PLANET
Networking & Communication

Bandwidth Management Gateway

BM-500

User's Manual

Copyright

Disclaimer

PLANET Technology does not warrant that the hardware will work properly in all environments and applications, and makes no warranty and representation, either implied or expressed, with respect to the quality, performance, merchantability, or fitness for a particular purpose.

PLANET has made every effort to ensure that this User’s Manual is accurate; PLANET disclaims liability for any inaccuracies or omissions that may have occurred.

Information in this User’s Manual is subject to change without notice and does not represent a commitment on the part of PLANET. PLANET assumes no responsibility for any inaccuracies that may be contained in this User’s Manual. PLANET makes no commitment to update or keep current the information in this User’s Manual, and reserves the right to make improvements to this User’s Manual and/or to the products described in this User’s Manual, at any time without notice.

If you find information in this manual that is incorrect, misleading, or incomplete, we would appreciate your comments and suggestions.

CE mark Warning

This is a class B device, In a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

Trademarks

The PLANET logo is a trademark of PLANET Technology.

This documentation may refer to numerous hardware and software products by their trade names. In most, if not all cases, these designations are claimed as trademarks or registered trademarks by their respective companies.

Customer Service

For information on customer service and support for the Bandwidth Management Gateway, please refer to the following Website URL:

http://www.planet.com.tw

Before contacting customer service, please take a moment to gather the following information:

- Bandwidth Management Gateway serial number and MAC address
- Any error messages that displayed when the problem occurred
- Any software running when the problem occurred
- Steps you took to resolve the problem on your own

Revision

User’s Manual for PLANET BM-500

Model: BM-500

Rev: 1.0 (March, 2004)

Part No. EM-BM500

Table of Contents

Chapter 1: Introduction

BM-500 is specifically designed for SOHO networks. It has built-in 4-port 10/100Mbps Ethernet LAN ports and NAT function. Thus, no broadband router is required for users which have only one public IP address. It also supports virtual server, Multi-DMZ and dynamic DNS function which is very useful for users to share local resource to Internet users.

For bandwidth management, packets can be classified based on IP address, IP subnet and TCP/UDP port number. The device has more than 40 of the most common protocols such as H.323, Oracle, HTTP, FTP, etc. for ease of definition; the administrator can then define policies to ensure committed and maximum bandwidth levels for inbound / outbound traffic in each class. The administrator can also define three priority levels for each policy to ensure that high priority packets receive the maximum available bandwidth. In addition, each policy can have a schedule defined for when the policy is activated or inactivated in increments of 30 minutes.

Both the NAT mode and transparent mode are supported, therefore allowing the existing network structure to remain the same without reconfiguring. The BM-500 provides policy-based firewall protection and several hacker protections to prevent any hacker attack. Besides, the comprehensive alarm and log function allow the network Management Gateway to easily enhance the security of local network.

1.1 Features

- Provides four 10/100Mbps LAN port and one 10/100Mbps WAN port
- Supports NAT mode and transparent mode
- Transparent mode requires no changing for the original network structure
- Traffic classification bases on IP, IP range/subnet, TCP/UDP port range
- Guaranteed and maximum bandwidth with 3 level of priorities
- Dynamic and prioritized bandwidth sharing with fairness between equal-level priority
- Assigns daily and weekly access schedule to each individual policy
- Professional Network Log and Accounting Report
- Supports MRTG-like Traffic Statistics, easy to trace and analyze
- Provides Multi-Servers Load Balancing
- Provides Dynamic DNS and DHCP server functions
- Supports Content Filter on scheduled time
- Supports Virtual Server and IP mapping (Multi-DMZ Host)
- Supports Multi-language web UI, easy to manage
- Support user authentication based user's user name and password

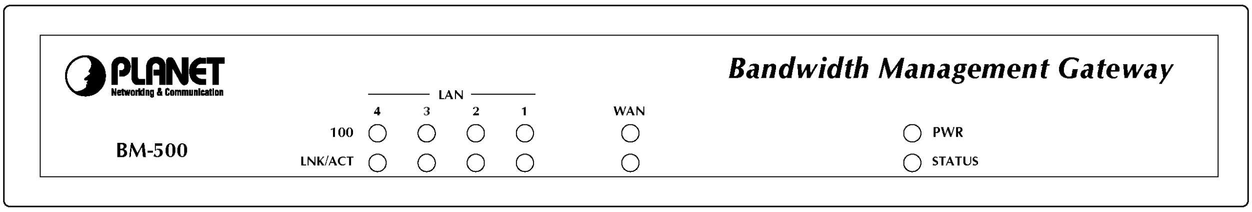
1.2 Package Contents

The following items should be included:

- Bandwidth Management Gateway
- Power Adapter
- Quick Installation Guide
- User's Manual CD

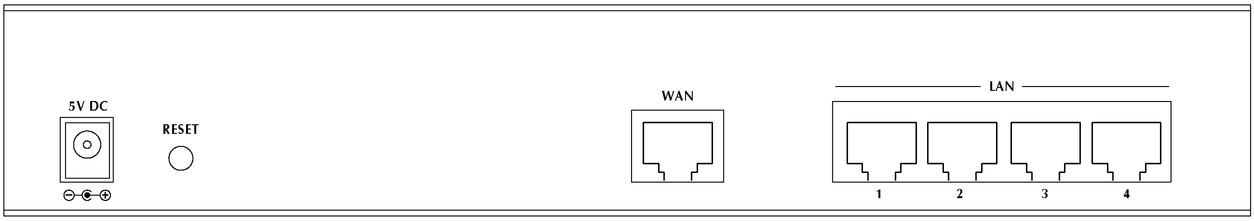
If any of the contents are missing or damaged, please contact your dealer or distributor immediately.

1.3 Bandwidth Management Gateway Front View



LED	Description	
PWR	Power is supplied to this device.	
STATUS	Blinks to indicate this devise is being turned on. After one minute, this LED indicator will stop blinking, it means this device is now ready to use.	
WAN & LAN	100	Steady on indicates the port operate on 100Mbps speed
	LNK/ACT	Steady on indicates the port is connected to other network device. Blink to indicates there is traffic on the port

1.4 Bandwidth Management Gateway Rear Panel



Port or button	Description
RESET	Press this button to restore to factory default settings.
WAN	Connect to your xDSL/Cable modem or other Internet connection device
LAN 1 to 4	Connect to your local PC, switch or other local network device

1.5 Specification

Product		Bandwidth Management Gateway
Model		BM-500
Hardware		
Connections	WAN	1 x 10/100Base-TX
	LAN	4 x 10/100Base-TX, Auto-MDI/MDI-X
Button		Reset button fro hardware reset / factory default
System LED		System: PWR, STATUS Network: LNK/ACT, 100
Power		5V DC, 2.4A
Operating Environment		Temperature: 0~50°C Relative Humidity: 5%~90%
Dimension W x D x H		220 x 149 x 37 mm
Regulatory		FCC, CE Mark
Software		
Maximum Bandwidth		Transparent: 10Mbps NAT: 8Mbps NAT + logging + statistics: 3Mbps
Maximum concurrent session		5000
Management		Web (English, Traditional Chinese, Simplified Chinese)
Operation Mode		Transparent, NAT
WAN connection type in NAT mode		PPPoE, DHCP and Fixed IP
Traffic Classification		IP, IP subnet, TCP/UDP port
Bandwidth Allocation		Policy rules with Inbound/Outbound traffic management Guaranteed and maximum bandwidth Scheduled in unit of 30 minutes 3 Priorities
Log		Traffic Log, Event Log, Connection Log, Log backup by mail or syslog server
Statistics		WAN port statistics and policy statistics with graph display
Firewall Security		Policy-based access control Stateful Packet Inspection (SPI) Scheduled in unit of 30 minutes
Hacker Alert		Detect SYN Attack, Detect ICMP Flood, Detect UDP Flood, Detect Ping of Death Attack, Detect Tear Drop Attack, Detect IP Spoofing Attack, Filter IP Route Option, Detect Port Scan Attack, Detect Land Attack
Alarm		w Traffic alarm for user-defined traffic level w Event alarm for hacker attack w The alarm message can sent to administrator by e-mail
Other Functions		Firmware Upgradeable through Web NTP support Configuration Backup and Restore through Web Dynamic DNS support Multiple NAT and multiple DMZ (mapped IP) support Multiple server load balancing

Chapter 2: Hardware Installation

2.1 Installation Requirements

Before installing the Bandwidth Management Gateway, make sure your network meets the following requirements.

- Mechanical Requirements

The Bandwidth Management Gateway is to be installed between your Internet connection and local area network. The Bandwidth Management Gateway can be placed on the table or rack. Locate the unit near the power outlet.

- Electrical Requirements

The Bandwidth Management Gateway is a power-required device, it means, the Bandwidth Management Gateway will not work until it is powered. If your networked PCs will need to transmit data all the time, please consider use an UPS (Uninterrupted Power Supply) for your Bandwidth Management Gateway. It will prevent you from network data loss. In some area, installing a surge suppression device may also help to protect your Bandwidth Management Gateway from being damaged by unregulated surge or current to the Bandwidth Management Gateway.

- Network Requirements

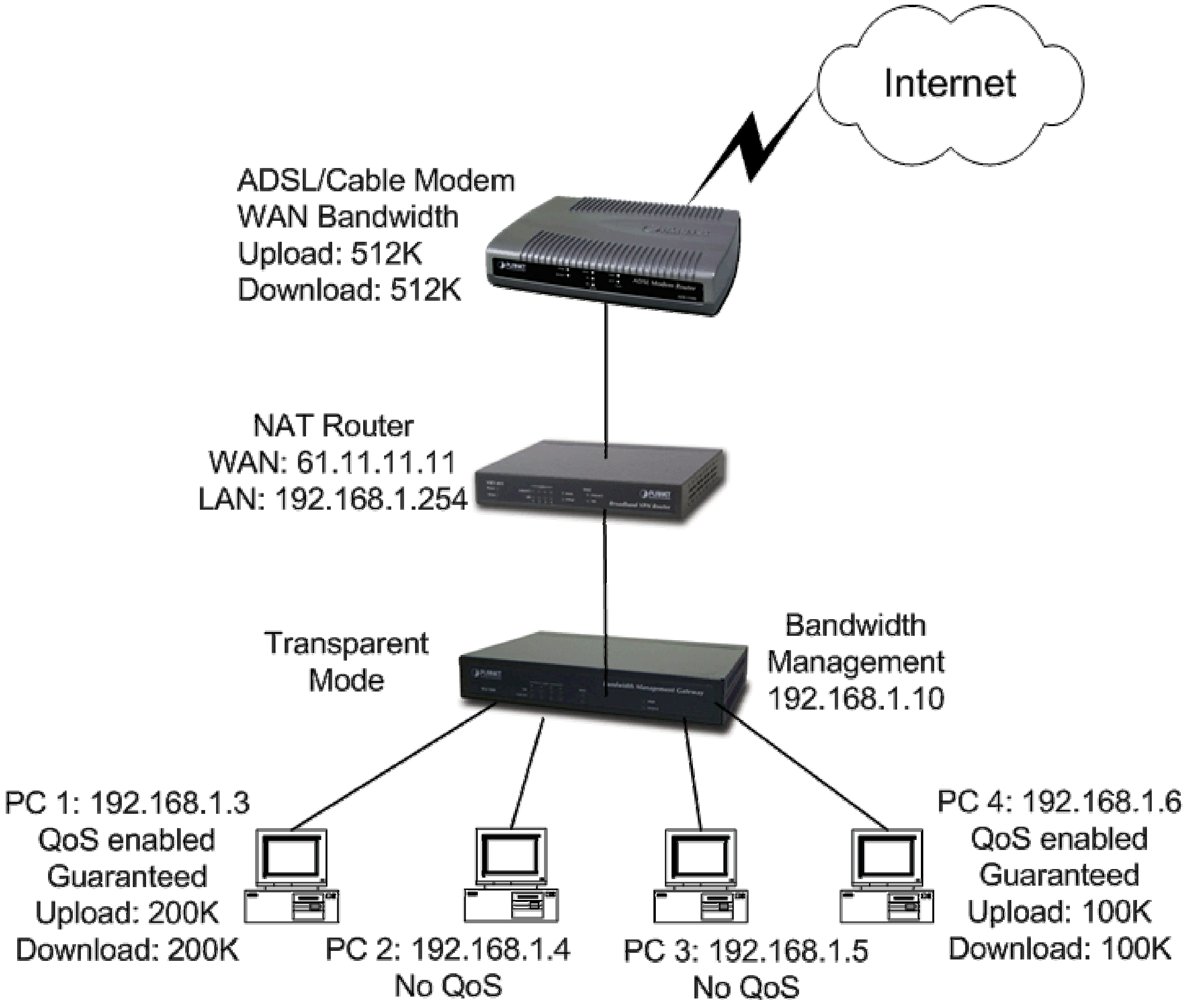
In order for Bandwidth Management Gateway to manage traffic, the traffic must pass through Bandwidth Management Gateway at a useful point in a network. In most situations, the bandwidth Management Gateway should be placed behind the Internet connection device.

This deployment allows the network administers to control all bandwidth based on business priorities and give business-critical and time-sensitive applications guarantee bandwidth and higher priority. Business-critical applications can receive maximum performance while other less urgent traffic is still available on remaining bandwidth. Bandwidth Management Gateway also provides comprehensive security, log and statistics functions to help monitor network and bandwidth usage and allow adjustment of the bandwidth management policies accordingly.

2.2 Operation Mode

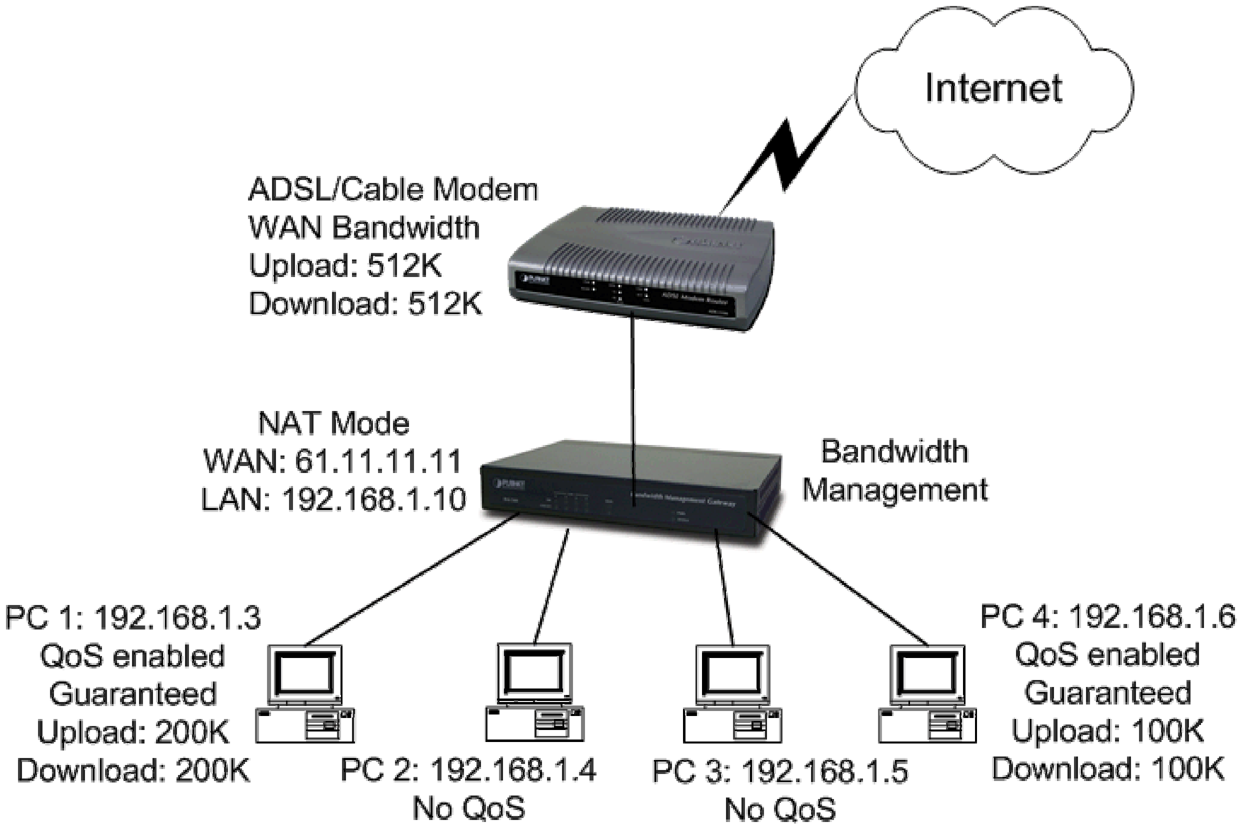
BM-500 supports two operation modes, Transparent and NAT. In transparent mode, BM-500 works as proxy with forward LAN packet to WAN and forward WAN packet to LAN. The LAN and WAN side IP addresses are in the same subnet. In NAT mode, LAN side user will share one public IP address of WAN port to make Internet connection. Please find the following two pictures for example.

2.2.1 Transparent Mode Connection Example



All the WAN and LAN side IP addresses are on the same subnet.

2.2.2 NAT Mode Connecting Example



LAN and WAN side IP addresses are on the different subnet.

Chapter 3: Getting Started

3.1 Web Configuration

STEP 1:

Connect both the Administrator's PC and the LAN port of the Bandwidth Management Gateway to a hub or switch. Make sure there is a link light on the hub/switch for both connections. The Bandwidth Management Gateway has an embedded web server used for management and configuration. Use a web browser to display the configurations of the Bandwidth Management Gateway (such as Internet Explorer 4(or above) or Netscape 4.0(or above) with full java script support). The default IP address of the Bandwidth Management Gateway is **192.168.1.1** with a subnet mask of 255.255.255.0. Therefore, the IP address of the Administrator PC must be in the range between 192.168.1.2– 192.168.1.254

If the company's LAN IP Address is not subnet of 192.168.1.0, (i.e. LAN IP Address is 172.16.0.1), then the Administrator must change his/her PC IP address to be within the same range of the LAN subnet (i.e. 172.16.0.2). Reboot the PC if necessary.

By default, the Bandwidth Management Gateway is shipped with its DHCP Server function enabled. This means the client computers on the LAN network including the Administrator PC can set their TCP/IP settings to automatically obtain an IP address from the Bandwidth Management Gateway.

The following table is a list of private IP addresses. These addresses may not be used as a WAN IP address.

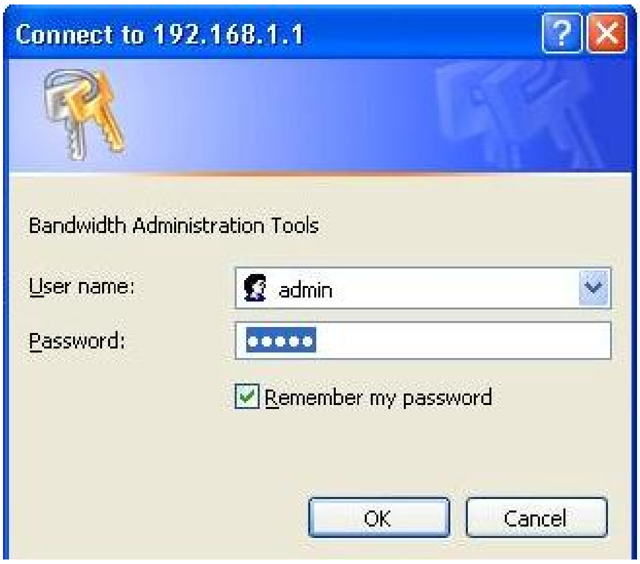
10.0.0.0 ~ 10.255.255.255
172.16.0.0 ~ 172.31.255.255
192.168.0.0 ~ 192.168.255.255

STEP 2:

Once the Administrator PC has an IP address on the same network as the Bandwidth Management Gateway, open up an Internet web browser and type in http://192.168.1.1 in the address bar.

