SmartAX MT882 ADSL Router

User Manual

HUAWEI

SmartAX MT882 ADSL Router

User Manual

V200R002

SmartAX MT882 ADSL Router

User Manual

Manual Version: T2-20060513-C-2.20-0J

Huawei Technologies Co., Ltd. provides customers with comprehensive technical support and service. Please feel free to contact our local office or company headquarters.

Huawei Technologies Co., Ltd.

About This Manual

This manual describes SmartAX MT882 ADSL Router V200R002 (hereinafter referred to as MT882).

Organization

- **1 Overview** introduces MT882 and its features.
- **2 Hardware Installation** introduces the hardware installation of MT882.
- **3 Preparations Before Configuration** introduces the preparations before configuring MT882.
- **4 Web-Based Management** describes how to configure MT882 by using the embedded Web-based management software.
- **5 Service Configuration** describes configuration of MT882 for six applications.
- **6 Troubleshooting** lists the FAQs and troubleshooting methods.
- **7 Technical Specifications** lists the technical specifications of MT882.
- **8 Appendix** lists the acronyms and abbreviation mentioned in this manual and the factory settings of MT882.

Intended Audience

This manual is intended for the following readers:

- Marketing personnel
- Installation engineers and technicians
- Operation and maintenance personnel

Conventions

This manual uses the following conventions:

I. General conventions

Convention	Description
Arial	Normal paragraphs are in Arial.
Arial Narrow	Cautions, Notes, Tips and table texts are in Arial Narrow.
Boldface	Headings are in **Boldface**.

II. Symbols

Eye-catching symbols are used in this manual to highlight the points worthy of special attention during the operation. They are defined as follows:

⚠ **Caution**: Means reader be extremely careful during the operation.

📖 **Note**: Means a complementary description.

Environmental Protection

This product has been designed to comply with the requirements on environmental protection. For the proper storage, use and disposal of this product, national laws and regulations must be observed.

Table of Contents

Huawei Technologies Proprietary

1 Overview

This chapter introduces the appearance and features of SmartAX MT882 ADSL Router (hereinafter referred to as MT882).

MT882 enables you to access small and private networks easily, securely, and cost-efficiently through ADSL connection. It provides many multimedia applications.

MT882 can be easily installed on a platform.

1.1 Appearance

1.1.1 Front Panel

Figure 1-1 shows the front panel of MT882. There are five indicators on the front panel.
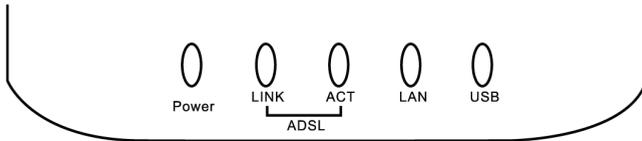
Figure 1-1 Front panel of MT882

Table 1-1 describes the indicators.

Table 1-1 Indicators on the front panel

LED Indicator	Color	Status	Description
Power	Green	On	MT882 is powered on.
ADSL LINK	Green	Blinking	The ADSL link is being activated.
		On	A valid ADSL connection is established.
	Orange	Blinking	The built-in PPP dial-up application is dialing.
		On	The built-in PPP dial-up application succeeds in dialing.
ADSL ACT	Green	Blinking	There is traffic over the ADSL line.
LAN	Green/Orange	On	A valid LAN connection is established.
	Green	Blinking	There is traffic over the Ethernet interface. The transmission rate is 10 Mbit/s.
	Orange	Blinking	There is traffic over the Ethernet interface. The transmission rate is 100 Mbit/s.
USB	Green	On	A valid USB connection is established.
		Blinking	There is traffic over the USB interface.

Note:

ADSL: Asymmetric Digital Subscriber Line

PPP: Point-to-Point Protocol

ACT: Active

1.1.2 Rear Panel

Figure 1-2 shows the rear panel of MT882. There are four interfaces, a reset button and a power switch on the rear panel.
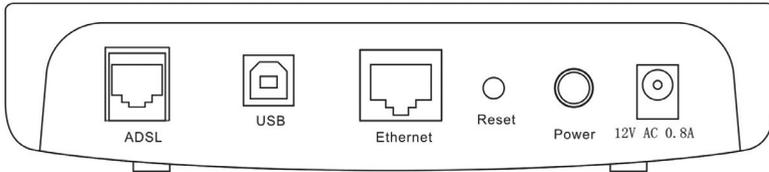
Figure 1-2 Rear panel of MT882

Table 1-2 describes the interfaces, the reset button and the power switch on the real panel.

Table 1-2 Interfaces, button and power switch on the rear panel

Interface/Button	Description
ADSL	It is used to connect with the Modem interface of a splitter.
USB	It is used to connect with a computer.
Ethernet	It is used to connect with a computer or switch.
Reset	It is used to restore the default settings of MT882. Once you use this function, all your custom settings will be lost. Therefore, be careful with it.
Power	It is used to turn on/off MT882.
12 V AC 0.8 A	It is used to connect with the power adapter.

> 📖 **Note:**
>
> Use a power adapter provided or approved by Huawei only. Make sure that the power adapter conforms to the sign on the rear panel (12 V AC 0.8 A).

1.1.3 External Splitter

MT882 provides an external splitter which can reduce the signal interference on the telephone line. The splitter has three interfaces:

- **LINE:** connecting to the Phone Jack.
- **PHONE:** connecting to the telephone.
- **MODEM:** connecting to the ADSL port of MT882.

1.2 MT882 Features

MT882 has the following features:

- Up to 24 Mbit/s for downstream transmission and 1.2 Mbit/s for upstream
- Friendly Web-based graphical user interface (GUI) for configuration and management
- Supporting up to eight concurrent virtual connections
- Various indicators for troubleshooting and maintenance
- Interoperability with various types of DSLAMs
- Built-in firewall and filter rules for protecting user data
- Upgrading firmware through TFTP
- Easy to install and use

2 Hardware Installation

This chapter introduces the hardware installation of MT882. It contains the following topics:

1) Preparation
2) Connecting MT882
3) Powering on MT882

2.1 Preparation

2.1.1 Checking Computer Configuration

Item	Requirement
OS	Web browser, such as IE, is installed
Web browser	Microsoft Internet Explorer®5.0 or Netscape Navigator®4.7 or above with JavaScript enabled
Ethernet interface	10MBase-T network adapter or above

2.1.2 Collecting ISP Information

You need to collect the following information about the internet service provider (ISP):

- Virtual path identifier (VPI) and virtual channel identifier (VCI)
- Encapsulation type
- Protocol type

- Modulation type
- User name, password

2.2 Connecting MT882

2.2.1 Connecting the ADSL Line

To connect the ADSL line, do as follows:

1) Plug one end of a twisted-pair telephone line into the Modem port of the splitter.
2) Plug the other end into the ADSL port on the rear panel of MT882.
3) Use another telephone line to connect the splitter and the Phone Jack on the wall.

2.2.2 Connecting MT882 to a PC

Connect MT882 to the 10/100Base-TX Ethernet adapter on your PC with the Ethernet cable provided. See Figure 2-1.

(1) Notebook   (2) Phone   (3) USB Cable
(4) RJ-11 Telephone line   (5) RJ-11 Telephone line   (6) Splitter
(7) MT882   (8) RJ-11 Telephone line   (9) Phone Jack
(10) RJ-45 Ethernet Cable   (11) PC
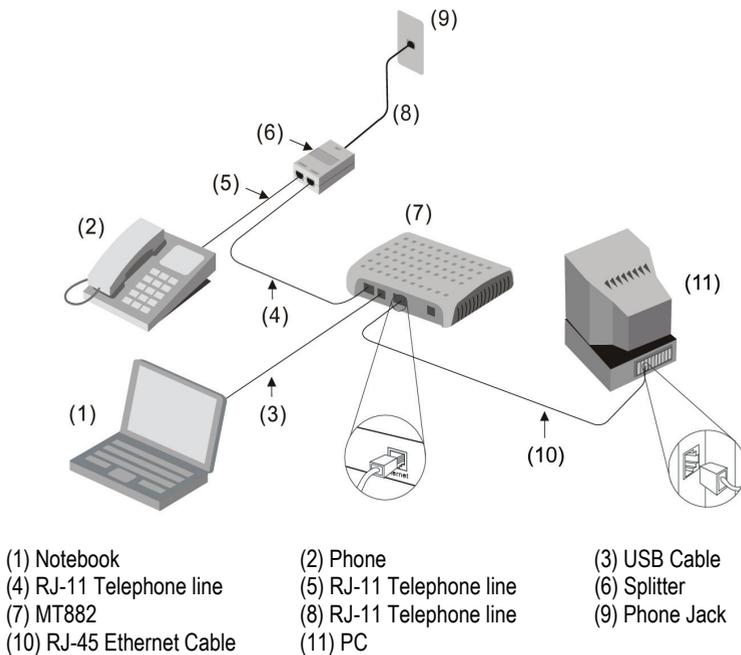
Figure 2-1 Connecting MT882 to PCs and a telephone

2.2.3 Connecting MT882 to the Ethernet LAN

MT882 can be connected to any 10/100Base-TX Ethernet interface. While connecting MT882 to any Ethernet device that is capable of transmitting data at 10 Mbit/s or above, set MT882 to the auto-sensing mode.

Use a crossover cable to connect MT882 and the uplink port of a switch or hub. The cable cannot exceed 100 meters.

2.3 Powering On MT882

To power on MT882, do as follows:

1) Plug the provided power adapter into a suitable power socket.

2) Press the power switch on the rear panel of MT882. The Power indicator on the front panel will be on. After a few seconds, the LAN LINK indicator will be on, indicating that the connection between MT882 and the PC is normal.

3 Preparations Before Configuration

The factory settings of MT882 optimize all functions and enable MT882 to operate in most network conditions. Usually you do not need to change the settings.

To meet special requirements, such as particular VPI and VCI, you can adjust the settings of MT882.

3.1 Setting Up the Configuration Environment

To configure MT882, you need to connect MT882 to a PC by using a straight-through cable. See Figure 3-1.

(1) PC   (2) RJ-45 Ethernet Cable   (3) MT882
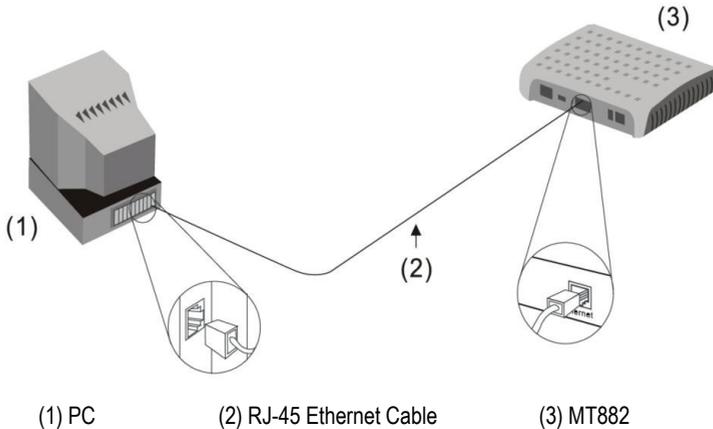
Figure 3-1 Connecting MT882 to a PC

Huawei Technologies Proprietary

3.2 Configuring the IP Address of Your PC

To set the IP address of your PC, do as follows:

1) Check the IP address of MT882.
    The IP address is 192.168.1.1 and the subnet mask is
    255.255.255.0 by default.
2) Check the TCP/IP settings on your PC.
*   If you have an Ethernet port on your PC, the TCP/IP is
    probably installed.
*   If you are using Windows XP, the TCP/IP is enabled by
    default.
3) Configure the IP address and subnet mask of your PC.
    Make sure that your PC is in the same subnet as MT882.
    For example, IP address is 192.168.1.100, and subnet
    mask is 255.255.255.0.

