServer

9.4.1 RADIUS Authentication



Scenario

You can configure RADIUS authentication on this interface.

Configuration steps

Step 1 In the navigation bar, choose **Basic > AuthenServer > RADIUS Authentication**. The **RADIUS Authentication** interface is displayed.

Step 2 View the RADIUS server list.

- To modify a configured item, click  to enter the modifying interface.
- To add an item, click **Add** to enter the adding interface.
- To delete an item, click the corresponding .

Step 3 Configure the required item, and click **OK**.

Step 4 After configurations are complete, click **Save Config** to save configurations.

Configuration items

Table 9-86 Configuration items on the RADIUS Authentication interface



Configuration item	Description
Server Name	Name of the RADIUS server, in a character string form, and ranging from 1 to 63 characters
Server IP	IP address of the RADIUS server
Server Password	Password of the RADIUS server, in a character string form, and ranging from 1 to 63 characters
Port	Port number of the RADIUS server for authentication, in a character string form, ranging from 1 to 65534, being 1812 by default

9.4.2 LDAP Authentication

Scenario

You can configure LDAP authentication on this interface.

Configuration steps

- Step 1 In the navigation bar, choose **Basic > AuthenServer > LDAP Authentication**. The **LDAP Authentication** interface is displayed.
- Step 2 View the LDAP server list.
- To modify a configured item, click  to enter the modifying interface.
 - To add an item, click **Add** to enter the adding interface.
 - To delete an item, click the corresponding .
- Step 3 Configure the required item, and click **OK**.
- Step 4 After configurations are complete, click **Save Config** to save configurations.

Configuration items

Table 9-87 Configuration items on the LDAP Authentication interface

Configuration item	Description
Server Name	Name of the LDAP server, in a character string form, and ranging from 1 to 63 characters
Server IP	IP address of the LDAP server
Port	Port number of the LDAP server for authentication, in a character string form, ranging from 1 to 65534, being 389 by default
Common Name Identification	ID of the user name on the LDAP, being "cn" by default
Distinguished Name	Specifying the starting location to query data on the LDAP server. When the binding method is easy , the distinguished name should completely specify the user's location.
Bind method	Support the easy method currently.

9.5 Configuration examples

9.5.1 Example for configuring user authentication

Networking requirements

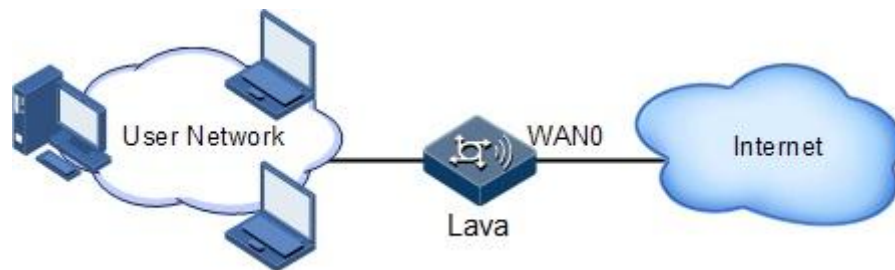
To authenticate users desiring of accessing the Internet by the LAVA, you can configure user authentication on the LAVA.

After you configure authentication, the HTTP request is redirected to the Web authentication login page on which the user is required to provide current user name and password. After the user is successfully authenticated, the system assigns a role for user by configured policies to implement access control over different users.

Detailed requirements are as below:

- The authentication interface is WAN0.
- The user is by local authentication.
- The logout method for the user is manual logout.

Figure 9-33 Web authentication application networking



Configuration steps

Step 1 Configure user management.

1. In the navigation bar, choose **Basic > Manage Users > Um**. The **User Management** interface is displayed.
2. In the **Username** area, click **Add** to enter the adding interface.
3. Configure related items, and click **OK**, as listed in Figure 9-34.

Figure 9-34 Adding a user

User-Add

Username *(1~32)

Auth Mode ▼

Password *(5~38)

Password Confirm *(5~38)

Prohibiting multi-pc-login

IP Address Binding

MAC Address Binding



User State Enable Disable

Groups belonged to ▼ *

Affiliated information ▾

4. On the **User Management** interface, view the created user, as shown in Figure 9-35.

Figure 9-35 User management interface

Username	Groups	User State	Operation
raisecom	Company	Enable	 

Total 1 records, current is the 1 page, total 1 pages

Jump to page

Step 2 Configure user authentication.

1. In the navigation bar, choose **Basic > Manage Users > WebAuth > Authentication Option**. The **Authentication Option** interface is displayed.
2. Configure related items, and click **OK**, as shown in Figure 9-36.

Figure 9-36 Authentication Option interface

Authentication Option White List

Webauth Global Switch

ON OFF

User Logout Method

Session Timeout Logout 1440 minutes(1-1440)

Web Manual Logout

Interface Configuration

Double click the mouse to choose Unauthenticated Interface

ath2
ath3
ath1

Double click the mouse to revoke Authenticated Interface

vlan1

Step 3 After configurations are complete, click **Save Config** to save configurations.

Checking configurations

Users that are connected by the VLAN1 interface cannot directly access the Internet. Instead, they are redirected to the Web authentication login page on which the user is required to provide the user name and password. After being successfully authenticated, the user can access the Internet.

10 Voice configurations

This chapter describes how to configure voice items on the **Voip** interface, including the following sections:

- System
- Line
- SIP
- H.248
- Fax
- Statistic
- Configuration examples

10.1 System

Scenario

System configuration is the basis of VoIP configuration. By configuring VoIP protocol and VoIP local address, you can further configure other VoIP items.

Configuration steps

- Step 1 In the navigation bar, choose **Voip > System**. The **System Configuration** interface is displayed.
- Step 2 Configure related items, and click **OK**.
- Step 3 After configurations are complete, click **Save Config** to save configurations.

Configuration items

Table 10-88 Configuration items in the VOIP System Configuration area




Configuration item	Description
The supported types of voice protocol	Display voice protocol types supported by the LAVA: <ul style="list-style-type: none"> • IMS-SIP • SIP • H.248
Voice Protocol Configuration	Choose voice protocol types: <ul style="list-style-type: none"> • IMS-SIP • SIP • H.248  Note After you choose a voice protocol, enter the corresponding voice protocol interface for configurations. The LAVA supports only one protocol at a time.
VOIP Local IP address	IP address and subnet mask of the voice subcard, for uplink interfaces, such as the WAN interface or VLAN interface, in colon hexadecimal notation, needless of filling, depending on the configuration in Bound Interface Configuration area
Bound Interfaces Configuration	Interface to be bound with the VoIP local IP address, including: <ul style="list-style-type: none"> • wan0 • eth0 • tr069 • vlan1 • 3gppp • ath1–ath3 (WLA interface)  Note Interface options depend on actual situation and are not limited to previous ones.

Table 10-89 Configuration items in the Media Configuration area

Configuration item	Description
VOIP Media IP	Enter the IP address of the VoIP local media. It is in dotted decimal notation. Enter the subnet mask of the IP address after the backslash

Configuration item	Description
Media Bound Interfaces Configuration	Select the interface bound to the media: <ul style="list-style-type: none"> • VLAN1 • 3gpp • WAN0  Note The interface types are based on the device type.

10.2 Line

Scenario

You can configure voice features of the Foreign Exchange Station (FXS) interface and basic features of the voice line. FXS uses the standard RJ-11 interface, and is connected by the telephone line to devices, such as common telephones, and fax. By configure line features, you can enable the LAVA to support some traditional voice features.

- DTMF transmission mode

Dual Tone Multi-Frequency (DTMF) signaling is widely used worldwide on touch tone telephones. With faster dialling speed, it replaces the dialling pulse signaling used by traditional dial telephones.

In a VoIP system, there are four modes to implement DTMF:

- Info message mode: encapsulate DTMF messages into the Info field for transmission.
- Transparent transmission: pack DTMF voice as voice to RTP for transmission.
- RFC2833 relay mode: send DTMF messages through the RFC2833 protocol.
- RFC2833 redundancy mode: send DTMF messages through the RFC2833+RFC2198 redundancy mode.

- DigitMap matching method

In soft exchange, the DigitMap resides in the Media Gateway (MG), detects and reports the dialling plan of dialling events received by the terminal. When the user hooks off the telephone, the DigitMap is enabled and requires the MG to judge whether the dialling string of the user is valid. When the detected dialling string matches a column, the DigitMap informs the Media Gateway Controller (MGC). In this way, the MG can send codes in groups. This also fits for SIP.

Numbers collected by the DigitMap are protected by three inter-event timers: the initial timer (T), short timer (S), and long timer (L). These three timers are used in different phases of the DigitMap:

- 1.Phase between off-hook and dialling: this phase is controlled by timer T. If timer T expires and no number is dialled, the MG sends a howler tone to remind you of hooking on.
- 2.Phase 1 between dialling and sending: when a number is being dialled, the MG judges by the DigitMap sent by the Central Office (CO). If one more digit to be dialled can make the current number uniquely match a DigitMap rule, the MG uses timer L. If the new

number collected after expiration of timer L still cannot match a DigitMap rule, the MG reports the new number to the MGC.

3. Phase 2 between dialling and sending: when a number is being dialled, the MG judges by the DigitMap sent by the Central Office (CO). If one more digit to be dialled can make the current number match multiple DigitMap rules, the MG uses timer S. If the new number collected before expiration of timer S matches a DigitMap rule, the MG reports the new number to the MGC; otherwise, the MG reports the new number to the MGC after expiration of timer S.

Configuration steps

Step 1 In the navigation bar, choose **Voip > Line**. The **Line Configuration** interface is displayed.

Step 2 In the **Line Configuration** guide, configure related items, and click **OK**.

Step 3 In the **Port Configuration** area, view port information.

1. To modify a configured item, click  to enter the modification interface.
2. Configure related items, and click **OK**.

Step 4 After configurations are complete, click **Save Config** to save configurations.

Configuration items

Table 10-90 Configuration items on the Line Configuration interface

Configuration item	Description
DTMF Transmission Mode	In a VoIP system, there are four modes to implement DTMF: <ul style="list-style-type: none"> • Info message mode: encapsulate DTMF messages into the Info field for transmission. • Transparent transmission: pack DTMF voice as voice to RTP for transmission. • RFC2833 relay mode: send DTMF messages through the RFC2833 protocol. • RFC2833 redundancy mode: send DTMF messages through the RFC2833+RFC2198 redundancy mode.
Initial timing	Initial timer, in unit of second, being 10 by default, ranging from 1 to 255
Long timing	Long timer, in unit of second, being 10 by default, ranging from 1 to 255
Short timing	Long timer, in unit of second, being 3 by default, ranging from 1 to 255
DIGITMAP Matching Way	<ul style="list-style-type: none"> • Max: if the current number collected uniquely matches a DigitMap rule and more digits to be added can make the new number match multiple DigitMap rules, number collection continues. • Min: if the current number collected uniquely matches a DigitMap rule, the MG immediately reports the current number to the MGC, and number collection terminates.

Configuration item	Description
Busy Tone Timing	Duration for sending busy tone, in unit of second, being 40 by default, and ranging from 1 to 100
Push Hang Sound Timing (howler tone)	Duration for sending howler tone, in unit of second, being 60 by default, and ranging from 1 to 100
Ringing Timeout Timing	Duration for sending ringing timeout tone, in unit of second, being 40 by default, and ranging from 1 to 100
Digital Map	Configure the rule of Digital Map.

Table 10-91 Configuration items on the Line Configuration Modify interface

Configuration item	Description
Port	Number of the Plain Old Telephone Service (POTS) port, unchangeable
CODEC	Primary codec options: <ul style="list-style-type: none"> • G711A (by default) • G729 • G711U • G723 • G726 • G722
Echo Cancellation	Enable/Disable echo cancellation.
Silence Suppression	Enable/Disable silence suppression.
Comfort noise	Enable/Disable comfort noise.
Output Gain	Configure the output gain, in unit of dB, integer, ranging from -50 to 50, and being 0 by default.
Input Gain	Configure the input gain, in unit of dB, integer, ranging from -50 to 50, and being 0 by default.

10.3 SIP

10.3.1 Server configuration

Scenario

The LAVA can works as the User Agent (UA) of SIP. To implement voice services based on SIP, you need to configure related servers or items on this interface as below:

- Register server

The register server is used for login to the User Agent Server (UAS). In the SIP system, all UASs have to be registered and logged in so that the User Agent Client (UAC) can find them. The register server can receive requests from UACs and register user addresses.

- Proxy server

The proxy server is used to send the session request from the calling UA to the called UA, and send back the session response from the called UA to the calling UA. The SIP server receives these requests and determines the destination for these requests. The proxy server sends a request to the location server to query location of the called UA, and calling policies of both the called UA and called UA. Only after it finds the called UA and the call is permitted, it forwards the request.

- Heartbeat

The heartbeat message is sent between the UA and UAS to detect link status.

- Local SIP Message listening socket

The SIP message listening is used to judge whether the adopted port number is consistent with the configured port number.

Configuration steps

- Step 1 In the navigation bar, choose **Voip > SIP > Server Configuration**. The **Server Configuration** interface is displayed.
- Step 2 Configure related items, and click **OK**.
- Step 3 After configurations are complete, click **Save Config** to save configurations.

Configuration items

Table 10-92 Configuration items in the Register Server area

Configuration item	Description
Main Server	IP address of the main register server, in colon hexadecimal notation, and usually provided by the ISP
Main Server Port	Port number of the main register server, being 5060 by default, default port number of SIP, and ranging from 1 to 65535
Standby Server	IP address of the standby register server, in colon hexadecimal notation, and usually provided by the ISP
Standby Server Port	Port number of the standby register server, being 5060 by default, default port number of SIP, and ranging from 1 to 65535
Automatically refresh interval	Period for the UA to register to the register server, interval for automatical refresh, in unit of second, being 900 by default, ranging from 60 to 65535

Table 10-93 Configuration items in the Proxy Server area

Configuration item	Description
Main Server	IP address of the main proxy server, in colon hexadecimal notation, and usually provided by the ISP
Main Server Port	Port number of the main proxy server, being 5060 by default, default port number of SIP, and ranging from 1 to 65535
Standby Server	IP address of the standby proxy server, in colon hexadecimal notation, and usually provided by the ISP
Standby Server Port	Port number of the standby proxy server, being 5060 by default, default port number of SIP, and ranging from 1 to 65535

Table 10-94 Configuration items in the Outbound Server area

Configuration item	Description
Outbound Server IP	Address of the primary Outbound server. Either the IP address or the domain name is available.
Outbound Server Port	Port ID of the primary Outbound server, ranging from 1 to 65535
Backup Outbound Server IP	Address of the secondary Outbound server. Either the IP address or the domain name is available.
Backup Outbound Server Port	Port ID of the secondary Outbound server, ranging from 1 to 65535

Table 10-95 Configuration items in the Heartbeat area

Configuration item	Description
Supervisor State	<ul style="list-style-type: none"> • ON: enable heartbeat registration. • OFF: disable heartbeat registration.
Heartbeat Timeout Period	<p>In unit of second, being 60 by default, and ranging from 10 to 43200.</p> <p>When the heartbeat registration time exceeds this period, it indicates that the link is disconnected.</p>
The number of heartbeat overtime	<p>Being 3 by default, and ranging from 1 to 100.</p> <p>When the number of heartbeat registration times exceeds this number, it indicates that the link is disconnected.</p>
Heartbeat mode	<ul style="list-style-type: none"> • send-option: send the Option message and receive the Option message. • receive-option: receive the Option message. • send-register: send the registration message.

Table 10-96 Configuration items in the Session Update area

Configuration item	Description
Session Expire Timeout	Set the session timeout time. The session will be disconnected if the time expires.
Min Session Expire Time	Set the minimum session update period. The session is updated periodically.

Table 10-97 Configuration items in the Local SIP Message listening socket area

Configuration item	Description
SIP Message listening socket	Port for listening SIM messages, being 5060 by default for UDP and TCP listening port, ranging from 10 to 43200

Table 10-98 Configuration items in the Advanced Options area

Configuration item	Description
Subcibe Enable	Enable/Disable SUB subscription.
Subcibe Expires	Enter the SUB subscription period, in unit of second and ranging from 1 to 2592000.
Update_phone_Time	Enable/Disable phone time synchronization.
Update_Syn_Time	Enable/Disable SIP synchronization system time.
Special Service Numbers	Preamble for the intelligent phone performing secondary dial, such as 10086 and 95526
Intelligent Public Phone Config	Intelligent public telephone refers to the public telephone that uses the intelligent network system or intelligent platform to realize services.
Update_Lava_Send	Enable/Disable Update session update.
user=phone	Enable/Disable user=phone identification.
Malicious Call operation code	Enter related characters (provided by the ISP) to query the telephone number of the caller who intends to hide it.


10.3.2 User authentication

Scenario

You can configure the user name and password for the user on each PORS port on this interface. When the server needs the SIP client to be authenticated, you need to configure user

authentication. When you do not need to configure the server, though you configure a user name and the password, they will not take effect and be not sent during registration.

Configuration steps

- Step 1 In the navigation bar, choose **Voip > SIP > User Authentication**. The **User Authentication** interface is displayed.
- Step 2 View port information.
To modify a configured item, click  to enter the modification interface.
- Step 3 Configure related items, and click **OK**.
- Step 4 After configurations are complete, click **Save Config** to save configurations.

Configuration items

Table 10-99 Configuration items on the User Authentication Configuration Add interface


Configuration item	Description
Port	Number of the POTS port, read-only
Username	User name for authentication
Password	Password for authentication

10.3.3 Local number

Scenario

You can configure the local telephone number and information for registration of the telephone number.

Configuration steps

- Step 1 In the navigation bar, choose **Voip > SIP > Local Number**. The **Local Number** interface is displayed.
- Step 2 View information about local number.
To modify a configured item, click  to enter the modification interface.
- Step 3 On the modification interface, configure related items, and click **OK**.
- Step 4 After configurations are complete, click **Save Config** to save configurations.

Configuration items

Table 10-100 Configuration items on the Local Number Modify interface

Configuration item	Description
Port	POTS port number, read-only
Supervisor State	<ul style="list-style-type: none"> • ON: enable this port. • Off: disable this port.
Phone Number	Telephone number of the POTS port
Username	User name of the POTS port, for identifying lines, string or special characters
Register/Unregistered	<ul style="list-style-type: none"> • Register: the POTS port registers a telephone number to the registration server. • Unregistered: the POTS port unregisters a telephone number to the registration server.

10.3.4 Service configuration

Scenario

Basic on voice configuration, service configuration enables you to use new functions to meet voice users' different service requirements, including:

- Caller ID

This function makes a calling number displayed on the telephone screen so that the user can know the identity of the caller and then determines whether to answer the phone. Of course, the telephone set should support this function.