A pop-up screen will appear and prompt for a username and password. A username and password is required to connect to the Bandwidth Management Gateway. Enter the default login username and password of Administrator (see below).

Username: admin
Password: admin
Click OK.



Connect to 192.168.1.1

Bandwidth Administration Tools

User name: admin

Password: •••••

☑ Remember my password

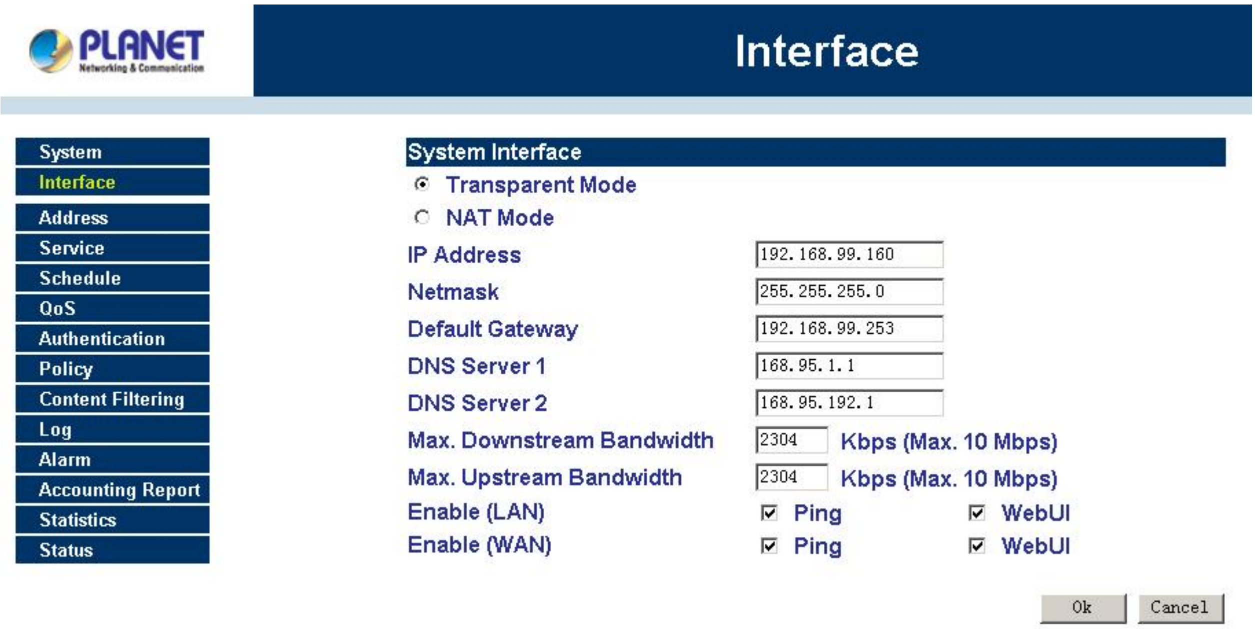
3.2 Setting Up in Transparent Mode

STEP 1:

After entering the username and password, the Bandwidth Management Gateway WEB UI screen will display. Select the **Interface** tab on the left menu and a sub-function list will be displayed.

- Select **Transparent Mode**.
- Enter required information to their corresponding fields.

LAN interface IP Address
NetMask
Default Gateway
DNS Server



System Interface

● Transparent Mode

○ NAT Mode

IP Address 192.168.99.160

Netmask 255.255.255.0

Default Gateway 192.168.99.253

DNS Server 1 168.95.1.1

DNS Server 2 168.95.192.1

Max. Downstream Bandwidth 2304 Kbps (Max. 10 Mbps)

Max. Upstream Bandwidth 2304 Kbps (Max. 10 Mbps)

Enable (LAN) ☑ Ping ☑ WebUI

Enable (WAN) ☑ Ping ☑ WebUI

.

***Note:** The above figures are only examples. Please fill in the appropriate IP address information provided to you by the ISP.*

STEP 2:

Click on the **Policy** tab from the main function menu, and then click on **Outgoing** from the sub-function list.

STEP 3:

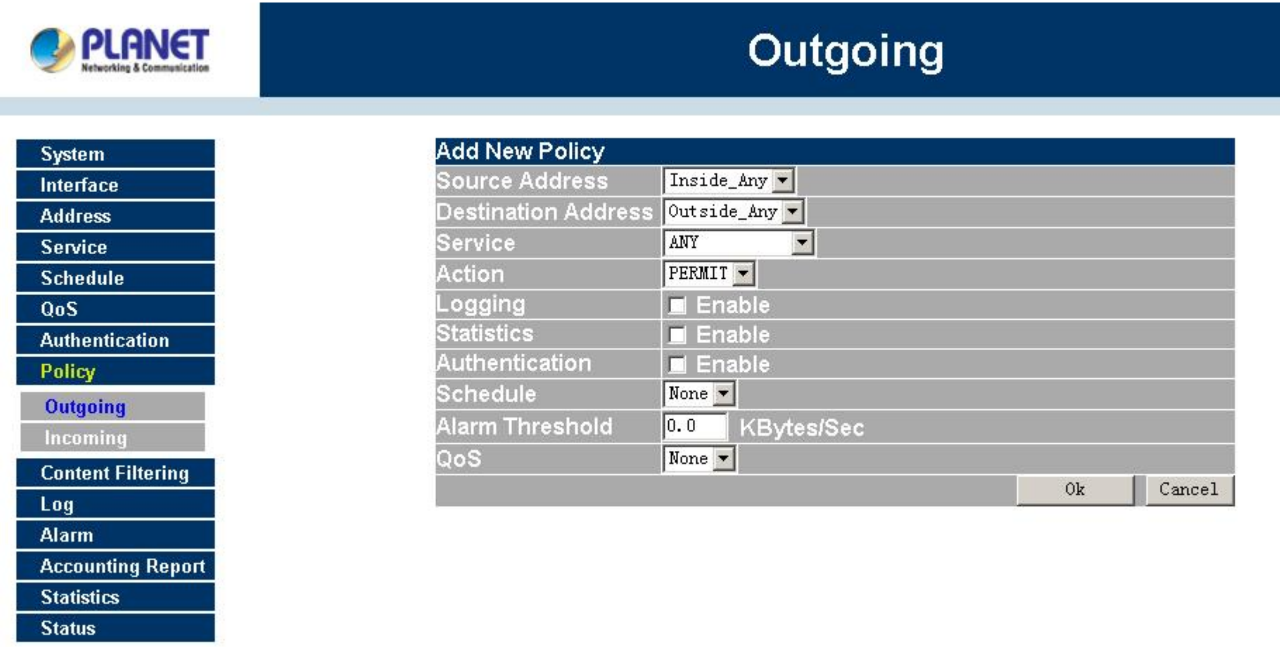
Click on **New Entry** button.

STEP 4:

When the **New Entry** option appears, enter the following configuration:

Source Address – select **“Inside_Any”**
Destination Address – select **“Outside_Any”**
Service - select **“ANY”**
Action - select **“Permit”**

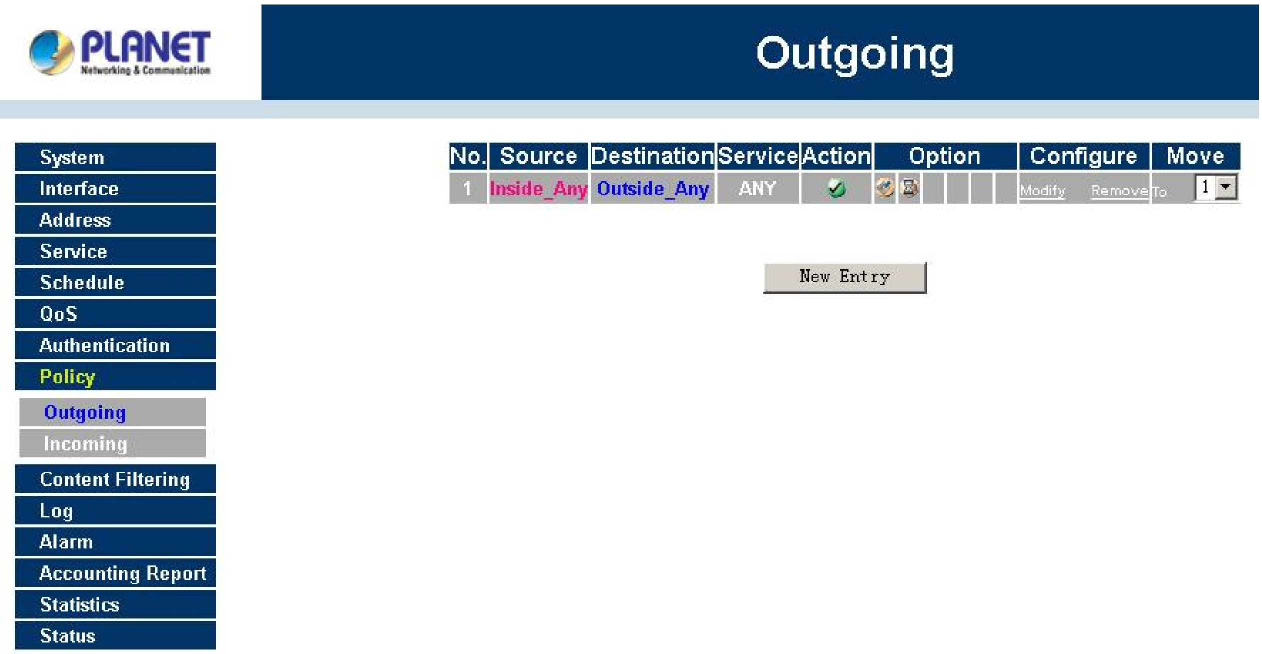
Click on **OK** to apply the changes.



Add New Policy	
Source Address	Inside_Any
Destination Address	Outside_Any
Service	ANY
Action	PERMIT
Logging	□ Enable
Statistics	□ Enable
Authentication	□ Enable
Schedule	None
Alarm Threshold	0.0 KBytes/Sec
QoS	None

STEP 5:

The configuration is successful when the screen below is displayed. Make sure that all the computers that are connected to the LAN port have their Default Gateway IP Address set to the Bandwidth Management Gateway’s LAN IP Address (i.e. 192.168.1.1). At this point, all the computers on the LAN network should gain access to the Internet immediately. If a Bandwidth Management Gateway filter function is required, please refer to the Policy section in the user’s manual.



No.	Source	Destination	Service	Action	Option	Configure	Move
1	Inside_Any	Outside_Any	ANY	✓		Modify Remove	To 1

3.3 Setting Up in NAT Mode

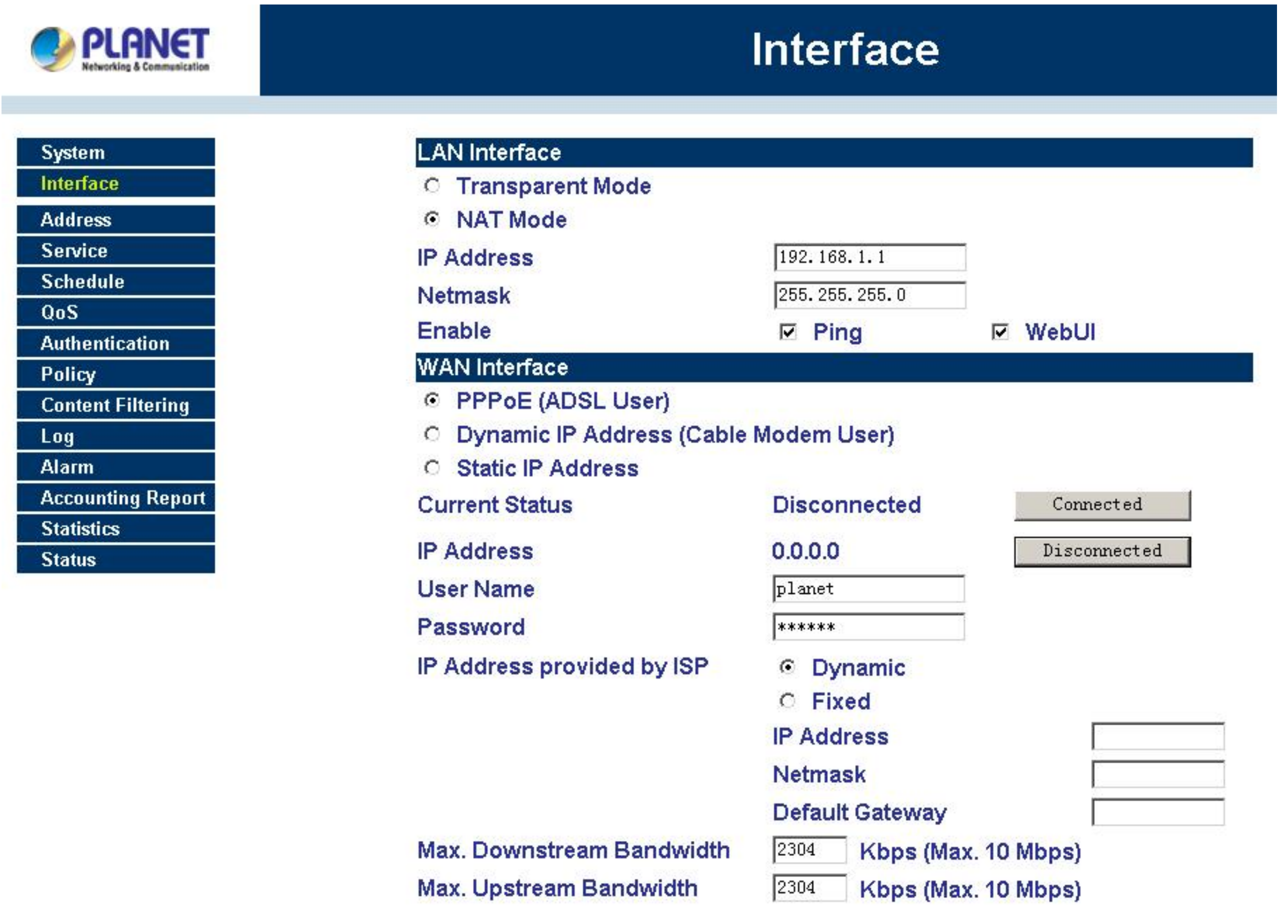
STEP 1:

After entering the Bandwidth Management Gateway WEB UI screen, select the **Interface** tab on the left menu and a sub-function list will be displayed.

Select the **NAT Mode**.

Enter the required information to their corresponding fields.

LAN Interface	IP Address	192.168.1.1
	NetMask	255.255.255.0



LAN Interface

○ Transparent Mode

● NAT Mode

IP Address: 192.168.1.1

Netmask: 255.255.255.0

Enable: ☑ Ping ☑ WebUI

WAN Interface

● PPPoE (ADSL User)

○ Dynamic IP Address (Cable Modem User)

○ Static IP Address

Current Status: Disconnected

IP Address: 0.0.0.0

User Name: planet

Password: ******

IP Address provided by ISP: ● Dynamic ○ Fixed

IP Address:

Netmask:

Default Gateway:

Max. Downstream Bandwidth: 2304 Kbps (Max. 10 Mbps)

Max. Upstream Bandwidth: 2304 Kbps (Max. 10 Mbps)

Enter the information that your ISP provided.

STEP 2:

Click on the **Policy** tab from the main function menu, and then click on **Outgoing** from the sub-function list.

Click on the **Policy** tab from the main function menu, and then click on **Incoming** from the sub-function list.

STEP 3:

Click on **New Entry** button.

STEP 4:

When the **New Entry** option appears, enter the following configuration:

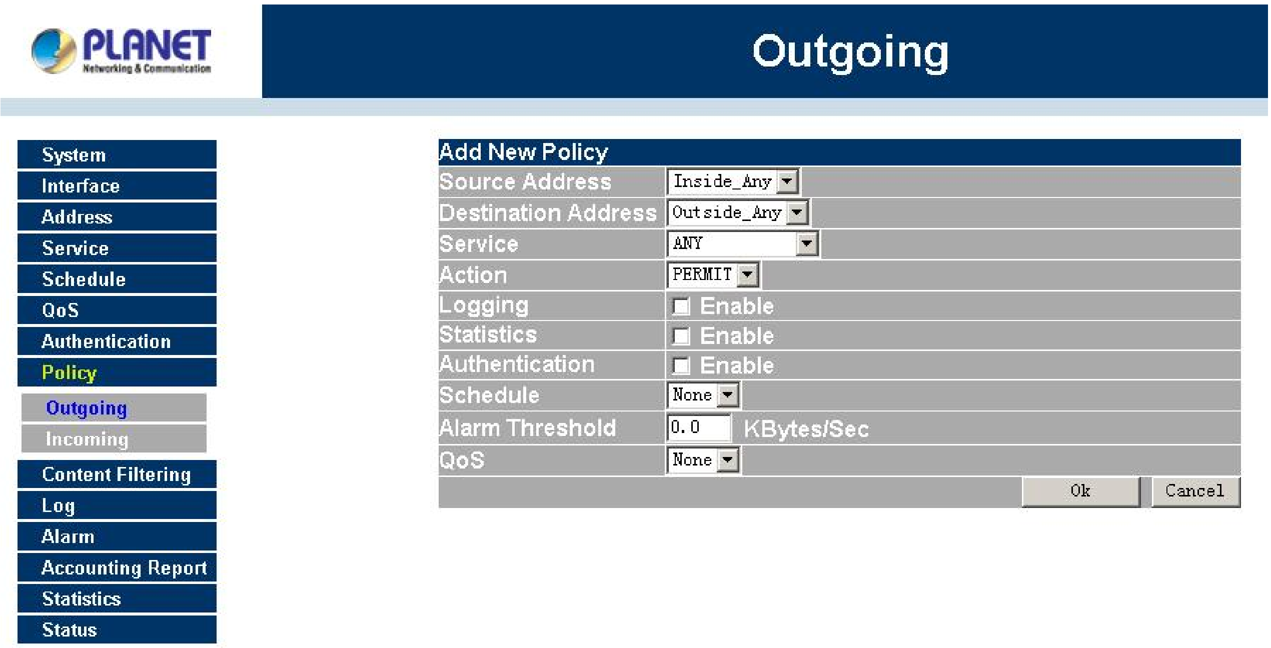
Source Address – select **"Inside_Any"**

Destination Address – select **"Outside_Any"**

Service - select **"ANY"**

Action - select **"Permit"**

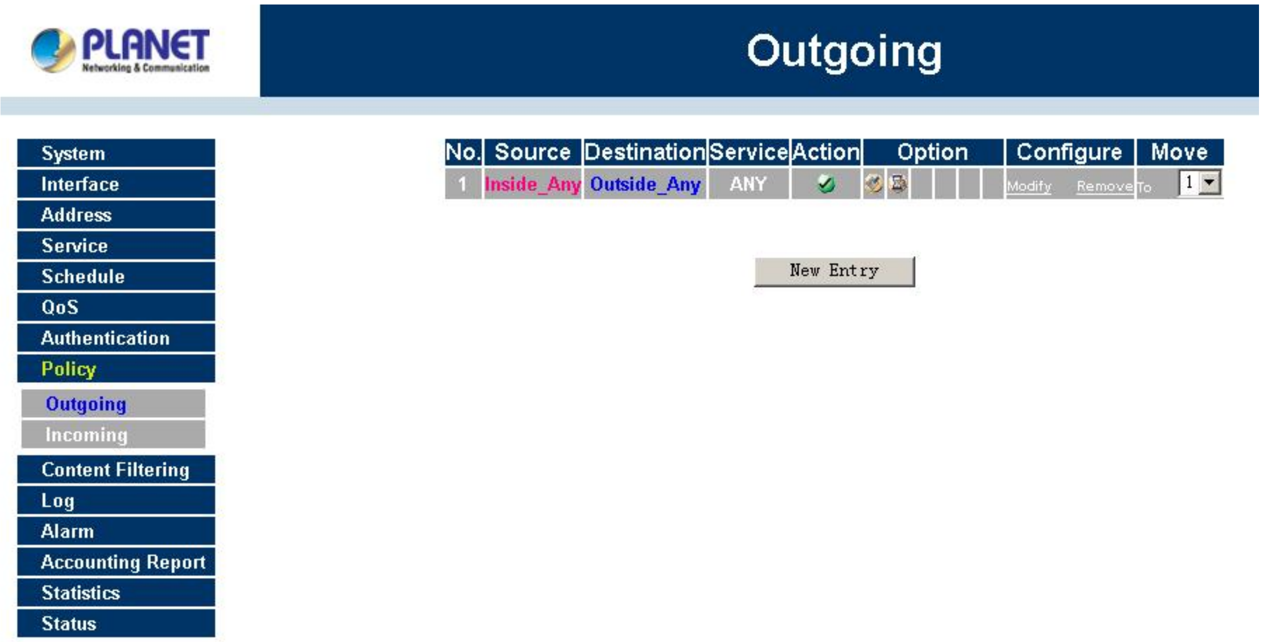
Click on **OK** to apply the changes.