📕 **Note:**

*   If your PC is not running on a Windows OS, configure the IP address of your PC
    according to the instructions of the OS.
*   Make sure that your PC is in the same subnet as MT882.

3.3 Accessing the Web-Based Manager

After setting the IP address of your PC, you can access the
web-based manager.

3.3.1 Checking the Proxy Settings

If your PC accesses the Internet through a proxy server, you need to disable the proxy service first. To check the proxy settings, do as follows (suppose you use Windows Internet Explorer):

1) In the IE window, select **Tools** > **Internet Options** to display the **Internet Options** dialog box.
2) Select the **Connections** tab and then click **LAN Settings**.
3) Make sure that the **Use proxy server** option is NOT selected.
   If it is selected, click the check box to deselect the option and click **OK**.

3.3.2 Logging In to MT882 through Web

To log in to MT882 through the Web-based manager, do as follows:

1) Launch your Web browser.
2) In the **Address** text box, enter the IP address of MT882 and then press **Enter**.
   If you log in to MT882 for the first time, enter **http://192.168.1.1**, this is the default IP address of MT882.
3) In the dialog box, enter the user name and password.The user name is user and the password is user

📕 **Note:**

Do not confuse this user name and password with that of the ADSL account. The former is used to access the Web-based manager of MT882, while the latter is used to access the ADSL service or the network of your ISP.

4 Web-Based Management

This chapter describes how to configure MT882 by using the Web-based manager. It also describes the parameters and settings in the configuration interface.

4.1 Manager Interface

The Manager interface consists of two parts:

- The left part is the navigation bar, providing links for you to access different pages.
- The right part is the information area, showing details of configuration and management.

4.2 Home Page

Figure 4-1 shows the home page of the Web-based manager. It is the system information showing the existing configuration of MT882.

System Information

Item	Description
Product Name	SmartAX MT882
Physical Address	00:05:5D:00:00:00
Software Release	V200R002B023 NOVIS
Firmware Release	E.37.5.5
Release Date	(2006-05-05)
Batch ID	RCC1P0.023.E3755
System Up Time	0:14:7
ADSL	**Description**
ADSL Status	Startup Handshake
DSL Up Time	0:0:0
Data Path	-
Standard	-
Bandwidth Down/Up(kbps)	0/0
SNR Margin Down/Up(dB)	0.0/0.0
Attenuation Down/Up(dB)	0.0/0.0
CRC Down/Up	0/0
FEC Down/Up	0/0
HEC Down/Up	0/0

Figure 4-1 Home page

The following describes the information shown on the home page:

- **Item**: Displaying the basic information and current status of hardware and software.
- **ADSL**: Displaying the basic information and current status of ADSL connection.

4.3 Service Information

Click **Status** > **Service Information** in the navigation bar to display the **Service Information** page as shown in Figure 4-2.

Service Information

LAN Interface						
IP Address	Submask	MAC Address		Speed	Duplex	Status
192.168.1.1	255.255.255.0	00:05:5D:00:00:00		100Mbps	Full	✔
192.168.1.2	255.255.255.0	-		-	-	✘
WAN Interface						
PVC	VPI/VCI	IP Address	Submask	Gateway	Encapsulation	Status
PVC-0	0/35	0.0.0.0	0.0.0.0	0.0.0.0	PPPoE	✘
PVC-1	8/35	0.0.0.0	0.0.0.0	0.0.0.0	Bridged	✘
PVC-2	0/100	0.0.0.0	0.0.0.0	0.0.0.0	Bridged	✘
PVC-3	0/32	0.0.0.0	0.0.0.0	0.0.0.0	Bridged	✘
PVC-4	8/81	0.0.0.0	0.0.0.0	0.0.0.0	Bridged	✘
PVC-5	8/32	0.0.0.0	0.0.0.0	0.0.0.0	Bridged	✘

Figure 4-2 Service information

The following describes the information shown on the **Service Information** page:

- **LAN Interface**: Displaying the basic information about LAN Interface such as IP Address, Submask, MAC Address, Speed, Duplex, and Status.
- **WAN Interface**: Displaying the basic information about WAN Interfaces such as PVC, VPI/VCI, IP Address, Submask, Gateway, Encapsulation, and Status.

4.4 Statistics

Click **Status** > **Statistics** in the navigation bar to display the **Traffic Statistics** page as shown in Figure 4-3.

Traffic Statistics

ATM Statistics			
PVC:	PVC-0 ▼	RAS Timer Expired count:	0
Tx Frame(s) count:	0	Rx Frame(s) count:	0
Tx Byte(s) count:	0	Rx Byte(s) count:	0
Large Packet(s) Rx count:	0	CIS Rx count:	0
CRC Error(s) count:	0	Invalid CPI SDU count:	0
Invalid PAD count:	0	Invalid Length SDU count:	0
LAN Statistics			
Align Error(s) count:	0	FCS Error(s) count:	0
Single Collisn Frame(s) count:	0	Two Collisn Frame(s) count:	0
SQE Test Error(s) count:	0	Deferred Transaction count:	0
Late Collisn count:	0	Excess Collisn count:	0
Internal MAC Rx Error(s) count:	0	Internal MAC Tx Error(s) count:	0
Carrier Sense Error(s) count:	0	Frame Too Long count:	0
Tx count:	4610	Rx count:	3857
Control Pause count:	0	Total Collisn count:	0
	Clear	Refresh	

Figure 4-3 Traffic statistics

The following describes the information shown on the **Traffic statistics** page:

- **ATM Statistics**: Displaying the traffic statistics gathered from ATM port.
- **LAN Statistics**: Displaying the traffic statistics gathered from local Ethernet.

To view the statistics of a specific PVC, please select a PVC from the drop-down menu of PVC in this page.

To view the real-time information, click **Refresh**. To clear the counter, click **Clear**.

4.5 ADSL Mode

Click **Basic** > **ADSL Mode** in the navigation bar to display the setting page as shown in Figure 4-4. The **ADSL Mode** interface is used to change the modes used for the ADSL connection. Please do not change this setting unless required by your ISP.

I. Configuration Page

ADSL Mode

Notice: Please Save & Reboot after changing the setting.

Item	Description
Standard	ALL ▼
Downstream Bitswap	Enable ▼
Upstream Bitswap	Enable ▼
	Submit

Figure 4-4 ADSL mode

The following describes the information shown on the **ADSL Mode** page:

- **Standard**: MT882 supports multiple standards. If you are required by your ISP to change the standard used by your service, select the required standard from the drop-down menu. The available standards include **All**, **ADSL2+**, **ADSL2**, **Multimode**, **G.DMT** and **T1.413**.
- **Downstream**/**Upstream Bitswap**: Select **Enable** from the drop-down menu to enable the function of simple rate control and adjusting rate automatically. Select **Disable** from the drop-down menu to disable it.

II. Save

- Click **Submit** to save the settings in the RAM
- To save this configuration changes permanently, enter the **Save & Reboot** page, select **Save** and click **Submit** to save new settings.

4.6 WAN Settings

Click **Basic** > **WAN Settings** in the navigation bar to display the setting page as shown in Figure 4-5.

WAN Settings

PVC	VPI/VCI	IP Address	Submask	Gateway	Mode	Encapsulation	Action(s)
PVC-0	0/35	0.0.0.0	0.0.0.0	0.0.0.0	PPPoE	LLC	✏ 🗑
PVC-1	8/35	0.0.0.0	0.0.0.0	0.0.0.0	Bridged	LLC	✏ 🗑
PVC-2	0/100	0.0.0.0	0.0.0.0	0.0.0.0	Bridged	LLC	✏ 🗑
PVC-3	0/32	0.0.0.0	0.0.0.0	0.0.0.0	Bridged	LLC	✏ 🗑
PVC-4	8/81	0.0.0.0	0.0.0.0	0.0.0.0	Bridged	LLC	✏ 🗑
PVC-5	8/32	0.0.0.0	0.0.0.0	0.0.0.0	Bridged	LLC	✏ 🗑
Click 'New' to create a new entry.							
			New				

Figure 4-5 WAN settings

Select a PVC and click the corresponding icon ✏ to display the modification page as shown in Figure 4-6.

PVC	PVC-0
Operation Mode	◉ Enable ○ Disable
VPI/VCI	0 / 35
Mode	PPPoE
Encapsulation	◉ LLC ○ VC-Mux
Default Route	◉ Enable ○ Disable
IGMP	◉ Enable ○ Disable
Traffic Index:	0
Service Name	
Username	guest @clix.pt
Password	•••••
IP Unnumber	○ Enable ◉ Disable
Use DNS	◉ Enable ○ Disable
Configured MTU:	1432
Actual MTU:	1432
Status	
	Submit

Figure 4-6 WAN settings-edit

4.6.1 Pure Bridge

I. Configuration Page

Select **Pure Bridge** from the drop-down menu of **Mode** to display the page as shown in Figure 4-7.

PVC	PVC-0
Operation Mode	⊙ Enable ○ Disable
VPI/VCI	0 / 35
Mode	Pure Bridge ▾
Encapsulation	⊙ LLC ○ VC-Mux
Configured MTU:	9164
Actual MTU:	1432
Traffic Index:	0 ▾
	Submit

Figure 4-7 Pure bridge mode

The following describes the information shown on the page:

- **PVC**: Displaying the PVC that you are making modification.
- **Operation Mode**: Select **Enable** to enable the PVC for initial connection.
- **VPI/VCI**: For the default value, see "8.1 Factory Settings". You can change it to the value provided by your ISP.
- **Encapsulation**: You can select either **LLC** or **VC**-**Mux**.
- **Configured MTU**: Enter the maximum transmission unit (MTU), that is, the maximum bytes of the packet transmitted during connection.
- **Actual MTU**: Read-only value, displaying the actual value of MTU.
- **Traffic Index**: Select the index for ATM traffic from the drop-down list.

II. Save

- Click **Submit** to save the settings in the RAM.

- To save this configuration changes permanently, enter the **Save & Reboot** page, select **Save** and click **Submit** to save new settings.

4.6.2 PPPoA

I. Configuration Page

Select **PPPoA** from the drop-down menu of **Mode** to display the page as shown in Figure 4-8.

PVC	PVC-0	
Operation Mode	⦿ Enable ○ Disable	
VPI/VCI	0 / 35	
Mode	PPPoA	
Encapsulation	⦿ LLC ○ VC-Mux	
Default Route	⦿ Enable ○ Disable	
IGMP	⦿ Enable ○ Disable	
Traffic Index:	0	
Username	guest	@clix.pt
Password	•••••	
IP Unnumber	○ Enable ⦿ Disable	
Use DNS	⦿ Enable ○ Disable	
Configured MTU:	1500	
Actual MTU:	1432	
	Submit	

Figure 4-8 PPPoA mode

The following describes the information shown on the page:

- **PVC**: Displaying the PVC that you are making modification.
- **Operation Mode**: Select **Enable** to enable the PVC for initial connection.