- Call waiting

When the caller is calling, a new call is forwarded to the caller. The new caller will be kept waiting until the original call terminates.

- Three-way call

The three-way call, also called conference call, enables a user to call the third party without interrupting the ongoing conversation, thus implementing conversation between multiple parties and a small conference call.

- Hotline service

It is a fixed telephone number. After a hotline number is specified to a port of the LAVA, it is automatically dialed when a user connected to the port hooks off the telephone.

-Immediate hotline: in this mode, the hotline number is automatically dialed upon off-hook.

-Immediate hotline: in this mode, the hotline number is automatically dialed a period after off-hook.

- Reverse business

It is used in accounting. After a telephone link is established, polarities of lines A and B are reversed, and then accounting starts; when the call ends, polarities recovers, and accounting ends.

Configuration steps

Step 1 In the navigation bar, choose **Voip > SIP > Service Configuration**. The **Service Configuration** interface is displayed.

Step 2 View user services.

Step 3 Click Advanced Options.

To modify a configured item, click  to enter the modification interface.

Step 4 On the modification interface, configure related items, and click **OK**.

Step 5 After configurations are complete, click **Save Config** to save configurations.

Configuration items

Table 10-101 Configuration items on the Business Configuration Modify interface

Configuration item	Description
Port	POTS number, read-only
Call ID	Enable/Disable caller ID display.
Call Waiting	Enable/Disable call waiting.
Three-Way Calling	Enable/Disable three-way calling.
Reverse Business	Enable/Disable polarity reversal.
Hotline Service	<ul style="list-style-type: none"> • Immediately hotline: enable the hotline number to be automatically dialed upon off-hook. • Delay hotline: enable the hotline number to be automatically dialed a period after off-hook. • Off: disable hotline service.
Hotline Number	Hotline number to be dialed

10.3.5 Dialling rules



Scenario

Dialling rules are used to match a telephone number with the IP address of the UA. If you know the IP address of the UA, you can directly initiate a SIP call. This is used for internal calls.

Dialling rules involves two aspects:


- Rule matching: the UA collects every digit dialed by the user and judges by dialling rules whether the number is a complete string. If yes, the UA initiates the call.
- Number mapping: after a number is mapped to the IP address of a UA, the SIP directly connected line is established.

Configuration steps

- Step 1 In the navigation bar, choose **Voip > SIP > Dialing Rules**. The **Dialing Rules** interface is displayed.
- Step 2 View dialling rules.
- To modify a configured item, click  to enter the modification interface.
 - To add an item, click **Add** to enter the adding interface.
 - To delete an item, and click the corresponding .
- Step 3 On the modifying or adding interface, configure related items, and click **OK**.
- Step 4 After configurations are complete, click **Save Config** to save configurations.

Configuration items

Table 10-102 Configuration items on the Dialling Rules Add interface

Configuration item	Description
No.	Number of the dialling rule, integer, ranging from 1 to 300
Dialling rules	<p>For matching the dialled number, and supporting "x", ".", "#", "*", "[]", "-", and digits 1 to 9.</p> <p>Detailed rules are as below:</p> <ul style="list-style-type: none"> • xxxxxxxx: 8-digit telephone number. The dialling with an 8-digit number is matched by the rule. The number of x's determines the number of digits in the telephone number to be matched, and it depends on the user. • x.#: match a telephone number ending with "#". • [0-9*#]: match all telephone numbers, including "*" and "#". • x.: match all telephone numbers, excluding "*" and "#". <p> Note</p> <p> "." indicates multiple duplicates. "x" indicates a digit. "x" is not capitalized. A dialling rule cannot begin with ".". During dialling, if multiple previous rules are matched, use the first matched rule.</p>
URL	URL of the SIP to which the SIP calling request message is sent, IP address

10.4 H.248

10.4.1 MG configuration

Scenario

You can configure MG on this interface. The LAVA can work as a MG to connect to the H.248 protocol network.

Configuration steps

- Step 1 In the navigation bar, choose **Voip > H.248 > MG Configuration**. The **MG Configuration** interface is displayed.
- Step 2 View information about MG configuration.
- Step 3 Configure related items, and click **OK**.
- To register the MG, click **Register** in the **MG Register** area.
 - To unregister the MG, click **Unregister** in the **MG Unregister** area.
- Step 4 After configurations are complete, click **Save Config** to save configurations.

Configuration items

Table 10-103 Configuration items on the MG Configuration area

Configuration item	Description
Status	<ul style="list-style-type: none"> • Registering • Registered • Log_out • Others • Stopped service
Local Number	Name of a MG, identifying the MG
CODEC	Coding scheme of the H.248 protocol, including <ul style="list-style-type: none"> • Text • Compressed text
Registered way	Mode for the MG to register to the MGC, including: <ul style="list-style-type: none"> • IP address • Domain name • Device name • MAC address • Message identifier
Transport Port	Port number of the MG transport layer (used by both TCP and UDP), ranging from 1 to 65535, being 2944 by default for text codec.

Configuration item	Description
Heart beat detection mode	<ul style="list-style-type: none"> • Closed: disable heartbeat detection. • Send SVC change new message: the MG periodically sends SVC message to the MGC. • ITO way: the MG periodically sends Inactivity Timeout (ITO) message to the MGC. • Audit way: the MG checks whether the audit period sent by the MGC is correct. If no, the MG takes the MGC faulty.
Heartbeat Cycle	Integer, ranging from 10 to 43200, in unit of second, being 60 by default. When the heartbeat registration time exceeds this period, the link is disconnected.
Heartbeat timeout count	Integer, ranging from 1 to 100, being 3 by default. When the heartbeat registration count exceeds this count, the link is disconnected.
Heartbeat Wait Delay	Integer, ranging from 0 to 1200, in unit of second, being 180 by default. After you click Register in the MG Register area, the LAVA will be registered with a random heartbeat wait delay.

10.4.2 MGC configuration

Scenario

You can configure MGC on this interface.

Configuration steps

- Step 1 In the navigation bar, choose **Voip > H.248 > MGC Configuration**. The **MGC Configuration** interface is displayed.
- Step 2 Configure related items, and click **OK**.
- Step 3 After configurations are complete, click **Save Config** to save configurations.

Configuration items

Table 10-104 Configuration items on the MGC Configuration interface

Configuration item	Description
Primary MGC IP	IP address of the primary MGC
Primary MGC Port	Transport layer port number of the primary MGC, being 2944 by default, ranging from 1 to 65535
Primary MGC Name	Identifying the primary MGC
Secondary MGC IP	IP address of the secondary MGC (different from that of the primary MGC)

Configuration item	Description
Secondary MGC Port	Transport layer port number of the secondary MGC, being 2944 by default, ranging from 0 to 65535. The value 0 indicates no registration.
Secondary MGC Name	Identifying the secondary MGC

10.4.3 TID configuration

Scenario


The H.248 protocol identifies terminals of the MG and MGC by Terminal ID (TID). The TID includes the following two types:

- POTS TID: it is the ID of the unique MG port of the MGC and bound with a specific numbers. You should configure the mode to generate POTS TIP, prefix and name of POTS TID.
- Real Time Protocol (RTP) TID: you should configure the following items:
 - Prefix of RTP TID
 - Number max length of RTP TID
 - Number start of RTP TID
 - Maximum Num

There are two modes to configure POTS TID:

- Auto: the TID of each line is generated by summing up the prefix and name of POTS TID configured on the MG.
- Handy: the TID of each port is configured respectively and may be irregularly from others.

Configuration steps

- Step 1 In the navigation bar, choose **Voip > H.248 > TID Configuration**. The **TID Configuration** interface is displayed.
- Step 2 Configure related items in the **RTP TID Configuration** area, and click **OK**.
- Step 3 Choose auto or handy in the **TID Mode** drop-down list.
 - If you choose auto, configure related items in the **POT TID Configuration** area.
 - If you choose handy, the POTS TID manual mode configuration list is displayed. Click  to enter the modification interface. Configure related items, and click **OK**.
- Step 4 After configurations are complete, click **Save Config** to save configurations.

Configuration items

Table 10-105 Configuration items in the RTP TID Configuration area

Configuration item	Description
Max Num	Number of RTP user terminals, twice of the maximum number of POTS ports as recommended
Prefix	Prefix of the RTP TID, made according to naming conventions of the MGC
Number Max Length	Length of the number part of RTP TID, integer, ranging from 1 to 16
Number start	Start value of the number part of RTP TID, ranging from 0 to 20000000

Table 10-106 Configuration items in auto mode in the POTS TID Configuration area

Configuration item	Description
TID Mode	Set the TID mode to manual or auto.
Prefix	Prefix of the RTP TID in auto TID mode, made according to naming conventions of the MGC
Name	Name of the RTP TID in auto TID mode, made according to naming conventions of the MGC

Table 10-107 Configuration items in handy mode in the POTS TID manual mode configuration modification area


Configuration item	Description
Port	Number of the POTS port, read-only
Name	Name of each POTS port for POTS TID, in a character string form and ranging from 1 to 32

10.4.4 Port status

Scenario

You can view supervisor state, port status, and port business state of the voice port on this interface, and can configure the supervisor state of the port.

Configuration steps

- Step 1 In the navigation bar, choose **Voip > H.248 > Port Status**. The **Port Status** interface is displayed.
- Step 2 View information about port status.
- To modify a configured item, click  to enter the modification interface.
- Step 3 Configure related items, and click **OK**.
- Step 4 After configurations are complete, click **Save Config** to save configurations.

Configuration items

Table 10-108 Configuration items on the Port State Modify interface

Configuration item	Description
Port	Number of POTS port, read-only
Port State	<ul style="list-style-type: none"> • ON: enable the port. • OFF: disable the port.
Register/Unregistered	<ul style="list-style-type: none"> • Register: the POTS port registers a telephone number to the registration server. • Unregistered: the POTS port unregisters a telephone number from the registration server.

10.5 Fax


Scenario

Fax over IP is implemented by sending fax through the Internet. After the fax over IP features is enabled on the LAVA, the LAVA can support fax over IP.

The LAVA supports two fax modes:

- T.38: it is a communication protocol for realtime fax through the IP network. It describes and defines the communication method, correction method, packet format, and communication process used for realtime fax over the IP network.
- Transparent: the fax is sent in the voice channel.

Configuration steps

- Step 1 In the navigation bar, choose **Voip > Fax**. The **Fax Configuration** interface is displayed.
- Step 2 Configure related items, and click **OK**.
- When you choose T.38 fax mode, the fax rate list is displayed. To modify a configured item, click  to enter the modification interface.
- Step 3 Configure related items, and click **OK**.

Step 4 After configurations are complete, click **Save Config** to save configurations.

Configuration items

Table 10-109 Configuration items on the Fax Configuration interface

Configuration item	Description
Modem Function	Enable/Disable the modem function. This function is used to manage remote devices; namely, remote PSTN users log in to a device on the Intranet through dialling.
Fax Mode	<ul style="list-style-type: none"> • Transparent • T.38
SDP ATTR	Select the SDP negotiation property for the SIP softswitch processing the fax: <ul style="list-style-type: none"> • fax • X-fax • silenceSupp:off---- • gpmd:8 vbd=yesx

Table 10-110 Configuration items on the Fax Modify interface

Configuration item	Description
Port	Number of the POTS port, read-only
Fax Rate	<ul style="list-style-type: none"> • 2400bps • 4800bps • 7200bps • 9600bps • 12000bps • 14400bps

10.6 Statistic

10.6.1 POTS call accounting

Scenario

You can take statistics of calling services on each voice port on this interface and learn the traffic information, including:


- Calling success times
- Calling failure times
- Called success times
- Called failure times

- The current talk time (s)
- Total talk time (s)
- Number of calls

Configuration steps

Step 1 In the navigation bar, choose **Voip > Statistic > POTS Call Accounting**. The **POTS Call Accounting** interface is displayed.

Step 2 View port state.

- To delete a configured item, click .
- To clear statistics of all ports, click **Clear**.

Step 3 After configurations are complete, click **Save Config** to save configurations.

Configuration items

N/A

10.6.2 RTP call accounting

Scenario

You can take statistics of RTP performance, including:

- Accept bag number (number of received packets)
- Accept bytes (number of received bytes)
- Send bag Number (number of sent packets)
- Send bytes (number of sent bytes)

Configuration steps

Step 1 In the navigation bar, choose **Voip > Statistic > RTP Call Accounting**. The **RTP Call Accounting** interface is displayed.

Step 2 View RTP performance statistics.

To clear statistics of all ports, click **Clear**.

Step 3 After configurations are complete, click **Save Config** to save configurations.

Configuration items

N/A

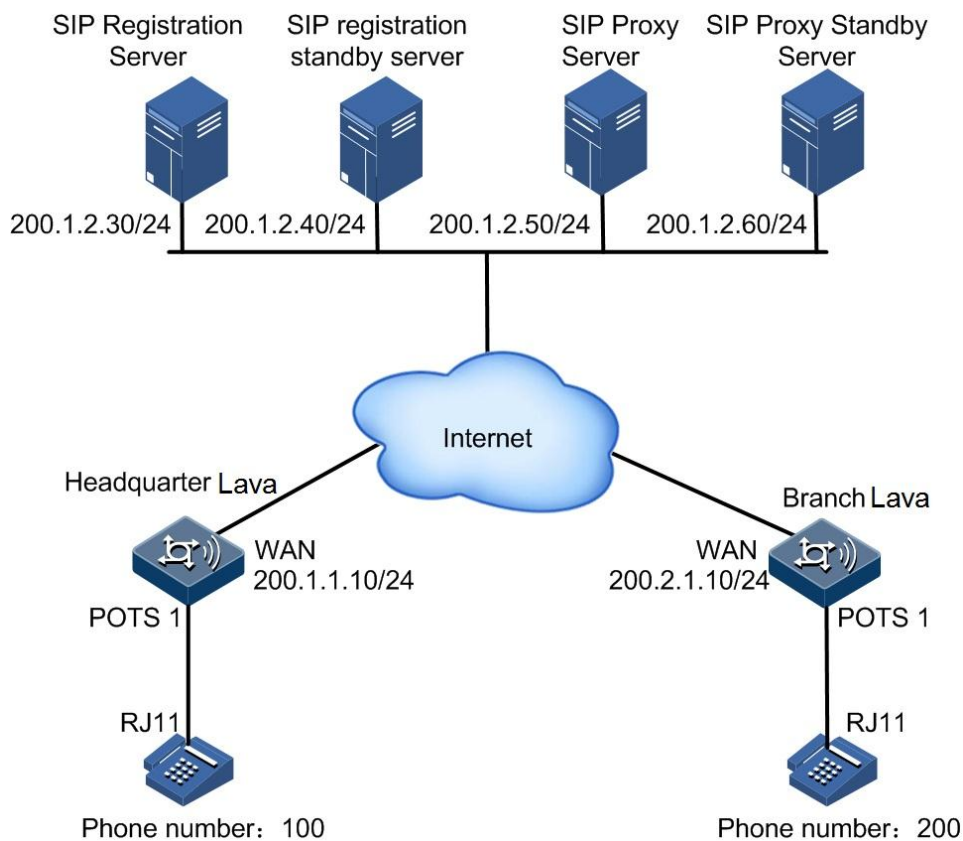
10.7 Configuration examples

10.7.1 Example for configure SIP-based VoIP phone

Networking requirements

The headquarter and branch of an enterprise need to establish a VoIP phone connection. You can use the VoIP function provided by the LAVA to enable users make VoIP calls between the headquarter and the branch, as shown in Figure 10-37.

Figure 10-37 SIP-based VoIP phone application networking



Detailed requirements are as below:

- Apply SIP.
- IP address of the WAN0 interface of the LAVA in the headquarter: 200.1.1.10/255.255.255.0.
- IP address of the WAN0 interface of the LAVA in the branch: 200.2.1.10/255.255.255.0.
- Requirements on the SIP server:
 - IP address of the SIP registration server: 200.1.2.30/255.255.255.0.
 - IP address of the SIP standby server: 200.1.2.40/255.255.255.0.
 - IP address of the SIP proxy server: 200.1.2.50/255.255.255.0.
 - IP address of the SIP standby proxy server: 200.1.2.60/255.255.255.0.
 - The SIP server is configured with user authentication.

- The SIP server is configured with user registration.
- Telephone number of the headquarter: 100. It is connected to the LAVA POTS1 interface. The user name and password for authentication are A1 and 111 respectively.
- Telephone number of the branch: 200. It is connected to the LAVA POTS1 interface. The user name and password for authentication are A2 and 222 respectively.
- All telephone services except hotline are enabled.

Configuration steps

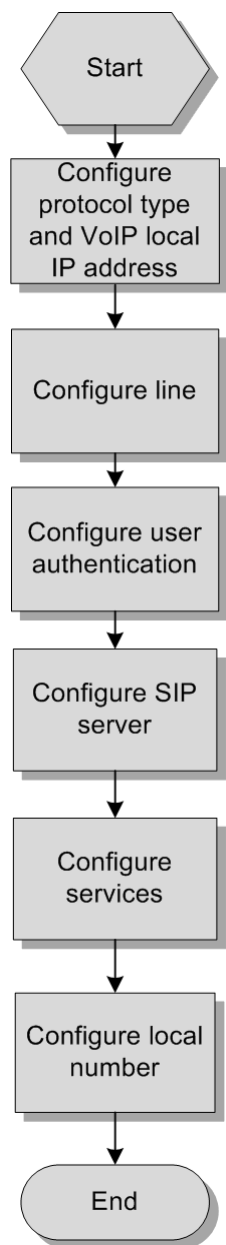
Configure the LAVAs in the headquarter and branch respectively, as shown in Figure 10-38.



Note

Before being configured with VoIP, the LAVA is configured with basic features so that users can access the Internet through it. For internet access, see chapter 4 Interface configurations.

Figure 10-38 SIP-based VoIP configuration flow



Configure the LAVA in the headquarter as below:

Step 1 Configure the protocol type and VoIP local IP address.

1. In the navigation bar, choose **Voip > System**. The **System Configuration** interface is displayed, as shown in Figure 10-39.
2. Configure related items as below:
 - Voice protocol configuration: IMS-SIP
 - Bound interfaces configuration: WAN0
3. After configurations are complete, click **Save Config** to save configurations.

Figure 10-39 Configure system items for SIP

VOIP System Configuration	
The supported types of voice protocol	IMS-SIP, H248
Voice Protocol Configuration	IMS-SIP <input type="button" value="v"/>
VOIP Local IP address	0.0.0.0 0.0.0.0
Bound Interfaces Configuration	<input type="button" value="v"/>

4. Click **OK**. A **Modified Successfully** prompt is displayed. Click **OK**.

Step 2 Configure the line.