Add New Policy	
Source Address	Inside_Any
Destination Address	Outside_Any
Service	ANY
Action	PERMIT
Logging	□ Enable
Statistics	□ Enable
Authentication	□ Enable
Schedule	None
Alarm Threshold	0.0 KBytes/Sec
QoS	None

STEP 5:

The configuration is successful when the screen below is displayed. Make sure that all the computers that are connected to the LAN port have their Default Gateway IP Address set to the Bandwidth Management Gateway’s LAN IP Address (i.e. 192.168.1.1). At this point, all the computers on the LAN network should gain access to Internet immediately. If a Bandwidth Management Gateway filter function is required, please refer to Address and Policy sections.



No.	Source	Destination	Service	Action	Option	Configure	Move
1	Inside_Any	Outside_Any	ANY	✓		Modify Remove	To 1

Chapter 4: Web Configuration

4.1 System

The Bandwidth Management Gateway Administration and monitoring control is set by the System Administrator. The System Administrator can add or modify System settings and monitoring mode. The sub Administrators can only read System settings but not modify them. In **System**, the System Administrator can:

1. Add and change the sub Administrator's names and passwords;
2. Back up all Bandwidth Management Gateway settings into local files;
3. Set up alerts for Hackers invasion.

"System" is the managing of settings such as the privileges of packets that pass through the Bandwidth Management Gateway and monitoring controls. Administrators may manage, monitor, and configure Bandwidth Management Gateway settings. All configurations are "read-only" for all users other than the Administrator; those users are not able to change any settings for the Bandwidth Management Gateway.

Admin: has control of user access to the Bandwidth Management Gateway. He/she can add/remove users and change passwords.

Setting: The Administrator may use this function to backup Bandwidth Management Gateway configurations and export (save) them to an **"Administrator"** computer or anywhere on the network; or restore a configuration file to the device; or restore the Bandwidth Management Gateway back to default factory settings. Under **Setting**, the Administrator may enable e-mail alert notification. This will alert Administrator(s) automatically whenever the Bandwidth Management Gateway has experienced unauthorized access or a network hit (hacking or flooding). Once enabled, an IP address of a SMTP (Simple Mail Transfer protocol) Server is required. Up to two e-mail addresses can be entered for the alert notifications.

Date/Time: This function enables the Bandwidth Management Gateway to be synchronized either with an Internet Server time or with the client computer's clock.

Language: Both Chinese and English are supported in the Bandwidth Management Gateway.

Multiple NAT Multiple NAT allows local port to set multiple subnet works and connect with the Internet through different WAN IP Addresses.

Address: Enables the Administrator to authorize specific internal/external IP address(s for Management Gateway.

Hack Alert When abnormal conditions occur, the Bandwidth Management Gateway will send an e-mail alert to notify the Administrator, and also display warning messages in the **Event** window of **Alarm.**

Route Table Use this function to enable the Administrator to add static routes for the networks when the dynamic route is not efficient enough.

DHCP Administrator can configure DHCP (Dynamic Host Configuration Protocol) settings for the LAN (LAN) network.

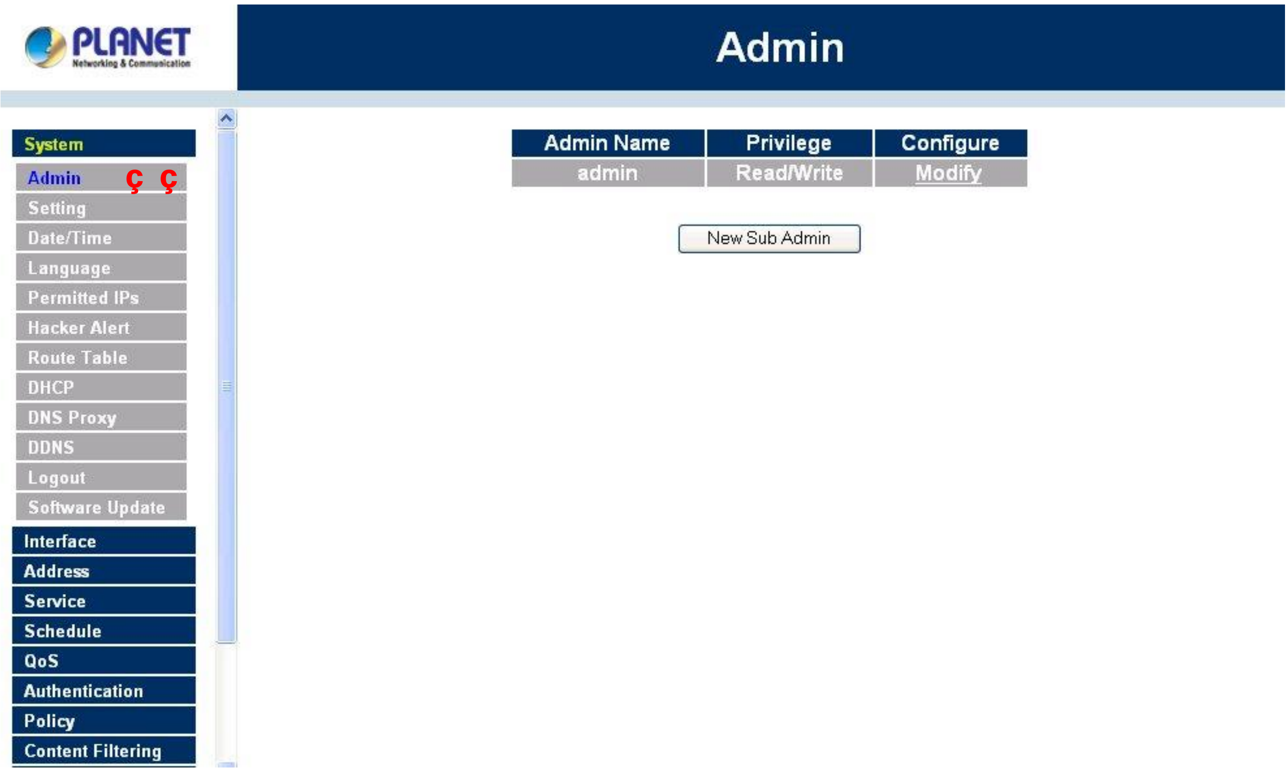
Dynamic DNS The Dynamic DNS (require Dynamic DNS Service) allows you to alias a dynamic IP address to a static hostname, allowing your device to be more easily accessed by specific name. When this function is enabled, the IP address in Dynamic DNS Server will be automatically updated with the new IP address provided by ISP

Logout Administrator logs out the Bandwidth Management Gateway. This function protects your system while you are away.

Software Update The administrator can update the device's software with the latest version. Administrators may visit distributor's web site to download the latest firmware. Administrators may update the device firmware to optimize its performance and keep up with the latest fixes for intruding attacks.

4.1.1 Admin

On the left hand menu, click on **Setup**, and then select **Admin** below it. The current list of Administrator(s) shows up.



Admin Name	Privilege	Configure
admin	Read/Write	Modify

Settings of the Administration table

Administrator Name: The username of Administrators for the Bandwidth Management Gateway. The user **admin** cannot be removed.

Privilege: The privileges of Administrators (Admin or Sub Admin)

The username of the main Administrator is **Administrator** with **read / write** privilege.

Sub Admins may be created by the **Admin** by clicking **New Sub Admin.** Sub Admins have **read only** privilege.

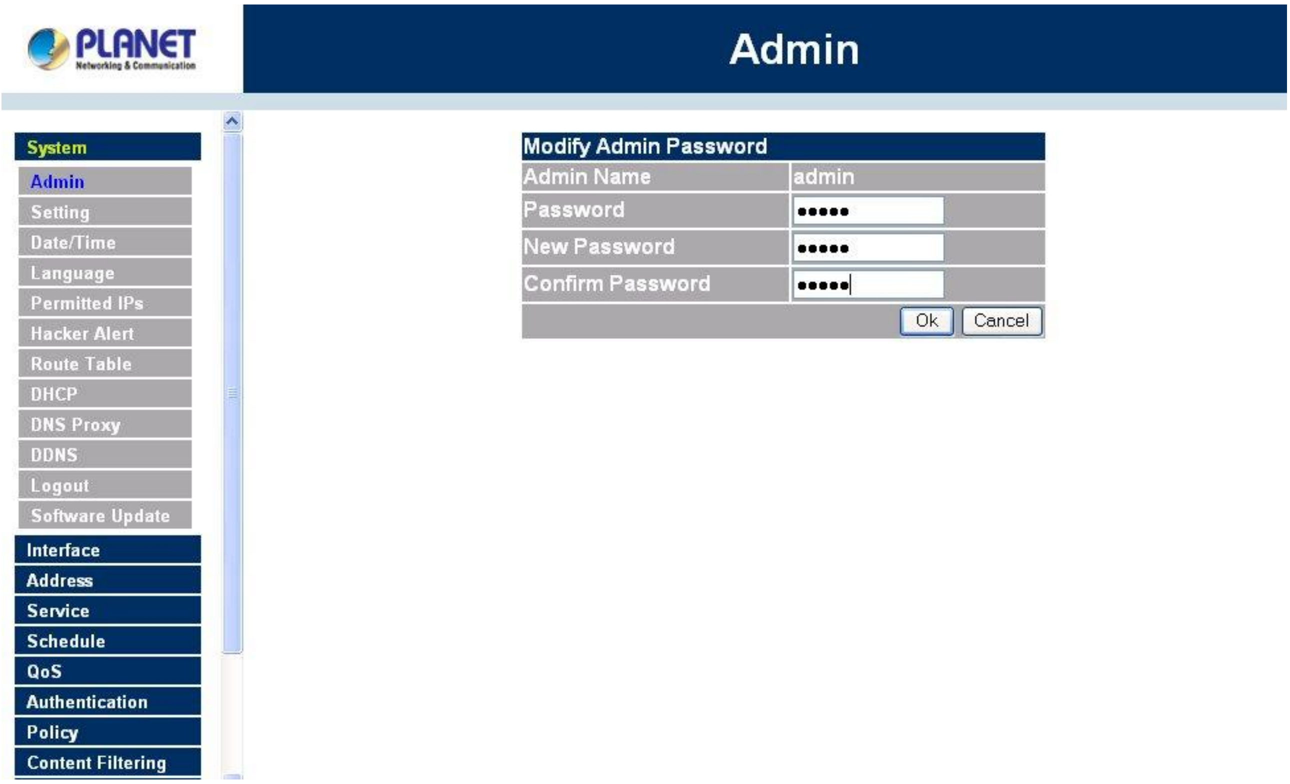
Configure: Click **Modify** to change the "Sub Administrator's" password and click **Remove** to delete a "Sub Administrator."

Changing the Main/Sub-Administrator’s Password

Step 1. The **Modify Administrator Password** window will appear. Enter in the required information:

- **Password:** enter original password.
- **New Password:** enter new password
- **Confirm Password:** enter the new password again.

Step 2. Click **OK** to confirm password change or click **Cancel** to cancel it.



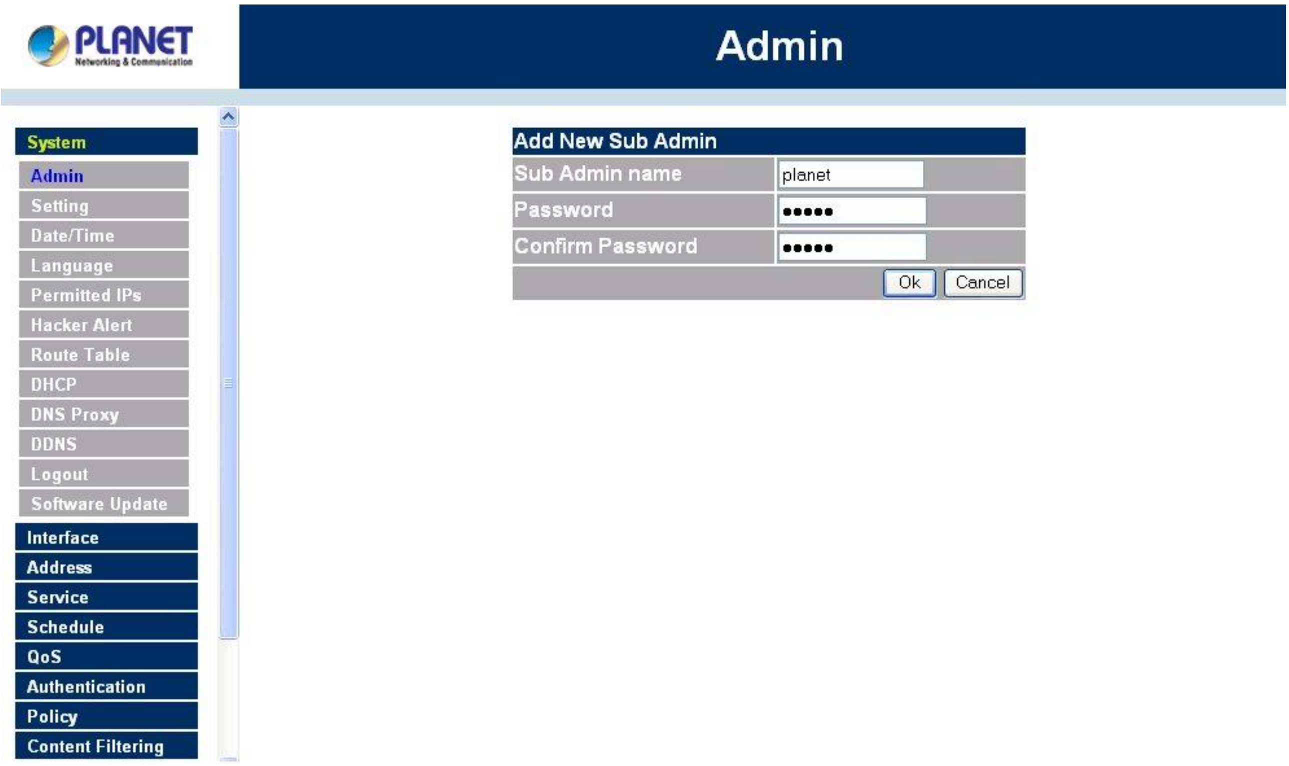
Modify Admin Password	
Admin Name	admin
Password	●●●●●
New Password	●●●●●
Confirm Password	●●●●●
	Ok Cancel

Adding a new Sub Administrator

Step 1. In the **Add New Sub Administrator** window:

- **Sub Admin Name:** enter the username of new **Sub Admin.**
- **Password:** enter a password for the new **Sub Admin.**
- **Confirm Password:** enter the password again.

Step 2. Click **OK** to add the user or click **Cancel** to cancel the addition.

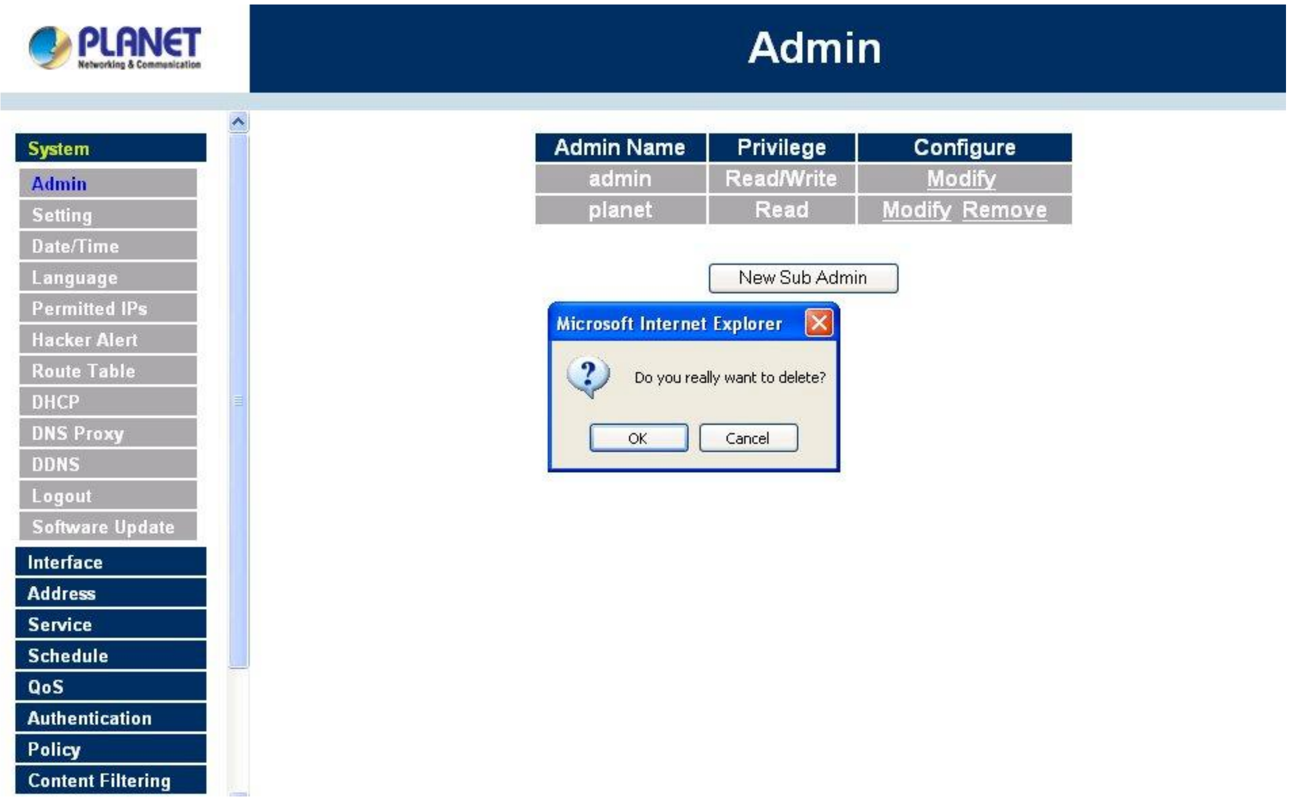


Add New Sub Admin	
Sub Admin name	planet
Password	•••••
Confirm Password	•••••

Removing a Sub Administrator

Step 1. In the Administration table, locate the Administrator name you want to edit, and click on the **Remove** option in the Configure field.