- **VPI/VCI**: For the default value, see "8.1 Factory Settings". You can change it to the value provided by your ISP.
- **Encapsulation**: You can select either **LLC** or **VC**-**Mux**.
- **Default Route**: If you select **Enable**, the gateway IP address will be used as the default route for data transmission.

  If you specify the default gateway, the data for which there is no route in the routing table will be forwarded through the WAN interface specified by the default route. If you do not specify the default gateway, the data for which there is no route in the routing table will be discarded. Only the data for which there is a route in the routing table will be forwarded through the WAN interface.
- **IGMP**: IGMP is a multicast protocol in the Internet protocol household, used for IP host computer reporting the status of their group members to any adjacent router. Select **Enable** or **Disable** to enable or disable it.
- **Traffic Index**: Select the index for ATM traffic from the drop-down list.
- **Username** and **Password**: Enter the username and password provided by ISP, and select the domain name from the dropping down list.
- **IP Unnumber**: You can select enable or disable. When **Enable** is selected, the Ethernet port address will be used as your IP address.
- **Use DNS**: It is recommended to select **Enable**, indicating that when PPP dial applies for IP and gateway, it also tries for DNS server IP at the same time. On the other hand, select **Disable**, indicating that obtaining DNS server not

from PPP dial, and needed to manually enter the addresses of primary DNS server and secondary DNS server on the DNS configuration page.

- **Configured MTU**: Enter the maximum transmission unit (MTU), that is, the maximum bytes of the packet transmitted during connection.
- **Actual MTU**: Read-only value, displaying the actual value of MTU.

II. Save

- Click **Submit** to save the settings in the RAM.
- To save this configuration changes permanently, enter the **Save & Reboot** page, select **Save** and click **Submit** to save new settings.

4.6.3 PPPoE

I. Configuration Page

Select **PPPoE** from the drop-down menu of **Mode** to display the page as shown in Figure 4-9.

PVC	PVC-0
Operation Mode	⊙ Enable ○ Disable
VPI/VCI	0 / 35
Mode	PPPoE ▼
Encapsulation	⊙ LLC ○ VC-Mux
Default Route	⊙ Enable ○ Disable
IGMP	⊙ Enable ○ Disable
Traffic Index:	0 ▼
Service Name	
Username	guest @clix.pt ▼
Password	•••••
IP Unnumber	○ Enable ⊙ Disable
Use DNS	⊙ Enable ○ Disable
Configured MTU:	1500
Actual MTU:	1432
Status	🔎
	Submit

Figure 4-9 PPPoE mode

The following describes the information shown on the page.

- **PVC**: Displaying the PVC that you are making modification.
- **Operation Mode**: Select **Enable** to enable the PVC for initial connection.
- **VPI/VCI**: For the default value, see "8.1 Factory Settings". You can change it to the value provided by your ISP.
- **Encapsulation**: You can select either **LLC** or **VC**-**Mux**.
- **Default Route**: If you select **Enable**, the gateway IP address will be used as the default route for data transmission.

  If you specify the default gateway, the data for which there is no route in the routing table will be forwarded through the WAN interface specified by the default route.

If you do not specify the default gateway, the data for which there is no route in the routing table will be discarded. Only the data for which there is a route in the routing table will be forwarded through the WAN interface.

- **IGMP**: IGMP is a multicast protocol in the Internet protocol household, used for IP host computer reporting the status of their group members to any adjacent router. Select **Enable** or **Disable** to enable or disable it.
- **Traffic Index**: Select the index for ATM traffic from the drop-down list.
- **Service Name**: If the service name is not designated, PPPoE will search for a server automatically and dial.
  If the service name is designated, PPPoE will dial the designated server only.
- **Username** and **Password**: Enter the username and password provided by ISP, and select the domain name from the dropping down list.
- **IP Unnumber**: You can select **Enable** or **Disable**. When **Enable** is selected, the Ethernet port address will be used as your IP address.
- **Use DNS**: It is recommended to select **Enable**, indicating that when PPP dial applies for IP and gateway, it also tries for DNS server IP at the same time. On the other hand, select **Disable**, indicating that obtaining DNS server not from PPP dial, and needed to manually enter the addresses of primary DNS server and secondary DNS server on the DNS configuration page.

- **Configured MTU**: Enter the maximum transmission unit (MTU), that is, the maximum bytes of the packet transmitted during connection.
- **Actual MTU**: Read-only value, displaying the actual value of MTU.
- **Status**; Click 🔎 to display the PPP status configuration page as shown in Figure 4-10.

PPP Status

Item	Description
WAN IP Address	0.0.0.0
Gateway IP Address	0.0.0.0
PPP Up Time	0:0:0
Oper. Status	No Activity
Inactivity TimeOut (mins)	5
Change Status	⦿ Always On ○ StartOnData ○ Manual
	Connect
	Submit Close Refresh

Figure 4-10 PPP status

The following describes the information shown on the page:

- **WAN IP Address**: Displaying the IP address of WAN port.
- **Gateway IP Address**: Displaying the gateway IP address of WAN port.
- **PPP Up Time**: Displaying the PPP up time.
- **Oper**. **Status**: Displaying the WAN port's operation status.
- **Inactivity TimeOut (mins)**: When you select **StartOnData** in **Change Status** option, you can set this value.
- **Change Status**: There are three options for selection: **Always On**, **StartOnData** and **Manual**. If you select

Always On, MT882 will establish the PPP dialing when it is powered on. If you select **StartOnData**, MT882 will establish the PPP dialing when receive a linking request. If you select **Manual**, the PPP dialing will be established manually.

After the configuration, click **Submit** to apply the settings, and click **Close** to return the main page.

II. Save

- Click **Submit** to save the settings in the RAM.
- To save this configuration changes permanently, enter the **Save & Reboot** page, select **Save** and click **Submit** to save new settings.

4.6.4 IPoA

I. Configuration Page

Select **IPoA** from the drop-down menu of **Mode** to display the page as shown in Figure 4-11.

PVC	PVC-0
Operation Mode	⊙ Enable ○ Disable
VPI/VCI	0 / 35
Mode	IPoA ▼
Encapsulation	⊙ LLC ○ VC-Mux
IP Address	0 0 0 0
Submask	0 0 0 0
Default Route	⊙ Enable ○ Disable
Gateway IP Address	0 0 0 0
IGMP	⊙ Enable ○ Disable
Traffic Index:	0 ▼
Configured MTU:	9180
Actual MTU:	1500
	Submit

Figure 4-11 IPoA mode

The following describes the information shown on the page:

- **PVC**: Displaying the PVC that you are making modification.
- **Operation Mode**: You can use the default value **Enable**, which enables the PVC for initial connection.
- **VPI/VCI**: For the default value, see "8.1 Factory Settings". You can change it to the value provided by your ISP.
- **Encapsulation**: You can select either **LLC** or **VC**-**Mux**.
- **IP Address** and **Submask**: Enter the IP address and submask of the WAN interface provided by your ISP. Never confuse it with the LAN IP address.
- **Default Route**: If you select **Enable**, the gateway IP address will be used as the default route for data transmission.
  If you specify the default gateway, the data for which there is no route in the routing table will be forwarded through the

WAN interface specified by the default route. If you do not specify the default gateway, the data for which there is no route in the routing table will be discarded. Only the data for which there is a route in the routing table will be forwarded through the WAN interface.

- **Gateway IP Address**: Enter the gateway IP address provided by your ISP.
- **IGMP**: IGMP is a multicast protocol in the Internet protocol household, used for IP host computer reporting the status of their group members to any adjacent router. Select **Enable** or **Disable** to enable or disable it.
- **Traffic Index**: Select the index for ATM traffic from the drop-down list.
- **Configured MTU**: Enter the maximum transmission unit (MTU), that is, the maximum bytes of the packet transmitted during connection.
- **Actual MTU**: Read-only value, displaying the actual value of MTU.

II. Save

- Click **Submit** to save the settings in the RAM.
- To save this configuration changes permanently, enter the **Save & Reboot** page, select **Save** and click **Submit** to save new settings.

4.6.5 Bridged+DHCP

I. Configurarion Page

Select **Bridged+DHCP** from the drop-down menu of **Mode** to display the page as shown in Figure 4-12. The IP address can be obtained automatically from DHCP server in this mode.

PVC	PVC-0
Operation Mode	⊙ Enable ○ Disable
VPI/VCI	0 / 35
Mode	Bridged+DHCP ▼
Encapsulation	⊙ LLC ○ VC-Mux
Default Route	⊙ Enable ○ Disable
IGMP	⊙ Enable ○ Disable
Traffic Index:	0 ▼
Configured MTU:	9164
Actual MTU:	1500
	Submit

Figure 4-12 Bridged+DHCP mode

The following describes the information shown on the page:

- **PVC**: Displaying the PVC that you are making modification.
- **Operation Mode**: You can use the default value **Enable**, which enables the PVC for initial connection.
- **VPI/VCI**: For the default value, see "8.1 Factory Settings". You can change it to the value provided by your ISP.
- **Encapsulation**: You can select either **LLC** or **VC-Mux**.
- **Default Route**: If you select **Enable**, the gateway IP address will be used as the default route for data transmission.
  If you specify the default gateway, the data for which there

is no route in the routing table will be forwarded through the WAN interface specified by the default route. If you do not specify the default gateway, the data for which there is no route in the routing table will be discarded. Only the data for which there is a route in the routing table will be forwarded through the WAN interface.

- **IGMP**: IGMP is a multicast protocol in the Internet protocol household, used for IP host computer reporting the status of their group members to any adjacent router. Select **Enable** or **Disable** to enable or disable it.
- **Traffic Index**: Select the index for ATM traffic from the drop-down list.
- **Configured MTU**: Enter the maximum transmission unit (MTU), that is, the maximum bytes of the packet transmitted during connection.
- **Actual MTU**: Read-only value, displaying the actual value of MTU.

II. Save

- Click **Submit** to save the settings in the RAM.
- To save this configuration changes permanently, enter the **Save & Reboot** page, select **Save** and click **Submit** to save new settings.

4.6.6 Bridged+Static IP

I. Configuration Page

Select **Bridged+Static IP** from the drop-down menu of **Mode** to display the page as shown in Figure 4-13.

PVC	PVC-0
Operation Mode	⊙ Enable ○ Disable
VPI/VCI	0 / 35
Mode	Bridged+Static IP ▾
Encapsulation	⊙ LLC ○ VC-Mux
IGMP	⊙ Enable ○ Disable
Traffic Index:	0 ▾
IP Address	0 0 0 0
Submask	0 0 0 0
Default Route	⊙ Enable ○ Disable
Gateway IP Address	0 0 0 0
Configured MTU:	9164
Actual MTU:	1500
	Submit

Figure 4-13 Bridged+Static IP mode

The following describes the information shown on the page:

- **PVC**: Displaying the PVC that you are making modification.
- **Operation Mode**: You can use the default value **Enable**, which enables the PVC for initial connection.
- **VPI/VCI**: For the default value, see "8.1 Factory Settings". You can change it to the value provided by your ISP.
- **Encapsulation**: You can select either **LLC** or **VC**-**Mux**.
- **IGMP**: IGMP is a multicast protocol in the Internet protocol household, used for IP host computer reporting the status of their group members to any adjacent router. Select **Enable** or **Disable** to enable or disable it.
- **Traffic Index**: Select the index for ATM traffic from the drop-down list.
- **IP Address** and **Submask**: Enter the IP address and submask of the WAN interface provided by your ISP.