1. In the navigation bar, choose **Voip > Line**. The **Line Configuration** interface is displayed.


2. Configure related items, as shown in Figure 10-40.

- DTMF transmission mode: transparent
- Initial timing: 10s
- Long timing: 8s
- Short timing: 5s
- DIGITMAP matching way: max
- Busy tone timing: 40s
- Push hang sound timing: 60s
- Ringing timeout timing: 60s

Figure 10-40 Configuring line items for SIP

Line Configuration		
DTMFTransmission Mode	Transparent <input type="button" value="v"/>	
Initial timing	10	Seconds*(1~255)
Long Timing	8	Seconds*(1~255)
Short Timing	5	Seconds*(1~255)
DIGITMAPMatching Way	min <input type="button" value="v"/>	
Busy Tone Timing	40	Seconds*(1~100)
Push Hang Sound Timing	60	Seconds*(1~100)
Ringing Timeout Timing	60	Seconds*(1~100)

3. Click **OK**. A **Modified Successfully** prompt is displayed. Click **OK**.

4. Click  corresponding to port 1 to enter the modification interface.

5. Configure related items, as shown in Figure 10-41.

- CODEC: G.711A
- Echo cancellation: ON
- Silence suppression: ON

-Comfort noise: ON


Figure 10-41 Modifying line configurations for SIP

Line Configuration Modify	
Port	1
CODEC	G711A
Echo Cancellation	<input checked="" type="radio"/> ON <input type="radio"/> OFF
Silence Suppression	<input checked="" type="radio"/> ON <input type="radio"/> OFF
Comfort noise	<input checked="" type="radio"/> ON <input type="radio"/> OFF

6. Click **OK**. A **Modified Successfully** prompt is displayed. Click **OK**.

Step 3 Configure user authentication.

1. In the navigation bar, choose **Voip > SIP > User Authentication**. The **User Authentication** interface is displayed.

2. Click  corresponding to port 1 to enter the modification interface.

3. Configure related items, as shown in Figure 10-42.

-Username: A1

-Password: 111

Figure 10-42 Adding user authentication

User Authentication Configuration Add	
Port	1
Username	A1
Password	111

4. Click **OK**. A **Modified Successfully** prompt is displayed. Click **OK**.

Step 4 Configure the SIP server.

1. In the navigation bar, choose **Voip > SIP > Server Configuration**. The **Server Configuration** interface is displayed.

2. In the **Register Server** area, configure related items, as shown in Figure 10-43.

-Main server: 200.1.2.30

-Main server port: 5060

-Standby server: 200.1.2.40

-Standby server port: 5060

-Automatically refresh interval: 3600s

Figure 10-43 Configuring the register server

Register Server		
Main Server	<input type="text" value="200.1.2.30"/>	
Main Server Port	<input type="text" value="5060"/>	*(1~65535)
Standby Server	<input type="text" value="200.1.2.40"/>	
Standby Server Port	<input type="text" value="5060"/>	*(1~65535)
Automatically refresh interval	<input type="text" value="3600"/>	*(60~65535)Seconds

3. In the **Proxy Server** area, configure related items, as shown in Figure 10-44.

- Main server: 200.1.2.50
- Main server port: 5060
- Standby server: 200.1.2.60
- Standby server port: 5060

Figure 10-44 Configuring the proxy server

Proxy Server		
Main Server	<input type="text" value="200.1.2.50"/>	
Main Server Port	<input type="text" value="5060"/>	*(1~65535)
Standby Server	<input type="text" value="200.1.2.60"/>	
Standby Server Port	<input type="text" value="5060"/>	*(1~65535)

4. In the **Heartbeat** area, configure related items, as shown in Figure 10-45.

- Supervisor State: ON
- Heartbeat timeout period: 60s
- The number of heartbeat overtime: 3
- Heartbeat mode: send-option

Figure 10-45 Configuring heartbeat

Heartbeat		
Supervisor State	<input checked="" type="radio"/> ON <input type="radio"/> OFF	
Heartbeat Timeout Period	<input type="text" value="60"/>	*(10~43200)Seconds
The number of heartbeat overtime	<input type="text" value="3"/>	*(1~100)
Heartbeat mode	<input type="text" value="send-option"/>	<input type="button" value="v"/>

5. In the **Local SIP Message listening socket** area, configure related items, as shown in Figure 10-46.

- SIP Message listening socket: 5060

Figure 10-46 Modifying local SIP message listening socket

Local SIP Message listening socket	
SIP Message listening socket	<input type="text" value="5060"/> *(10~43200)

6. Click **OK**. A **Modified Successfully** prompt is displayed. Click **OK**.

Step 5 Configure services.


1. In the navigation bar, choose **Voip > SIP > Service Configuration**. The **Service Configuration** interface is displayed.
2. Click **Advanced Options**.
3. Click  corresponding to port 1 to enter the modification interface.
4. Configure related items, as shown in Figure 10-47.
 - Caller ID: ON
 - Call waiting: ON
 - Three-way calling: ON
 - Reverse business: ON
 - Hotline service: OFF

Figure 10-47 Modifying service configurations

Business Configuration Modify	
Port	<input type="text" value="1"/>
Caller ID	<input checked="" type="radio"/> ON <input type="radio"/> OFF
Call Waiting	<input checked="" type="radio"/> ON <input type="radio"/> OFF
Three-Way Calling	<input checked="" type="radio"/> ON <input type="radio"/> OFF
Reverse Business	<input checked="" type="radio"/> ON <input type="radio"/> OFF
Hotline Service	<input type="radio"/> Immediate Hotline <input type="radio"/> Delay Hotline <input checked="" type="radio"/> OFF
Hotline Number	<input type="text"/>

5. Click **OK**. A **Modified Successfully** prompt is displayed. Click **OK**.

Step 6 Configure local number.


1. In the navigation bar, choose **Voip > SIP > Local Number**. The **Local Number** interface is displayed.
2. Click  corresponding to port 1 to enter the modification interface.
3. Configure related items, as shown in Figure 10-48.
 - Supervisor: ON
 - Phone number: 100
 - Username: pots-uni-1

Figure 10-48 Modifying the local number

Local Number Modify	
Port	<input type="text" value="1"/>
Supervisor State	<input checked="" type="radio"/> ON <input type="radio"/> OFF
Phone Number	<input type="text" value="100"/>
Username	<input type="text" value="pots-uni-1"/>

4. Click **OK**. A **Modified Successfully** prompt is displayed. Click **OK**.

Step 7 After configurations are complete, click **Save Config** to save configurations.

Configure the LAVA in the branch in the same way.

Configuring SIP-based VoIP phone is complete.

Checking configurations

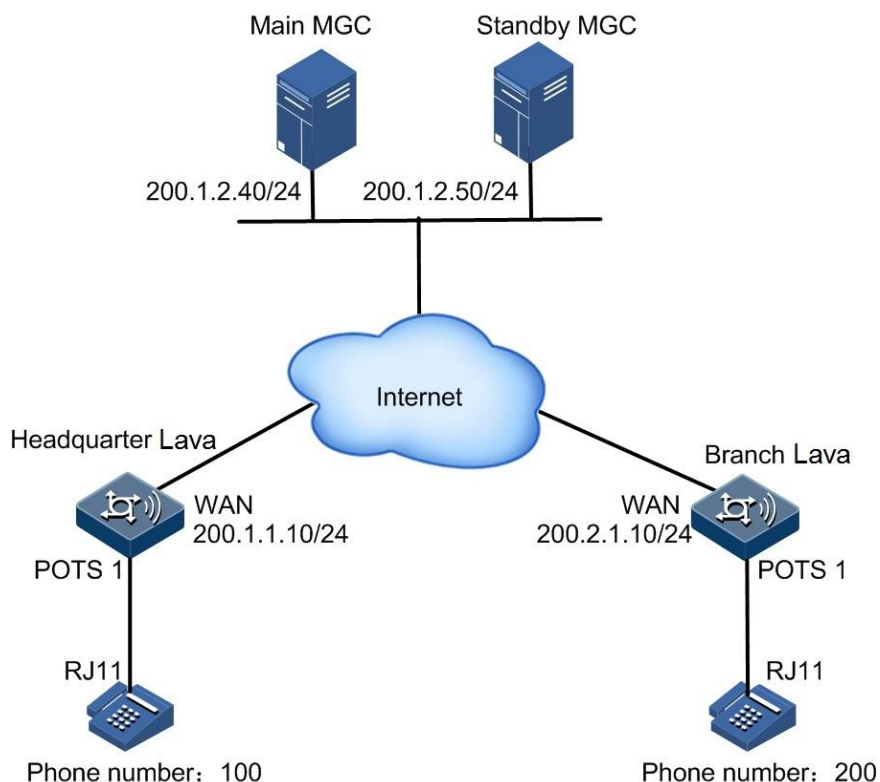
The headquarter and branch can make calls with each other.

10.7.2 Example for configuring H.248-based VoIP phone

Networking requirements

The headquarter and branch of an enterprise need to establish a VoIP phone connection. You can use the VoIP function provided by the LAVA to enable users make VoIP calls between the headquarter and the branch, as shown in Figure 10-49.

Figure 10-49 H.248-based VoIP phone application networking



Detailed requirements are as below:

- Adopt the H.248 protocol.
- IP address of the WAN0 interface of the LAVA in the headquarter: 200.1.1.10/255.255.255.0.
- IP address of the WAN0 interface of the LAVA in the branch: 200.2.1.10/255.255.255.0.
- Requirements on the MGC server:
 - IP address of the main MGC server: 200.1.2.40/255.255.255.0.
 - IP address of the standby MGC server: 200.1.2.50/255.255.255.0.
 - The MGC requires MG registration.
- Telephone number of the headquarter: 100. It is connected to the LAVA POTS1 interface. The port name is 1.
- Telephone number of the branch: 200. It is connected to the LAVA POTS1 interface. The port name is 2.
- All telephone services except hotline are enabled.

Configuration steps

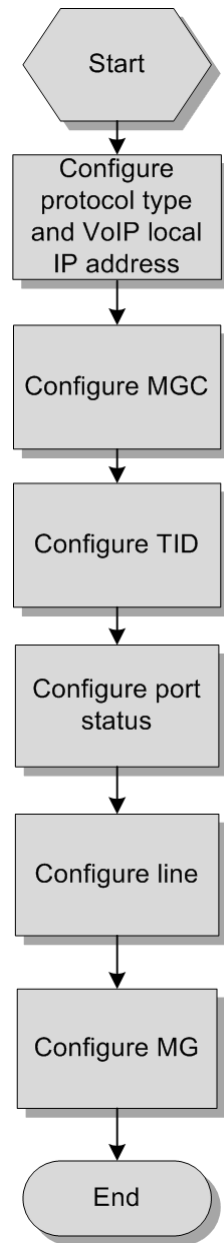
Configure the LAVAs in the headquarter and branch respectively, as shown in Figure 10-50.



Note

Before being configured with VoIP, the LAVA is configured with basic features so that users can access the Internet through it. For internet access, see section 4 Interface configurations.

Figure 10-50 H.248-based VoIP configuration flow



Configure the LAVA in the headquarter as below:

Step 2 Configure the protocol type and VoIP local IP address.

1. In the navigation bar, choose **Voip** > **System**. The **System Configuration** interface is displayed, as shown in Figure 10-39.
2. Configure related items as below:
 - Voice protocol configuration: H.248
 - Bound interfaces configuration: WAN0

Figure 10-51 Configuring system items for H.248

VOIP System Configuration	
The supported types of voice protocol	IMS-SIP, H248
Voice Protocol Configuration	H.248
VOIP Local IP address	0.0.0.0 / 0.0.0.0
Bound Interfaces Configuration	WANO

3. Click **OK**. A **Modified Successfully** prompt is displayed. Click **OK**.

Step 3 Configure the MGC.

1. In the navigation bar, choose **Voip > H.248 > MGC Configuration**. The **MGC Configuration** interface is displayed.

2. Configure related items, as shown in Figure 10-52.

- Primary MGC IP: 200.1.1.2.40
- Primary MGC port: 2944
- Primary MGC name: primary MGC
- Secondary MGC IP: 200.1.1.2.50
- Secondary MGC port: 2944
- Secondary MGC name: secondary MGC

Figure 10-52 Configuring the MGC

MGC Configuration	
Primary MGC IP	200.1.2.40
Primary MGC Port	2944 <small>*(1~65535)</small>
Primary MGC Name	Primary MGC
Secondary MGC IP	200.1.2.50
Secondary MGC Port	2944 <small>*(0~65535, 0 means MGC secondary server does not registered)</small>
Secondary MGC Name	Secondary MGC

3. Click **OK**. A **Modified Successfully** prompt is displayed. Click **OK**.

Step 4 Configure TID.

- Configure RTP TID.

1. In the navigation bar, choose **Voip > H.248 > TID Configuration**. The **TID Configuration** interface is displayed.

2. In the **RTP TID Configuration** area, configure related items, as shown in Figure 10-53.

- Max num: 16
- Prefix: rtp/
- Number max length: 1
- Number start: 0

Figure 10-53 Configuring RTP TID

RTP TID Configuration		
Max Num :	<input type="text" value="16"/>	*(Less than 2 times of the port number)
Prefix :	<input type="text" value="rtp/"/>	
Number Max Length :	<input type="text" value="1"/>	*(1~16)
Number Start :	<input type="text" value="0"/>	*(0~20000000)

3. Click **OK**. A **Modified Successfully** prompt is displayed. Click **OK**.

- Configure POTS TID.

1. In the **POT TID Configuration** area, configure related items, as shown in Figure 10-54.

-TID mode: handy

Figure 10-54 Configuring POT TID

POT TID Configuration	
TID Mode :	<input type="text" value="Handy"/>

2. Click **OK**. A **Modified Successfully** prompt is displayed. Click **OK**.

3. In the **POTS TID manual mode configuration list** area, click  corresponding to port 1 to enter the modification interface.

4. Configure related items, as shown in Figure 10-55.

-Name: 1


Figure 10-55 Configuring POTS TID in manual mode

POTS TID manual mode configuration modification	
port	<input type="text" value="1"/>
Name :	<input type="text" value="1"/> *(1-32)

5. Click **OK**. A **Modified Successfully** prompt is displayed. Click **OK**.

Step 5 Configure port status.

1. In the navigation bar, choose **Voip > H.248 > Port Status**. The **Port Status** interface is displayed.

2. Click  corresponding to port 1 to enter the modification interface.

3. Configure related items, as shown in Figure 10-56.

- Port State: ON

Figure 10-56 Port State Modify interface

Port State Modify	
port	<input type="text" value="1"/>
Port State	<input checked="" type="radio"/> ON <input type="radio"/> OFF

4. Click **OK**. A **Modified Successfully** prompt is displayed. Click **OK**.

Step 6 Configure the line.

1. In the navigation bar, choose **Voip > Line**. The **Line Configuration** interface is displayed.

2. Configure related items, as shown in Figure 10-40.

- DTMF transmission mode: transparent
- Initial timing: 10s
- Long timing: 20s
- Short timing: 5s
- DIGITMAP matching way: max
- Busy tone timing: 40s
- Push hang sound timing: 60s
- Ringing timeout timing: 60s

Figure 10-57 Line Configuration interface for H.248

Line Configuration		
DTMFTransmission Mode	<input type="text" value="Transparent"/>	<input type="button" value="v"/>
Initial timing	<input type="text" value="10"/>	Seconds*(1~255)
Long Timing	<input type="text" value="20"/>	Seconds*(1~255)
Short Timing	<input type="text" value="5"/>	Seconds*(1~255)
DIGITMAPMatching Way	<input type="text" value="max"/>	<input type="button" value="v"/>
Busy Tone Timing	<input type="text" value="40"/>	Seconds*(1~100)
Push Hang Sound Timing	<input type="text" value="60"/>	Seconds*(1~100)
Ringing Timeout Timing	<input type="text" value="60"/>	Seconds*(1~100)

3. Click **OK**. A **Modified Successfully** prompt is displayed. Click **OK**.

4. In the **Port Configuration** area, click  corresponding to port 1 to enter the modification interface.

5. Configure related items, as shown in Figure 10-58.

- Echo cancellation: ON
- Silence suppression: ON
- Comfort noise: ON

Figure 10-58 Line Configuration Modify for H.248

Line Configuration Modify	
Port	<input type="text" value="1"/>
CODEC	<input type="text" value="G711A"/> ▼
Echo Cancellation	<input checked="" type="radio"/> ON <input type="radio"/> OFF
Silence Suppression	<input checked="" type="radio"/> ON <input type="radio"/> OFF
Comfort noise	<input checked="" type="radio"/> ON <input type="radio"/> OFF

Step 7 Configure the MG.

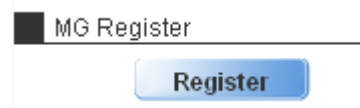
- In the navigation bar, choose **Voip > H.248 > MG Configuration**. The **MG Configuration** interface is displayed.
- Configure related items, as shown in Figure 10-59.
 - Local name: headquarter LAVA
 - CODEC: text
 - Registered way: IP address
 - Transport port: 2944
 - Heart beat detection mode: ITO way
 - Heartbeat cycle: 60s
 - Heartbeat timeout count: 3
 - Max wait delay: 180s

Figure 10-59 MG Configuration interface

MG Configuration	
Status	<input type="text" value="Log_out"/>
Local Number	<input type="text" value="Primary MGC"/>
CODEC	<input type="text" value="Text"/> ▼
Registered way	<input type="text" value="IP Address"/> ▼
Transport Port	<input type="text" value="2944"/> *(1~65535)
Heart Beat Detection Mode	<input type="text" value="ITO Way"/> ▼
Heartbeat Cycle	<input type="text" value="60"/> *(10~43200)Seconds
Heartbeat Timeout Count	<input type="text" value="3"/> *(1~100)time
Heartbeat Wait Delay	<input type="text" value="180"/> *(0~1200)Seconds

- Click **OK**. A **Modified Successfully** prompt is displayed. Click **OK**.
- Click **Register**, as shown in Figure 10-60.

Figure 10-60 MG Register area



Step 8 After configurations are complete, click **Save Config** to save configurations.

Configure the LAVA in the branch in the same way.

Configuring H.248-based VoIP phone is complete.

Checking configurations

The headquarter and branch can make calls with each other.

11 Security configurations

This chapter describes how to configure security on the **Security** interface, including the following sections:

- Firewall
- Web Filter
- Access control
- IPv6 AC
- MAC filter
- ARP prevent
- Anti-DDoS
- Configuration examples

11.1 Firewall

Scenario

A firewall prevents unauthorized access to the protected network from the Internet, and also allows internal users to access Web pages or receive and send Email on the Internet. It also works as an authority control gateway, such as allowing internal specified hosts to access the Internet.

The firewall not only controls Internet connections, but also protects mainframe and key resources (such as data). The access to protected data is filtered by the firewall, even the access is by internal users.