Step 2. The Remove confirmation pop-up box will appear. Click **OK** to remove that Sub Admin or click **Cancel** to cancel.



Admin Name	Privilege	Configure
admin	Read/Write	Modify
planet	Read	Modify Remove

Microsoft Internet Explorer

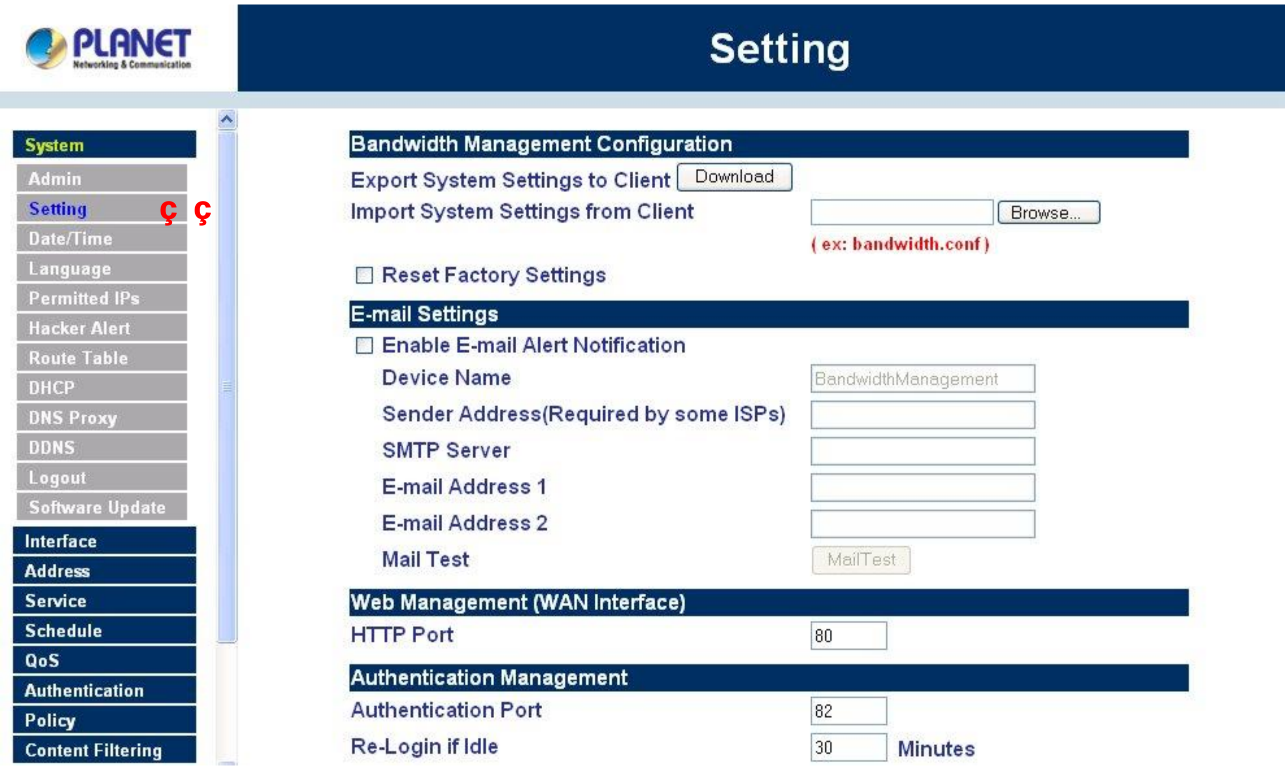
Do you really want to delete?

4.1.2 Settings

The Administrator may use this function to backup Bandwidth Management Gateway configurations and export (save) them to an **"Administrator"** computer or anywhere on the network; or restore a configuration file to the device; or restore the Bandwidth Management Gateway back to default factory settings.

Entering the Settings window

Click **Setting** in the **System** menu to enter the **Settings** window. The **Bandwidth Management Gateway Configuration** settings will be shown on the screen.



Bandwidth Management Configuration

Export System Settings to Client

Import System Settings from Client (ex: bandwidth.conf)

□ Reset Factory Settings

E-mail Settings

□ Enable E-mail Alert Notification

Device Name: BandwidthManagement

Sender Address(Required by some ISPs)

SMTP Server

E-mail Address 1

E-mail Address 2

Mail Test

Web Management (WAN Interface)

HTTP Port: 80

Authentication Management

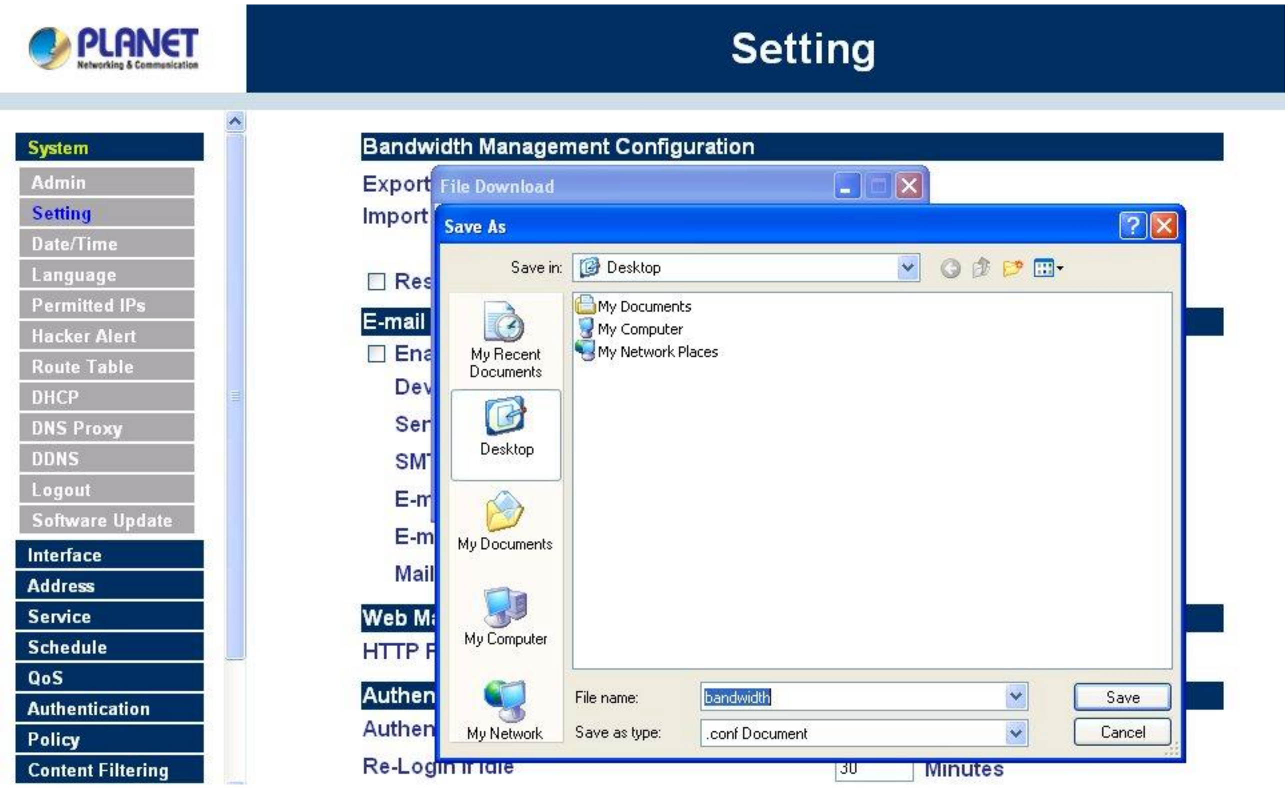
Authentication Port: 82

Re-Login if Idle: 30 Minutes

Exporting Bandwidth Management Gateway settings

Step 1. Under **Bandwidth Management Configuration**, click on the **Download** button next to **Export System Settings to Client**.

Step 2. When the **File Download** pop-up window appears, choose the destination place to save the exported file. The **Administrator** may choose to rename the file if preferred.



Save in: Desktop

My Documents

My Computer

My Network Places

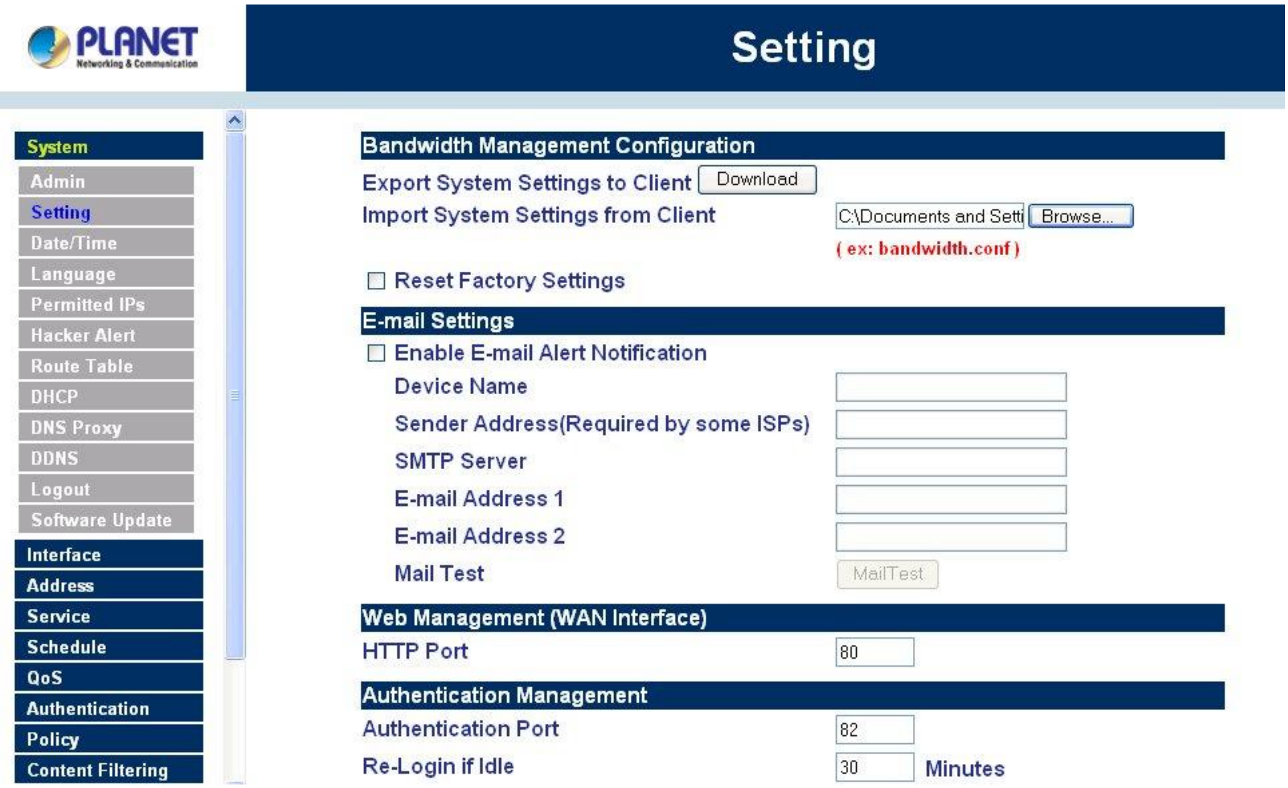
File name: bandwidth

Save as type: .conf Document

Importing Bandwidth Management Gateway settings

Under **Bandwidth Management Gateway Configuration**, click on the **Browse** button next to **Import System Settings**. When the **Choose File** pop-up window appears, select the file which contains the saved Bandwidth Management Gateway Settings, then click **OK**.

Click **OK** to import the file into the **Bandwidth Management Gateway** or click **Cancel** to cancel importing.



Bandwidth Management Configuration

Export System Settings to Client [Download]

Import System Settings from Client C:\Documents and Setti [Browse...]

(ex: bandwidth.conf)

□ Reset Factory Settings

E-mail Settings

□ Enable E-mail Alert Notification

Device Name

Sender Address(Required by some ISPs)

SMTP Server

E-mail Address 1

E-mail Address 2

Mail Test [MailTest]

Web Management (WAN Interface)

HTTP Port 80

Authentication Management

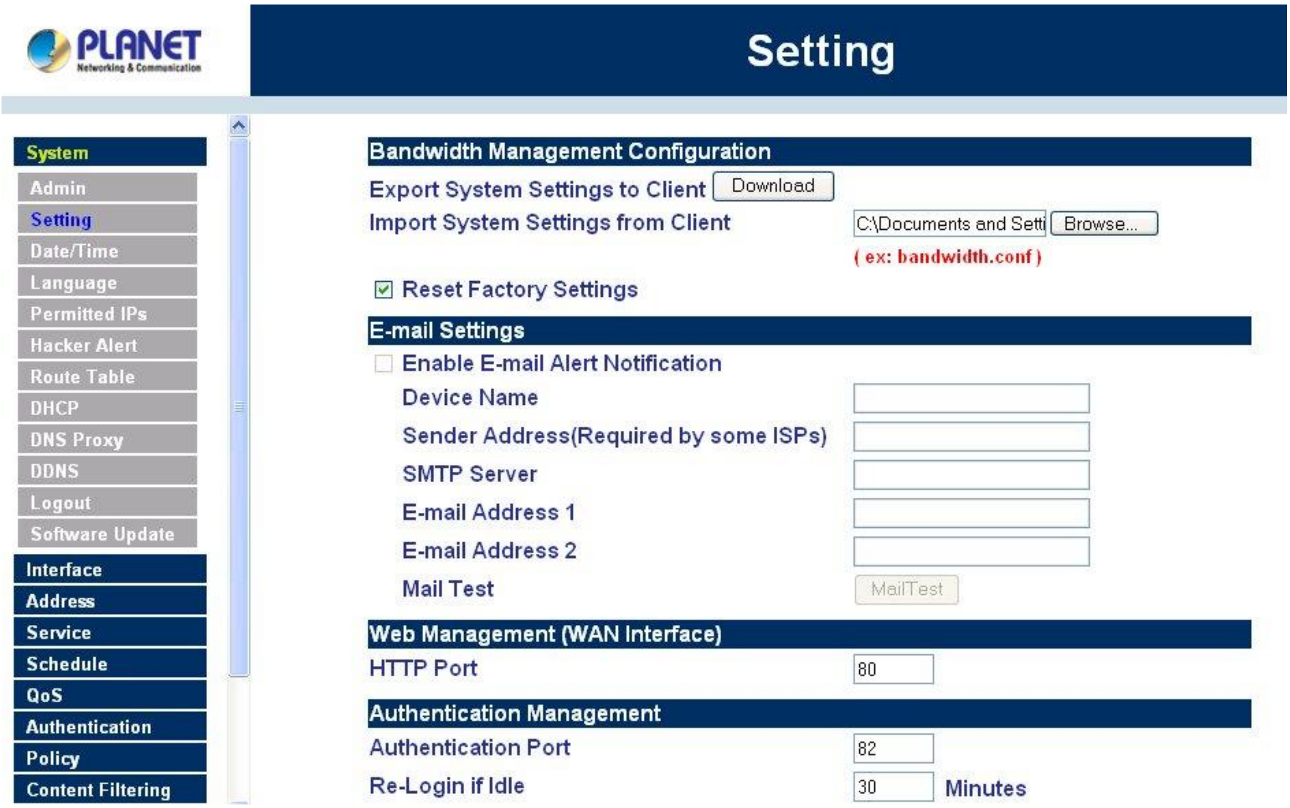
Authentication Port 82

Re-Login if Idle 30 Minutes

Restoring Factory Default Settings

Step 1. Select **Reset Factory Settings** under **Bandwidth Management Configuration**.

Click **OK** at the bottom-right of the screen to restore the factory settings.



Bandwidth Management Configuration

Export System Settings to Client

Import System Settings from Client: C:\Documents and Setti

(ex: bandwidth.conf)

☑ Reset Factory Settings

E-mail Settings

□ Enable E-mail Alert Notification

Device Name

Sender Address(Required by some ISPs)

SMTP Server

E-mail Address 1

E-mail Address 2

Mail Test

Web Management (WAN Interface)

HTTP Port: 80

Authentication Management

Authentication Port: 82

Re-Login if Idle: 30 Minutes

Enabling E-mail Alert Notification

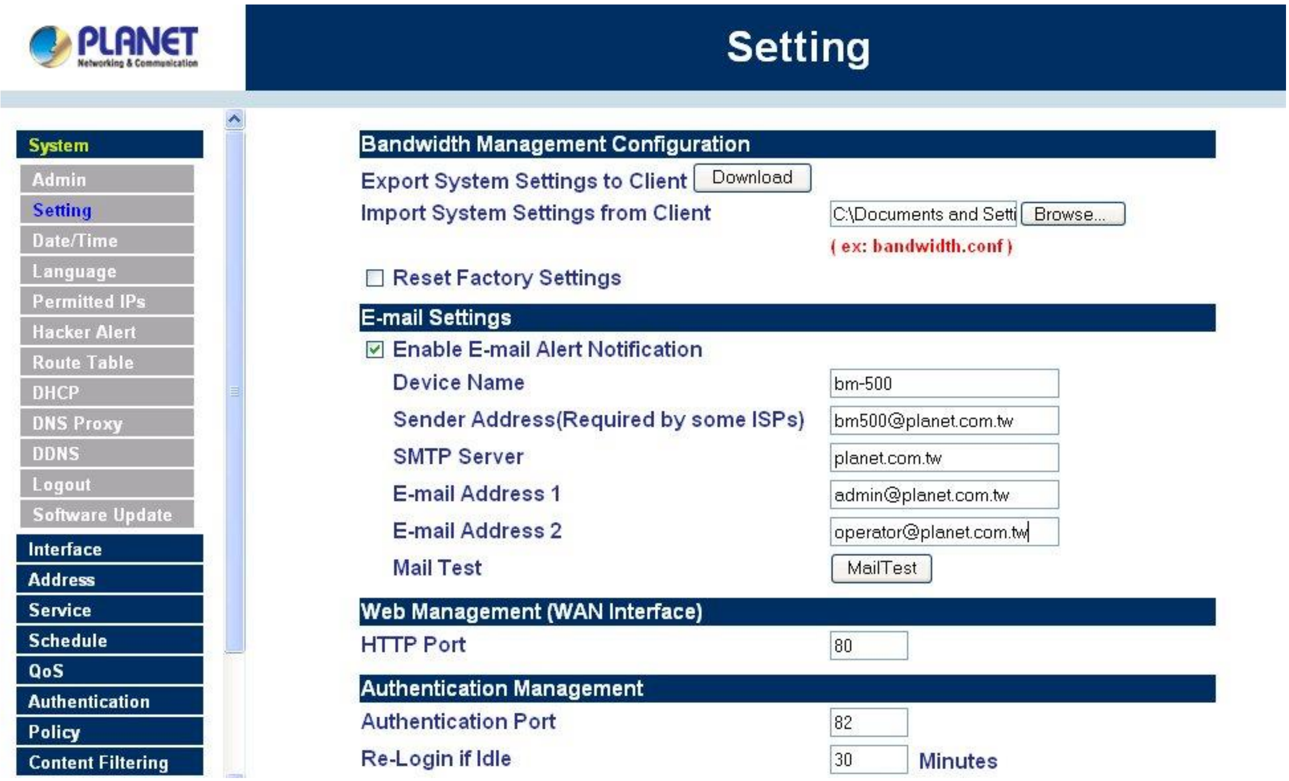
Step 1. Select **Enable E-mail Alert Notification** under **E-Mail Settings**. This function will enable the Bandwidth Management Gateway to send e-mail alerts to the System Administrator when the network is being attacked by hackers or when emergency conditions occur.