- **Default Route**: If you select **Enable**, the gateway IP address will be used as the default route for data transmission.
  If you specify the default gateway, the data for which there is no route in the routing table will be forwarded through the WAN interface specified by the default route. If you do not specify the default gateway, the data for which there is no route in the routing table will be discarded. Only the data for which there is a route in the routing table will be forwarded through the WAN interface.
- **Gateway IP Address**: Enter the gateway IP address provided by your ISP.
- **Configured MTU**: Enter the maximum transmission unit (MTU), that is, the maximum bytes of the packet transmitted during connection.
- **Actual MTU**: Read-only value, displaying the actual value of MTU.

II. Save

- Click **Submit** to save the settings in the RAM.
- To save this configuration changes permanently, enter the **Save & Reboot** page, select **Save** and click **Submit** to save new settings.

4.7 LAN Settings

Click **Basic** > **LAN Settings** in the navigation bar to display the **LAN Settings** page as shown in Figure 4-14. The default setting of LAN IP address can be changed to meet customer's LAN.

LAN Settings

Notice:Please check that mask must be same as your local PC.

LAN Configuration				
IP Address	192	168	1	1
Subnet Mask	255	255	255	0
IGMP	⦿ Enable ○ Disable			
USB IP Address	192	168	1	2
USB Subnet Mask	255	255	255	0
IGMP	⦿ Enable ○ Disable			
	Submit			

Figure 4-14 LAN settings

Make sure that the IP address of LAN and the local PCs are in the same subnet.

The following describes the information shown on the page.

- **IP Address**: Enter the IP address of Ethernet interface.
- **Subnet Mask**: Enter the subnet mask of Ethernet interface.
- **IGMP**: IGMP is a multicast protocol in the Internet protocol household, used for IP host computer reporting the status of their group members to any adjacent router. Select **Enable** or **Disable** to enable or disable it.
- **USB IP Address**: Enter the IP address of USB interface.
- **USB Subnet Mask**: Enter the subnet mask of USB interface.

Note:

The public IP address that ISP assigned is not LAN IP address. The public IP address identifies the WAN interface through which the ADSL router connects to Internet.

II. Save

- Click **Submit** to save the settings in the RAM.
- To save this configuration changes permanently, enter the **Save & Reboot** page, select **Save** and click **Submit** to save new settings.

Note:

You need to log in again after you change the IP address.

4.8 DHCP Settings

Click **Basic** > **DHCP** in the navigation bar to display the **DHCP Settings** page. MT882 provides two types of DHCP service: DHCP Server and DHCP Relay.

I. None

In this mode, the DHCP service is disabled. You need to assign the IP address to your PC manually, or set the PC to obtain the IP address automatically from the DHCP server in LAN or from ISP.

DHCP Settings

DHCP Mode		
⦿ None	○ DHCP Server	○ DHCP Relay

Figure 4-15 DHCP mode-None

II. DHCP Server

MT882 can be configured as DHCP server of LAN. Then the ADSL terminal will provide IP settings for your PC. The DHCP mode-DHCP Server page is shown in Figure 4-16. You do not need to configure the gray items.

DHCP Settings

DHCP Mode

○ None	● DHCP Server	○ DHCP Relay

DHCP Server Settings

Start IP Address	192	.168	.1	.3
End IP Address	192	.168	.1	.65
Netmask	255	.255	.255	.0
Lease time:	86400	seconds		
DNS Address	0	.0	.0	.0
SDNS Address	0	.0	.0	.0

Excluded IP	**Excluded IP Address**			**Action(s)**
	No Excluded IP!			
	0	.0	.0	.0 [Add]

[Submit]

Lease IP Address	Netmask	Mac Address	Time Remaining
No entry!			

[Refresh]

Figure 4-16 DHCP mode-DHCP Server

The following describes the information shown on the page:

- **Start/End IP Address**: The range of IP addresses that released by DHCP server.
- **Netmask**: Enter the subnet mask of Ethernet interface.
- **Lease Time**: When the lease time is up, the PC will release the current address and apply for a new IP address.
- **DNS Address**: Enter the primary DNS address provided by ISP.
- **SDNS Address**: Enter the secondary DNS address provided by ISP.
- **Excluded IP**: the IP address that can not be released from address pool.

III. DHCP Relay

MT882 can also be configured to relay DHCP packets, and the PC will be assigned IP address automatically. The **DHCP mode-DHCP Relay** page is shown in Figure 4-17.

DHCP Settings

DHCP Mode		
○ None	○ DHCP Server	⊙ DHCP Relay
DHCP Relay Settings		
DHCP Server Address	0 . 0 . 0 . 0	

Interfaces Running DHCP Relay	Action(s)
eth-0	🗑
ppp-0	🗑
usb-0	🗑
eth-0 ▼	Add

Submit

Figure 4-17 DHCP mode-DHCP Relay

The following describes the information shown on the page.

- **DHCP Server Address**: Enter the assigned address in the field.
- **Interfaces Running DHCP Relay**: Select the eth value from drop-down menu, then click **Add**.
- **Action**: Click the icon 🗑 to delete the added DHCP interface.

IV. Save

- Click **Submit** to save the settings in the RAM.

- To save this configuration changes permanently, enter the **Save & Reboot** page, select **Save** and click **Submit** to save new settings.

4.9 DNS Settings

Click **Basic** > **DNS** in the navigation bar to display the **DNS Settings** page as shown in Figure 4-18.

I. Configuration Page

DNS Settings

DNS Configuration	
DNS Relay	⊙ Enable ○ Disable
Primary DNS Server	0 . 0 . 0 . 0
Secondary DNS Server	0 . 0 . 0 . 0
	Submit

Figure 4-18 DNS settings

ISP provides primary and secondary DNS addresses. Normally the primary DNS is responsible for domain name service. When primary DNS server is shut down or overloaded, the secondary DNS can provide the service.

The following describes the information shown on the page:

- **DNS Relay**: If you select **Enable**, you need to enter the primary and secondary DNS IP address provided by ISP.
- **Primary DNS Server**: Enter the IP address of primary DNS server.

- **Secondary DNS Server**: Enter the IP address of secondary DNS server.

II. Save

- Click **Submit** to save the settings in the RAM.
- To save this configuration changes permanently, enter the **Save & Reboot** page, select **Save** and click **Submit** to save new settings.

4.10 NAT Settings

Click **Basic** > **NAT** in the navigation bar to enter the **NAT Settings** pages. Network Address Translation (NAT) is a method for disguising the private IP addresses on your LAN as the public IP address on the Internet. You define NAT rules that specify exactly how and when to translate between public and private IP addresses.

I. Configuration Page

Select **DMZ** and click **New** to display the page as shown in Figure 4-19.

NAT

Figure 4-19 NAT settings-DMZ

The following describes the specific information shown on the **NAT Settings-DMZ** page.

- **Rule Flavor**: There are three rules: **DMZ**, **NAPT** and **Redirect**.
- **Protocol**: This selection specifies which type of Internet communication will be subject to this translation rule.
- **Local IP From**: Enter the starting IP of the range of private address you want to translate. You can specify that data from all LAN addresses should be translated by typing 0 (zero) in each From field and 255 in each To field. Or, enter the same address in both fields if the rule only applies to one LAN computer.
- **Local IP To**: Enter the ending IP of the range of private address you want to translate.
- **Global IP From**: The beginning public IP address that will be used to disguise the private IP address.
- **Global IP To**: The ending IP address of public address that will be used to disguise the private IP address.

Huawei Technologies Proprietary

- **Action**: View or delete a NAT rule.
- **Local Address**: Enter the private IP address you want to translate.

Select **NAPT** to display the page shown as below.

NAT

NAT Settings						
○ DMZ		⊙ NAPT		○ Redirect		○ None

Rule Flavor	Protocol	Local IP From	Local IP To	Global IP From	Global IP To	Action (s)
NAPT	ANY	0.0.0.0	255.255.255.255	-	-	🗑🔍
Click 'New' to create a new entry.						
			New			

Figure 4-20 NAT settings-NAPT

Click the icon 🔍 to display the pages shown as below.

NAT

NAT Settings						
○ DMZ		⊙ NAPT		○ Redirect		○ None

Rule Flavor	Protocol	Local IP From	Local IP To	Global IP From	Global IP To	Action (s)
NAPT	ANY	0.0.0.0	255.255.255.255	-	-	🗑🔍
Click 'New' to create a new entry.						
			New			

Rule Flavor	NAPT
IF Name	All
Local Address From	0.0.0.0
Local Address To	255.255.255.255
Global IP From	0.0.0.0
Global IP To	0.0.0.0

Figure 4-21 NAT settings-NAPT Detail

Click **New** to display the page shown as below.

Figure 4-22 NAT settings-New Entry

The following describes the specific information shown on the page as Figure 4-21 and Figure 4-22.

- **Local Address From**: Enter the starting IP of the range of private address you want to translate. You can specify that data from all LAN addresses should be translated by typing 0 (zero) in each From field and 255 in each To field. Or, enter the same address in both fields if the rule only applies to one LAN computer.

- **Local Address To**: Enter the ending IP of the range of private address you want to translate.

  If you use the default settings both in **Local Address From** and **Local Address To**, all the IP address in LAN will be translated.

  If there is only one PC, please enter the same IP address in **Local Address From** and **Local Address To**.

Select **Redirect** firstly, and then click **New** to display the page as shown in Figure 4-23.

Figure 4-23 NAT settings-Redirect

The following describes the specific information shown on the **NAT Settings-Redirect** page as.

- **Protocol**: This selection specifies which type of Internet communication will be subject to this translation rule. You can select **TCP** or **UDP**.
- **Local Address**: Enter the private IP address you want to translate.
- **Global IP From**: Enter the beginning public IP address provided by ISP.
- **Global IP To**: Enter the ending public IP address provided by ISP. If there is only one PC, please enter the same IP address in both **Global IP From** and **Global IP To**.

- **Destination Port From**: Enter the starting port ID (or a range) that you expect to see on incoming packets destined for the LAN computer for which this rule is being created. With the ending port ID (or a range) specified in the next field, incoming traffic that meets these criteria will be redirected to the Local Port number you specified.
- **Destination Port To**: Enter the ending port ID (or a range).

Select **None** to display the page shown as below.

Figure 4-24 NAT settings-None

II. Save

- Click **Submit** to save the settings in the RAM.
- To save this configuration changes permanently, enter the **Save & Reboot** page, select **Save** and click **Submit** to save new settings.

4.11 IP Route

Click **Basic** > **IP Route** in the navigation bar to display the **IP Route** page as shown in Figure 4-25.

IP routes are used to define gateways and hops used to route data traffic. Most users will not need to use this feature as the

previously configured default gateway and LAN IP settings on your host computers should be sufficient.

I. Configuration Page

The IP route configuration page is shown as below.

IP Route

Destination	Netmask	NextHop	IF Name	Route Type	Action(s)
127.0.0.0	255.0.0.0	127.0.0.1	lo-0	Direct	
192.168.1.0	255.255.255.0	192.168.1.1	eth-0	Direct	🗑
192.168.1.1	255.255.255.255	127.0.0.1	lo-0	Direct	
192.168.1.2	255.255.255.255	127.0.0.1	lo-0	Direct	
Click 'New' to create a new entry.					
New					

Figure 4-25 IP route

II. Add Route

If there are more than two networks or subnets in LAN, or customers are connecting to more than two ISPs or to remote intranet, the additional routes are required. Click **New** to add new IP route, the setting page is shown in Figure 4-26.