The security level of the firewall is high, medium, and low. You can enable or disable it and configure its security level.

Configuration steps

Step 1 In the navigation bar, choose **Security > Security > Firewall**. The **Firewall** interface is displayed.

Step 2 Enable/Disable the firewall.

If you enable the firewall, configure require items including security level, and then click **OK**.

Step 3 After configurations are complete, click **Save Config** to save configurations.



Note

For detailed security level definitions, see the note in the **Firewall Configuration** area.

Configuration items

Table 11-111 Configuration items on the Firewall interface

Configuration item	Description
Firewall Configuration	Enable/Disable firewall.
Security Level	Three security levels are available: <ul style="list-style-type: none"> • low • medium • high

11.2 Web Filter

Web Filter

This interface contains the following areas:

- Filter Type Set

The LAVA supports filtering domain name by blacklist/whitelist. This method filters the name of the head domain in the HTTP request, and matches it with configured filtering rules. Then it determines whether to permit or deny the HTTP request. You can configure domain name rules, and resolute the IP address of the domain name, and filter the IP address.

- URL Keywords Filter

This method filters keys words in the URL to prevent users from accessing web sites complying with key words.

- HTTP Protocol Verify

This method checks HTTP correctness and prevents non-HTTP. To prevent non-HTTP applications which use the port 80, you can use this method.

- Max Length of URL Set

This method limits the length of the URL in the HTTP request head, and prevents the request with over long URL.

- Type of HTTP response file.

In the HTTP head, there is a type called Content-type. It is used to specify the media type of the entity sent to the receiver. You need to configure the type of files (extension name) to be blocked. If the type is common, the system automatically blocks the HTTP media type. If the type is not common, you need to specify the corresponding HTTP media type. When the system receives a HTTP message with the Content-type entity head and the media type specified for blocking, the HTTP message will be discarded.

- Security Defend

If the format of HTTP response content is uncompressed or unencrypted HTML, it can be filtered by the LAVA, such as APPLET, OBJECT, and SCRIPT.

In addition, the LAVA supports filtering HTTP request with HTTP proxy, and filtering HTTP request or response with cookie.

Local update

You can download the blacklist/whitelist from the LAVA to the local PC or upload the blacklist/whitelist from the local PC to the LAVA.

11.2.2 Web Filter

Scenario

You can configure basic items and advanced items of web filtering by configuring URL and key words so that intranet users can access allowed web pages on the Internet.

Configuration steps

Configure basic items for Web filter as below:

- Step 1 In the navigation bar, choose **Security > Security > URL Filter > Web Filter**. The **Web Filter** interface is displayed.
- Step 2 Enable Web filter.
- Step 3 In the **Page Redirect Set** area, configure related items, and click **OK**.
- Step 4 In the **Filter Type Set** area, configure related items, and click **OK**.
- Step 5 In the **Add Filter Rule** area, configure related items, and click **OK**.
 - To delete a filtering rule, select it, and click **Delete**.
 - To delete all filtering rules, click **Select All**, and click **Delete**.
- Step 6 After configurations are complete, click **Save Config** to save configurations.



Note

If a filtering rule is deleted, it will be deleted from rules for the blacklist/whitelist.

Configure advanced items for Web filter as below:

- Step 7 In the navigation bar, choose **Security > Security > URL Filter > Web Filter**. The **Web Filter** interface is displayed.
- Step 8 Click **Advanced Options**.
- Step 9 In the **URL Keywords Filter** area, configure related items, and click **OK**.

To delete a keyword, double click it in the URL Keyword List.
- Step 10 In the **Filter Type Filter** area,
 - If the type to be filtered is in the list, select it.

- If the type to be filtered is not in the list, unselect **File Type Lists**, input the file type and content type, and click **Add**.
- To delete a type, double click it in the File Type Filter List.

Step 11 Configure related items, and click **OK**.

Step 12 After configurations are complete, click **Save Config** to save configurations.



Note

The format of Content-type entity head in HTTP messages is type/subtype;parameters. Filter type involves type and subtype parts only. The maximum length of file type is 15 characters, and the maximum type of HTTP media type is 31 characters. The system requires that file type be unique but one media type can be corresponding to multiple file types. The URL in HTTP request messages consists of three parts: host, interface name, and file path. The file path contains the file name and extension name. Thus, you can configure keywords to prevent accessing files with specified file extension name. However, the file extension name is not necessarily the actual file type.

Configuration items

Table 11-112 Configuration items on the Web Filter interface

Configuration item	Description
Web Filter	Enable/Disable web filtering.
Redirect URL	URL to be redirected to upon web access. The IE displays the Web pushing page for internal users, reminding users of access limit.
Filter Type Filter	Choose the whitelist or blacklist.
URL	Add the access control filtering rules. It is in a character string form, ranging from 1 to 99.
Delete Filter Rule	Support deleting one or all filtering rules.
URL Keywords Filter	Configure the URL keywords to be filtered. You can configure the extension name as a URL keyword to filter a type of files. For example, to filter GIF files, you can add ".gif" to the URL keyword filtering list.
File Type Filter	Configure the file type to be filter. For common file types, select them from the file type list. For others, add them by configuring the file type and multimedia type corresponding to the file type.
HTTP Protocol Verify	<ul style="list-style-type: none"> • ON: enable HTTP protocol verification. • OFF: disable HTTP protocol verification.
Max Length of URL Set	Configure the maximum length of URL upon HTTP request. The request with an over long URL is rejected. It is an integer ranging from 10 to 2048. By default, it is set to 1024.

Configuration item	Description
Security Defend	<p>Filter HTTP response content, including:</p> <ul style="list-style-type: none"> • SCRIPT: filter contents with script marks in HTML files sent back to the user. • OBJECT: filter contents with object marks in HTML files sent back to the user. • APPLET: filter contents with applet marks in HTML files sent back to the user. • PROXY: prevent HTTP proxy request. • COOKIE: clear cookie head entity in HTTP request and response. <p>The prevented content contains HTTP response with specified marks, or the HTTP response contains HTTP head entity of specified type. Content filtering is valid for uncompressed and unencrypted HTML files.</p>
Time Range for URL Filter	<ul style="list-style-type: none"> • Always: filter web always. • Select Time: filter web during specified time.

11.2.3 Local update

Scenario

You can import or export the blacklist/whitelist on this interface. Namely, you can download the blacklist/whitelist from the LAVA to the local PC or upload the blacklist/whitelist from the local PC to the LAVA.

Configuration steps

Import the blacklist/whitelist as below:

- Step 1 In the navigation bar, choose **Security > Security > URL Filter > Local Update**. The **Local Update** interface is displayed.
- Step 2 Click **Browse** to choose a blacklist/whitelist.
- Step 3 Click **Upload** to upload it to the system.
After uploading is complete, the system will prompt with "Operation Success!".
- Step 4 Click **OK**.
- Step 5 After configurations are complete, click **Save Config** to save configurations.



Note

The blacklist/whitelist file to be uploaded must obey the following rules:

- Only TXT files are supported.
- Only one rule can be created in each line, and the rule is a complete domain name without spaces.
- The last line must be empty.
- You can view contents of the blacklist/whitelist in the **Delete Filter Rule** area from **Security > Security > URL Filter > Web Filter**.

Export the blacklist/whitelist as below:

Step 6 In the navigation bar, choose **Security > Security > URL Filter > Local Update**. The **Local Update** interface is displayed.

Step 7 Click **Download**.

The system displays a prompt, prompting you to choose a path to save the file.

Step 8 Choose a path, and click **Save**.

Step 9 After configurations are complete, click **Save Config** to save configurations.

Configuration items

N/A

11.3 Access control

11.3.1 Policy of access control

Scenario



You can allow or permit other devices in a specified internal IP address segment to access the specified port by period or protocol. Configure policies of access control in two parts:

- Security policy: filter by combination of source interface, source address name, destination interface/security domain, destination address name, service, and time object.
- Connection count: with above filtering, limit total connections or host connections. Limit on total connections can be by destination address or source address.

Configuration steps

Step 1 In the navigation bar, choose **Security > Security > Access Control > Policy of Access Control**. The **Policy of Access Control** interface is displayed.

Step 2 View configured policies.

- To modify a configured item, click  to enter the modifying interface.
- To add an item, click **Add** to enter the adding interface.
- To delete an item, click the corresponding .

Step 3 On the adding or modifying interface, configure required item, and click **Submit**.

Step 4 After configurations are complete, click **Save Config** to save configurations.

Configuration items

Table 11-113 Configuration items on the Policy of Access Control interface

Configuration item	Description
Source Interface	Configure the ingress interface of packets to be controlled. You can specify an interface. The value any indicates all interfaces.
Source Address Name	Configure the range of source IP addresses of packets to be controlled. You can use a defined address object or address object group. The value any indicates any source addresses.
Destination Interface	Configure the egress interface of packets to be controlled. You can specify an interface. The value any indicates all interfaces.
Destination Address Name	Configure the range of destination IP addresses of packets to be controlled. You can use a defined address object or address object group. The value any indicates any destination addresses.
Service	Configure the packet type of interface of packets to be controlled. The value any indicates any service.
Time Object	Policy validation time. You can use a configured time object. The value always indicates all time.
State of Security Policy	<ul style="list-style-type: none"> • On: the policy takes effect. • Off: the policy does not take effect.
Mode	Execute the following actions for packets compliant with matching conditions: <ul style="list-style-type: none"> • PERMIT: permit these packets to pass. • DENY: deny these packets to pass.
Total Connection Count	Limit on the total connections matching the current polices, ranging from 10 to 65535
Host Connection Count	<ul style="list-style-type: none"> • Source address: limit on the host connections matching the policy in source direction • Destination address: limit on the host connections matching the policy in destination direction
Log of Traffic	Enable/Disable traffic logs.
Description	Describe the policy.

11.3.2 Time object

Scenario

Configure the time object for access control so that you can perform access control over packets by period. The time object is a specified time range. As a user's requirement, some access control rules take effect in one or more specified periods and do not filter packets in other periods. In this case, you can configure one or more periods and use the time object upon configuring access control rules, thus implementing access control based on time object.



Configure the time object as below:

- Absolute time object: allow access control between a starting time and an end time.
- Period time object: allow access control on the specified days of a week.

Configuration steps

Step 1 In the navigation bar, choose **Security > Security > Access Control > Time Object**. The **Time Object** interface is displayed.

Step 2 View configured time objects.

- To modify a configured item, click  to enter the modifying interface.
- To add an item, click **Add** to enter the adding interface.
- To delete an item, click the corresponding .

Step 3 On the adding or modifying interface, configure required item, and click **Add**.

- To delete a time object, double-click it

Step 4 After configurations are complete, click **Save Config** to save configurations.



Note

- You can create up to 20 time objects. A periodical time object can be configured with up to 20 periods.
- When you modify a time object, its name cannot be modified.

Configuration items

Table 11-114 Configuration items on the Time Object interface

Configuration item	Description
Name	Name of a time object
Description	Describe the time object.
Week	Week days to take effect for the time object
Start time	Start time of the time object
End time	End time of the time object



Caution

- You must concurrently configure or not configure the start/end time and week. When you do not configure them, the access control policy takes effect in all hours.
- The start time should be earlier or equal to the end time.

11.3.3 Service object

Scenario

When configuring access control items, you may configure the service object. During system initialization, some famous service objects are created. If they cannot meet requirements, you can create more to customize access control.



The service object can be a combination of:

- TCP source port and destination port
- UDP source port and destination port
- ICMP type and code
- IP number
- All above

Configuration steps

Step 1 In the navigation bar, choose **Security** > **Security** > **Access Control** > **Service Object**. The **Service Object** interface is displayed.

Step 2 View configured service objects.

- To modify a configured item, click  to enter the modifying interface.
- To add an item, click **Add** to enter the adding interface.
- To delete an item, click the corresponding .

Step 3 On the adding or modifying interface, configure required item.

If the service object to be added is a combination of multiple protocols, click **Add** to add other service types.

To delete a service object, double-click it.

Step 4 Click **Submit** to save it or **Back** to cancel it.

Step 5 After configurations are complete, click **Save Config** to save configurations.



Note

The system-defined famous service objects cannot be modified. The maximum number of services objects is 200, including these famous service objects.

Configuration items

Table 11-115 Configuration items on the Service Object interface

Configuration item	Description
Name	Name of a service object
Description	Describe the service object.

Configuration item	Description
Protocol	Type of protocol, used to conduct access control over packets, including TCP, UDP, ICMP, and IP
Source Port Number	Range of the source port number for TCP or UDP only, ranging from 1 to 65535
Destination Port Number	Range of the destination port number for TCP or UDP only, ranging from 1 to 65535
Type	Specify the type of ICMP packets, and configure it only when the protocol is ICMP, ranging from 1 to 255.
Code	Specify the message code of ICMP packets, and configure it only when the protocol is ICMP, ranging from 1 to 255.
Protocol number	Number of IP packets. Configure it only when the protocol is IP.

11.3.4 Address object

Scenario

When configuring access control, you may configure IP address object. Through IP address object, the system uniformly manages network sessions to be filtered.

The address object can be a single host address, network segment address, MAC address, MAC address range, or a combination of them.

Configuration steps

Step 1 In the navigation bar, choose **Security > Security > Access Control > Address Object**. The **Address Object** interface is displayed.

Step 2 On the adding or modifying interface, configure required item.

If the address object to be added is a combination of multiple address types, click **Add** to add other address types.

To delete a service object, double-click it.

Step 3 After configurations are complete, click **Save Config** to save configurations.



Note

- When you modify an address object, its name cannot be modified.
- You can configure up to 512 IP address objects.

Configuration items

Table 11-116 Configuration items on the Address Object interface

Configuration item	Description
Name	Name of a service object
Description	Describe the service object.
Type of Node	<ul style="list-style-type: none"> • Host: IP address of a single host as the address object • Subnet/Mask: a network segment as the address object • MAC address: a MAC address as the address object • Scope: a range of IP addresses as the address object
Host	IP address of the host, configured only when you choose Host in the Type of Node drop-down list
Subnet/Mask	Subnet information for the address object, configured only when you choose Subnet/Mask in the Type of Node drop-down list
MAC address	MAC address for the address object, configured only when you choose MAC address in the Type of Node drop-down list
Scope	Range of IP addresses of PCs to be controlled in the LAN, configured only when you choose Scope in the Type of Node drop-down list



11.4 IPv6 AC

11.4.1 IPv6 policy of access control

Scenario

You can configure IPv6 access control policy on this interface.

Configuration steps

- Step 1 In the navigation bar, choose **Security > Security > IPv6 AC**. The **IPv6 Policy of Access Control** interface is displayed.
- Step 2 View configured policies.
 - To modify a configured item, click  to enter the modifying interface.
 - To add an item, click **Add** to enter the adding interface.
 - To delete an item, click the corresponding .
- Step 3 On the adding or modifying interface, configure required item, and click **Submit**.
- Step 4 After configurations are complete, click **Save Config** to save configurations.

Configuration items

Table 11-117 Configuration items on the IPv6 Policy of Access Control interface

Configuration item		Description
Source_interface /security_domain		Configure the ingress interface of packets to be controlled. You can specify an interface. The value any indicates all interfaces.
Type of Node		Configure the source IP address range/subnet address of the packet to be controlled. <ul style="list-style-type: none"> • Subnet/mask • Scope
Source Address		When the "Type of Node" is set to Subnet/mask, enter the source subnet address. It is in dotted decimal notation, such as 192.168.1.1/24.
Scope		When the "Type of Node" is set to Scope, enter the source IP address RANGE. It is in dotted decimal notation.
Destination_interface /security_domain		Configure the egress interface of packets to be controlled. You can specify an interface. The value any indicates all interfaces.
Type of Node		Configure the destination IP address range/subnet address of the packet to be controlled. <ul style="list-style-type: none"> • Subnet/mask • Scope
Destination Address		When the "Type of Node" is set to Subnet/Mask, enter the destination subnet address. It is in dotted decimal notation, such as 192.168.1.1/24.
Scope		When the "Type of Node" is set to Scope, enter the destination IP address RANGE. It is in dotted decimal notation.
TC domain		Type of traffic, similar with the TOS domain in IPv4, ranging from 0 to 255
Flow label domain		Identifying packets of a specified flow for later distinguish on the network layer, ranging from 0 to 1 048 575
Rate Limit		Configure the limited rate of access control.
Security strategy state		<ul style="list-style-type: none"> • Enable: enable the policy. • Disable: disable the policy.
Mode	PERMIT	Permit packets complying with policies to pass. <ul style="list-style-type: none"> • TC domain for mark: for matching TC domain, ranging from 0 to 255 • Flow label domain for mark: for matching flow label domain, ranging from 0 to 1 048 575 • Priority Queuing: high, second, normal, and low
	DENY	Deny packets complying with policies of passing.

11.5 MAC filter


Scenario

By configuring filtering parameters for the MAC address, you can conduct access control over users to access the enterprise intranet.

MAC address filtering includes:

- Ethernet frames with Non-IP packet encapsulation
- Ethernet frames with a multicast address as the destination address
- Ethernet frames with a source or destination MAC address which matches configured MAC filtering rules

Configuration steps

- Step 1 In the navigation bar, choose **Security > Security > MAC Filter**. The **Filter MAC Address** interface is displayed.
- Step 2 Configure related items, and click **OK**.
- Step 3 In the **List of MAC Address** area, view configured MAC addresses.
- To add an item, click **Add** to enter the adding interface.
 - To delete an item, click the corresponding .
- Step 4 On the adding interface, configure required item.
- Step 5 After configurations are complete, click **Save Config** to save configurations.

Configuration items

Table 11-118 Configuration items on the MAC Filter interface

Configuration item	Description
Enable Switch	Enable/Disable MAC address filtering.
Type of Filter	After you enable MAC address filtering, you can choose: <ul style="list-style-type: none"> • Allow to access external network • Not allow to access external network
MAC address	MAC address to be filtered

11.6 ARP prevent

11.6.1 Prevent ARP attack

Scenario

By forging IP addresses and MAC addresses for ARP spoofing, attackers can generate enormous ARP traffic and makes network congested. By continuously sending forged ARP response packets, attackers can change the ARP cache of the destination host, causing network failure or intermediate attacks.

Under ARP attacks, a PC may encounter the following phenomena:

- It fails to access to the network.
- ARP packets increasing sharply.
- The MAC address is abnormal or incorrect.
- A MAC address corresponds to multiple IP addresses.
- The IP address conflicts with others.

Configuration steps

- Step 1 In the navigation bar, choose **Security > Security > ARP Prevent > Prevent ARP Attack**. The **Prevent ARP Attack** interface is displayed.
- Step 2 Configure related items, and click **OK**.
- Step 3 After configurations are complete, click **Save Config** to save configurations.