Step 2. **SMTP Server IP:** Enter SMTP server's IP address.

Step 3. **E-Mail Address 1:** Enter the first e-mail address to receive the alarm notification.

Step 4. **E-Mail Address 2:** Enter the second e-mail address to receive the alarm notification. (Optional)

Click **OK** on the bottom-right of the screen to enable E-mail alert notification.



Bandwidth Management Configuration

Export System Settings to Client [Download]

Import System Settings from Client: C:\Documents and Setti [Browse...] (ex: bandwidth.conf)

□ Reset Factory Settings

E-mail Settings

☑ Enable E-mail Alert Notification

Device Name: bm-500

Sender Address(Required by some ISPs): bm500@planet.com.tw

SMTP Server: planet.com.tw

E-mail Address 1: admin@planet.com.tw

E-mail Address 2: operator@planet.com.tw

Mail Test: [MailTest]

Web Management (WAN Interface)

HTTP Port: 80

Authentication Management

Authentication Port: 82

Re-Login if Idle: 30 Minutes

Web Management (WAN Interface) (Remote UI Management)

The administrator can change the port number used by HTTP port anytime. (Remote UI Management)

Step 1. **Set Web Management (WAN Interface).** The administrator can change the port number used by HTTP port anytime.

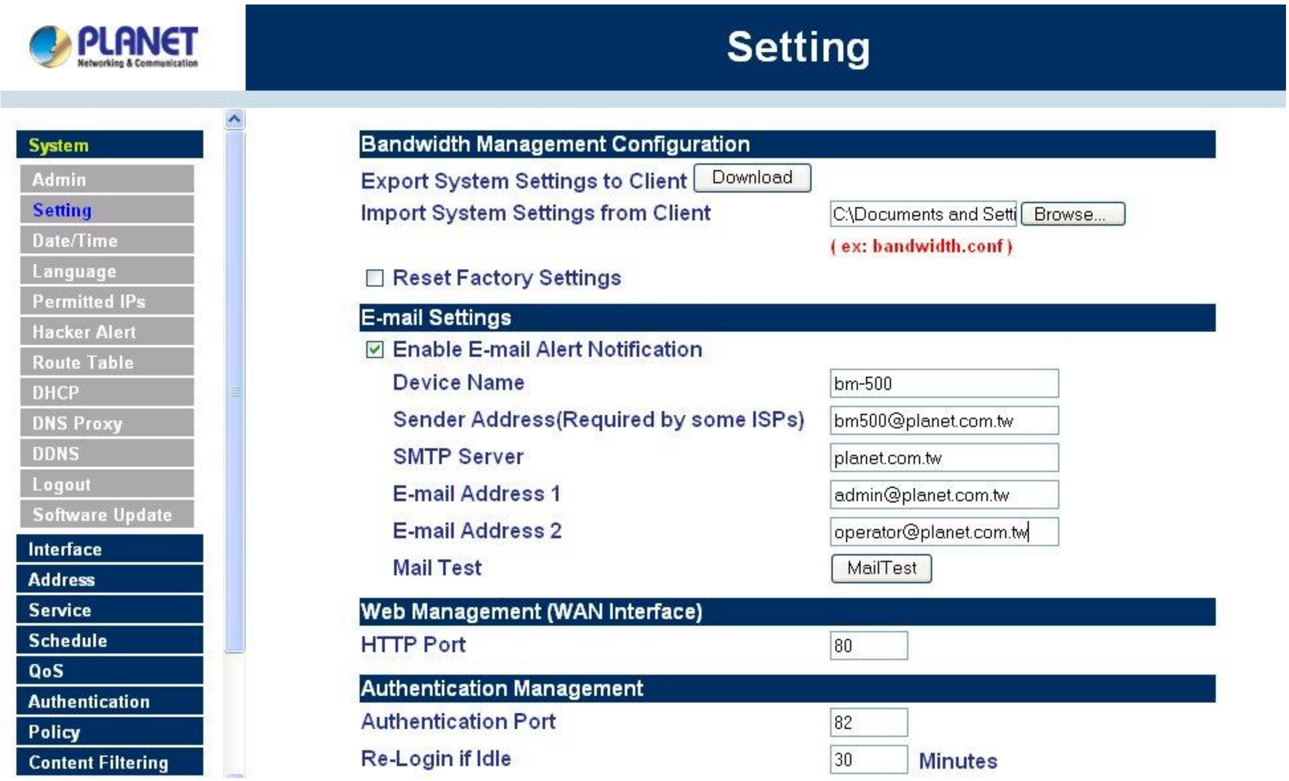
Authentication

The administrator can specify the port number and authentication time of authentication management system for LAN user to access WAN network. (Needs to setup authentication table in advance)

Authentication functions:

Authentication Port: The port number used for user login page. When user want to access WAN network and the authentication (Policy -> Outgoing) is enabled, the user has to send http request with this port number. The Bandwidth Management Gateway will send a User Login page for user to input user name and password. For example, if the gateway IP address is 192.168.1.1 and authentication port is 82, user have to open a web browser and input http://192.168.1.1:82 on the address file to have the user login page.

Re-Login if Idle: When the LAN user access to WAN network and do not use for a while, the connection will be time-out. User has to re-login again. The default time is 30 minutes and you can configure this time by "System"-> "Setting" page.



Bandwidth Management Configuration

Export System Settings to Client

Import System Settings from Client: C:\Documents and Setti

(ex: bandwidth.conf)

□ Reset Factory Settings

E-mail Settings

☑ Enable E-mail Alert Notification

Device Name	bm-500
Sender Address(Required by some ISPs)	bm500@planet.com.tw
SMTP Server	planet.com.tw
E-mail Address 1	admin@planet.com.tw
E-mail Address 2	operator@planet.com.tw
Mail Test	

Web Management (WAN Interface)

HTTP Port	80

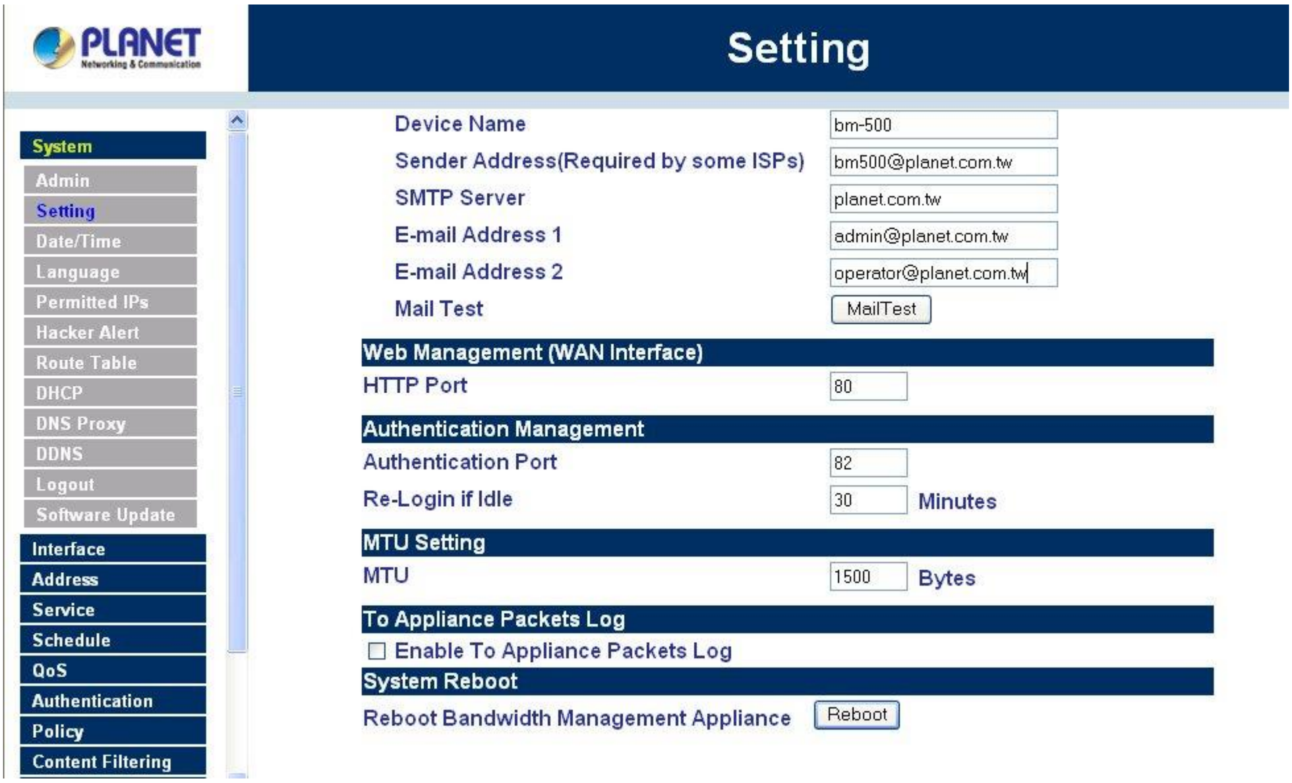
Authentication Management

Authentication Port	82
Re-Login if Idle	30 Minutes

MTU (set networking packet length)

The administrator can modify the networking packet length.

Step 1. **MTU Setting.** Modify the networking packet length.



Setting

Device Name: bm-500
Sender Address(Required by some ISPs): bm500@planet.com.tw
SMTP Server: planet.com.tw
E-mail Address 1: admin@planet.com.tw
E-mail Address 2: operator@planet.com.tw
Mail Test

Web Management (WAN Interface)

HTTP Port: 80

Authentication Management

Authentication Port: 82
Re-Login if Idle: 30 Minutes

MTU Setting

MTU: 1500 Bytes

To Appliance Packets Log

□ Enable To Appliance Packets Log

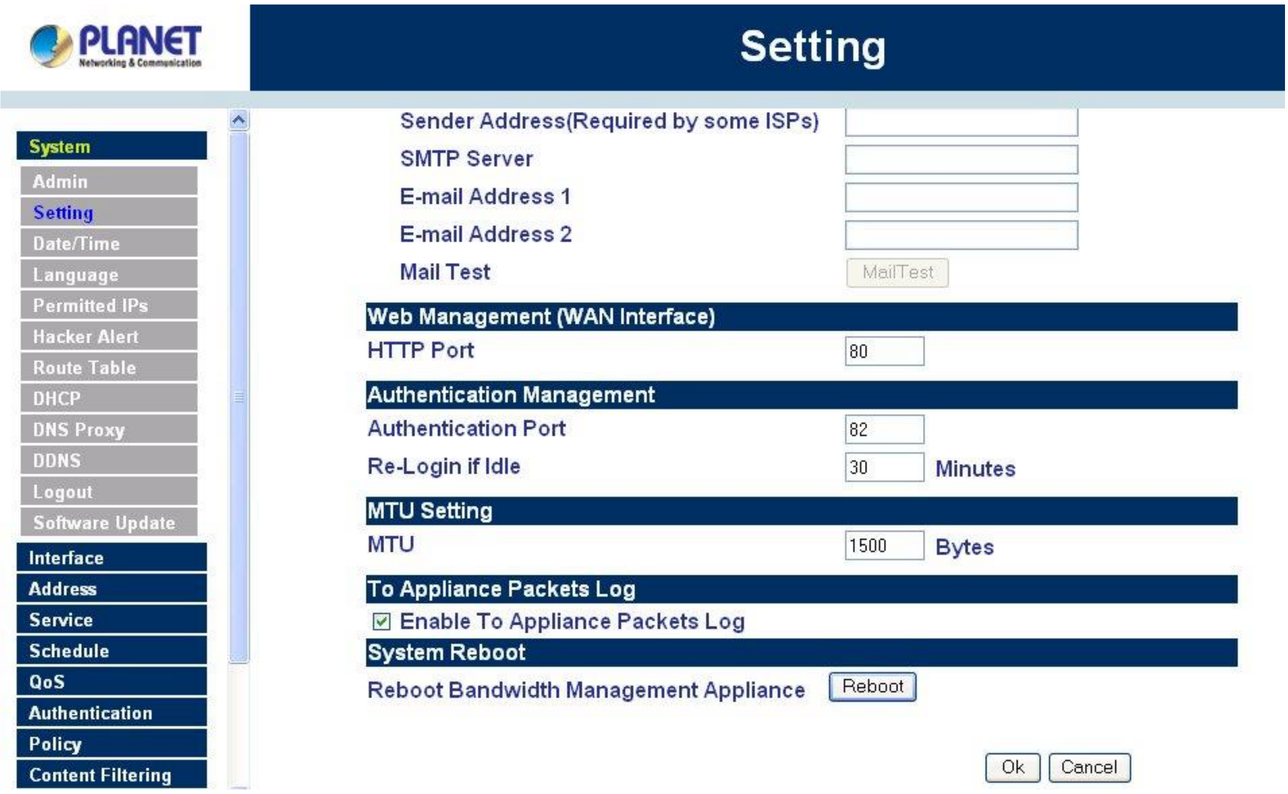
System Reboot

Reboot Bandwidth Management Appliance

To-Appliance Packets Log

Once this function is enabled, every packet to this appliance will be recorded for the administrator to trace.

Step 1. Select this option to the device's **To-Appliance Packets Log.** Once this function is enabled, every packet to this appliance will be recorded for system administrator to trace.



Setting

Sender Address(Required by some ISPs):
SMTP Server:
E-mail Address 1:
E-mail Address 2:
Mail Test

Web Management (WAN Interface)

HTTP Port: 80

Authentication Management

Authentication Port: 82
Re-Login if Idle: 30 Minutes

MTU Setting

MTU: 1500 Bytes

To Appliance Packets Log

☑ Enable To Appliance Packets Log

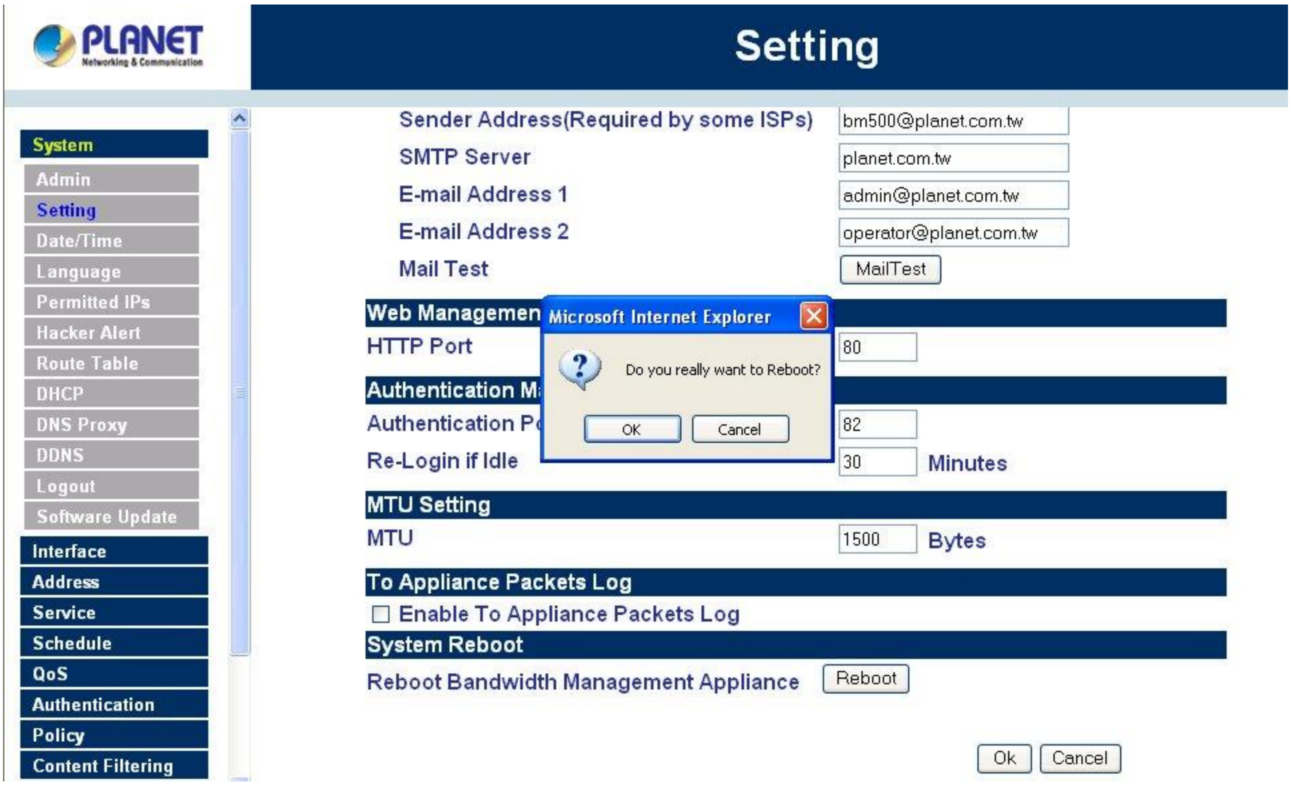
System Reboot

Reboot Bandwidth Management Appliance

System Reboot

Once this function is enabled, the Bandwidth Management Gateway will be rebooted**.**

Reboot Bandwidth Management Gateway: Click **Reboot.**
A confirmation pop-up box will appear. Follow the confirmation pop-up box, click **OK** to restart Bandwidth Management Gateway or click **Cancel** to discard changes



Sender Address(Required by some ISPs) bm500@planet.com.tw
SMTP Server planet.com.tw
E-mail Address 1 admin@planet.com.tw
E-mail Address 2 operator@planet.com.tw
Mail Test

Web Managemen
HTTP Port 80

Authentication M
Authentication P 82
Re-Login if Idle 30 Minutes

Microsoft Internet Explorer
Do you really want to Reboot?

MTU Setting
MTU 1500 Bytes

To Appliance Packets Log
□ Enable To Appliance Packets Log

System Reboot
Reboot Bandwidth Management Appliance

4.1.3 Date/Time

Synchronizing the Bandwidth Management Gateway with the System Clock
Administrator can configure the Bandwidth Management Gateway's date and time by either syncing to an Internet Network Time Server (NTP) or by syncing to your computer's clock.

Follow these steps to sync to an Internet Time Server

Step 1. Enable synchronization by checking the box.

Step 2. Click the down arrow to select the offset time from GMT.