IP Route

Destination	Netmask	NextHop	IF Name	Route Type	Action(s)
127.0.0.0	255.0.0.0	127.0.0.1	lo-0	Direct	
192.168.1.0	255.255.255.0	192.168.1.1	eth-0	Direct	🗑
192.168.1.1	255.255.255.255	127.0.0.1	lo-0	Direct	
192.168.1.2	255.255.255.255	127.0.0.1	lo-0	Direct	
Click 'New' to create a new entry.					
		New			
Destination		0 . 0 . 0 . 0			
Netmask		0 . 0 . 0 . 0			
Gateway/NextHop		0 . 0 . 0 . 0			
		Submit			

Figure 4-26 IP route-New

The following describes the information shown on each page.

- **Destination**: Specifying the IP address of the destination computer. The destination can specify the IP address of a specific computer or an entire network. It can also be specified as all zeros to indicate that this route should be used for all destinations for which no other routes are defined (this is the route that creates the default gateway).
- **Netmask**: Indicating which parts of the destination address refer to the network and which parts refer to a computer on the network. The default gateway uses a netmask of 0.0.0.0.
- **NextHop**: Specifying the next IP address to send data to when its final destination is that shown in the destination column.
- **IF Name**: Displaying the name of the interface through which to data is forwarded to the specified next hop.

- **Route Type**: Displaying whether the route is direct or indirect. In a direct route, the source and destination computers are on the same network, and MT882 attempts to directly deliver the data to the computer. In an indirect route, the source and destination computers are on different networks, and MT882 forwards data to a device on another network for further handling.

III. Save

- Click **Submit** to save the settings in the RAM.
- To save this configuration changes permanently, enter the **Save & Reboot** page, select **Save** and click **Submit** to save new settings.

4.12 ATM Traffic

I. Configuration Page

Click **Basic** > **ATM Traffic** to display the **ATM Traffic** page as shown in Figure 4-27. ATM traffic refers to the traffic in ATM mode.

ATM Traffic

Traffic Index	Type	Service Category	Creator	Action(s)
0	NOCLP_NOSCR	UBR	nonilmi	🗑 🔎
1	NOCLP_NOSCR	UBR	ilmi	🗑 🔎
Click 'New' to create a new entry.				
		New		

Figure 4-27 ATM traffic

Click **New** to add new traffic, the setting page is shown in Figure 4-28.

ATM Traffic

Traffic Index	Type	Service Category	Creator	Action(s)
0	NOCLP_NOSCR	UBR	nonilmi	🗑🔍
1	NOCLP_NOSCR	UBR	ilmi	🗑🔍

Click 'New' to create a new entry.

New

Traffic Index:	____ (range: 0~8)
Service Category:	UBR ▼
Type:	NOCLP_NOSCR ▼
pcr:	____
mcr:	____
scr:	____
cdvt:	____
mbs:	____

Submit

Figure 4-28 ATM traffic-New

The following describes the information shown on the page:

- **Traffic Index**: the ID number of ATM traffic.
- **Type**: the traffic type of created ATM.
- **Service Category**: the service category of created ATM.
- **Creator**: the name of creator.
- **Action**: Click icon 🗑 to delete an existed ATM from table; Click icon 🔍 to view the parameters of an existed DHCP server.
- **New:** Click this button to add a new traffic ID.
- **Traffic Index**: create a traffic index to control ATM traffic.
- **pcr:** maximum rate for cell transmitting.
- **mcr:** minimum acceptable cell transmitting rate.

- **scr:** average cell transmitting rate of long time.
- **cdvt:** maximum acceptable cell vibration.
- **mbs:** maximum burst size.

II. Save

- Click **Submit** to save the settings in the RAM.
- To save this configuration changes permanently, enter the **Save & Reboot** page, select **Save** and click **Submit** to save new settings.

4.13 RIP

Click **Advanced** > **RIP** in the navigation bar to display the **RIP** page as shown in Figure 4-29. Routing Information Protocol (RIP) is an Internet protocol. By using the protocol, the routing information can be shared through ADSL lines with LAN, ISP and other remote networking devices.

I. Configuration Page

RIP

RIP Settings	
RIP Status	○ Enable ⦿ Disable
Age(seconds)	180
Update Time(seconds)	30

IF Name	Metric	Send Mode	Receive Mode	Action(s)
ppp-0	1	RIP1	RIP1	🗑
eth-0 ▾	1	RIP1COMPAT ▾	RIP1 ▾	Add

Submit

Figure 4-29 RIP

The following describes the information shown on the **RIP** page.

- **RIP Status**: There are two statuses: **Enable** and **Disable**.
- **Age (seconds)**: The length of time in seconds that the device's RIP table will retain each route that it learns from adjacent computers.
- **Update Time (seconds)**: Specifying how frequently MT882 will send out its routing table to its neighbors.
- **IF Name**: Select the name of interface on which you want to enable RIP.
- **Metric**: Enter the hop count of interface. RIP uses a "hop count" as a way to determine the best path to a given destination in the network. The hop count is the sum of the metric values assigned to each port through which data is passed before reaching the destination. Among several alternative routes, the one with the lowest hop count is considered the fastest path.
- **Send Mode**: Indicating the RIP version this interface will use when it sends its route information to other devices.
- **Receive Mode**: Indicating the RIP version(s) in which information must be passed to MT882 in order for it to be accepted into its routing table.
- **Action**: Click **Add** to add the new entry.

- RIP version 1 is the original RIP protocol. If the device only support RIP version 1, please select RIP1.

- RIP version 2 is preferred. It is developed to support the features such as prefix routing, subnet mask, next hop and authentication. If all the devices in LAN support RIP version 2, please select RIP2.

II. Save

- Click **Submit** to save the settings in the RAM.
- To save this configuration changes permanently, enter the **Save & Reboot** page, select **Save** and click **Submit** to save new settings.

4.14 Firewall

Click **Advanced** > **Firewall** in the navigation bar to display the **Firewall** page as shown in Figure 4-30. The firewall enables you to protect the system against denial of service (DoS) attacks and other types of malicious accesses to your LAN. You can also specify how to monitor attempted attacks, and who should be automatically notified.

I. Configuration Page

Firewall

Item	Status
Blacklist Status	⦿ Enable ○ Disable
Blacklist Period(min)	10
Attack Protection	⦿ Enable ○ Disable
DOS Protection	⦿ Enable ○ Disable
Max Half open TCP Conn.	25
Max ICMP Conn.	25
Max Single Host Conn.	70
Submit	

Figure 4-30 Firewall

The following describes the information shown on the **Firewall** page.

- **Blacklist Status**: If you want the device to maintain and use a blacklist, select **Enable**. Select **Disable** if you do not want to maintain a list.
- **Blacklist Period (min)**: Specifying the number of minutes that a computer's IP address will remain on the blacklist (that is, all traffic originating from that computer will be blocked from passing through any interface on MT882).
- **Attack Protection**: Select **Enable** to protect network against the attack such as IP Spoofing, Tear Drop, Smurf and Fraggle, Land attack, Ping of Death.
- **DoS Protection**: Select **Enable** to use the following denial of service protections: SYN DoS, ICMP DoS, Per-host DoS protection.

- **Max Half open TCP Conn**.: Set the percentage of concurrent IP sessions that can be in the half-open state. In ordinary TCP communication, packets are in the half-open state only briefly as a connection is being initiated; the state changes to active when packets are being exchanged, or closed when the exchange is complete. TCP connections in the half-open state can use up the available IP sessions. If the percentage is exceeded, then the half-open sessions will be closed and replaced with new sessions as they are initiated.
- **Max ICMP Conn**.: Set the percentage of concurrent IP sessions that can be used for ICMP messages. If the percentage is exceeded, then older ICMP IP sessions will be replaced by new sessions as they are initiated.
- **Max Single Host Conn**.: Set the percentage of concurrent IP session that can originate from a single computer. This percentage should take into account the number of hosts on the LAN.

II. Save

- Click **Submit** to save the settings in the RAM.
- To save this configuration changes permanently, enter the **Save & Reboot** page, select **Save** and click **Submit** to save new settings.

4.15 IP Filter Settings

The IP filter feature enables you to create rules that control the forwarding of incoming and outgoing data between your LAN and the Internet and within your LAN.

4.15.1 IP Filter

Click **Advanced** > **IP Filter** in the navigation bar to display the page as shown in Figure 4-31.

I. Configuration Page

IP Filter

Item	Status
Security Level	High
Public Default Action	Accept
Private Default Action	Accept

Rule ID	Interface	Rule Status	Direction	Rule Action	In Interface	Log	Rule Description	Oper. Status	Action (s)
510	Private	Disable	Incoming	Accept	N/A	Disable	1.Protocol eq TCP 2.TCP Flag All 3.Dest Port equal to 80	🟢	🗑
511	Private	Disable	Incoming	Accept	N/A	Disable	1.Protocol eq TCP 2.TCP Flag All 3.Dest Port equal to 23	🟢	🗑
512	Private	Disable	Incoming	Accept	N/A	Disable	1.Protocol eq TCP 2.TCP Flag All 3.Dest Port equal to 21	🟢	🗑
513	Private	Disable	Incoming	Accept	N/A	Disable	1.Protocol eq TCP 2.TCP Flag All 3.Dest Port equal to 22	🟢	🗑
514	Private	Disable	Incoming	Accept	N/A	Disable	1.Protocol eq UDP 2.Dest Port equal to 69	🟢	🗑
515	Private	Disable	Incoming	Accept	N/A	Disable	1.Protocol eq ICMP	🟢	🗑
520	Public	Disable	Incoming	Accept	N/A	Disable	1.Protocol eq TCP 2.TCP Flag All 3.Dest Port equal to 80	🟢	🗑

Figure 4-31 IP filter

II. Parameters Explanation

- **Security Level**: This setting determines which IP filter rules take effect, based on the security level specified in each rule. For example, when **High** is selected, only those rules that are assigned a security value of **High** will be in effect. The same is true for the **Medium** and **Low** settings. When **None** is selected, IP filtering is disabled.

- **Public/Private Default Action**: This setting specifies a default action to be taken (**Accept** or **Deny**) on private or public-type device interfaces when they receive packets that do not match any of the filtering rules. You can specify a different default action for each interface type.

4.15.2 Add IP Filter Rules

Click **New** in the **IP Filter** page to display the **IP Filter-New** page as shown in Figure 4-32.