Configuration items

Table 11-119 Configuration items on the Prevent ARP Attack interface

Configuration item	Description
Prevent ARP Flood	<ul style="list-style-type: none"> • Enable: enable ARP flood protection. • Disable: disable ARP flood protection.
ARP Flooding Threshold	In unit of packet/second, being 300 by default, ranging from 10 to 10000. If a host sends packets to the host with a higher rate than this value, this is taken as flood attack.
Attack Host Inhibition Time	In unit of second, being 60 by default, ranging from 10 to 65535. If the LAVA encounters flood attack, it stops receiving packets from the host.



11.6.2 Active protection

Scenario

You can configure active protection list on this interface.

- If you enable active protection, the LAVA sends free packets with the source IP address as the interface IP address and the source MAC address as the interface MAC address.
- If you add an active protection list, the LAVA sends free packets with the source IP address as the specified IP address and the source MAC address as the specified MAC address.

Configuration steps

- Step 1 In the navigation bar, choose **Security > Security > ARP Prevent > Active Protection**. The **Active Protection** interface is displayed.
- Step 2 Configure required item and click **OK**.
- Step 3 View configured active protection items.
- To modify a configured item, click  to enter the modifying interface.
 - To add an item, click **Add** to enter the adding interface.
 - To delete an item, click the corresponding .
- Step 4 On the adding or modifying interface, configure required item, and click **Add**.
- Step 5 After configurations are complete, click **Save Config** to save configurations.

Configuration items

Table 11-120 Configuration items on the Active Protection interface

Configuration item	Description
Active Protection	Enable/Disable active protection.
ARP Broadcast Interval	Interval for ARP broadcast packets, in unit of millisecond, being 1000 by default, ranging from 100 to 10000 Configure it only when the active protection is enabled. The system sends free ARP packets by configured interval according to the configured active protection list and IP address.
Interface	Enable the interface with active protection.
Protection Interface	Enable/Disable interface protection.
Protection List	<ul style="list-style-type: none"> • IP address: IP address to be specified to the protection list • MAC address: MAC address to be specified to the protection list



Note

The packets in the active protection list are as below:

- Ethernet head: send packets with the source MAC address as the interface or configured MAC address in the active protection list, and with the MAC address as FF:FF:FF:FF:FF:FF.
- ARP packets: packets with the source IP/MAC address as the interface or configured IP/MAC address in the active protection list, and with the MAC address as 00:00:00:00:00:00.

11.6.3 IP-MAC bind



Scenario

To bind the IP address and the MAC address is important to prevent IP address spoofing and ARP spoofing attacks. The character of these attacks is that the IP address of the attacker and the MAC address do not logically match. For example, a host uses its IP address but not its MAC address to broadcast ARP packets or a host uses its MAC address but spoofs others' IP address for communication.

Before binding the IP address and the MAC address, master the actual mapping between them. If the mapping changes, update configurations accordingly; otherwise, service may run improperly.

The binding with this function is static, and fits for static IP addresses. Thus it does not fit for dynamic IP addresses; otherwise, communication may be interrupted.

Configuration steps

- Step 1 In the navigation bar, choose **Security > Security > ARP Prevent > IP-MAC Bind**. The **IP-MAC Bind** interface is displayed.
- Step 2 Configure required item and click **OK**.
- Step 3 View configured bound items.
 - To modify a configured item, click  to enter the modifying interface.
 - To add an item, click **Add** to enter the adding interface.
 - To delete an item, click the corresponding .
- Step 4 On the adding or modifying interface, configure required item, and click **Add**.
- Step 5 After configurations are complete, click **Save Config** to save configurations.

Configuration items

Table 11-121 Configuration items on the IP-MAC Bind interface

Configuration item	Description
Auto Learning	Enable/Disable auto learning. Enabling it is recommended. If you need to disable it, configure the binding between the IP address and the MAC address in advance.
Name	Name of the IP-MAC binding
IP address	Bound IP address. If you use an IP address in multiple bindings, the last binding overrides previous ones.
MAC address	Bound MAC address. When the unique check is disabled, a MAC address can be bound with multiple IP addresses.

Configuration item	Description
Unique Check	<ul style="list-style-type: none"> • Enable: a MAC address can be bound with only one IP address. • Disable: a MAC address can be bound with multiple IP addresses

11.6.4 Custom contract

Scenario

You can configure customized sending of ARP packets from a specified interface.

Configuration steps

- Step 1 In the navigation bar, choose **Security > Security > ARP Prevent > Custom Contract**. The **Custom Contract** interface is displayed.
- Step 2 View the created packet sending policy.
- Step 3 Click **Edit** to enter the editing interface.
- Step 4 Configure related items, and click **OK** to submit or **Cancel** to cancel editing.
- Step 5 After configurations are complete, click **Save Config** to save configurations.

Configuration items

Table 11-122 Configuration items on the Custom Contract Configuration Information interface

Configuration item	Description
Operation	<ul style="list-style-type: none"> • ON: enable customized packet sending. • OFF: disable customized packet sending.
Direction	<ul style="list-style-type: none"> • Request: send request packets. • Reply: send reply packets.
Source IP	Customize the source IP address for sending packets.
Destination IP	Customize the destination IP address receiving sending packets.
Source MAC	Customize the source MAC address for sending packets. By default, it is 00:00:00:00:00:00.
Destination MAC	Customize the destination MAC address for receiving packets. By default, it is 00:00:00:00:00:00.
Contract number	Number of times for sending packets, being 1 by default, ranging from 1 to 1000
Time Interval	Interval for sending packets, in unit of second, being 1 by default, ranging from 1 to 10
Send Interface	Configure the interface for sending packets.



Rules for the customized packets for sending are as below:


- The source MAC address and destination MAC address in the Ethernet head and ARP packets are the configured MAC address of customized packets.
- The source IP address and destination IP address of ARP packets are the configured IP address of customized packets

11.6.5 ARP table

Scenario

After resolution of the destination MAC address through ARP, the LAVA adds a mapping entry of an IP address and an MAC address for later forwarding packets to the same destination. The ARP table contains ARP entries of the LAVA.

Configuration steps

- Step 1 In the navigation bar, choose **Security > Security > ARP Prevent > ARP Table**. The **ARP Table** interface is displayed as below.
- Step 2 View all ARP entries.
- Step 3 To delete a configured item, click the corresponding . The system prompts you with a confirmation dialog box.
- Step 4 Click **OK**.

Configuration items

N/A

11.6.6 Monitor

Scenario

You can view ARP flood attacks on this interface.

Configuration steps

- Step 1 In the navigation bar, choose **Security > Security > ARP Prevent > Monitor**. The **Monitor** interface is displayed as below.
- Step 2 View flood and spoofing attacks.

Configuration items

N/A

11.7 Anti-DDoS

Scenario

Packets are transmitted on the internet through TCP/IP. They are harmless; however, excessive packets cause a Network Element (NE) or server to be overloaded. In addition, the attacker takes use of defects of some protocols or applications to manually create incomplete or abnormal packets, so the NE or server have to take much longer time to process them and consume too much system resources. In this case, the NE or server fails to respond to normal services in time.

Anti-DDoS attack can prevent DDoS attacks, abnormal packet attacks, and scanning attacks. By configuring anti-DDoS attack, the server can prevent DDoS attacks on the CPU and keep operating properly upon DDoS attacks.

Configuration steps

- Step 1 In the navigation bar, choose **Security > Security > DDoS Prevent**. The **Anti-DDoS** interface is displayed.
- Step 2 Configure required item, and click **OK**.
- Step 3 After configurations are complete, click **Save Config** to save configurations.

Configuration items

Table 11-123 Configuration items in the DDoS Attack Defence area

Configuration item	Description
Attack Type	Type of packets to be defended with, including SYN Flood, TCP Flood, DNS Flood, UDP Flood, and ICMP Flood
Defend Action	Defend action upon attack: discard packets.
Threshold	Threshold for link rate upon flood attacks. For SYN Flood and TCP Flood packets, the unit is set to half-connection/second. For other packets, the unit is set to connection/second. It ranges from 400 to 60000 and is set to 2000 by default.

Table 11-124 Configuration items in the Abnormal Packet Attack Defence area

Configuration item	Description
Jolt2	Enable/Disable Jolt2 attack detection.
Land-Base	Enable/Disable Land-Base attack detection.
PING of death	Enable/Disable PING of death attack detection.
TCP flag	Enable/Disable TCP flag attack detection.
Tear Drop	Enable/Disable Tear Drop attack detection.

Configuration item	Description
Winnuke	Enable/Disable Winnuke attack detection.
Smurf	Enable/Disable Smurf attack detection.
ICMP Redirect	Enable/Disable ICMP Redirect attack detection.

Table 11-125 Configuration items in the Scan Attack Defence area

Configuration item	Description
TCP scan	Detect TCP packets.
UDP scan	Detect UDP packets.
ICMP scan	Detect ICMP packets.
Scan Identify Threshold	Threshold of the link rate for scan attack defense, in unit of connection/second, being 1000 by default, ranging from 10 to 65535
Host Suppression Duration	Duration for stopping receiving packets from the attacking host, in unit of second, being 20 by default, ranging from 1 to 65535

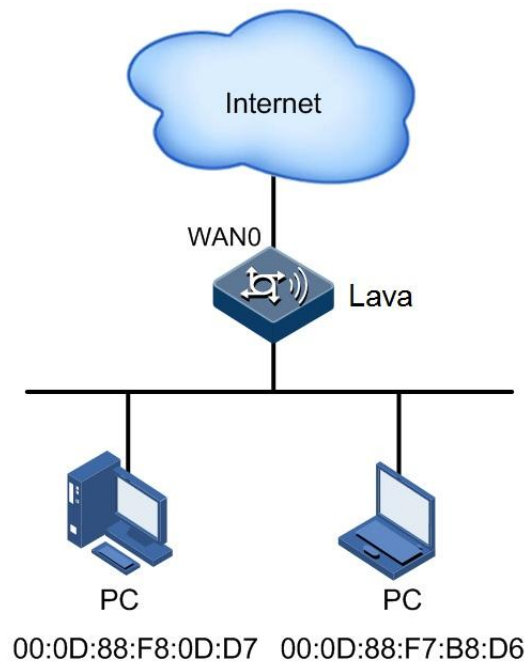
11.8 Configuration examples

11.8.1 Example for configuring MAC filter

Networking requirements

Internal users of an enterprise access the Internet through the LAVA, as shown in Figure 11-61. By configuring MAC filter, the LAVA forbids users with the MAC address 00:0D:88:F8:0D:D7 and 00:0D:88:F7:B8:D6 from accessing the Internet.

Figure 11-61 MAC filter application networking



Configuration steps

Step 1 In the navigation bar, choose **Security > Security > MAC Filter**. The **Filter MAC Address** interface is displayed.

Filter MAC Address

Function Set

Enable Switch On Off

Type of filter Allow access to external network Not allow access to external network

OK

List of MAC Address

	MAC Address
<input type="checkbox"/>	

Total 0 records, current is the 1 page, total 1 pages

First
Previous
Next
Last
Jump to page
Jump

Add
Delete

Step 2 Enable MAC filter and choose **Not allow access to external network**, and click **OK**.

Step 3 Click **Add** to enter the adding interface, as shown below.

Step 4 Configure the required items, and click **OK**.

Step 5 After configurations are complete, click **Save Config** to save configurations.

Checking configurations

The users with the MAC addresses 00:0D:88:F8:0D:D7 and 00:0D:88:F7:B8:D6 cannot access the Internet.

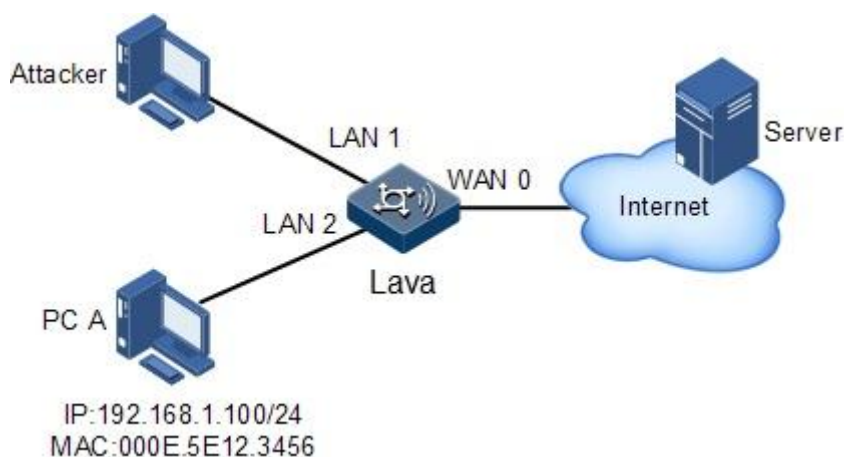
11.8.2 Example for configuring anti-ARP attack

Networking requirements

To prevent attackers from forging IP addresses or MAC addresses for ARP spoofing, configure anti-ARP attack, as shown in Figure 11-62. Detailed requirements are as below:

- Enable IP-MAC binding, and enable user uniqueness check. If one of the bound IP address and bound MAC address for packets received by the LAVA does not comply with the other, these packets are discarded.
- Configure the active protection list, and protect resources on the internal key PC A. By actively sending ARP information about PC A, the LAVA can prevent ARP spoofing.
- Enable anti-ARP attacks and active protection.

Figure 11-62 Anti-ARP attack application networking



Configuration steps

Step 1 Configure IP-MAC binding.

1. In the navigation bar, choose **Security** > **Security** > **ARP Prevent** > **IP-MAC Bind**. The **IP-MAC Bind** interface is displayed.

2. Enable auto-learning, click **Add** to enter the **IP-MAC Bind Configuration** interface, as shown in Figure 11-63.

Figure 11-63 Configuring IP-MAC binding

IP-MAC Bind Configuration

Name *

IP Address *(e.g.:192.168.1.1)

MAC Address *(e.g.:00:0E:5E:0E:0E:01)

Unique Check Enable Disable

3. Configure required item and click **OK**.

Step 2 Configure the active protection list.

1. In the navigation bar, choose **Security > Security > ARP Prevent > Active Protection**. The **Active Protection** interface.
2. Enable active protection, and click **Add** to enter the **Auto Protection Configuration** interface, as shown in Figure 11-64.

Figure 11-64 Configuring active protection

Auto Protection Configuration

Interface ▾

Prevent Interface ON OFF

Protection List

IP Address (e.g.:192.168.1.1)

MAC Address (e.g.:00:0E:5E:0E:0E:01)

3. Configure related items, click **Add**, and then click **OK**.

Step 3 Configure anti-ARP attack.

1. In the navigation bar, choose **Security > Security > ARP Prevent > Prevent ARP Attack**. The **Prevent ARP Attack** interface is displayed as below.

Prevent ARP Attack	Active Protection	IP-MAC Bind	Custom Contract	ARP Table	Monitor
--------------------	-------------------	-------------	-----------------	-----------	---------

Prevent ARP Flood

Prevent ARP Flood	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
ARP Flooding Threshold	<input type="text" value="300"/> (10-10000 Packets/Sec)
Attack Host Inhibition Time	<input type="text" value="60"/> (10-65535 Seconds)

2. Configure related items, and click **OK**.

Step 4 After configurations are complete, click **Save Config** to save configurations.

Checking configurations

If one of the bound IP address and bound MAC address for packets received by the LAVA does not comply with the other, these packets are discarded.

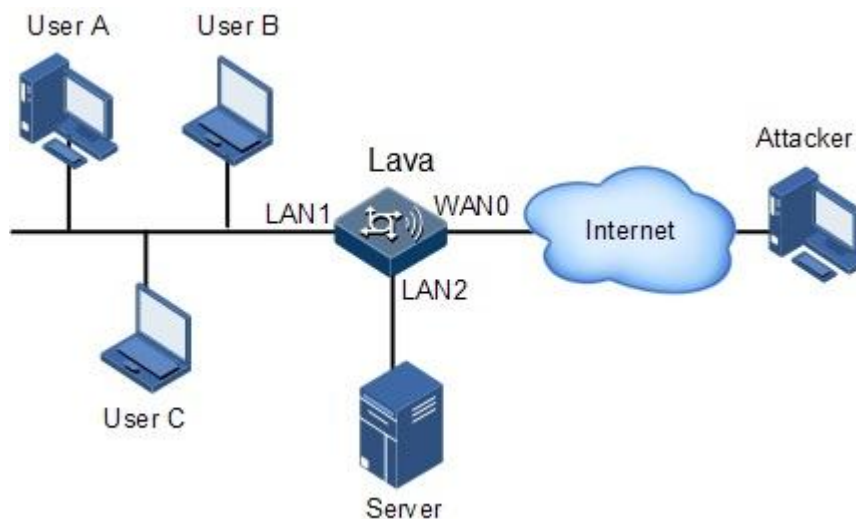
11.8.3 Example for configuring anti-DDoS attack

Networking requirements

Internal users User A, User B, and User C accesses the Internet through the WAN0 interface of the LAVA, as shown in Figure 11-65. To prevent flooding attacks, abnormal packet attacks, and scanning attacks on internal user from external malicious users, configure DDoS attack protection as below:

- Prevent Smurf attack, Land-base attack, and scanning attack.
- Prevent SYN Flood attack with a threshold of 4000 half-connection/second.
- Set the host suppression duration to 20s.

Figure 11-65 Anti-DDoS attack application networking



Configuration steps

Step 1 In the navigation bar, choose **Security > Security > DDoS Prevent**. The **Anti-DDoS** interface is displayed as below.

Figure 11-66 Configuring anti-DDoS attack

Anti-DDos

DDoS Attack Defence

Attack Type	Defend Action	Threshold	
<input type="checkbox"/> SYN Flood	Discard ▼	2000	(400-60000)half-connct/second
<input type="checkbox"/> DNS Flood	Discard ▼	2000	(400-60000)connct/second
<input type="checkbox"/> UDP Flood	Discard ▼	2000	(400-60000)connct/second
<input type="checkbox"/> ICMP Flood	Discard ▼	2000	(400-60000)connct/second

Abnormal Packet Attack Defence

<input type="checkbox"/> Jolt2	<input type="checkbox"/> Land-Base	<input type="checkbox"/> PING of death	<input type="checkbox"/> TCP flag
<input type="checkbox"/> Tear Drop	<input type="checkbox"/> Winnuke	<input type="checkbox"/> Smurf	<input type="checkbox"/> ICMP Redirect

Scan Attack Defence

<input type="checkbox"/> TCP Scan	<input type="checkbox"/> UDP Scan	<input type="checkbox"/> ICMP Scan
Scan Identify Threshold	1000	(10-65535 connct/second)
Host Suppression Duration	20	(1-65535 second)

OK

Step 2 Configure related items, and click **OK**.

Step 3 After configurations are complete, click **Save Config** to save configurations.