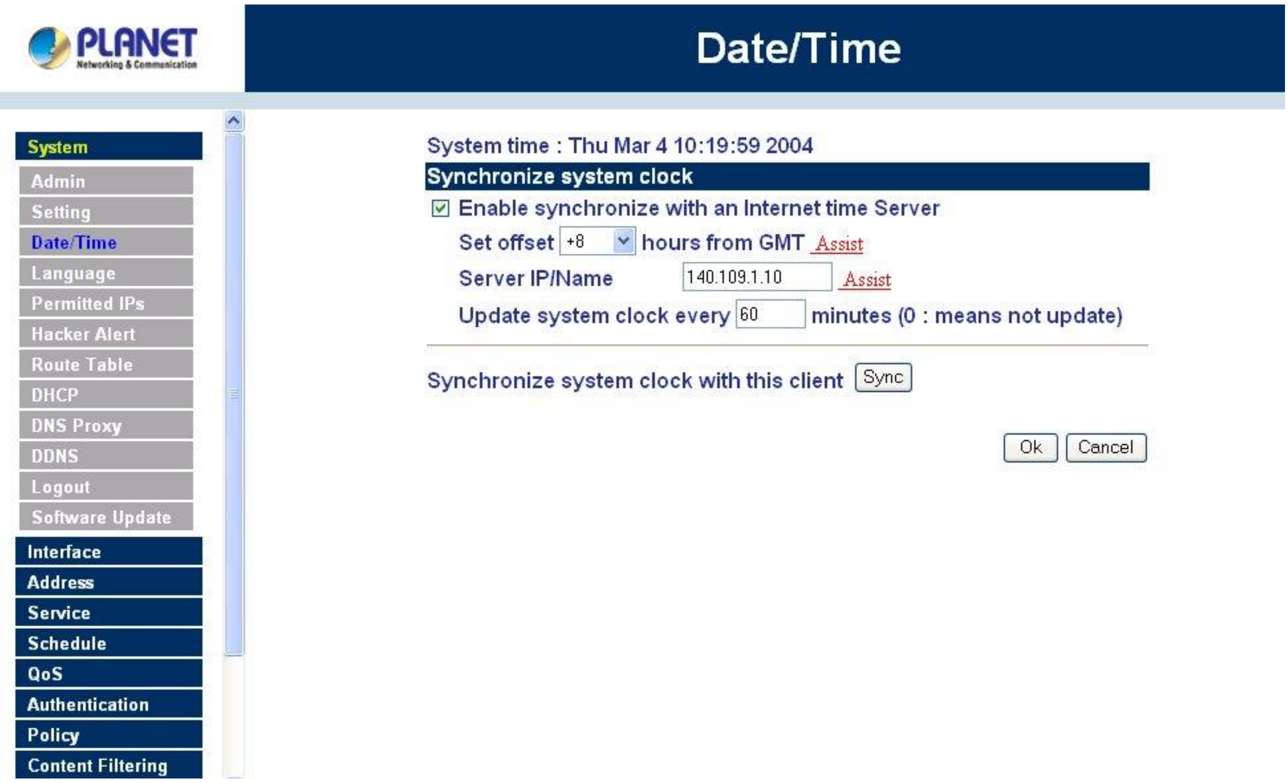
Step 3. Enter the Server IP Address or Server name with which you want to synchronize.

Step 4. **Update system clock every 5 minutes** You can set the interval time to synchronize with outside servers. If you set it to 0, it means the device will not synchronize automatically.

Follow this step to sync to your computer's clock.

Step 1. Click on the **Sync** button.

Click **OK** to apply the setting or click **Cancel** to discard changes.



Date/Time

System time : Thu Mar 4 10:19:59 2004

Synchronize system clock

☑ Enable synchronize with an Internet time Server

Set offset +8 hours from GMT Assist

Server IP/Name 140.109.1.10 Assist

Update system clock every 60 minutes (0 : means not update)

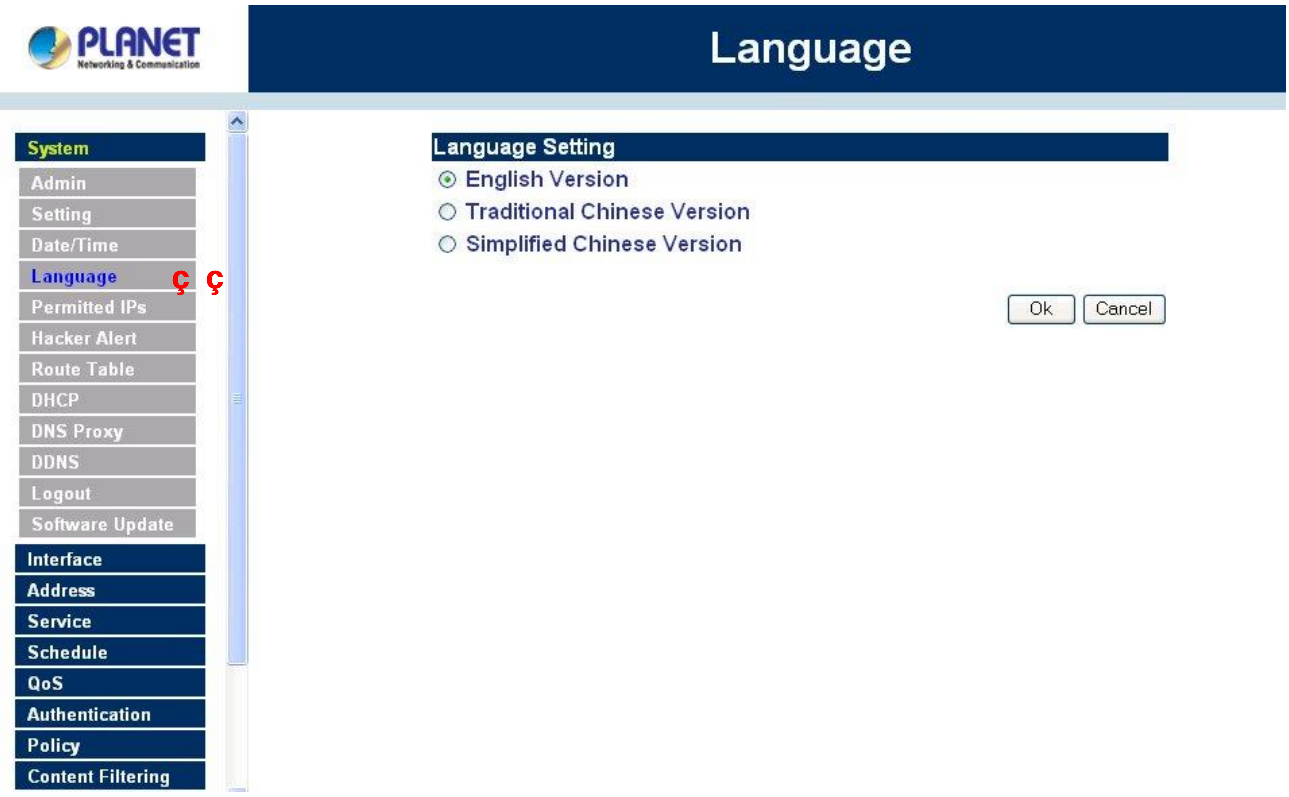
Synchronize system clock with this client Sync

4.1.4 Language

Administrator can configure the Bandwidth Management Gateway Select the Language version

Step 1. Select the Language version (**English Version, Traditional Chinese Version** or **Simplified Chinese Version**).

Step 2. Click 【**OK**】to set the Language version or click **Cancel** to discard changes.

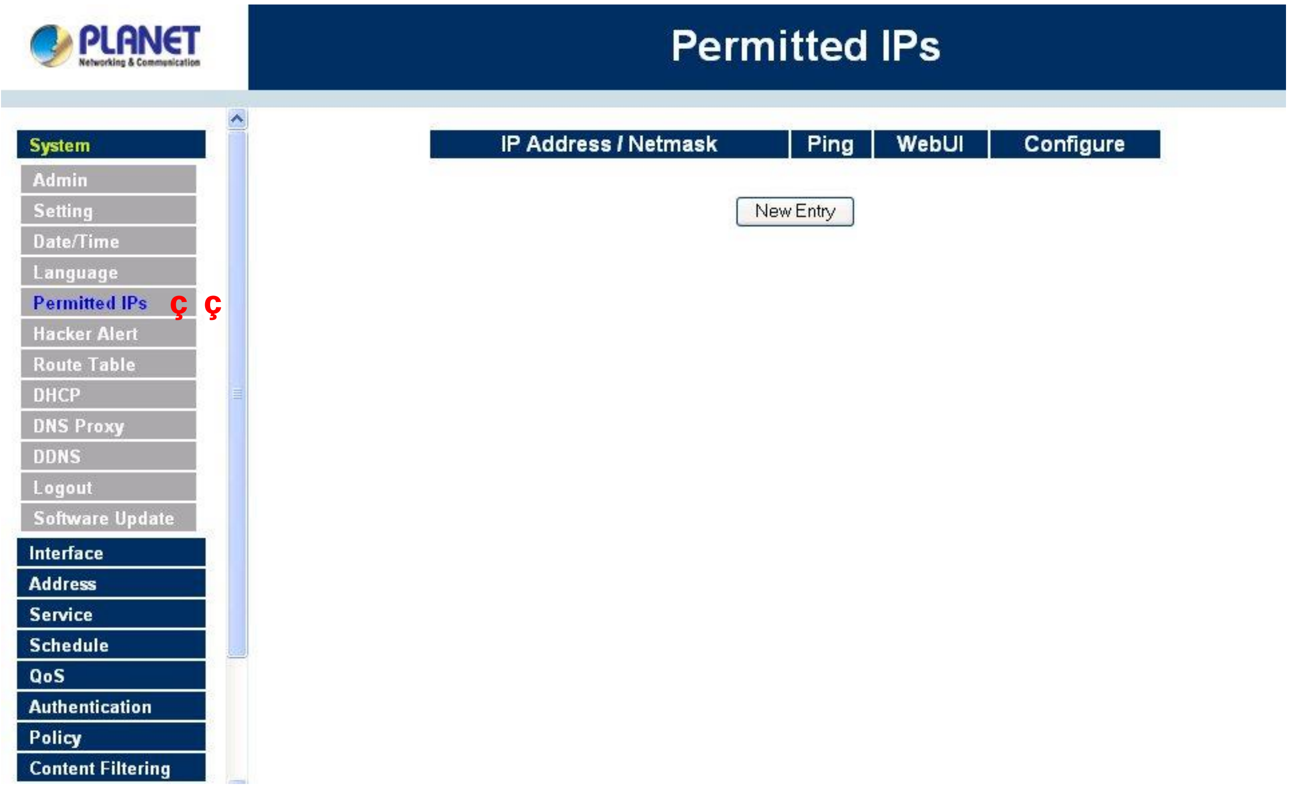


Language Setting

● English Version
○ Traditional Chinese Version
○ Simplified Chinese Version

4.1.5 Permitted IPs

Only the authorized IP address is permitted to manage the Bandwidth Management Gateway.



IP Address / Netmask	Ping	WebUI	Configure

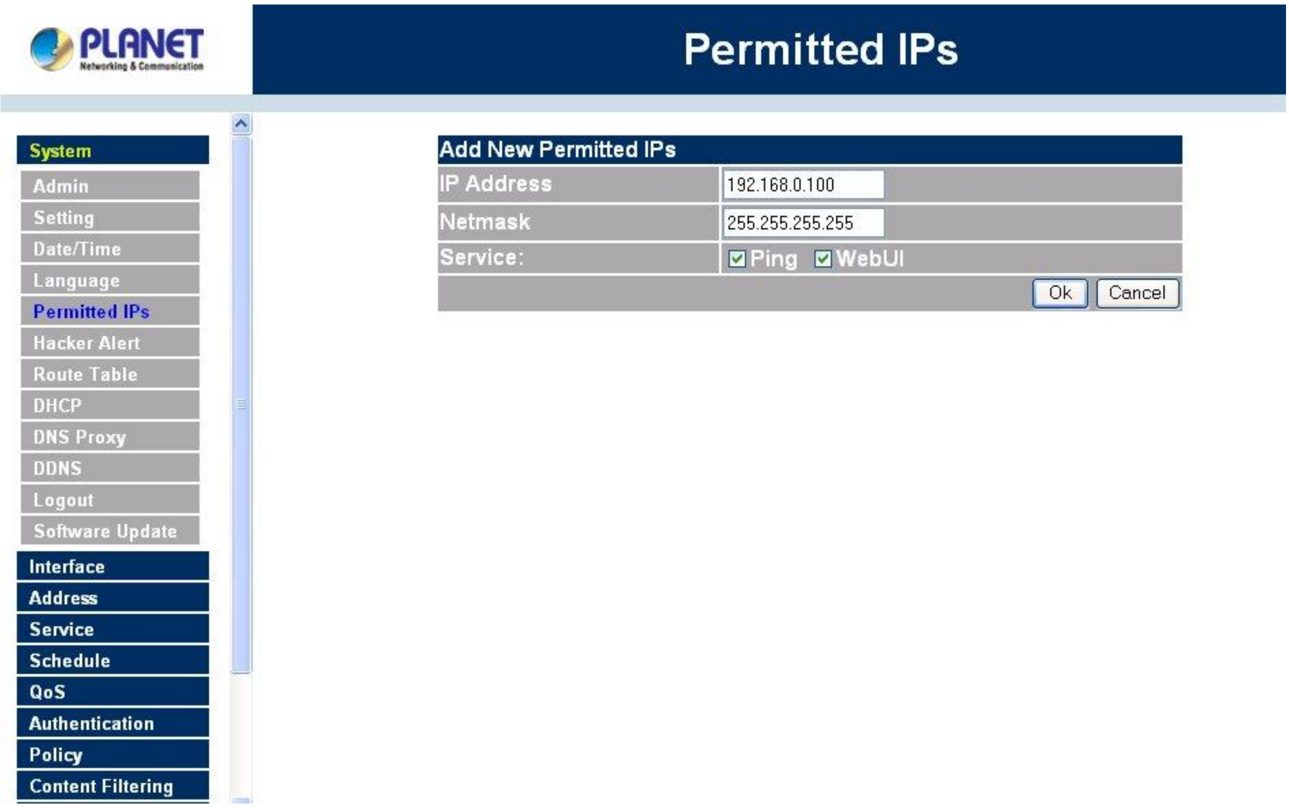
Add Permitted IP Address

Step 1. Click **New Entry** button.

Step 2. In IP Address field, enter the LAN IP address or WAN IP address.

- **IP address**: Enter the LAN IP address or WAN IP address.
- **Netmask**: Enter the netmask of LAN/WAN.
- **Ping**: Select this to allow the external network to ping the IP Address of the Firewall.
- **WebUI**: Check this item, Web User can use HTTP to connect to the Setting window of BandWidth Management Gateway.

Step 3. Click **OK** to add Permitted IP or click **Cancel** to discard changes.



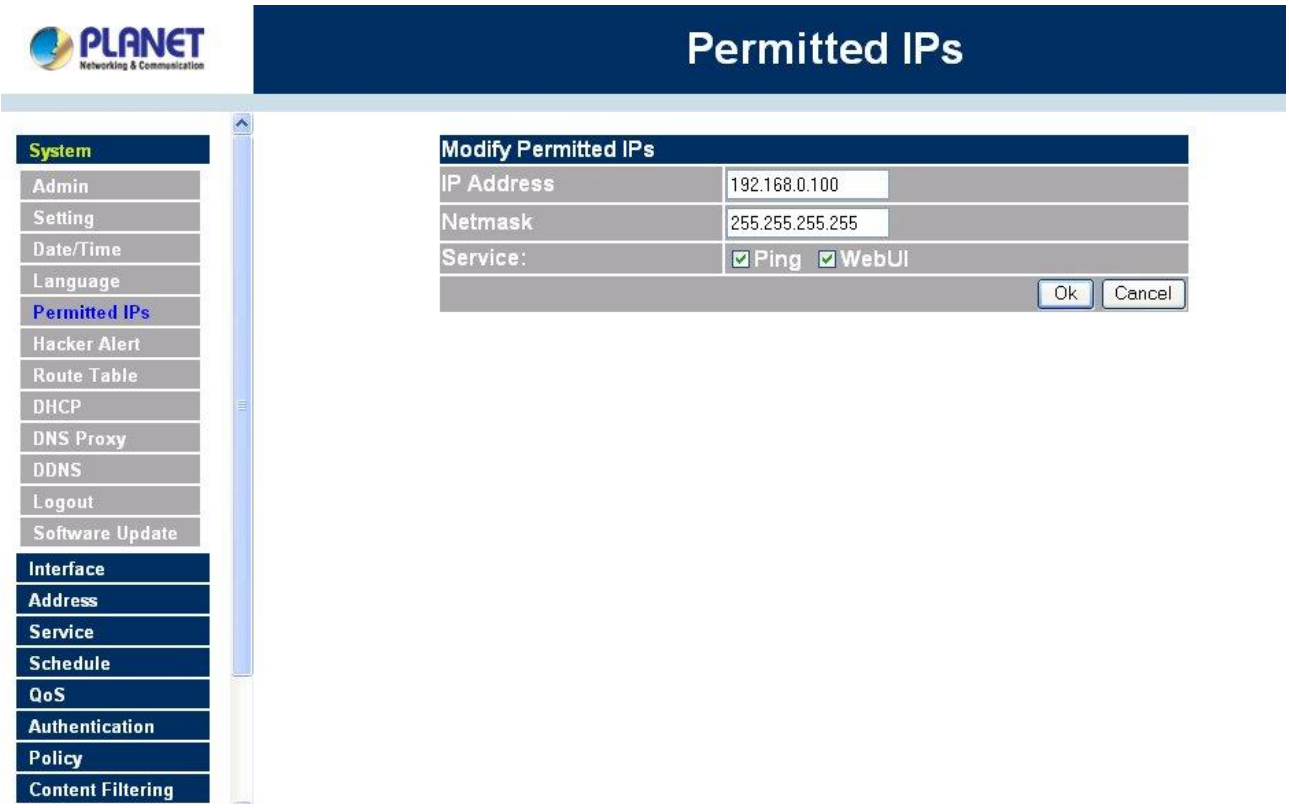
Add New Permitted IPs	
IP Address	192.168.0.100
Netmask	255.255.255.255
Service:	☑ Ping ☑ WebUI

Modify Permitted IP Address

Step 1. In the table of **Permitted IPs**, highlight the IP you want to modify, and then click **Modify**.

Step 2. In **Modify Permitted IP**, enter new IP address.

Step 3. Click **OK** to modify or click **Cancel** to discard changes.



Modify Permitted IPs

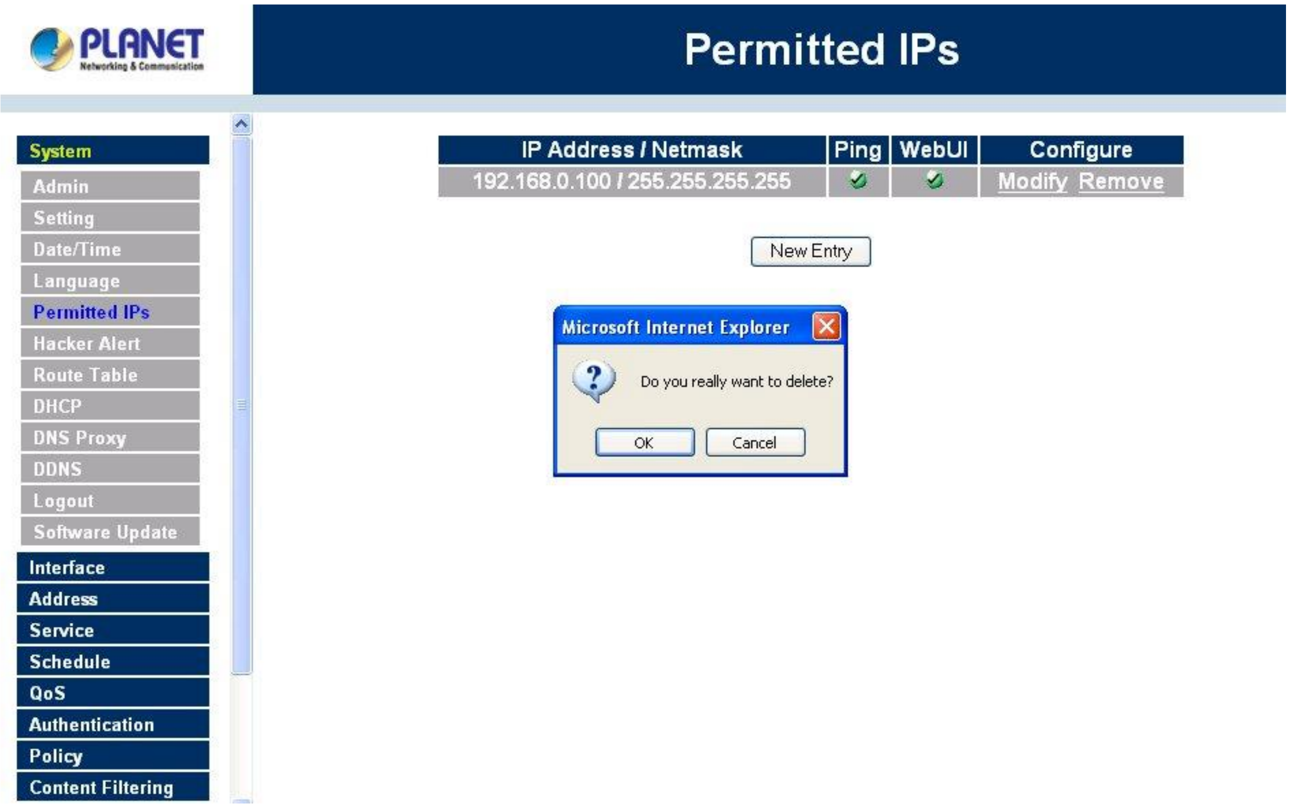
IP Address	192.168.0.100
Netmask	255.255.255.255
Service:	☑ Ping ☑ WebUI

Remove Permitted IP addresses

Step 1. In the table of **Permitted IPs**, highlight the IP you want to remove, and then click **Remove**.