I. Configuration Page

IP Filter

Figure 4-32 IP filter-New

The following describes the information shown on the **IP Filter**-**New** page:

- **Rule Status**: Select **Enable** to enable the IP filter rule.
- **Rule ID**: Each rule must be assigned a sequential ID number. Rules are processed from lowest to highest on each data packet, until a match is found. It is recommended that you assign rule IDs in multiples of 5 or 10 (for example, 10, 20, 30) so that you leave enough room between them for inserting a new rule if necessary.
- **Action**: Specifying what the rule will do to a packet when the packet matches the rule criteria. The action can be **Accept** (forward to destination) or **Deny** (discard the packet).
- **Direction**: Specifying whether the rule should apply to data packets that are incoming or outgoing on the selected interface. **Incoming** refers to packets coming in to the LAN on the interface, and **Outgoing** refers to packets going out from the LAN. You can use rules that specify the incoming direction to restrict external computers from accessing your LAN.
- **Interface**: The interface on the device on which the rule will take effect.
- **In Interface**: The interface from which packets must have been forwarded to the interface specified in the previous selection. This option is valid only on rules defined for the outgoing direction.
- **Log Option**: When **Enable** is selected, a log entry will be created on the system each time this rule is invoked. The log entry will include the time of the violation, the source

address of the computer responsible for the violation, the destination IP address, the protocol being used, the source and destination ports, and the number of violations occurring in the previous **x** minutes. (Logging may be helpful when troubleshooting.) This information can also be e-mailed to administrators.

- **Security Level**: The security level that must be enabled globally for this rule to take affect. A rule will be active only if its security level is the same as the globally configured setting (shown on the main IP Filter page). For example, if the rule is set to **Medium** and the global firewall level is set to **Medium**, then the rule will be active; but if the global firewall level is set to **High** or **Low**, then the rule will be inactive.
- **Blacklist Status**: If you want the device to maintain and use a blacklist, select **Enable**. Select **Disable** if you do not want to maintain a list.
- **Log Tag**: A description of up to 16 characters to be recorded in the log in the event that a packet violates this rule. Be sure to set the Log Option to **Enable** if you configure a Log Tag.
- **Src IP Address**: IP address criteria for the source computer(s) from which the packet originates. In the drop-down list, you can configure the rule to be invoked on packets containing:
- **any**: any source IP address.
  - **lt**: any source IP address that is numerically less than the specified address.

- **lteq**: any source IP address that is numerically less than or equal to the specified address.
- **gt**: any source IP address that is numerically greater than the specified address.
- **gteq:** any source IP address that is numerically greater than or equal to the specified address.
- **eq**: any source IP address that is numerically equal to the specified address.
- **neq**: any source IP address that is not equal to the specified address.
- **range**: any source IP address that is within the specified range, inclusive.
- **out of range**: any source IP address that is outside the specified range.
- **self**: the IP address of MT882 interface on which this rule takes effect.

- **Dest IP Address**: IP address criteria for the destination computer(s) (that is, the IP address of the computer to which the packet is being sent). In addition to the options described for the Src IP Address field, the following option is available:
  - **bcast:** Specifies that the rule will be invoked for any packets sent to the broadcast address for the receiving interface. When you select this option, you do not need to specify the address, so the address fields are dimmed.

- **Protocol**: IP protocol criteria that must be met for rule to be invoked. You can specify that packets must contain the selected protocol (eq), that they must not contain the

specified protocol (neq), or that the rule can be invoked regardless of the protocol (any). TCP, UDP, and ICMP are commonly used IP protocols; others can be identified by number, from 0-255, as defined by the Internet Assigned Numbers Authority (IANA).

- **Apply Stateful Inspection**: If this option is selected, then **Stateful Filtering** is performed and the rule is also applied in the other direction on the given interface during an IP session.

- **Source Port**: Port number criterion for the computer(s) from which the packet originates. This field will be dimmed (unavailable for entry) unless you have selected TCP or UDP as the protocol. See the description of Src IP Address for the selection options.

- **Dest Port**: Port number criterion for the destination computer(s) (that is, the port number of the type of computer to which the packet is being sent). This field will be dimmed (unavailable for entry) unless you have selected TCP or UDP as the protocol. See the description of Src IP Address for the selection options.

- **TCP Flag**: Specifies whether the rule should apply only to TCP packets that contain the synchronous (SYN) flag, or to all TCP packets. This field will be dimmed (unavailable for entry) unless you selected TCP as the protocol.

- **ICMP Type**: Specifies whether the value in the type field in ICMP packet headers will be used as a criterion. The value can be any decimal value from 0-255. You can specify that the value must equal (eq) or not equal (neq) to the specified value, or you can select **any** to enable the rule to

be invoked on all ICMP packets. This field will be dimmed (unavailable for entry) unless you specify ICMP as the protocol.

- **ICMP Code**: Specifies whether the value in the code field in ICMP packet headers will be used as a criterion. The code value can be any decimal value from 0-255. You can specify that the value must equal (eq) or not equal (neq) the specified value, or you can select **any** to enable the rule to be invoked on all ICMP packets. This field will be dimmed (unavailable for entry) unless you specify ICMP as the protocol.

- **IP Frag Pkt**: Determines how the rule applies to IP packets that contain fragments. You can choose from the following options:

  - **Yes**: The rule will be applied only to packets that contain fragments.

  - **No**: The rule will be applied only to packets that do not contain fragments

  - **Ignore**: The rule will be applied to packets whether or not they contain fragments, assuming that they match the other criteria.

- **IP Option Pkt**: Determines whether the rule should apply to IP packets that have options specified in their packet headers.

  - **Yes**: The rule will be applied only to packets that contain header options.

  - **No**: The rule will be applied only to packets that do not contain header options.

- **Ignore**: The rule will be applied to packets whether or not they contain header options, assuming that they match the other criteria.

- **Packet Size**: Specifies that the IP Filter rule will take affect only on packets whose size in bytes matches this criterion. (**lt** = less than, **gt** = greater than, **lteq** = less than or equal to.)

When you finished selecting criteria, make sure that the **Enable** check box is selected at the top of the page, and then click **Submit**. After a confirmation page displays, the IP filter-configuration page will redisplay with the new rule showing in the table.

II. Save

- Click **Submit** to save the settings in the RAM.
- To save these configuration changes permanently, enter the **Save & Reboot** page, select **Save** and click **Submit** to save new settings.

4.16 QoS

Various applications that operated in MT882 have different requirements of priority level. Different applications will be classified by MT882 according to the different requirement of priority level, and the different priority level will be provided to each level with mode of Diffserv. MT882 sets the individual queue for each priority level, and then controls the output of each queue of priority.

Click **Advanced** > **QoS** in the navigation bar to set the priority level to the applications that operated in MT882.

The available options of QoS include: Application, ToS, Diffserv, 802.1p and VLAN Tag.

I. No QoS

Figure 4-33 QoS-No QoS

II. 802.1p

The label of 802.1p specifies 8 settings of priority weight from 0 (lowest) to 7 (highest). MT882 will determine the priority queue of traffic according to these labs of priority weight.

Figure 4-34 QoS-802.1p

The following describes the information shown on the **QoS**-**802.1p** page:

- **Priority Queue**: 4 priority queues. MT882 will set the received traffic into one of 4 priority queues for output. The packet with highest priority will be outputted firstly. If this queue is empty, the next packet with highest priority will be outputted, the rest may be deduced by analogy.
- **802.1p Range**: Select the priority range from drop-down menu.

III. DiffServ

DiffServ field is defined in RFC 2474 and 2475 that in order to replace ToS field. DiffServ integrates edge monitor and management, assignment and service priority. DiffServ provides different service priorities according to different requirements of QoS, in order to meet the requirement of different service.

Figure 4-35 QoS-DiffServ

The following describes the information shown on the **QoS**-**DiffServ** page:

- **Priority Queue**: 4 priority queues. MT882 will set the received traffic into one of 4 priority queues for output. The packet with highest priority will be outputted firstly. If this queue is empty, the next packet with highest priority will be outputted, the rest may be deduced by analogy.
- **DiffServ Range**: Select the priority range from drop-down menu.

IV. ToS

ToS is an 8-bit field, and also the second field of header group in IP packet. It is consist of two sub-fields: priority level sub-field and service type sub-field. The priority level sub-field will assign the priority for group within the queue. The group with higher priority will be sent firstly.

Figure 4-36 QoS-ToS

The following describes the information shown on the **QoS**-**ToS** page:

- **Priority Queue**: 4 priority queues. MT882 will set the received traffic into one of 4 priority queues for output. The

packet with highest priority will be outputted firstly. If this
queue is empty, the next packet with highest priority will be
outputted, the rest may be deduced by analogy.

- **ToS Range**: Select the priority range of field from
  drop-down menu.

V. VLAN Tag

VLAN Tag is a hexadecimal number, which added to the packet
that transmitted in VLAN. The VLAN tag is to indicate which VLAN is
the packet belongs to. Thus, the packet with the specified Tag will be
transmitted in priority while it is received by MT882.

Figure 4-37 QoS-VLAN Tag

The following describes the information shown on the
QoS-**VLAN Tag** page:

- **Priority Queue**: 4 priority queues. MT882 will set the
  received traffic into one of 4 priority queues for output. The
  packet with highest priority will be outputted firstly. If this

queue is empty, the next packet with highest priority will be outputted, the rest may be deduced by analogy.

- **VLAN Tag (in Hex)**: Enter the tag with hexadecimal number that needed to add into priority queue.

VI. Application

Some special applications, such as network game, videoconference, network phone, will transmit the audio, video and data synchronously. So you can set the priority level to the different types of traffic. So the traffic with higher priority will be processed firstly while the network is jammed.

Figure 4-38 QoS-Application

The following describes the information shown on the **QoS**-**Application** page:

- **Priority Queue**: 4 priority queues. MT882 will set the received traffic into one of 4 priority queues for output. The packet with highest priority will be outputted firstly. If this

queue is empty, the next packet with highest priority will be outputted, the rest may be deduced by analogy.

- **Application Type**: Select the application type from drop-down menu, which include: Voice, Video, IGMP, and Data.
- **RTP**: Enter the start and end port number in the blank of **Voice Data Start/End Port** and **Video Data Start/End Port**.

VII. Save

- Click **Submit** to save the settings in the RAM.
- To save this configuration changes permanently, enter the **Save & Reboot** page, select **Save** and click **Submit** to save new settings.

4.17 Blocked Protocols

Click **Advanced** > **Blocked Protocols** in the navigation bar to set the blocked protocols. MT882 is capable of sending and receiving information in a variety of protocol formats. The blocked protocols feature enables you to prevent MT882 from passing any data that uses a particular protocol.

Unlike the IP filter feature, you cannot specify additional criteria for blocked protocols, such as particular users or destinations. However, when you are certain that a particular protocol is not needed or wanted on your network, this feature provides a convenient way to discard such data before it is passed.

I. Configuration Page

Figure 4-39 Blocked protocols

To block a protocol, select the appropriate check box.

II. Save

- Click **Submit** to save the settings in the RAM.
- To save these configuration changes permanently, enter the **Save & Reboot** page, select **Save** and click **Submit** to save new settings.

4.18 ILMI

Click **Advanced** > **ILMI** in the navigation bar to enter the setting page of ILMI. ILMI (Interim Local Management Interface) allow user to set an interface, which to be activated while the existing ATM interfaces is toggling or temporarily failed.

ILMI

Notice: After the setting is finished, the system will reboot.

ILMI Settings	
ILMI Status	⦿ Enable ○ Disable
VPI	0
VCI	16
	Submit

Figure 4-40 ILMI

The following describes the information shown on the **ILMI** page:

- **ILMI Status**: Select the check box to enable or disable the ILMI mode.
- **VPI**: For the default value, see "8.1 Factory Settings". You can change it to the VPI provided by your ISP.
- **VCI**: For the default value, see "8.1 Factory Settings". You can change it to the VCI provided by your ISP.