Checking configurations

Upon Land or Smurf attack, the LAVA discards these packets. It also discards the following packets which exceeds the threshold:

- SYN Flood packets
- TCP packets
- UDP packets
- ICMP packets

12 System configurations

This chapter describes how to configure the **System** interface, including the following sections:

- Reboot
- Administrator
- One key recovery
- Configuration file
- Software Update
- Diagnose tool
- NTP
- Session statistic
- Local Log
- SMTP server settings

12.1 Reboot

Scenario

When the LAVA is faulty, you can try to resolve the problem by rebooting it according to actual situations.



Caution

- Rebooting the LAVA will interrupt services. Use this method with care.
- Save configurations accordingly before reboot to avoid configuration loss.
- After rebooting the LAVA, you have to log in to it again.

Configuration steps

- Step 1 In the navigation bar, choose **System** > **Reboot**. The **Reboot** interface is displayed as below.
- Step 2 Click **Reboot**.
 - If you select **Save config**, the system saves current configurations, and then reboot itself.

- If you do not select **Save config**, the system directly reboot itself without saving configurations.

Configuration items

N/A



12.2 Administrator

12.2.1 Administrator

Scenario

You can modify user timeout time, enable or disable unique users, add, modify, delete, or view user information.

Configuration steps

- Step 1 In the navigation bar, choose **System > Administrator > Administrator**. The **Administrator** interface is displayed as below.
- Step 2 Configure the required item, and click **OK**.
- Step 3 View the user information list.
- To modify a configured item, click  to enter the modifying interface.
 - To add an item, click **Add** to enter the adding interface.
 - To delete an item, click the corresponding .
- Step 4 On the modifying or adding interface, configure related items, and click **OK**.
- Step 5 After configurations are complete, click **Save Config** to save configurations.

Configuration items

Table 12-126 Configuration items in the User Configuration area

Configuration item	Description
User Timeout	Configure the user timeout value. If no operation is performed when the value expires, the user exits the Web configuration interface automatically. It is in unit of minute, ranges from 1 to 480, and is set to 10 minutes by default.
Unique Users	Enable/Disable user uniqueness. After it is enabled, at some time, only one user of a user type is allowed to log in to the Web configuration interface.

Table 12-127 Configuration items on the Add Administrator interface


Configuration item	Description
Username	Configure the user name of the newly-added administrator.
User Permission	Configure the authority of the newly-added administrator. <ul style="list-style-type: none"> • Super Administrator • Ordinary Administrator • General User
User Type	Configure the type of the newly-added administrator. <ul style="list-style-type: none"> • Local User • Radius User • Ldap User
Password	You need to enter the password when the User Type is set to Local User. It is in a character string form, ranging from 5 to 38. We recommend that the password contains letters, digits, and special characters simultaneously.
Confirm Password	You need to enter the password again when the User Type is set to Local User.
Radius Server	You need to select a RADIUS server when the User Type is set to Radius User.
Ldap Server	You need to select a LDAP server when the User Type is set to Ldap User.
User Information	Describe the newly-added administrator.
User Status	Activate/Deactivate the newly added administrator.

12.2.2 Online administrator

Scenario

You can delete current online users, view authorities of current online users and those whose authorities are smaller than the ones of current online users.

Configuration steps

- Step 1 In the navigation bar, choose **System** > **Administrator** > **Online Administrator**. The **Online Administrator** interface is displayed as below.
- Step 2 View the online user list.
- Step 3 To delete a user, click the corresponding . The system prompts you with a confirmation dialog box. Click **OK**.

Configuration items

N/A

12.3 One key recovery

Scenario

One key recovery consists of:

- Recovery of factory settings: this clears all configurations, recovers to the factory settings (namely, default configuration status, including default Web login IP address, user name, and password), and reboots the LAVA.
- Recovery of installing configurations: this clears all configurations, and recovers to the saved installing configurations. If no installing configurations were done before, this recovers to the factory settings. Then, this reboots the LAVA.



Caution

- One key recovery will reboot the LAVA and interrupts services. Use this method with care.
- One key recovery loses all current configurations.
- After recovery, use the system IP address, user name, and password specified in the installing configuration file to log in. If no installing configurations were done before, use the default system IP address, user name, and password.

Configuration steps

- Step 1 In the navigation bar, choose **System > One Key Recovery**. The **One Key Recovery** interface is displayed as below.
- Step 2 Click **OK** in the **Restore Setup Configuration** or **Restore Factory Configuration** area to recover them respectively.

Configuration items

N/A

12.4 Configuration file

12.4.1 Saving configurations

Scenario

You can save configurations to the configuration file or the installation configuration file.

Configuration steps

- Step 1 In the navigation bar, choose **System > Configuration File > Save Configuration**. The **Save Configuration** interface is displayed.
- Step 2 Select **ON/OFF** in the **Auto Save Config** area.
- Step 3 Click **OK** in the **Save the current configuration** or **Save the installing configuration** area to save them respectively.

The system prompts you with a confirmation dialog box.

Step 4 Click **OK**.



Note

After auto saving is enabled, during the subsequent configuration process, the system will automatically save configurations when you click **OK**. Therefore, there is no need to click **Save Config**.

Configuration items

N/A

12.4.2 Importing and exporting configuration files

Scenario

You can update the configuration files by importing or exporting them on this interface.



Note

The configuration file to be imported has a ".con" suffix.

Configuration steps

Step 1 In the navigation bar, choose **System > Configuration File > Import and Export Configuration Files**. The **Import and Export Configuration Files** interface is displayed.

Step 2 Click **Browse** to choose a configuration file.

Step 3 Click **Upload** to upload the configuration file.

After uploading is complete, the system prompts a confirmation dialog box.

Step 4 Click **OK**.

Step 5 Click **Export** to save the configuration file to a path.

Configuration items

N/A

12.4.3 Uploading configuration file

Scenario

You can upload a configure file to the NView NNM system or the server for backup.

Configuration steps

Step 1 In the navigation bar, choose **System > Configuration File > Import and Export Configuration Files**. The **Import and Export Configuration Files** interface is displayed.

Step 2 Click **Upload** to send the configuration file to the Nview NNM system.

Step 3 Click **OK**.

Configuration items

N/A

12.5 Software Update

Scenario

Software update helps you obtain the system startup file from the local host.

System startup files consist of:

- Master version file: it is used to guide the system and start application programs.
- Slave version file: it is used to guide the system and start application programs when the master version file fails.

When the slave version file also fails, the system searches the CF card for available system startup file.

The system allows you to update the master version file and slave version file respectively. You should always keep them the same.



Note

- Save the system startup file to the local host for facilitate later use.
- The system startup file has a ".bin" suffix.

Configuration steps

Step 1 In the navigation bar, choose **System > Software Update**. The **Software Update** interface is displayed.

Step 2 Click **Browse** to choose a startup file for update.

Step 3 Click **Upload** to upload the startup file.

After uploading is complete, the system prompts a confirmation dialog box.

Step 4 Click **OK**.

Step 5 Reboot the LAVA.

The software update is complete.

Configuration items

N/A

12.6 Diagnose tool

12.6.1 Ping

Scenario

The PING is a network diagnosis tool and is used to detect whether the destination host is reachable and learn the link status.

Configuration steps

- Step 1 In the navigation bar, choose **System > Diagnose Tool > Ping**. The **Ping** interface is displayed.
- Step 2 Configure related items, and click **Start**.

The Ping operation takes a time. After it is complete, the result will be displayed, which helps you learn link status.

Configuration items

Table 12-128 Configuration items on the Ping interface

Configuration item	Description
Destination Address or Domain Name	Destination address or domain name used for Ping diagnostics
Packet Length	Size of packets sent for Ping diagnostics, ranging from 0 to 68807
Number of Packets	Number of packets sent for Ping diagnostics, ranging from 1 to 10
Source Address	Select the Source Address radio button to configure the source address of packets used for Ping diagnostics.
Outgoing Interface	Select the Outgoing Interface radio button to configure the egress interface of packets used for Ping diagnostics.

12.6.2 Tracert

Scenario

Similar with Ping, Traceroute is also a network diagnosis tool. It is used to detect whether the link between the sender and the destination is available and show faulty points if any.

Configuration steps

- Step 1 In the navigation bar, choose **System > Diagnose Tool > Tracert**. The **Tracert** interface is displayed.

Step 2 Configure related items, and click **Start**.

The Traceroute operation takes a time. After it is complete, the result will be displayed, which helps you learn link status.

Configuration items

Table 12-129 Configuration items on the Tracert interface

Configuration item	Description
Trace Route	Destination address or domain name used for Tracert diagnostics
UDP Port Probe	Enable/Disable UDP port probe.
UDP Port Number	Configure the ID of UDP port where UDP port probe is enabled. It ranges from 0 to 65535.

12.6.3 HTTP get

Scenario

The **http get** command is used to check connectivity to the specified HTTP server and helps you learn access right.

Configuration steps

Step 1 In the navigation bar, choose **System > Diagnose Tool > HTTP Get**. The **HTTP Get** interface is displayed.

Step 2 Configure related items, and click **Start**.

The operation takes a time. After it is complete, the result will be displayed.

Configuration items

Table 12-130 Configuration items on the HTTP Get interface

Configuration item	Description
Destination Address or Domain Name	Destination address or domain name used for HTTP Get diagnostics
Port	Configure the ID of the port used for HTTP Get diagnostics. It ranges from 1 to 65535 and is set to 80 by default.

12.6.4 DNS Query

Scenario

The DNS translates between the domain name and IP address.

To query the IP address corresponding to a domain name, use DNS Query.

Configuration steps

Step 1 In the navigation bar, choose **System > Diagnose Tool > DNS Query**. The **DNS Query** interface is displayed.

Step 2 Configure related items, and click **Start**.

The operation takes a time. After it is complete, the result will be displayed.

Configuration items

Table 12-131 Configuration item on the DNS Query interface

Configuration item	Description
Destination Domain Name	Domain name used for DNS Query diagnostics

12.6.5 TCP Query

Scenario

TCP Query is used to whether a TCP connection to the destination host can be established.

Configuration steps

Step 1 In the navigation bar, choose **System > Diagnose Tool > TCP Query**. The **TCP Query** interface is displayed.

Step 2 Configure related items, and click **Start**.

The operation takes a time. After it is complete, the result will be displayed.

Configuration items

Table 12-132 Configuration items on the DNS Query interface

Configuration item	Description
Destination Address or Domain Name	Destination address or domain name used for TCP Query diagnostics
Port Number	Configure the ID of the port where TCP Query diagnostics is enabled. It ranges from 0 to 65535.

Configuration item	Description
Number of Packets	Number of packets sent for TCP Query diagnostics, ranging from 1 to 10 and being 4 by default

12.7 NTP

12.7.1 NTP

Scenario

To make the LAVA cooperate with other NEs, you must configure system time correctly.

The Network Time Protocol (NTP) is used to configure the network clock source for automatic and periodical clock synchronization by the LAVA so that it is synchronized with the network clock source.

The LAVA also supports manual configuration of system time.

Configuration steps

- Step 1 In the navigation bar, choose **System** > **NTP**. The **NTP** interface is displayed.
- Step 2 Configure related items, and click **OK**.
- Step 3 After configurations are complete, click **Save Config** to save configurations.

Configuration items

Table 12-133 Configuration items on the NTP interface

Configuration item		Description
Current system time		Display current system time.
Time zone choices		Choose current time zone.
Automatic synchronization	Server	NTP server
	Recommend	List common time servers on the Internet.
	Synchronization	Period for time synchronization, in unit of minute, being 60 by default, ranging from 5 to 65535. The LAVA synchronizes time periodically with the NTP server.
Manually Set		Manually configure the system time.

12.8 Session statistics

12.8.1 Statistics monitor configuration

Scenario

You can start statistics monitoring to view statistics on this interface.

Configuration steps

- Step 1 In the navigation bar, choose **System > Session Statistics > Statistics Monitor Configuration**. The **Statistics Monitor Configuration** interface is displayed.
- Step 2 Configure related items, and click **OK**.
- Step 3 After configurations are complete, click **Save Config** to save configurations.

Configuration items

Table 12-134 Configuration items on the Statistics Monitor Configuration interface

Configuration item	Description
Enable Statistics Monitor	Enable statistics monitoring.

12.8.2 Real-time session statistics

Scenario

Realtime session statistics are for query realtime sessions, help you learn session usage, and temporarily block a session.

Configuration steps

- Step 1 In the navigation bar, choose **System > Session Statistics > Real-time Session Statistics**. The **Real-time Session Statistics** interface is displayed.
- Step 2 Configure related items, and click **Search**.
The result will be displayed according to search conditions.

Configuration items

Table 12-135 Configuration items on the Real-time Session Statistics interface

Configuration item	Description
Statistics Type	– Take statistics of realtime session under certain conditions, and display them in the list.

Configuration item		Description
	Source IP Statistics	Input the source IP address to be taken statistics of. If you leave it blank, the LAVA takes statistics of sessions of all source IP addresses.
	Destination IP Statistics	Input the destination IP address to be taken statistics of. If you leave it blank, the LAVA takes statistics of sessions of all destination IP addresses.
	Destination Port Statistics	Input the number of destination port to be taken statistics of, and choose protocols as below: <ul style="list-style-type: none"> • ALL • TCP • UDP

12.8.3 Real-time traffic statistics

Scenario

Traffic statistics are for monitoring network traffic. You can learn the users with over high or abnormal traffic on this interface.

Configuration steps

Step 1 In the navigation bar, choose **System** > **Session Statistics** > **Real-time Traffic Statistics**. The **Real-time Traffic Statistics** interface is displayed.

Step 2 Configure related items, and click **Search**.

The result will be displayed according to search conditions.

Configuration items

Table 12-136 Configuration items on the Real-time Traffic Statistics interface

Configuration item		Description
Statistics Type	–	Take statistics of realtime traffic under certain conditions, and display them in the list.
	Source IP Statistics	Input the source IP address to be taken statistics of. If you leave it blank, the LAVA takes statistics of traffics of all source IP addresses.
	Destination IP Statistics	Input the destination IP address to be taken statistics of. If you leave it blank, the LAVA takes statistics of traffics of all destination IP addresses.
	Destination Port Statistics	Input the number of destination port to be taken statistics of, and choose protocols accordingly.

12.9 Local Log

Scenario

You can query or clear local logs.



Caution

Before querying logs, enable the log server in advance and enable the corresponding type of logs. After logs are recorded, you can successfully query logs. For how to enable logging, see section 8.4 Syslog.

Configuration steps

Step 1 In the navigation bar, choose **System** > **Local log**. The **Local Log** interface is displayed.

Step 2 Choose the type, level, time range, and number of records of logs, and click **Search**.

This operation takes a time. After it is complete, the result will be displayed.

Step 3 To delete logs, choose the type, level, time range, and number of records of logs, and click **Clear Log**.

This operation allows you to clear logs of a specified type, period, and number of records.

Configuration items

Table 12-137 Configuration items on the Local Log interface

Configuration item	Description
Type	Support the following logs: <ul style="list-style-type: none"> • All logs • Equipment alarm log • Login log • Operation log • ARP attack log • DDoS log • URL filtering hit • Flow log
Level	Support the following levels: <ul style="list-style-type: none"> • All • Emergency • Alert • Critical • Error • Warning • Notice • Informational • Debug
Time range	The format is year-month-day hour:minute:second, such as 2010-04-19 01:02:03.

Configuration item	Description
Number of records	Number of logs displayed on each screen

12.10 SMTP server settings

Scenario

You can configure the SMTP server on this interface to support mail-based features.

Configuration steps

- Step 1 In the navigation bar, choose **System > SMTP Server**. The **SMTP Server Settings** interface is displayed.
- Step 2 Configure related items, and click **OK**.
- Step 3 Input an Email in the **Send a test message to** area, and click **Send**.
Check whether the mail account has received the test mail.
- Step 4 After configurations are complete, click **Save Config** to save configurations.

Configuration items

Table 12-138 Configuration items on the SMTP Server Settings interface

Configuration item	Description
SMTP Server	Uniform Resource Locator (URL) or IP address of the SMTP server
SMTP Server Port	Port number of the SMTP, ranging from 1 to 65535, and being 25 by default
This server need safety connection	Enable server security connection on the condition that the SMTP server supports security connection..
Sender E-Mail	Email for sending a mail, such as abc@123.com
Authentication	Enable user authentication of the sender Email.
SMTP user	Email user name
Password	Email password
Send a test message to	Send a test mail to the input Email box.

13 Typical configuration examples

This chapter provides typical configuration examples for the LAVA, including the following sections:

- Example for configuring Internet access for wired users
- Example for configuring Internet access for wireless users
- Example for configuring Internet access through 3G
- Example for configuring Web filtering
- Example for configuring Internet access for wired users in limited period
- Example for configuring EoIP
- Example for configuring the NAT virtual server
- Example for configuring route backup and sharing

13.1 Example for configuring Internet access for wired users

Networking requirements

PCs in a LAN of an enterprise access the Internet through the LAVA, as shown in Figure 13-67.

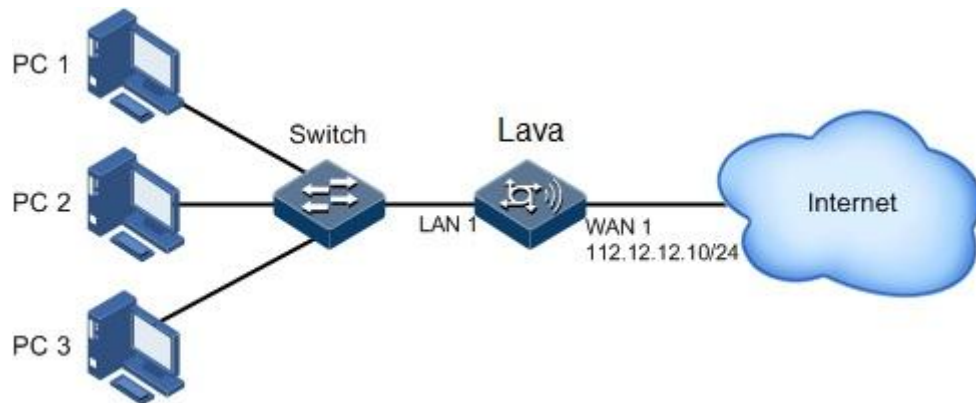
PCs are configured with the private address. With NAT of the LAVA, the private address is translated to the public address. Therefore, PCs can access to the network. PCs need to get the IP address through the DHCP Server (LAVA). The LAVA is taken as the DNS Proxy of PCs.

Configuration thoughts

Thoughts for configuring Internet access for wired users are shown as below:

- Configure the WAN interface.
- Configure the LAN interface.
- Enable DNS Proxy.