Step 2. In **Remove Permitted IP**, enter new IP address.

Step 3. In the confirm window, click **OK** to remove or click **Cancel** to discard changes.



IP Address / Netmask	Ping	WebUI	Configure
192.168.0.100 / 255.255.255.255	✓	✓	Modify Remove

Microsoft Internet Explorer

Do you really want to delete?

4.1.6 Multiple NAT

Multiple NAT allows local port to set multiple subnetworks and connect with the Internet through different WAN IP Addresses.

NOTE: This function is only available when the device is configured to NAT mode.

For instance, the lease line of a company applies several real IP Addresses 168.95.88.0/24, and the company is divided into R&D department, service, sales department, procurement department, accounting department, the company can distinguish each department by different subnetworks for the purpose of convenient Management Gateway. The settings are as the following:

1.R&D department subnetwork: 192.168.1.11/24(Internal) **ß à** 168.95.88.253(WAN)

2. Service department subnetwork: 192.168.2.11/24(Internal) **ß à** 168.95.88.252(WAN)

3.Sales department subnetwork: 192.168.3.11/24(Internal) **ß à** 168.95.88.251(WAN)

4.Procurement department subnetwork 192.168.4.11/24(Internal) **ß à** 168.95.88.250(WAN)

5.Accounting department subnetwork 192.168.5.11/24(Internal) **ß à** 168.95.88.249(WAN)

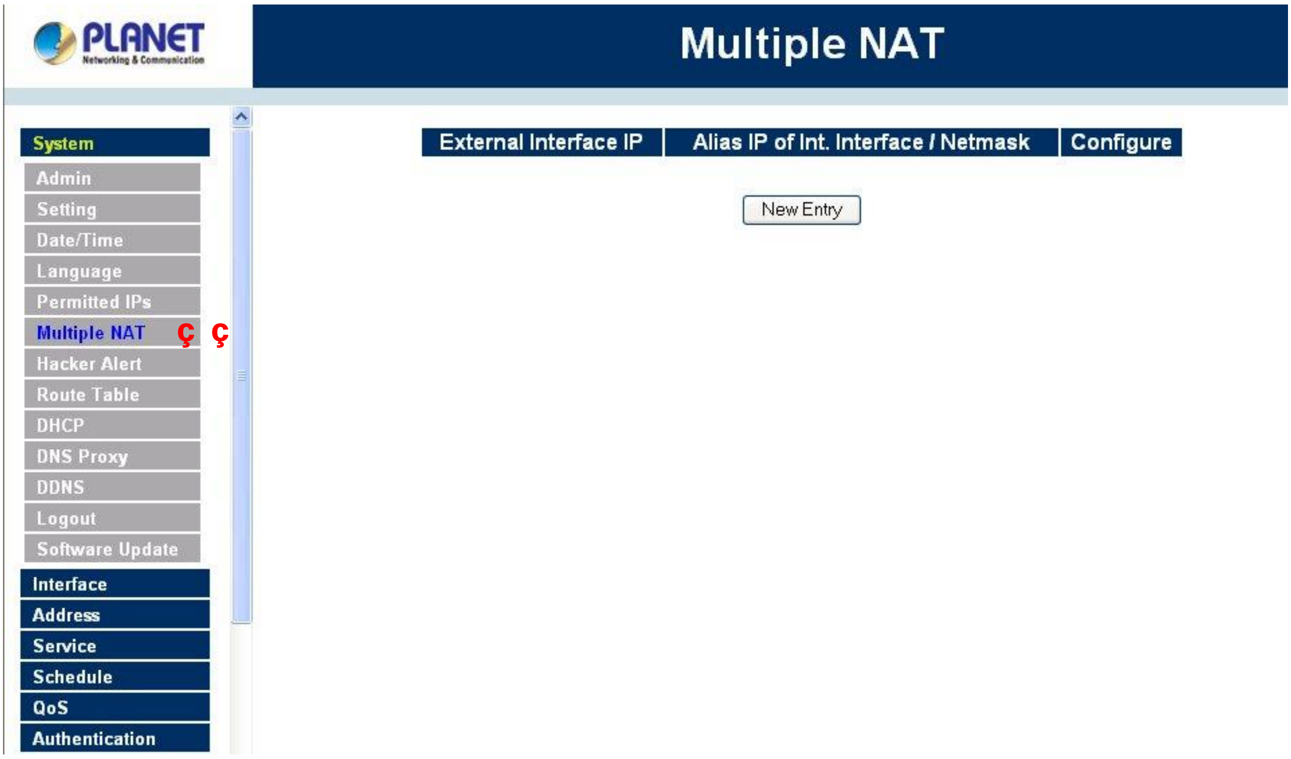
The first department(R&D department) was set while setting interface IP, the other four ones have to be added in Multiple NAT，after completing the settings, each department use the different WAN IP Address to connect to the Internet. The settings of each department are as the following

Service IP Address: 192.168.2.1
Subnet Mask: 255.255.255.0
Default Gateway: 192.168.2.11

The other departments are also set by groups, this is the function of Multiple NAT.

Multiple NAT settings

Step 1. Click **Multiple NAT** in the **System** menu to enter Multiple NAT window.



External Interface IP: WAN port IP Address.

Alias IP of Int. Interface / Netmask: Local port IP Address and subnet Mask.

Configure: Modify the settings of Multiple NAT. Click **Modify** to modify the parameters of Multiple NAT or click **Delete** to delete settings.

Add Multiple NAT

Step 1. Click the **Add** button below to add Multiple NAT.

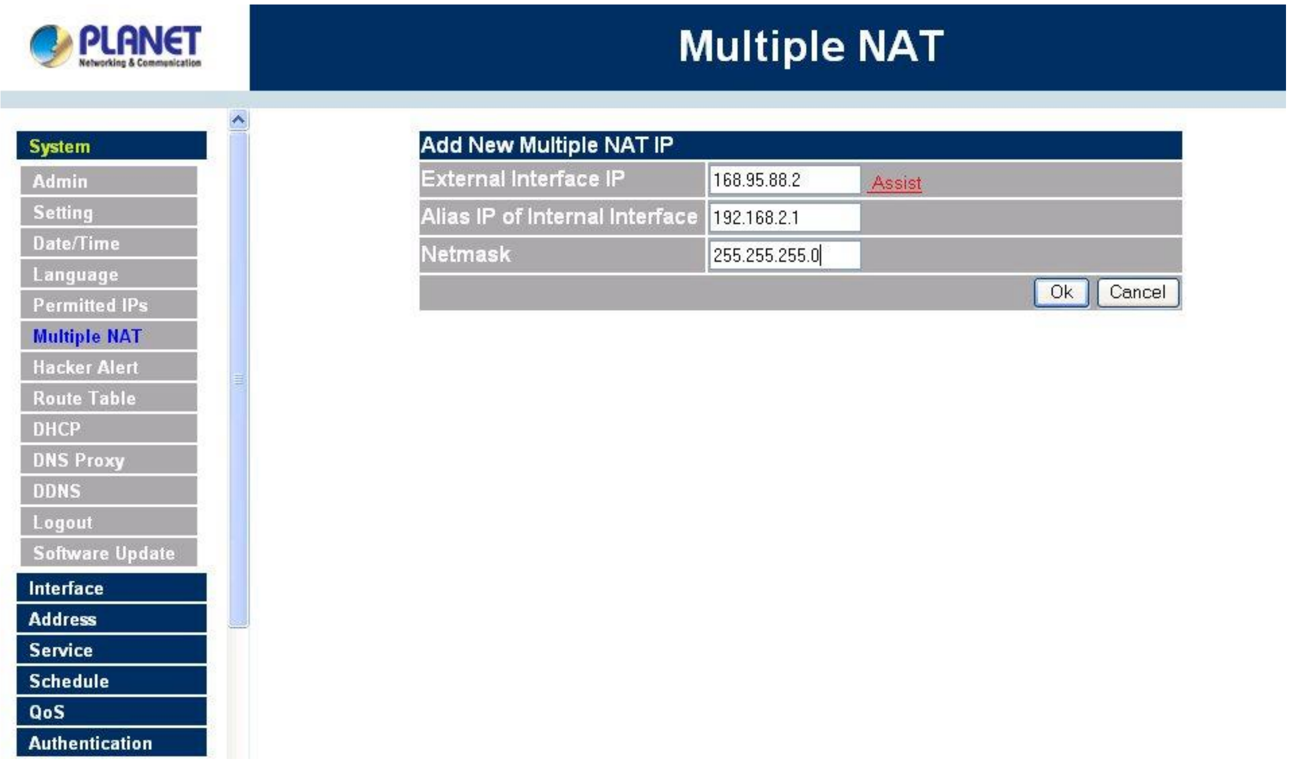
Step 2. Enter the IP Address in the website name column of the new window.

n **External interface IP Address:** Select Global port IP Address.

n **Alias IP of Internal Interface:** Enter Local port IP Address.

n **NetMask:** Enter Local port subnet Mask.

Step 3. Click **OK** to add Multiple NAT or click **Cancel** to discard changes.



Add New Multiple NAT IP

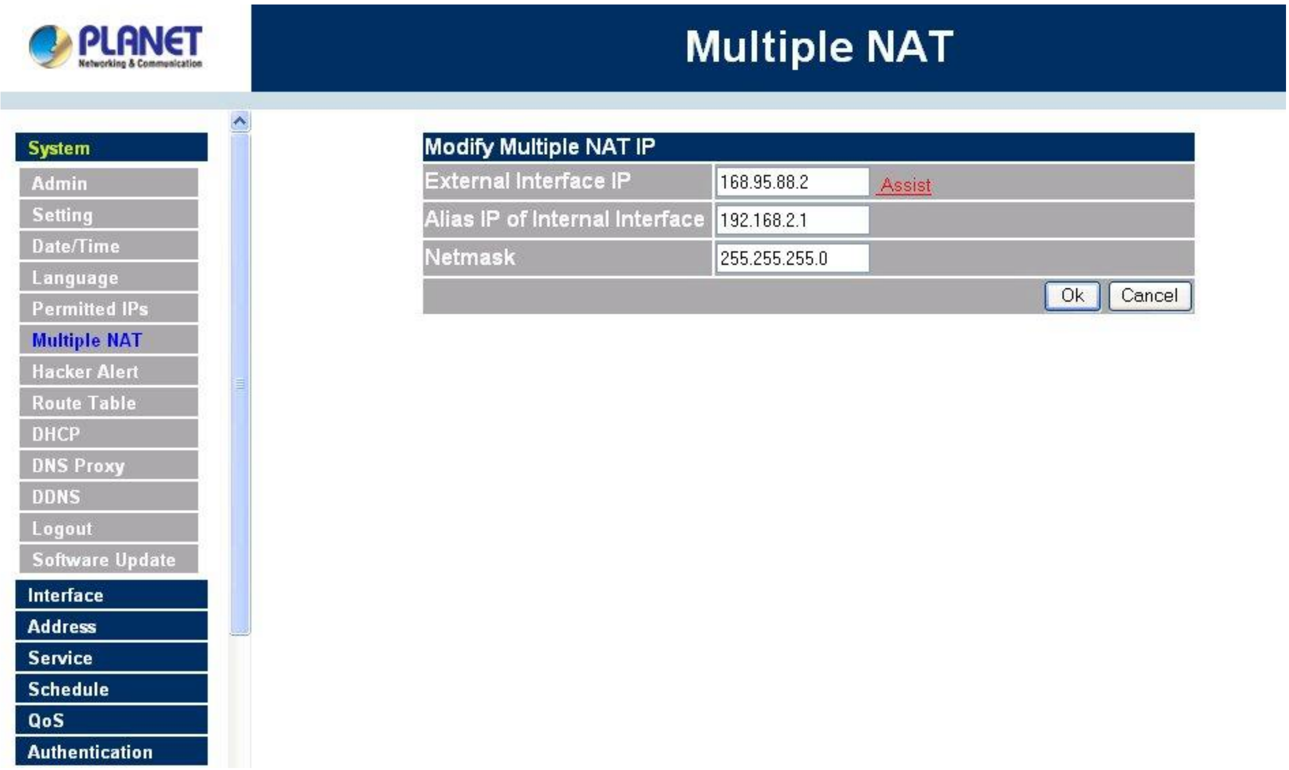
External Interface IP	168.95.88.2 Assist
Alias IP of Internal Interface	192.168.2.1
Netmask	255.255.255.0

Modify Multiple NAT

Step 1. Find the IP Address you want to modify and click **Modify**

Step 2. Enter the new IP Address in **Modify Multiple NAT** window.

Step 3. Click the **OK** button below to change the setting or click **Cancel** to discard changes.



Modify Multiple NAT IP

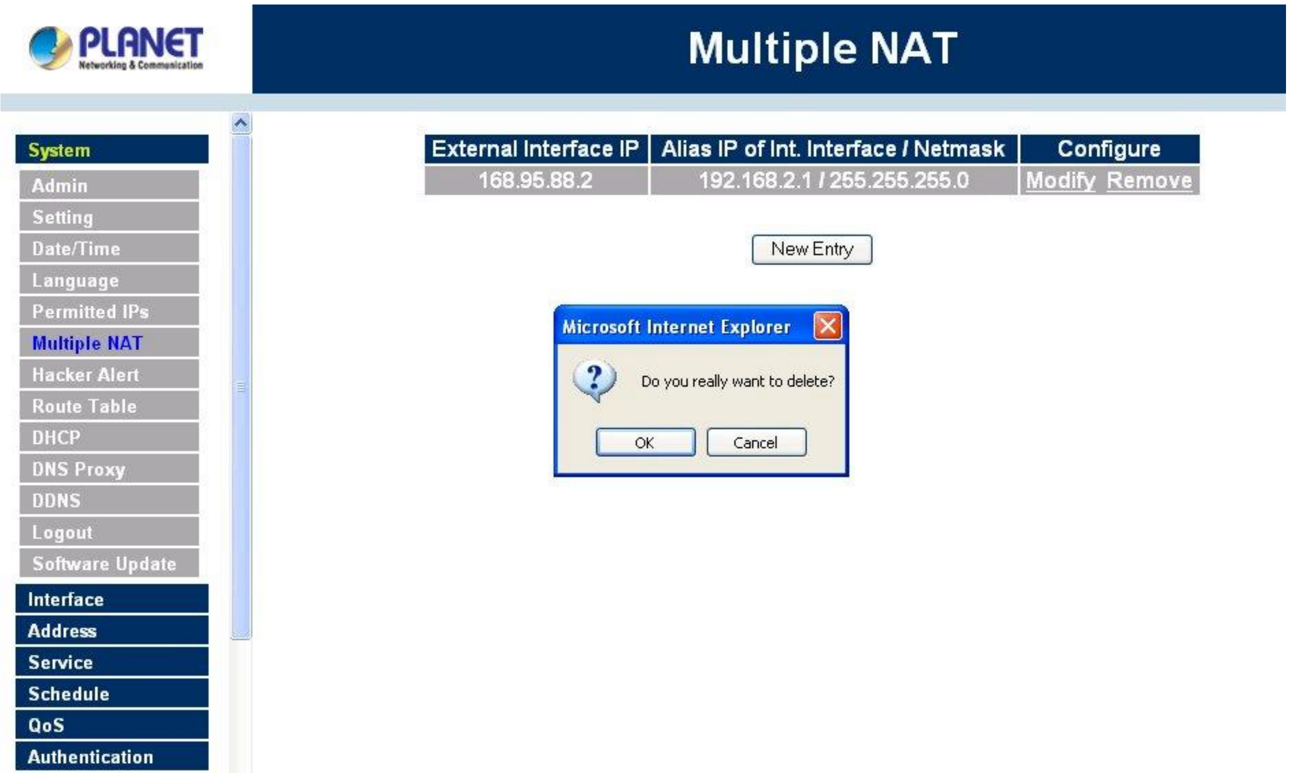
External Interface IP	168.95.88.2 Assist
Alias IP of Internal Interface	192.168.2.1
Netmask	255.255.255.0

Figure 1-22 Modify Multiple NAT

Delete Multiple NAT

Step 1. Find the IP Address you want to delete and click **Remove**.

Step 2. A confirmation pop-up box will appear, click **OK** to delete the setting or click **Cancel** to discard changes.

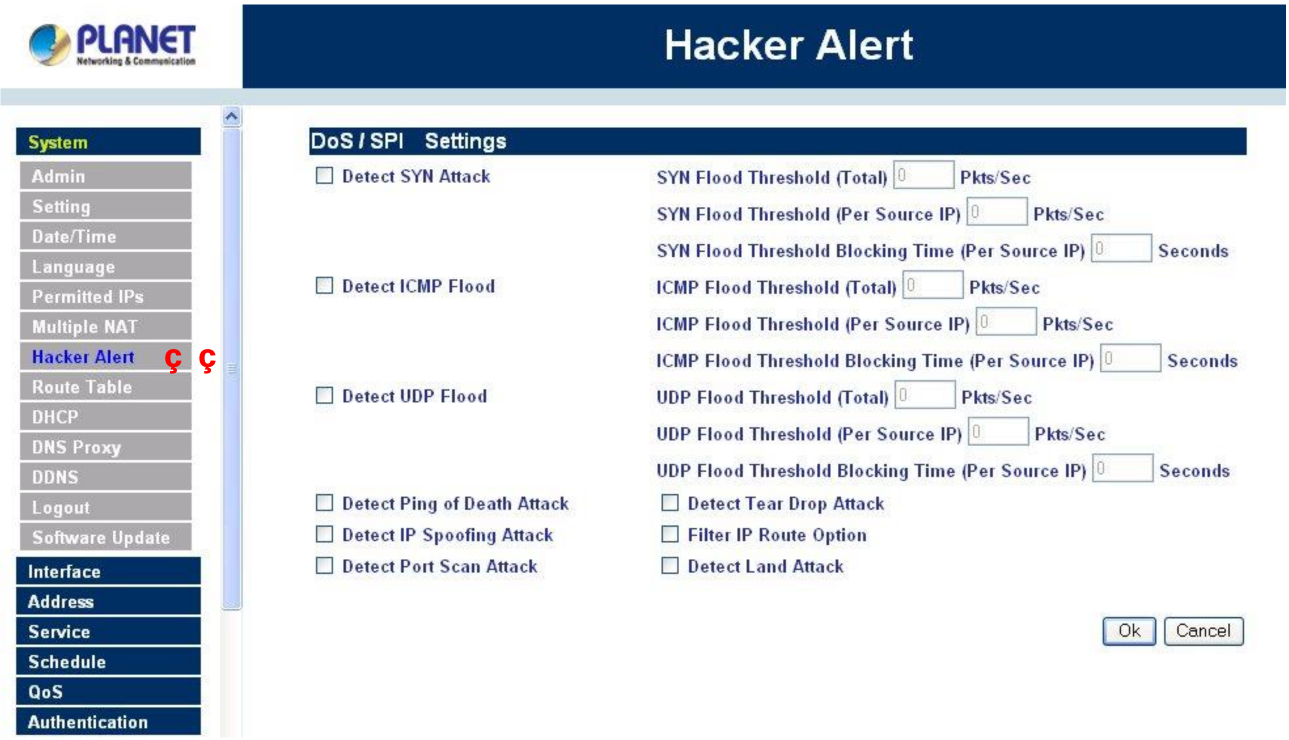


External Interface IP	Alias IP of Int. Interface / Netmask	Configure
168.95.88.2	192.168.2.1 / 255.255.255.0	Modify Remove

Do you really want to delete?