4.19 ACL

Click **Advanced** > **ACL** in the navigation bar to enter the setting page of ACL. Access control list is used to allow or deny the access from one or more specific IP addresses in LAN and WAN.

I. Configuration Page

Figure 4-41 Access control list

The following describes the information shown on the **Access Control List** page:

- **ACL**: Select the check box to allow or deny the access LAN interface or WAN interface.
- **Add IP Address (max 5)**: Enter the IP address for the LAN interface or WAN interface. The maximum number of IP address can be entered is 5.

II. Save

- Click **Submit** to save the settings in the RAM.
- To save these configuration changes permanently, enter the **Save & Reboot** page, select **Save** and click **Submit** to save new settings.

4.20 UPnP

Click **Advanced** > **UPnP** in the navigation bar to enter the setting page of UPnP. Enable UPnP to allow the device that supports

UPnP to join in network dynamically, obtain IP address, transmit performance, find other devices and learn performance. If DHCP and DNS services are available on network, device can also use them. UPnP permit device to be off-line automatically without any ill effects on the device itself or in network.

I. Configuration Page

UPnP Configuration

Notice: Please Save & Reboot after changing the setting.

Item	Description
Status	○ Enable ● Disable
	Submit

Figure 4-42 UPnP

II. Save

- Click **Submit** to save the settings in the RAM.
- To save these configuration changes permanently, enter the **Save & Reboot** page, select **Save** and click **Submit** to save new settings.

4.21 System Management

Click **Tools** > **System Management** in the navigation bar to display the setting page as shown in Figure 4-43.

System Management

Username	Privilege	Action(s)
admin	Root	
user	Username	✏ 🗑
Click 'New' to create a new entry.		
	New	

Figure 4-43 System management

I. Change the password

For the normal user, only the password can be changed. Perform the following steps to change the password:

1) Open the System Management page;
2) Click the ✏ in the **Action(s)** column;
3) Enter the new password, confirm it and submit.

Username	user
Privilege	User
Password	••••
Confirm Password	••••
	Submit

Figure 4-44 User configuration-Modify

Save the settings in the **Save & Reboot** page and then restart the system to take effect the settings.

4.22 Diagnostics

Click **Tools** > **Diagnostics** in the navigation bar to perform the basic diagnostics for system. The diagnostics feature executes a series of test of your system software and hardware connections. Use this feature when working with your ISP to solve problems.

Diagnostics

Item	Description
PVC PVC-0 ▾	
Modem Connection Test	
Testing Ethernet connection	-----
Testing ADSL line for sync	-----
Testing Ethernet connection to ATM	-----
ATM Connection Test	
Testing ATM OAM segment ping	-----
Testing ATM OAM end to end ping	-----
ISP Connection Test	
Testing PPPoE server connectivity	-----
Testing PPPoE server session	-----
Testing authentication with server	-----
Validating assigned IP address 0.0.0.0	-----
Internet Connection Test	
Ping default gateway 0.0.0.0	-----
Ping Primary Domain Name Server	-----
Submit	

Figure 4-45 Diagnostics

Select the PVC from the drop-down list and click **Submit**. A message will appear, informing you whether the loop test succeeded or failed.

The diagnostics utility will run a series of test to check whether the device's connections are up and working. This takes only a few seconds. The program reports whether the test passed or failed. A test may be skipped if the program determines that no suitable interface is configured on which to run the test.

4.23 Log

Click **Tools** > **Log** in the navigation bar to display the **log** page as shown in Figure 4-46.

Log

Log Information
Wed May 10 10:57:17 2006 : STATUS ALARM : ETHER Interface Up : Interface - eth-0
Wed May 10 10:57:11 2006 : STATUS ALARM : System Up
Save Alarm   Clear
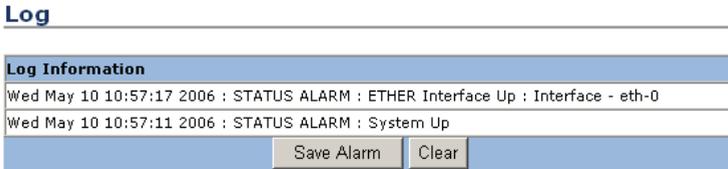
Figure 4-46 Log

You can view the logs of alarm triggered by system events. Click **Save Alarm** to save the log file to local disk. Click **Clear** to clear the logs.

4.24 Backup & Restore

Click **Tools** > **Backup & Restore** in the navigation bar to display the page as shown in Figure 4-47.

Backup & Restore

Configuration File	
	Browse...
Save Config	Upload

Figure 4-47 Backup & Restore

After finishing all the configurations, and if you want to save all the current configurations you have made, please click **Save Config** to save the configurations in the system. To make use of this configuration again later, you may click **Browse** to search for the file on your system, and then click **Upload** to start loading the configuration.

4.25 Save & Reboot

Click **Tools** > **Save & Reboot** in the navigation bar to specify the method of restart.

I. Configuration Page

Save & Reboot

Action		
⦿ Save	○ Reboot	○ Factory Setting Reboot
	Submit	

Figure 4-48 Save & Reboot

II. Parameters Explanation

- **Save:** Save the current settings into the permanent storage.
- **Reboot:** Put into effect any configuration changes that have been successfully saved to flash memory.
- **Factory Setting Reboot:** Reboot the device to default settings provided by your ISP or the manufacturer. Select this option to erase all custom settings.

You need to select the proper method to restart the system.

⚠ Caution:

Do not reboot the device using the Reset button on the rear panel of MT882 to activate new changes. This button resets the device settings to the manufacturer's default values. All custom settings will be lost.

---

5 Service Configuration

This section describes the configuration for six modes provided by MT882. The contents include:

- Preparation
- Pure Bridge configuration
- PPPoA configuration
- PPPoE configuration
- IPoA configuration
- Bridged+DHCP configuration
- Bridged+Static IP configuration

5.1 Preparation

Collect the following data before you start configuration:

Protocol Types	Virtual Dialup Mode	
	PPPoE	PPPoA
Preparing Information	Connection type	Connection type
	PPPoE user name	PPPoA user name
	PPPoE password	PPPoA password
	VPI/VCI	VPI/VCI
	Security protocol	Security protocol
	None	None

Protocol types	DSL mode			
	Pure Bridge	Bridged + Static IP	Bridged + DHCP	IPoA
Preparing information	Connection Type	Connection Type	Connection Type	Connection Type
	VPI/VCI	VPI/VCI	VPI/VCI	VPI/VCI
	None	WAN IP	None	WAN IP
	None	Subnet mask	None	Subnet mask
	None	Default gateway	None	Default gateway
	None	DNS	DNS	DNS

5.2 Pure Bridge Configuration

Configurations on MT882		
Location	Parameters	Comments
WAN Settings	PVC	Select any one from the six PVCs.
	Operation Mode	Select **Enable**.
	VPI/VCI	Enter the value provided by your ISP.
	Mode	Select **Pure Bridge**.
	Encapsulation	Enter the value provided by your ISP. You can use the default value **LLC**.
	Configured MTU	You can use the default value.
	Traffic Index	You can use the default value **0**.

Configurations on MT882		
Location	**Parameters**	**Comments**
Configurations on Your PC		
PPPoE Dial–up Application	Before connecting to the Internet, you need to have PPPoE dial–up application installed on the PC.	

5.3 PPPoA Configuration

Configurations on MT882		
Location	**Parameters**	**Comments**
WAN Settings	PVC	Select any one from the six PVCs.
	Operation Mode	Select **Enable**.
	VPI/VCI	Enter the value provided by your ISP.
	Mode	Select **PPPoA**.
	Encapsulation	Enter the value provided by your ISP. You can use the default value **LLC**.
	Default Route	Select **Enable**.
	IGMP	Select **Enable**.
	Traffic Index	You can use the default value **0**.
	User name and Password	Enter the values provided by your ISP, The default domain name is @clix.pt.
	IP Unnumber	Select **Disable**.
	DNS	Select **Enable**.
	Configured MTU	You can use the default value.
NAT	Enable the NAT function.	

Huawei Technologies Proprietary

Configurations on MT882		
Location	Parameters	Comments
DNS	Enable the DNS Relay function.	
DHCP Mode	Enable the DHCP Server function.	
Configurations on Your PC		
IP Address and Network Mask	Set to the mode of obtaining an IP address automatically.	
DNS	Set to the mode of obtaining a DNS server's IP address automatically.	

5.4 PPPoE Configuration

Configurations on MT882		
Location	Parameters	Comments
WAN Settings	PVC	Select any one from the six PVCs.
	Operation Mode	Select **Enable**.
	VPI/VCI	Enter the value provided by your ISP.
	Mode	Select **PPPoE**.
	Encapsulation	Enter the value provided by your ISP. You can use the default value **LLC**.
	Default Route	Select **Enable**.
	IGMP	Select **Enable**.
	Traffic Index	You can use the default value **0**.
	Service Name	Enter the name provided by your ISP.
	User name and Password	Enter the values provided by your ISP, The default domain name is @clix.pt.

Configurations on MT882		
Location	**Parameters**	**Comments**
	IP Unnumber	Select **Disable**.
	DNS	Select **Enable**.
	Configured MTU	You can use the default value.
NAT	Enable the NAT function.	
DNS	Enable the DNS Relay function.	
DHCP Mode	Enable the DHCP Server function.	
Configurations on Your PC		
IP Address and Network Mask	Set to the mode of obtaining an IP address automatically.	
DNS	Set to the mode of obtaining a DNS server's IP address automatically.	

5.5 IPoA Configuration

Configurations on MT882		
Location	**Parameters**	**Comments**
WAN Settings	PVC	Select any one from the six PVCs.
	Operation Mode	Select **Enable**.
	VPI/VCI	Enter the value provided by your ISP.
	Mode	Select **IPoA**.
	Encapsulation	Enter the value provided by your ISP. You can use the default value **LLC**.
	IP Address and Submask	Enter the values provided by your ISP.

Huawei Technologies Proprietary

Configurations on MT882		
Location	**Parameters**	**Comments**
	Default Route	Select **Enable**.
	Gateway IP Address	Enter the values provided by your ISP.
	IGMP	Select **Enable**.
	Traffic Index	You can use the default value **0**.
	Configured MTU	You can use the default value.
NAT	Enable the NAT function.	
DNS	Enable the DNS Relay function.	
DHCP Mode	Enable the DHCP Server function.	
Configurations on Your PC		
IP Address and Network Mask	Set to the mode of obtaining an IP address automatically.	
DNS	Set to the mode of obtaining a DNS server's IP address automatically.	

5.6 Bridged+DHCP Configuration

Configurations on MT882		
Location	**Parameters**	**Comments**
WAN Settings	PVC	Select any one from the six PVCs.
	Operation Mode	Select **Enable**.
	VPI/VCI	Enter the value provided by your ISP.
	Mode	Select **Bridged+DHCP**.

Huawei Technologies Proprietary

Configurations on MT882		
Location	**Parameters**	**Comments**
	Encapsulation	Enter the value provided by your ISP. You can use the default value **LLC**.
	Default Route	Select **Enable**.
	IGMP	Select **Enable**.
	Traffic Index	You can use the default value **0**.
	Configured MTU	You can use the default value.
NAT	Enable the NAT function.	
DNS	Enable the DNS Relay function.	
DHCP Mode	Enable the DHCP Server function.	
Configurations on Your PC		
IP Address and Network Mask	Set to the mode of obtaining an IP address automatically.	
DNS	Set to the mode of obtaining a DNS server's IP address automatically.	