Figure 13-67 Networking application for Internet access from a LAN through the LAVA




Configuration steps

Step 1 Log in to the Web configuration interface.

For details, see section 1.2 Web mode.

Step 2 Configure the WAN interface.

1. In the navigation bar, choose **Basic > Interface > WAN**. The **WAN0 Configuration** interface is displayed.

2. Click  to enter the modification interface.

3. Configure related items, as shown in Figure 13-68.

Figure 13-68 Configuring the WAN0 interface

WAN0 Modify	
Connection Name:	<input type="text" value="1_Management_R_46"/>
Connection Mode:	<input type="text" value="Router Mode"/>
<input type="radio"/> DHCP	Choose this option to obtain an IP address automatically from your ISP.
<input checked="" type="radio"/> Static	Choose this option to set an static IP address provided by your ISP.
<input type="radio"/> PPPoE	Choose this option if your ISP use PPPoE(For most DSL users).
IP Address:	<input type="text" value="112.12.12.10"/> *(e.g. "10.12.1.2")
Subnet Mask:	<input type="text" value="255.255.255.0"/> *(e.g. "255.255.255.0")
Default Gateway:	<input type="text" value="112.12.12.1"/>
Primary DNS:	<input type="text" value="112.12.34.1"/>
Secondary DNS:	<input type="text" value="112.12.34.8"/>
Access Control:	<input checked="" type="checkbox"/> HTTPS <input checked="" type="checkbox"/> PING <input checked="" type="checkbox"/> TELNET <input checked="" type="checkbox"/> SSH <input checked="" type="checkbox"/> HTTP
Enable NAT	<input type="checkbox"/> NAT
Subinterface ID:	<input type="text" value="46"/> *[1-4095]
802.1p Priority:	<input type="text" value="0"/> [0-7]
MAC Address:	<input type="text" value="00:0e:5e:0e:4c:21"/> (XX:XX:XX:XX:XX:XX)
Service Type	<input type="text" value="Management"/>



Note

- The default gateway and IP address of the DNS server are provided by the carrier.

Step 3 Configure the VLAN interface.

- In the navigation bar, choose **Basic > Interface > LAN > VLAN Interface Configuration**. The **VLAN Interface Configuration** interface is displayed.
- Configure related items, as shown in Figure 13-69.

Figure 13-69 Configuring the VLAN interface

VLAN Interface Configuration	
VLAN:	vlan1
IP Address:	192.168.1.1 * (xxx.xxx.xxx.xxx)
Netmask:	255.255.255.0 * (xxx.xxx.xxx.xxx)
Management Access:	<input checked="" type="checkbox"/> HTTPS <input checked="" type="checkbox"/> PING <input checked="" type="checkbox"/> TELNET <input checked="" type="checkbox"/> SSH <input checked="" type="checkbox"/> HTTP
DHCP Server:	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Subnet	192.168.1.1 * (xxx.xxx.xxx.xxx)
Netmask:	255.255.255.0 * (xxx.xxx.xxx.xxx)
Start IP:	192.168.1.2 * (xxx.xxx.xxx.xxx)
End IP:	192.168.1.254 * (xxx.xxx.xxx.xxx)
Gateway Address:	192.168.1.1 (xxx.xxx.xxx.xxx)
Primary DNS:	192.168.1.1 (xxx.xxx.xxx.xxx)
Secondary DNS:	(xxx.xxx.xxx.xxx)
Reserved IP:	(max 8 IP, split by ',')
Lease Time:	2 Days 0 Hours 0 Minutes * (0 means indefinitely)

(*) Asterisk must be filled

OK



Note

Enable and then configure the DHCP server. Wherein, the gateway address, and IP address of the DNS server are the VLAN interface address.

Step 4 Enable DNS proxy.

1. In the navigation bar, choose **Basic > Network > DNS > DNS Configuration**. The **DNS Configuration** interface is displayed.
2. Choose **ON**, and then click **OK**.

Figure 13-70 Configuring DNS proxy

DNS Proxy	
DNS Proxy	<input checked="" type="radio"/> Enable <input type="radio"/> Disable

Step 5 After configurations are complete, click **Save Config** to save configurations.

Checking configurations

After being configured to **Obtain an IP address automatically**, the PC can access the Internet.

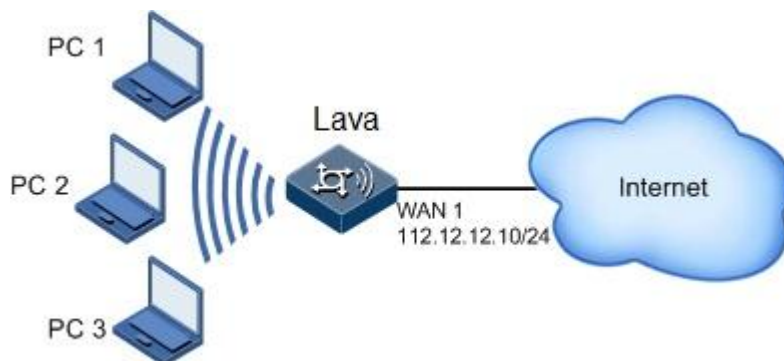
13.2 Example for configuring Internet access for wireless users

Networking requirements

Wireless users access the Internet by using WiFi through the LAVA, as shown in Figure 13-71.

PCs are configured with the private address. With NAT of the LAVA, the private address is translated to the public address. Therefore, PCs can access to the network. PCs need to get the IP address through the DHCP Server (LAVA). The LAVA is taken as the DNS Proxy of PCs.

Figure 13-71 Networking with Internet access from a WLAN through the LAVA



Configuration thoughts

Thoughts for configuring Internet access for wireless users are shown as below:

- Configure the WAN interface.
- Configure the VLAN interface.
- Configure the WLAN interface.
- Enable wireless status.
- Enable DNS Proxy.

Configuration steps

Step 1 Log in to the Web configuration interface.

For details, see section 1.2 Web mode.

Step 2 Configure the WAN interface.


For details, see section 13.1 Example for configuring Internet access for wired users.

Step 3 Configure the VLAN interface.

For details, see section 13.1 Example for configuring Internet access for wired users.

Step 4 Configure the WLAN interface.

1. In the navigation bar, choose **Basic > Interface > WLAN > Basic Configuration**. The **Basic Configuration** interface is displayed.

2. Click  corresponding to SSID-0001 to enter the modification interface.

3. Configure related items, as shown in Figure 13-72.

Figure 13-72 Modifying basic WLAN configurations

Modify Basic WLAN Configuration	
Network Name(SSID)	SSID-0001 (31 characters)
Address Mode	VLAN Binding
VLAN	vlan1 (VLAN created in LAN configuration!)
SSID Hide	<input type="checkbox"/>
WMM	<input type="checkbox"/>
AP Isolation	<input type="checkbox"/>
SSID Rate	auto
Beacon Interval	100 (40– 1000)
DTIM Interval	1 (1– 31)
BSS Max Associations Limit	32 (2– 32)
Authentication Mode	WPA2-PSK
WPA Pre-Shared Key	••••••••
WPA Encryption	TKIP-AES
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	



Note

To assign IP addresses to wireless terminals, you need to enable DHCP service of the VLAN interface. Configure related items in VLAN configuration interface, where the gateway address and IP address of the DNS server are the WLAN management IP address.

Step 5 Enable wireless connection.

1. In the navigation bar, choose **Basic > Interface > WLAN > Advanced Configuration**. The **Advanced Configuration** interface is displayed.
2. Choose **ON** in the **Service Status** area, and click **OK**, as shown in Figure 13-73.

Figure 13-73 Configuring WLAN advanced items

The screenshot shows the LAVA Telecom web interface. The top navigation bar includes 'Device', 'Quick Guide', 'Basic', and 'Voip'. The 'Basic' section is expanded to show 'Basic Configuration', 'Advanced Configuration', and 'Wireless Interface'. The 'Advanced Configuration' section is further expanded to show 'WLAN Advanced Configuration'. The configuration area includes the following fields:

WLAN Function:	<input checked="" type="radio"/> ON <input type="radio"/> OFF
Country Code:	United States
Working Mode:	auto
Working Channel:	Auto
Power:	100%

Step 6 Enable DNS proxy.

For details, see section 13.1 Example for configuring Internet access for wired users.

Step 7 After configurations are complete, click **Save Config** to save configurations.

Checking configurations

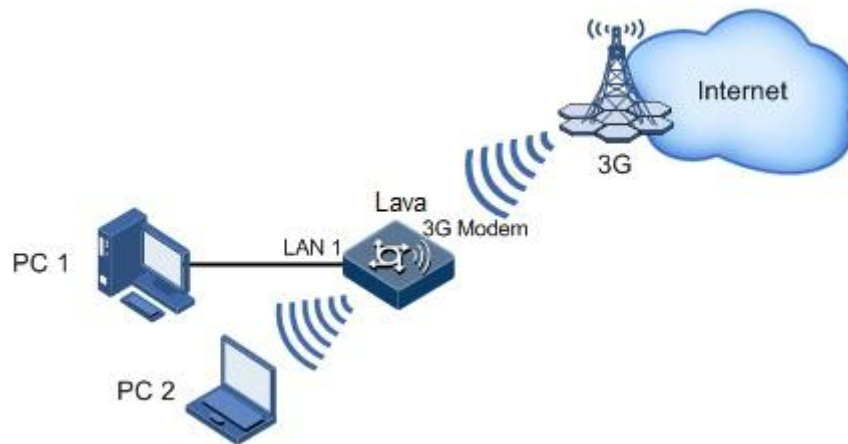
After being connected to the SSID-0001 network and inputting the password in Step 4, the wireless terminal can correctly obtain the IP address from the DHCP address pool, gateway, and DNS server. The wireless terminal can access the Internet. If the visiting is successful, the service is activated.

13.3 Example for configuring Internet access through 3G

Networking requirements

Wired users are connected to the LAVA through LAN while wireless users are connected to the LAVA through WiFi. The LAVA accesses the Internet through a 3G card, as shown in Figure 13-74.

Figure 13-74 3G Internet access networking application



Configuration thoughts

Thoughts for configuring Internet access through 3G are shown as below:

- Check the working status of the 3G network interface card.
- Configure basic configurations of the 3G interface.
- Configure advanced configurations of the 3G interface.
- Configure flow warning of the 3G interface.
- Configure the LAN interface.
- Enable DNS Proxy.

Configuration steps

Step 1 Insert a 3G card into the USB port of the LAVA.

Step 2 In the navigation bar, choose **Device > Information** to view 3G connection status.

Step 3 Configure the 3G interface.

1. In the navigation bar, choose **Basic > Interface > 3G > Basic Configuration**. The **Basic Configuration** interface is displayed.

2. Configure related items, as shown in Figure 13-75.

Figure 13-75 3G Interface Basic Configuration interface

Basic Configuration		Advanced Configuration	Flow Warning
3G Interface Basic Configuration			
Interface Name	3gppp	3G Wireless Interface	
Dial Network	3G	(3G Access Type)	
Username	card	(1– 80 characters)	
Password	••••	(1– 48 characters)	
Dial-string		(1– 30 characters)	
Online Mode	<input type="radio"/> All the time Interval-time <input type="text" value="15"/> seconds(1– 65535) Idle-time <input type="text" value="120"/> seconds(0– 65535) <input checked="" type="radio"/> Disconnect automatically after a period of time <input type="text" value="60"/> seconds(1– 65535)		
	<input type="button" value="Disconnect"/>		
<input type="button" value="OK"/>			

 **Note**

- The dialling string is provided by the carrier.
- 3.In the navigation bar, choose **Basic > Interface > 3G > Advanced Configuration**. The **Advanced Configuration** interface is displayed.
- 4.Configure related items, as shown in Figure 13-76.

Figure 13-76 Configuring 3G advanced items

Basic Configuration		Advanced Configuration	Flow Warning
3G Advanced Configuration			
Authentication Methods	CHAP	(PPP Protocol Authentication Methods)	
DNS		(xxx.xxx.xxx.xxx)	
TCP-MSS	1460	(128– 2048, Default:1460)	
MTU	1500	(128– 1500, Default:1500)	
Enable NAT	<input checked="" type="checkbox"/>		
APN		(1– 30 characters)	
Normally, the above content should not be modified. The default is better!			
<input type="button" value="OK"/>			

 **Note**

- The IP address of the DNS server should be provided by the carrier.
- Use default values in **TCP-MSS** and **MTU** area.

Step 4 Configure Internet access for wired users.

To enable wired users to access the Internet, you must configure the VLAN interface and enable DNS proxy.

For details, see 13.1 Example for configuring Internet access for wired users.

Step 5 Configure Internet access for wireless users.

To enable wireless users to access the Internet, you must configure the WLAN interface and the DHCP server, and enable DNS proxy and wireless connection.

For details, see section 13.1 Example for configuring Internet access for wired users.

Checking configurations

You can view the working status of the LAVA in the **3G Wireless State** area on the **Device** interface.

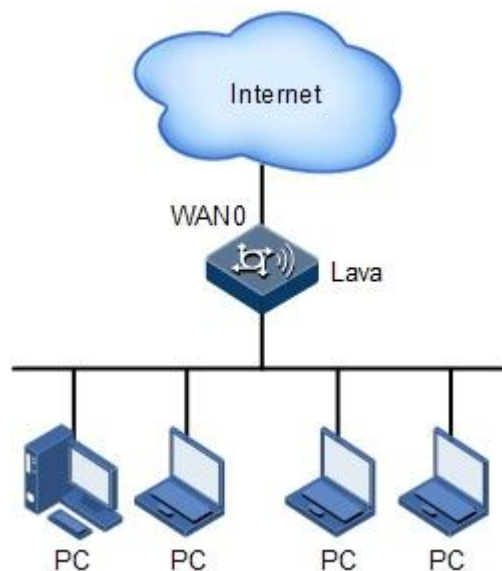
A PC or wireless terminal can access the Internet. If the visiting is successful, the service is activated.

13.4 Example for configuring Web filtering

Networking requirements

Intranet users of an enterprise access the Internet through the gateway, as shown in Figure 13-77. To ensure network security, enable firewall and configure Web filtering. After configurations, all intranet users cannot visit <http://www.google.com.au/> and <http://www.bbc.com/>.

Figure 13-77 Web Filter application networking



Configuration thoughts

Thoughts for configuring Web filtering are shown as below:

- Configure basic configurations of the firewall.
- Configure web filtering.

Configuration steps

Step 1 Configure basic firewall functions.

1. In the navigation bar, choose **Security > Security > Firewall**. The **Firewall** interface is displayed.
2. Configure related items, and click **OK**, as shown in Figure 13-78.

Figure 13-78 Firewall Configuration interface

The screenshot shows the 'Firewall Configuration' interface. At the top, there is a blue header 'Firewall Configuration'. Below it, there is a sub-header 'Firewall Configuration'. Underneath, there are two radio buttons: 'on(recommend)' (selected) and 'off(Not recommended)'. Below the radio buttons, there is a 'Security Level' dropdown menu set to 'low'. At the bottom right, there is an 'OK' button.

Step 2 Configure Web filtering.

1. In the navigation bar, choose **Security > Security > URL Filter > Web Filter**. The **Web Filter** interface is displayed.
2. Configure related items, as shown in Figure 13-79.

Figure 13-79 Web Filter interface

The screenshot shows the 'Web Filter' configuration page. At the top, there are tabs for 'Web Filter' and 'Local Update'. The 'Web Filter' section has radio buttons for 'ON' and 'OFF', with 'OFF' selected. Below this is the 'Page Redirect Set' section with a text input for 'Redirect URL' and an 'OK' button. The 'Filter Type Set' section has radio buttons for 'Black List' (selected) and 'White List', with explanatory text: 'The URL in Black Lists will be blocked, the others pass. The URL in White Lists will pass, the others are blocked.' Below this is the 'Add Filter Rule' section with a text input for 'URL' and an 'Add' button. The 'Delete Filter Rule' section contains a table with columns for 'Filter Type' and 'Value'.

<input type="checkbox"/>	Filter Type	Value
<input type="checkbox"/>	Black List	www.bbc.com/
<input type="checkbox"/>	Black List	www.google.com.au/

Total 2 records, current is the 1 page, total 1 pages [First](#) [Previous](#) [Next](#) [Last](#)

Buttons: [Select All](#) [Select None](#) [Delete](#)

Step 3 Choose **Blacklist**, and add <http://www.google.com.au/> and <http://www.bbc.com/> to the blacklist.

Step 4 After configurations are complete, click **Save Config** to save configurations.

Checking configurations

Intranet users can access Internet except for the <http://www.google.com.au/> and <http://www.bbc.com/>.

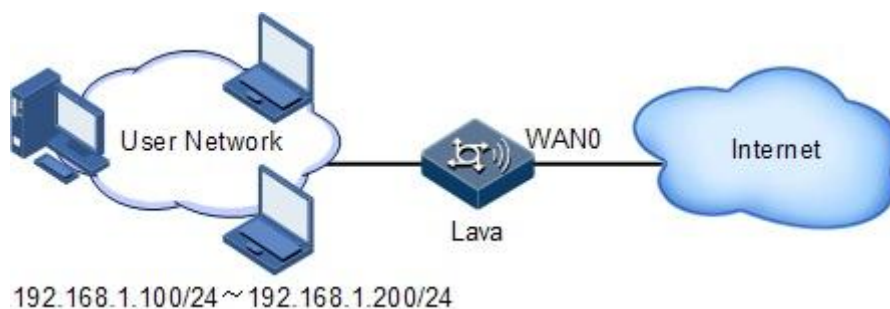
13.5 Example for configuring Internet access for wired users in limited period

Networking requirements

Internal users of an enterprise access the Internet through the LAVA, as shown in Figure 13-80. The enterprise forbids some internal users from accessing the Internet through HTTP 9:00 to 18:00 Monday to Friday, and these users have the IP addresses ranging from 192.168.1.100 to 192.168.1.200, namely:

- Time object: 9:00 to 18:00 Monday to Friday
- Address object: 192.168.1.100 to 192.168.1.200
- Service object: HTTP

Figure 13-80 Access control application networking



Configuration thoughts

Thoughts for configuring Internet access for wired users in limited period are shown as below:

- Configure the time object.
- Configure the address object.
- Configure the security policy.

Configuration steps

Step 1 Configure the time object.

1. In the navigation bar, choose **Security** > **Security** > **Access Control** > **Time Object**. The **Time Object** interface is displayed as below.
2. Click **Add** to enter the adding interface, as shown in Figure 13-81.

Figure 13-81 Configuring the time object

The screenshot shows the 'Time Object' configuration page. At the top, there are tabs for 'Policy of Access Control', 'Time Object', 'Service Object', and 'Address Object'. The 'Time Object' tab is selected. The 'Name' field contains 'example_time' with an asterisk. The 'Description' field is empty. Below this, there are two main sections. The left section is for configuring the time period, with 'Week' options (Mon, Tue, Wed, Thu, Fri, Sat, Sun) and 'Start Time' (09:00) and 'End Time' (18:00) dropdowns. An 'Add>>' button is located between the two sections. The right section is for configuring the IP address, with a text box containing '9:0 18:0 1111100'. At the bottom right, there are 'Submit' and 'Back' buttons.

3. Configure related items, and click **Add**.
4. Click **Submit** to submit the time object.

Step 2 Configure the address object.

1. In the navigation bar, choose **Security** > **Security** > **Access Control** > **Address Object**. The **Address Object** interface is displayed as below.
2. Click **Add** to enter the adding interface, as shown in Figure 13-82.

Figure 13-82 Configuring the address object

3. Select **Scope** in the **Type of Node** drop-down list, configure other related items, click **Add**, and click **Submit** to submit the address object.

Step 3 Configure security policies.

1. In the navigation bar, choose **Security > Security > Access Control > Policy of Access Control**. The **Policy of Access Control** interface is displayed as below.

1. Click **Add** to enter the adding interface, as shown in Figure 13-83.

Figure 13-83 Configuring access control policies

2. Configure related items, select **DENY** in the **Mode** drop-down list, and click **Submit**.

Step 4 After configurations are complete, click **Save Config** to save configurations.

Checking configurations

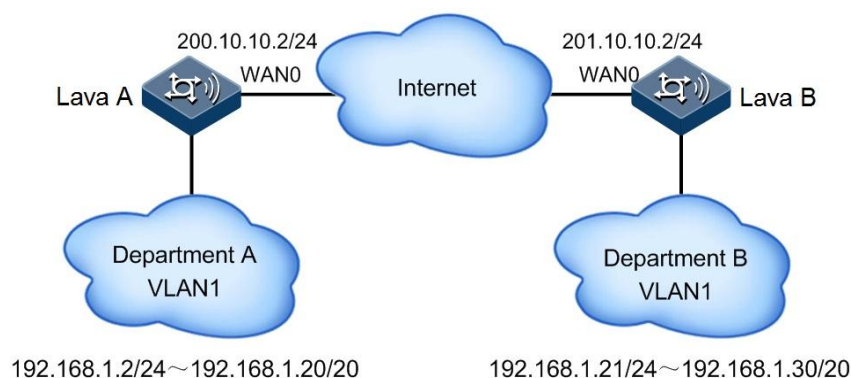
PCs in the segment of 192.168.1.100 to 192.168.1.200 cannot access the Internet through HTTP 9:00 to 18:00 Monday to Friday. They can access the Internet in other periods.

13.6 Example for configuring EoIP

Networking requirements

Department A and Department B of an enterprise, located in different spots, need to visit the network of each other, as shown in Figure 13-84.

Figure 13-84 EoIP application networking



Configuration thoughts

Thoughts for configuring EoIP are shown as below:

- Configure IP addresses of WAN interfaces of LAVA A and LAVA B.
- Configure EoIP of LAVA A.
- Configure EoIP of LAVA B.

Configuration steps

Step 1 Configure the IP address of the WAN interface for LAVA A and LAVA B (this part is omitted).

Step 2 Configure EoIP on LAVA A.

1. In the navigation bar, choose **Basic > Network > EoIP**. The **EoIP Configuration** interface is displayed as below.
2. Click **Add** to enter the adding interface.
3. Configure related items, as shown in Figure 13-85.

Figure 13-85 Configuring EoIP on LAVA A

EoIP Configuration	
Configure EoIP Tunnel	
Tunnel ID	1
Interface	WANO
Remote Address	201.10.10.2
Tunnel master/backup:	<input type="radio"/> backup <input checked="" type="radio"/> master
Monitor ip	

4. Click **OK**.

5. After configurations are complete, click **Save Config** to save configurations.

Step 3 Configure EoIP on LAVA A.

1. In the navigation bar, choose **Basic > Network > EoIP**. The **EoIP Configuration** interface is displayed as below.
2. Click **Add** to enter the adding interface.
3. Configure related items, as shown in Figure 13-86.

Figure 13-86 Configuring EoIP on LAVA B

EoIP Configuration	
Configure EoIP Tunnel	
Tunnel ID	1
Interface	WANO
Remote Address	200.10.10.2
Tunnel master/backup:	<input type="radio"/> backup <input checked="" type="radio"/> master
Monitor ip	

4. Click **OK**.

5. After configurations are complete, click **Save Config** to save configurations.

Checking configurations

Department A and Department B can visit the network of each other.

13.7 Example for configuring the NAT virtual server

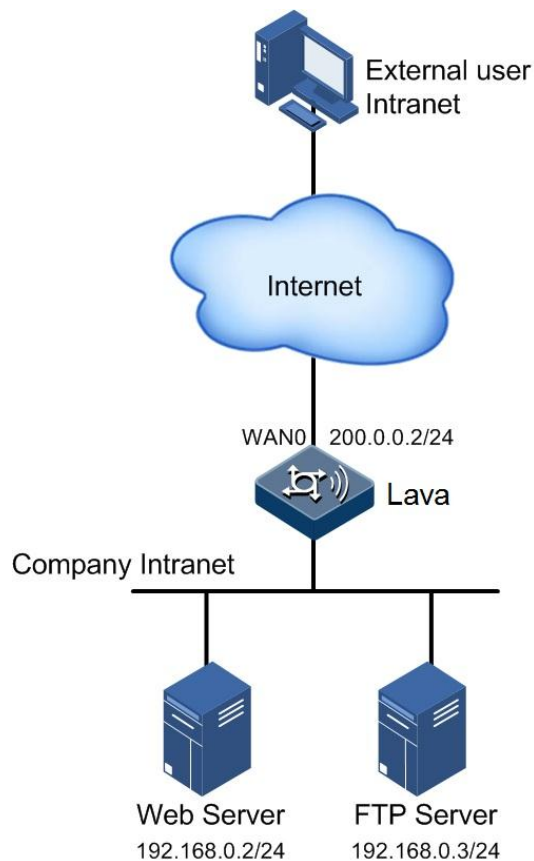
Networking requirements

An enterprise has two servers, providing Web and FTP services respectively, as shown in Figure 13-87. The IP addresses are as below:

- IP address of the Web server: 192.168.0.2/255.255.255.0

- IP address of the FTP server: 192.168.0.3/255.255.255.0
- IP address of the WAN0 interface: 200.0.0.2/255.255.255.0

Figure 13-87 NAT virtual server application networking



Configuration thoughts

Thoughts for configuring the NAT virtual server are shown as below:

- Configure the IP address of the WAN interface.
- Add the service object to the access control.
- Configure the Web service of the NAT virtual server.
- Configure the FTP service of the NAT virtual server.

Configuration steps

Step 1 Configure the IP address of the WAN0 interface on the LAVA (this part is omitted).

Step 2 Add a service target in access control.

1. In the navigation bar, choose **Security > Security > Access Control > Service Object**. The **Service Object** interface is displayed.
2. Click **Add** to enter the adding interface.
3. Configure related items, and click **OK**.



- You need to customize service objects in the following cases:
- The default port is not adopted.
 - The port used by the user is limited by the Carrier.

Step 3 Configure a FTP service object as below.

Figure 13-88 Adding a FTP service object

Policy of Access Control | Time Object | **Service Object** | Address Object

Name

Description

Protocol

Source port number - (1-65535)

Destination port number - (1-65535)

Click **Add** to add it to the right list.

Step 4 Configure the Web service object, as shown in Figure 13-89.

Figure 13-89 Adding a HTTP port service target

Policy of Access Control | Time Object | **Service Object** | Address Object

Name

Description


Protocol

Source port number - (1-65535)

Destination port number - (1-65535)

1. Click **Add** to add it to the right list.
2. Click **Submit** to submit them. They are displayed in the **List of Customed Service**.

Figure 13-90 List of Customed Service

List of Customed Service				
Service Name	Cited Times	Content	Description	Operation
server	0	TCP/20-21:20-21;TCP/8080:8080;		 

Total 1 records, current is the 1 page, total 1 pages

Jump to page

Step 5 Configure virtual server Web service on the LAVA.

1. In the navigation bar, choose **Basic > Network > NAT > Virtual Server**. The **Virtual Server** interface is displayed.
2. Configure related items, as shown in Figure 13-91.

Figure 13-91 Creating a virtual server for Web service

Create Virtual Servers

Interface:

Type of protocol:

External IP address:

IP address of current interface

IP address:

Internal IP address:

IP address:

Address segment: -

Internal Port: (1 - 65535)

 **Note**

Choose a configured service target in the **Type of protocol** drop-down list.

3. Click **Add**. A virtual server for Web service is successfully created.

Step 6 Configure virtual server Web service on the LAVA.

1. In the navigation bar, choose **Basic > Network > NAT > Virtual Server**. The **Virtual Server** interface is displayed.
2. Configure related items, as shown in Figure 13-92.

Figure 13-92 Creating a virtual server for FTP service

Create Virtual Servers

Interface WANO ▾

Type of protocol server ▾

External IP address

IP address of current interface

IP address

Internal IP address

IP address

Address segment —

Internal Port Default Port ▾ (1 – 65535)



Note

Choose a configured service target in the **Type of protocol** drop-down list.
 3.Click **Add**. A virtual server for FTP service is successfully created.

Step 7 After configurations are complete, click **Save Config** to save configurations.

Checking configurations

After previous configurations, you can see the configured virtual servers, as shown in Figure 13-93.

Figure 13-93 Internal server list

Select the internal servers you want to delete					
	Interface	External IP address	Internal IP address	Internal Port	Type of protocol
<input type="checkbox"/>	WANO	IP address of current interface	192.168.0.3	Default Port	server
<input type="checkbox"/>	WANO	IP address of current interface	192.168.0.2	Default Port	server

External users can use services provided by the Web server and FTP server.

13.8 Example for configuring route backup and sharing

Networking requirements

An enterprise uses a router to connect internal users to the Internet. Now it uses the LAVA to provide:

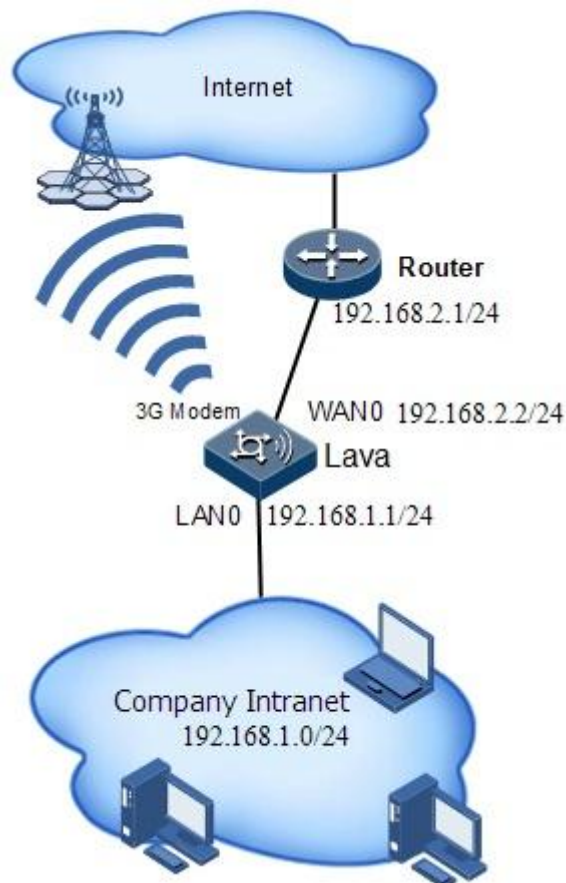
- Load sharing between wired Internet access and 3G Internet access.

- 3G Internet access upon failure in wired Internet access

As shown in Figure 13-94, detailed requirements are as below:

- IP address of the WAN0 interface: 192.168.2.2/255.255.255.0
- IP address of Intranet: 192.168.1.0/255.255.255.0
- IP address of the downlink interface of the router: 192.168.2.1/255.255.255.0
- IP address of the LAN0 interface: 192.168.1.1/255.255.255.0

Figure 13-94 Route backup and sharing application networking



Configuration thoughts

Thoughts for configuring route backup and sharing are shown as below:

- Configure the IP address of the LAVA WAN0 interface.
- Configure the IP address of the LAVA LAN interface.
- Configure the 3G interface.
- Configure the default route of the WAN interface.
- Configure the default route of the 3G interface.

Configuration steps

Step 1 Configure the IP address of the WAN0 interface on the LAVA.

For details, see related configuration examples.

Step 2 Configure the IP address of the LAN0 interface on the LAVA.

For details, see related configuration examples.

Step 3 Configure the 3G interface on the LAVA and establish a 3G connection.

For details, see related configuration examples.

Step 4 Configure default route of the WAN0 interface on the LAVA.

1. In the navigation bar, choose **Basic** > **Network** > **Static Route**. The **Static Route** interface is displayed.

2. Click **Add** to enter the adding interface.

3. Configure related items, as shown in Figure 13-95.

Figure 13-95 Configuring default route of the WAN0 interface

Static Route	
Network Destination	<input type="text" value="0.0.0.0"/>
Subnet Mask	<input type="text" value="0.0.0.0"/>
<input checked="" type="radio"/> Next Hop	<input type="text" value="192.168.2.1"/>
<input type="radio"/> Interface	<input type="text" value="WAN0"/>
Weight	<input type="text" value="1"/> (1-100)
Distance	<input type="text" value="1"/> (1-255)
<input checked="" type="checkbox"/> Monitor Address	<input type="text" value="192.168.2.1"/>
Send Interval(seconds)	<input type="text" value="10"/> (1-300)
The number of packets	<input type="text" value="3"/> (1-10)

4. Click **OK**.

Step 5 Configure default route of the 3G interface on the LAVA.

1. In the navigation bar, choose **Basic** > **Network** > **Static Route**. The **Static Route** interface is displayed.

2. Click **Add** to enter the adding interface.

3. Configure related items, as shown in Figure 13-96.

Figure 13-96 Configuring default route of the 3G interface

Static Route

Network Destination	0.0.0.0	*
Subnet Mask	0.0.0.0	*
<input type="radio"/> Next Hop		
<input checked="" type="radio"/> Interface	3gppp	▼
Weight	1	(1-100)
Distance	1	(1-255)
<input type="checkbox"/> Monitor Address		
Send Interval(seconds)		(1-300)
The number of packets		(1-10)

4. Click **OK**.

Step 6 View route configurations.

1. In the navigation bar, choose **Basic > Network > Static Route**. The **Static Route** interface is displayed.
2. View configured static routes, as shown in Figure 13-97.

Figure 13-97 Static route list

Static Route List

<input type="checkbox"/>	Network Destination	Subnet Mask	Next Hop/Interface	Distance	Weight	Operation
<input type="checkbox"/>	0.0.0.0	0.0.0.0	192.168.27.1	1	1	
<input type="checkbox"/>	0.0.0.0	0.0.0.0	3gppp	1	1	

Total 2 records, current is the 1 page, total 1 pages

Jump to page

Step 7 After configurations are complete, click **Save Config** to save configurations.

Checking configurations

- When wired connection and 3G connection work normally, they have traffic, and intranet users can access the Internet normally.
- When wired connection fails, 3G connection works normally, and intranet users can access the Internet normally.
- When 3G connection fails, wired connection works normally, and intranet users can access the Internet normally.

14 Appendix

This chapter lists terms, acronyms, and abbreviations involved in this document, including the following sections:

- Terms
- Acronyms and abbreviations

14.1 Terms

B

Black list & white list Black list: those comply with rules are forbidden from passing.
White list: those comply with rules are allowed to pass

Bridging It divides a physical network into two independent network segments without creating a new IP sub-network and using a router to connect two segments. The device that connects two segments is called a network bridge. The way that implements this is called bridging.

F

Firewall It is an application security technology based on network communication technology and information security technology. It is the unique ingress&egress for different networks or secure domains. It can control ingress and egress flow according to security policies of an enterprise. It has strong resistance to attacks.

M

Multicast It is a point-to-multipoint data transmission method. It effectively solve of problem of single point sending and multiple points receiving. During data transmission, it saves network resources and enhances information security.

T

TR-069 It is a network management protocol made by the Digital Subscriber Line (DSL) Forum for terminal devices, also called Customer Premised Equipment WAN Management Protocol (CWMP). It provides a general framework and protocol for managing and configuring home network devices in the next generation network. It can remotely and centrally manage gateways, routers, and Set Top Boxes (STBs) in a home network at network side.

V

VPN It is a temporary, secure, and stable connection through an unsafe public network (usually Internet).

W

Web pushing With it, servers forward organized information to the user interface as Web pages. It implements users' multi-level requirements, enables users to customize information channels, and sends users with customized information.

14.2 Acronyms and abbreviations

Numerics

A

ACL Access Control List
ARP Address Resolution Protocol
ALG Application Layer Gateway

C

CDMA Code Division Multiple Access
CHAP Challenge Handshake Authentication Protocol

D

DDoS Distributed Denial of Service
DHCP Dynamic Host Configuration Protocol

E

EVDO	Evolution-Data Optimized
EoIP	Ethernet over IP
F	
FTP	File Transfer Protocol
G	
GRE	Generic Routing Encapsulation
I	
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IP	Internet Protocol
ITU-T	International Telecommunications Union - Telecommunication Standardization Sector
IGMP	Internet Group Management Protocol
IPSec	IP Security
N	
NTP	Network Time Protocol
L	
L2TP	Layer Two Tunneling Protocol
LAN	local area network
LDAP	Lightweight Directory Access Protocol
M	
MAC	Medium Access Control
MIB	Management Information Base
LAVA	multi-service Intelligence Gateway
MG	Media Gateway
MGC	Media Gateway Controller

N	
NTP	Network Time Protocol
NAT	Network Address Translation
O	
OAM	Operation, Administration, and Maintenance
OSPF	Open Shortest Path First
P	
PC	Personal Computer
PPPoE	Point-to-Point Protocol over Ethernet
PTP	Precision Time Protocol
PON	Passive Optical Network
PAP	Password Authentication Protocol
Q	
QoS	Quality of Service
R	
RADIUS	Remote Authentication Dial In User Service
RIP	Routing Information Protocol
S	
SNMP	Simple Network Management Protocol
SIM	subscriber identity module
Syslog	System Lo
SSH	Secure Shell
SSL	Security Socket Layer
SIP	Session Initiation Protocol
T	
TCP	Transmission Control Protocol
TD-SCDMA	Time Division-Synchronous Code Division Multiple Access

U

URL Uniform Resource Locator

UA User Agent

V

VLAN Virtual Local Area Network

VPDN Virtual Private Dial Network

VoIP Voice over IP

W

WLAN Wideband Code Division Multiple Access

WAN Wide Area Network