5.7 Bridged+Static IP Configuration

Configurations on MT882		
Location	**Parameters**	**Comments**
WAN Settings	PVC	Select any one from the six PVCs.
	Operation Mode	Select **Enable**.
	VPI/VCI	Enter the value provided by your ISP.
	Mode	Select **Bridged+Static IP**.

Configurations on MT882		
Location	**Parameters**	**Comments**
	Encapsulation	Enter the value provided by your ISP. You can use the default value **LLC**.
	IGMP	Select **Enable**.
	Traffic Index	You can use the default value **0**.
	IP Address and Submask	Enter the values provided by your ISP.
	Default Route	Select **Enable**.
	Gateway IP Address	Enter the values provided by your ISP.
	Configured MTU	You can use the default value.
NAT	Enable the NAT function.	
DNS	Enable the DNS Relay function.	
DHCP Mode	Enable the DHCP Server function.	
Configurations on Your PC		
IP Address and Network Mask	Set to the mode of obtaining an IP address automatically.	
DNS	Set to the mode of obtaining a DNS server's IP address automatically.	

📖 **Note:**

For other advanced configurations, please refer to 4 Web-Based Management.

6 Troubleshooting

6.1 Locating Problems Quickly

Problem	Resolution
The Power indicator is off.	1) Make sure that MT882 is connected to the power supply properly. 2) Make sure that the power switch is turned on. 3) Make sure that the power supply conforms to the specification of MT882.
The ADSL LINK indicator is off.	1) Make sure the ADSL line is well connected. 2) Try to test with a telephone to ensure the telephone line before entering the house is valid. 3) Make sure that there is no capacitance or diode in the junction box. 4) Make sure MT882 and telephones are connected in the right way.
The LAN LINK indicator is off.	1) Make sure you use the right cables from MT882 to your PC. 2) Make sure the connection is secured. 3) Check if the NIC LED lights up. 4) Make sure your Network Adapter works normally by examining whether the item of "Networking Adapters" is labeled with "?" or "!". If it is, you may delete it and then click **Refresh** to reinstall. Otherwise, you may try the NIC in another slot. As a last resort, you have to replace the NIC.

Problem	Resolution
I cannot access the Internet.	Take the most common access mode as an example, in which a dial-up application is installed on the your computer: 1) Make sure that any of the problems above is not the reason. 2) Make sure that the dial-up application is correctly installed and set on your PC. 3) Make sure that you have entered the right user name and password. 4) Make sure "Use Proxy Server" is set properly for IE, if the problem still remains even after you have log into successfully. 5) Try to access different web sites, in case some Web server fails.

6.2 FAQs

Q: Why my PC is not able to access the Internet, even when the physical connections are normal?

Check whether the indicators are in normal status. If they are, adjust the MT882 settings by following the instructions of your ISP.

Q: What can I do if I forget my username and password for the Web-based Manager, or if I just cannot access the Web-based Manager?

1) Press the Reset button on the rear panel to restore the factory settings of MT882.

2) Change the IP address of the network adapter in your PC to 192.168.1.3.

3) Disable the proxy service.

4) Launch your Web browser and access http://192.168.1.1.

5) Use the default user name and password.

Q: My configuration is gone after rebooting MT882.

If you want to keep your settings after reboot MT882. Please go to Web-based Configuration Manager >**Tools** > **Save & Reboot**> **Save** to save your configurations.

Save & Reboot

Action		
⦿ Save	○ Reboot	○ Factory Setting Reboot
	Submit	

Figure 6-1 Save the changed settings

Q: I cannot upgrade with the new firmware.

Please make sure the file that you have downloaded is valid.

Q: Why does my PC fall off line sometimes even with all indicators are in normal status?

There are several scenarios may cause this problem.

1) Be disconnected by the ISP.
2) Some ISPs will have idle timeout setting to avoid wasting IP. When the end user connects to the Internet too long without any packet, the ISP will drop the connection. Please contact with your ISP about this problem.
3) Some ISPs do not provide a good quality ADSL signal line. Therefore, when the ADSL line is unstable, your connection will be dropped. Try with a telephone and find the status of your ADSL signal line.

4) If you have contacted the ISP and they promised the quality of ADSL line, it may be the hardware issue and please contact your vendor.

Q: When can I use the "Factory Setting Reboot" option?

If you changed some setting unconsciously in the Web Management Interface and you forgot the detailed values that you modified, please use the **Factory Setting Reboot** option to recover the factory default settings.

Q: How to restore the factory default setting?

Totally two methods:

1) Press the Reset button on the rear panel to take the factory default setting into effect;
2) Select the option **Factory Setting Reboot** in the **Save & Reboot** page, and then click **Submit**.

Q: How to connect MT882 with multiple telephones?

Connect MT882 and telephones as shown in Figure 6-2 and Figure 6-3. Note that MT882 needs splitters for proper working.
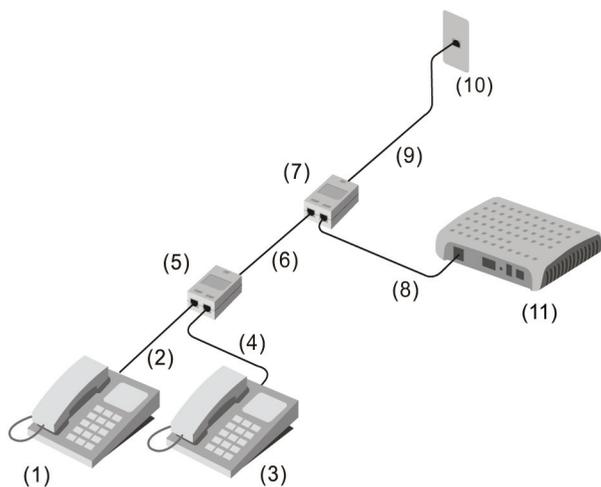
(1) Phone   (2) RJ-11 Telephone line   (3) Phone
(4) RJ-11 Telephone line   (5) Connection box   (6) RJ-11 Telephone line
(7) Splitter   (8) RJ-11 Telephone line   (9) RJ-11 Telephone line
(10) Phone Jack   (11) MT882

Figure 6-2 Connecting MT882 with multiple phones — Mode 1
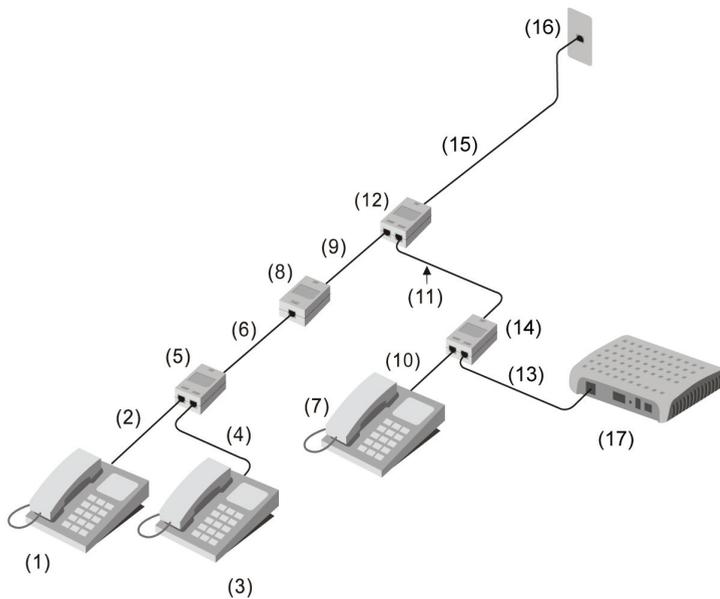
(1) Phone   (2) RJ-11 Telephone line   (3) Phone
(4) RJ-11 Telephone line   (5) Connection box   (6) RJ-11 Telephone line
(7) Phone   (8) Microfilter   (9) RJ-11 Telephone line
(10) RJ-11 Telephone line   (11) RJ-11 Telephone line   (12) Connection box
(13) RJ-11 Telephone line   (14) Splitter   (15) RJ-11 Telephone line
(16) Phone Jack   (17) MT882

Figure 6-3 Connecting MT882 with multiple phones — Mode 2

7 Technical Specifications

General Specifications	
Standards	**ADSL Standards:** ANSI T1.413 Issue 2 ITU G.992.1 (G.dmt) Annex A ITU G.992.2 (G.lite) Annex A ITU G.994.1 (G.hs)
	ADSL2 Standards: ITU G.992.3 (G.dmt.bis) Annex A ITU G.992.4 (G.lite.bis) Annex A
	ADSL2+Standards: ITU G.992.5 Annex A (Comply with **DSL Forum TR-048/TR-067** performance criteria)

General Specifications	
Data Transfer Rate	G.dmt full rate: Downstream up to 8 Mbit/s Upstream up to 896 Kbit/s G.lite: Downstream up to 1.5 Mbit/s Upstream up to 512 Kbit/s T1.413: Downstream up to 8 Mbit/s Upstream up to 896 Kbit/s G.992.5 (ADSL2+): Downstream up to 24 Mbit/s Upstream up to 1.2 Mbit/s.
External Interface	One RJ-11 port for ADSL line connection One RJ-45 port for 10/100 Base-T Ethernet connection

Physical and Environmental Specifications	
Power Adapter	12 V AC 0.8 A
Power Consumption	< 4 W
Operating Temperature	0°C – 40°C (32°F – 104°F)
Humidity	5% – 95% (non-condensing)
Dimensions	135 mm × 110 mm × 28 mm
Weight	180 g

📖 Note:

- Use a power adapter provided or approved by Huawei only. Make sure that the power adapter conforms to the sign on the rear panel (12 V AC 0.8 A).
- Take waterproof measures during the storage, transportation and running of MT882.

8 Appendix

8.1 Factory Settings

User name	user		
Password	user		
IP address	192.168.1.1		
Subnet mask	255.255.255.0		
DSL Mode	All		
Bridged Mode	PVC0	VPI=0	VCI=35
	PVC1	VPI=8	VCI=35
	PVC2	VPI=0	VCI=100
	PVC3	VPI=0	VCI=32
	PVC4	VPI=8	VCI=81
	PVC5	VPI=8	VCI=32
NAT	Enable		
Firewall	Enable		

8.2 Abbreviations and Acronyms

A

ADSL   Asymmetric Digital Subscriber Line

ATM   Asynchronous Transfer Mode

D

DHCP   Dynamic Host Configuration Protocol

DNS   Domain Name Server

DSLAM   Digital Subscriber Line Access Multiplex

I

IP   Internet Protocols

ICMP   Internet Control Message Protocol

IPoA   Internet Protocols Over ATM

ISP   Internet Service Provider

L

LAN   Local Area Network

M

MAC   Media Access Control

N

NIC   Network Interface Card

P

PPP   Point to Point Protocol

PPPoA   PPP over ATM

PPPoE   PPP over Ethernet

PVC   Permanent Virtual Connection

Q

QoS   Quality of Service

R

RAM   Random Access Memory

RIP   Routing Information Protocol

T

TCP   Transfer Control Protocol

TFTP   Trivial File Transfer Protocol

U

UDP   User Datagram Protocol

V

VCI   Virtual Channel Identifier

VPI   Virtual Path Identifier

W

WAN   Wide Area Network

Huawei Technologies Co., Ltd.