4.1.7 Hacker Alert

The Administrator can enable the device's auto detect functions for hacker attackin this section. When abnormal conditions occur, the Bandwidth Management Gateway will send an e-mail alert to notify the Administrator, and also display warning messages in the **Event** window of **Alarm.**



Hacker Alert

DoS / SPI Settings

□ Detect SYN Attack
SYN Flood Threshold (Total) 0 Pkts/Sec
SYN Flood Threshold (Per Source IP) 0 Pkts/Sec
SYN Flood Threshold Blocking Time (Per Source IP) 0 Seconds

□ Detect ICMP Flood
ICMP Flood Threshold (Total) 0 Pkts/Sec
ICMP Flood Threshold (Per Source IP) 0 Pkts/Sec
ICMP Flood Threshold Blocking Time (Per Source IP) 0 Seconds

□ Detect UDP Flood
UDP Flood Threshold (Total) 0 Pkts/Sec
UDP Flood Threshold (Per Source IP) 0 Pkts/Sec
UDP Flood Threshold Blocking Time (Per Source IP) 0 Seconds

□ Detect Ping of Death Attack
□ Detect Tear Drop Attack
□ Detect IP Spoofing Attack
□ Filter IP Route Option
□ Detect Port Scan Attack
□ Detect Land Attack

Ok Cancel

Auto Detect functions

- **Detect SYN Attack**: Select this option to detect TCP SYN attacks that hackers send to server computers continuously to block or cut down all the connections of the servers. These attacks will prevent valid users from connecting to the servers. After enabling this function, the System Administrator can enter the number of SYN packets per second that is allowed to enter the network/Bandwidth Management Gateway. Once the SYN packets exceed this limit, the activity will be logged in Alarm and an email alert is sent to the Administrator. The default SYN flood threshold is set to 200 Pkts/Sec .

- **Detect ICMP Flood**: Select this option to detect ICMP flood attacks. When hackers continuously send PING packets to all the machines of the LAN networks or to the Bandwidth Management Gateway, your network is experiencing an ICMP flood attack. This can cause traffic congestion on the network and slows the network down. After enabling this function, the System Administrator can enter the number of ICMP packets per second that is allowed to enter the network/Bandwidth Management Gateway. Once the ICMP packets exceed this limit, the activity will be logged in Alarm and an email alert is sent to the Administrator. The default ICMP flood threshold is set to 1000 Pkts/Sec.

- **Detect UDP Flood**: Select this option to detect UDP flood attacks. A UDP flood attack is similar to an ICMP flood attack. After enabling this function, the System Administrator can enter the number of UDP packets per second that is allow to enter the network/Bandwidth Management Gateway. Once the UDP packets exceed this limit, the activity will be logged in Alarm and an email alert is sent to the Administrator. The default UDP flood threshold is set to 1000 Pkts/Sec .

- **Detect Ping of Death Attack**: Select this option to detect the attacks of tremendous trash data in PING packets that hackers send to cause System malfunction This attack can cause network speed to slow down, or even make it necessary to restart the computer to get a normal operation.
- **Detect Tear Drop Attack**: Select this option to detect tear drop attacks. These are packets that are segmented to small packets with negative length. Some Systems treat the negative value as a very large number, and copy enormous data into the System to cause System damage, such as a shut down or a restart.
- **Detect IP Spoofing Attack**: Select this option to detect spoof attacks. Hackers disguise themselves as trusted users of the network in Spoof attacks. They use a fake identity to try to pass through the Bandwidth Management Gateway System and invade the network.
- **Filter IP Source Route Option**: Each IP packet can carry an optional field that specifies the replying address that can be different from the source address specified in packet's header. Hackers can use this address field on disguised packets to invade LAN networks and send LAN networks' data back to them.
- **Detect Port Scan Attack**: Select this option to detect the port scans hackers use to continuously scan networks on the Internet to detect computers and vulnerable ports that are opened by those computers.
- **Detect Land Attack**: Some Systems may shut down when receiving packets with the same source and destination addresses, the same source port and destination port, and when SYN on the TCP header is marked.
  Enable this function to detect such abnormal packets.
- **Default Packet Deny**: Denies all packets from passing the Bandwidth Management Gateway. A packet can pass only when there is a policy that allows it to pass.

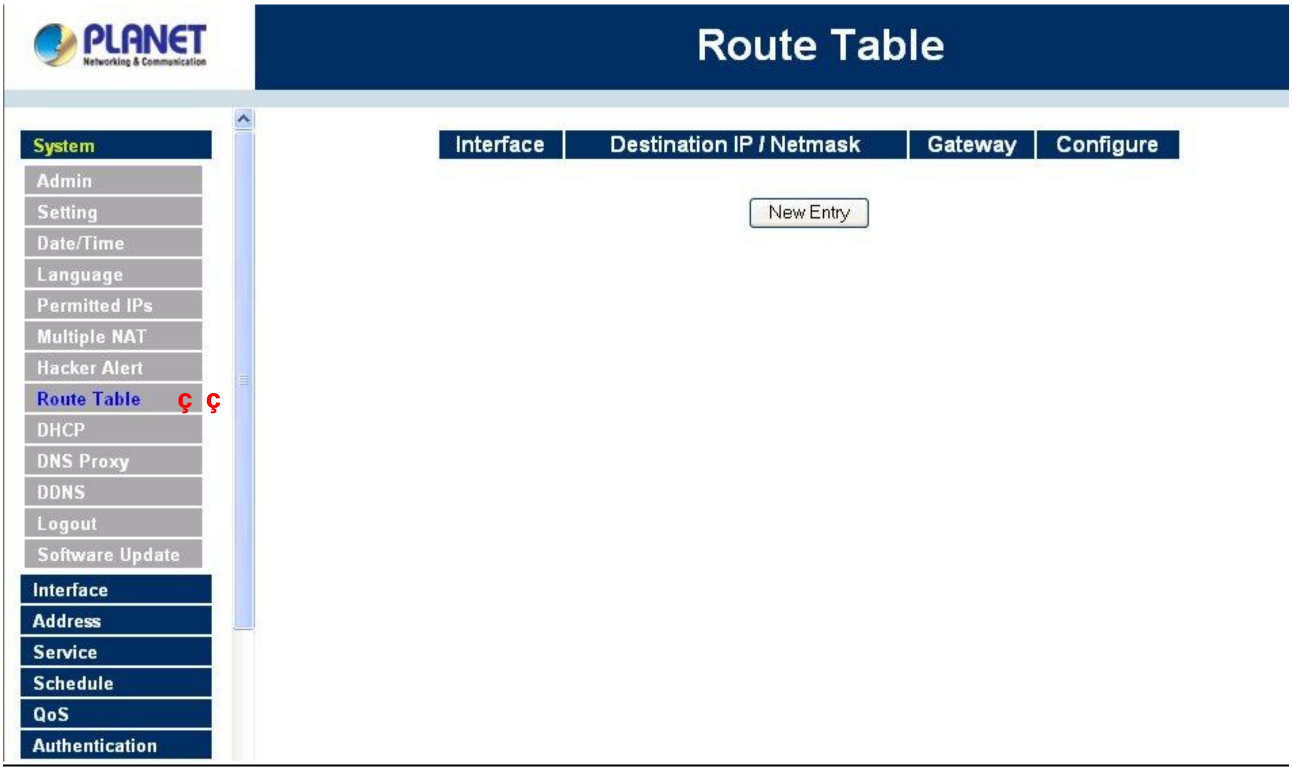
After enabling the needed detect functions, click OK to activate the changes.

4.1.8 Route Table

In this section, the Administrator can add static routes for the networks.

Entering the Route Table screen

Step 1. Click **System** on the left side menu bar, then click **Route Table** below it. The Route Table window appears, in which current route settings are shown.



Route Table functions

- **Interface:** Destination network, LAN or WAN 1 networks.
- **Destination IP:** IP address of destination network.
- **NetMask:** Netmask of destination network.
- **Gateway:** Gateway IP address for connecting to destination network.
- **Configure:** Change settings in the route table.

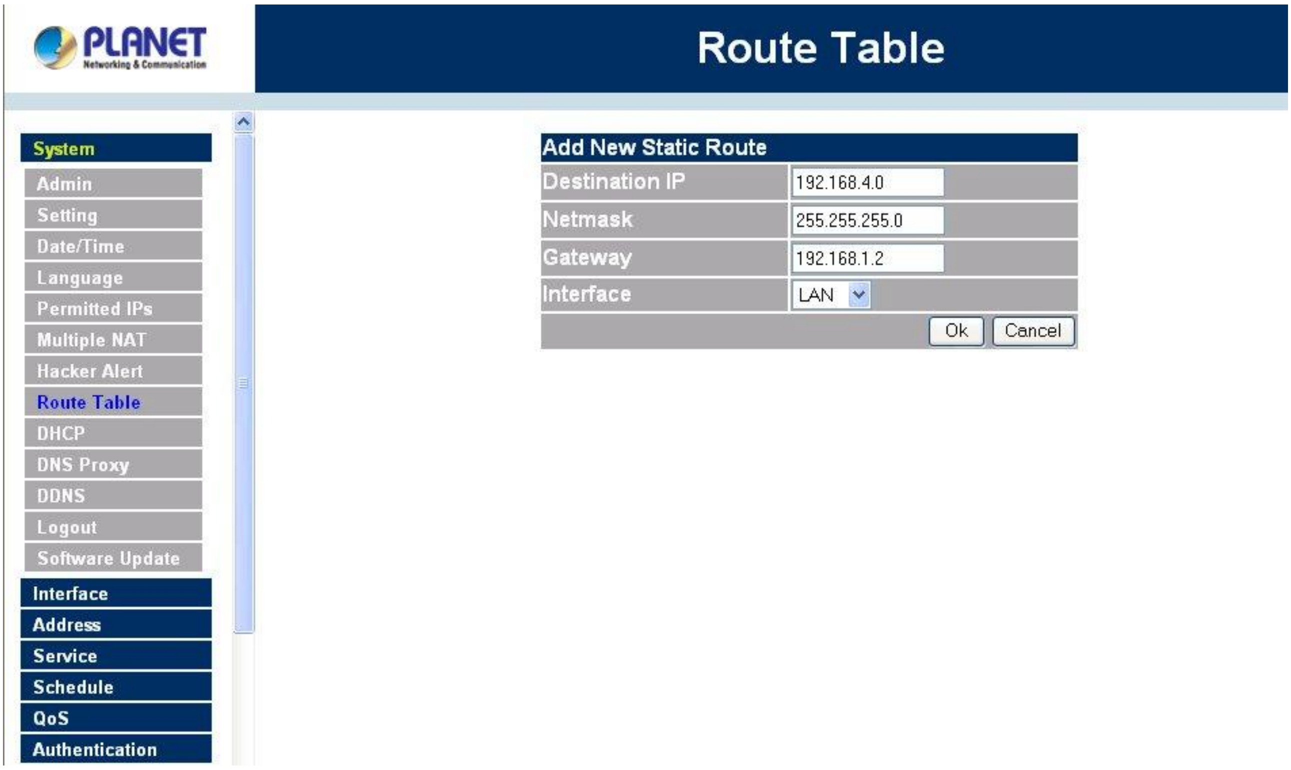
Adding a new Static Route

Step 1. In the Route Table window, click the **New Entry** button.

Step 2. In the Add New Static Route window, enter new static route information.

Step 3. In the Interface field's pull-down menu, choose the network to connect (LAN, WAN).

Step 4. Click **OK** to add the new static route or click **Cancel** to cancel.



Add New Static Route

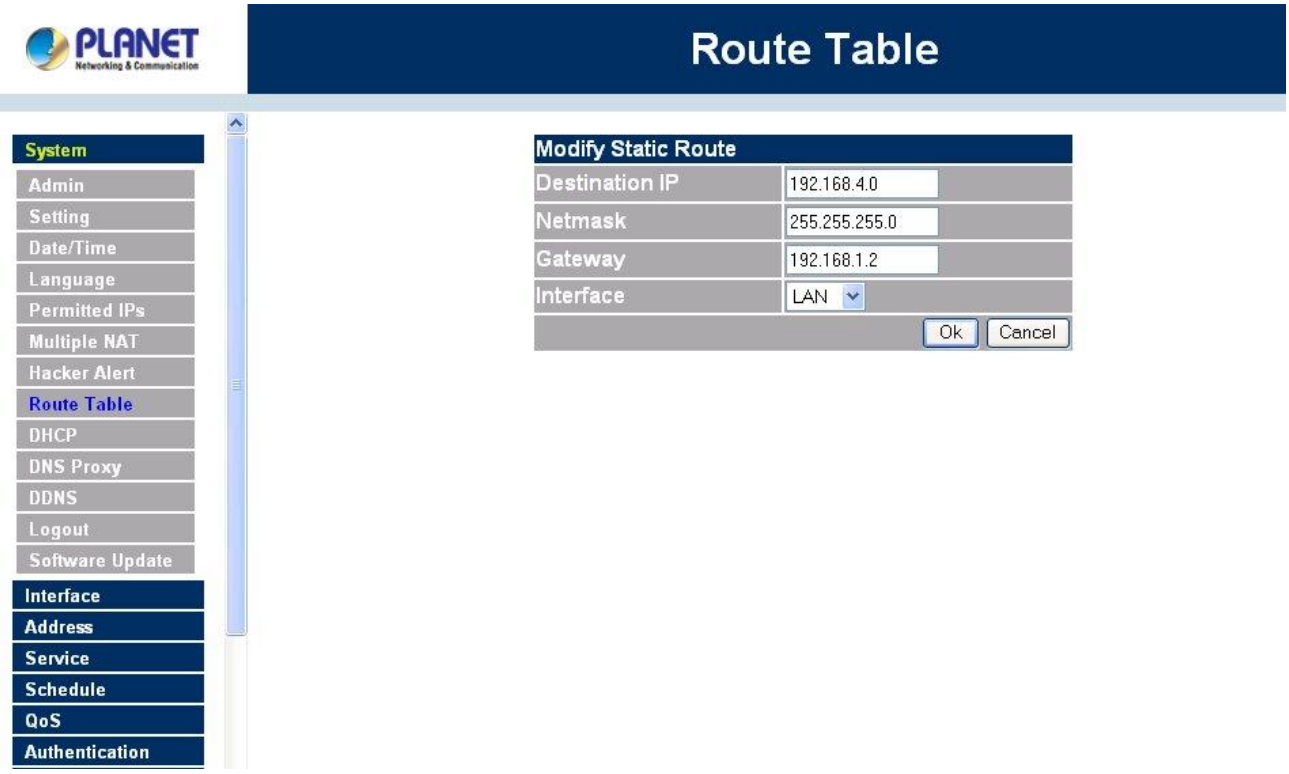
Destination IP	192.168.4.0
Netmask	255.255.255.0
Gateway	192.168.1.2
Interface	LAN

Modifying a Static Route:

Step 1. In the Route Table menu, find the route to edit and click the corresponding Modify option in the Configure field.

Step 2. In the **Modify Static Route** window, modify the necessary routing addresses.

Step 3. Click **OK** to apply changes or click **Cancel** to cancel it.

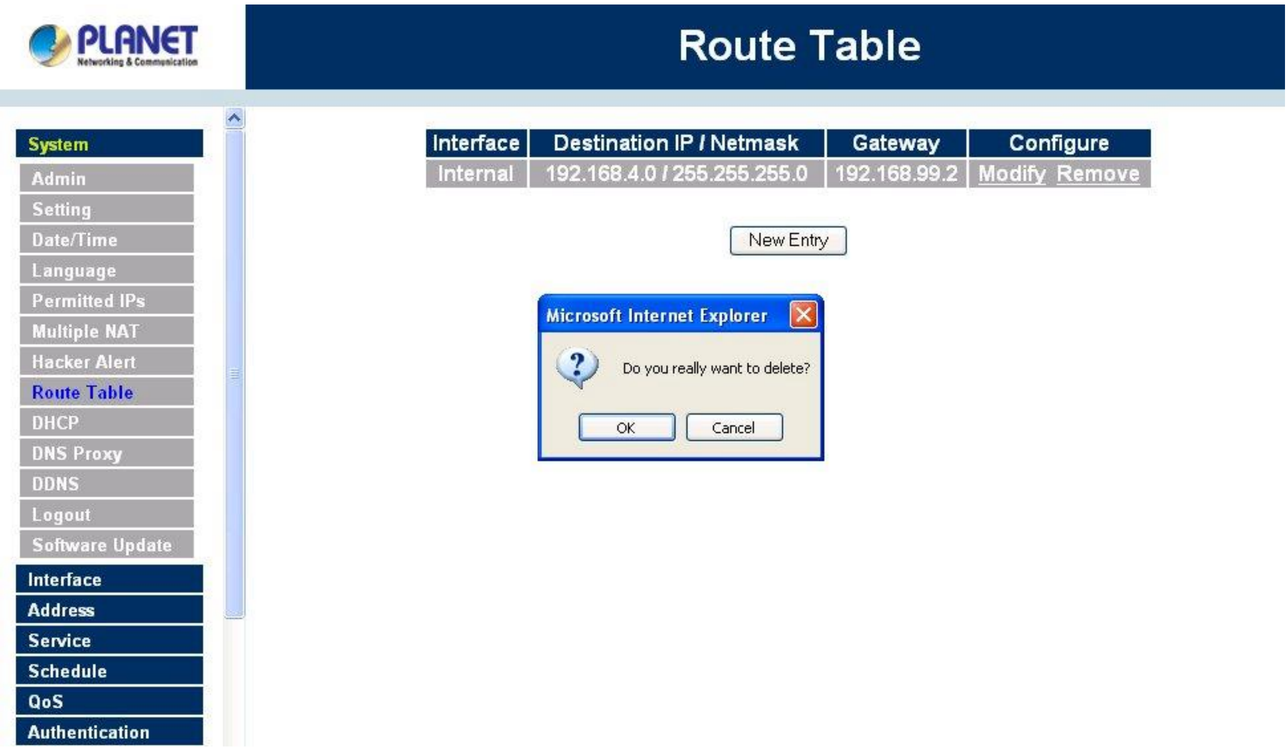


Modify Static Route	
Destination IP	192.168.4.0
Netmask	255.255.255.0
Gateway	192.168.1.2
Interface	LAN

Removing a Static Route

Step 1. In the Route Table window, find the route to remove and click the corresponding Remove option in the Configure field.

Step 2. In the Remove confirmation pop-up box, click **OK** to confirm removing or click **Cancel** to cancel it.



Interface	Destination IP / Netmask	Gateway	Configure
Internal	192.168.4.0 / 255.255.255.0	192.168.99.2	Modify Remove

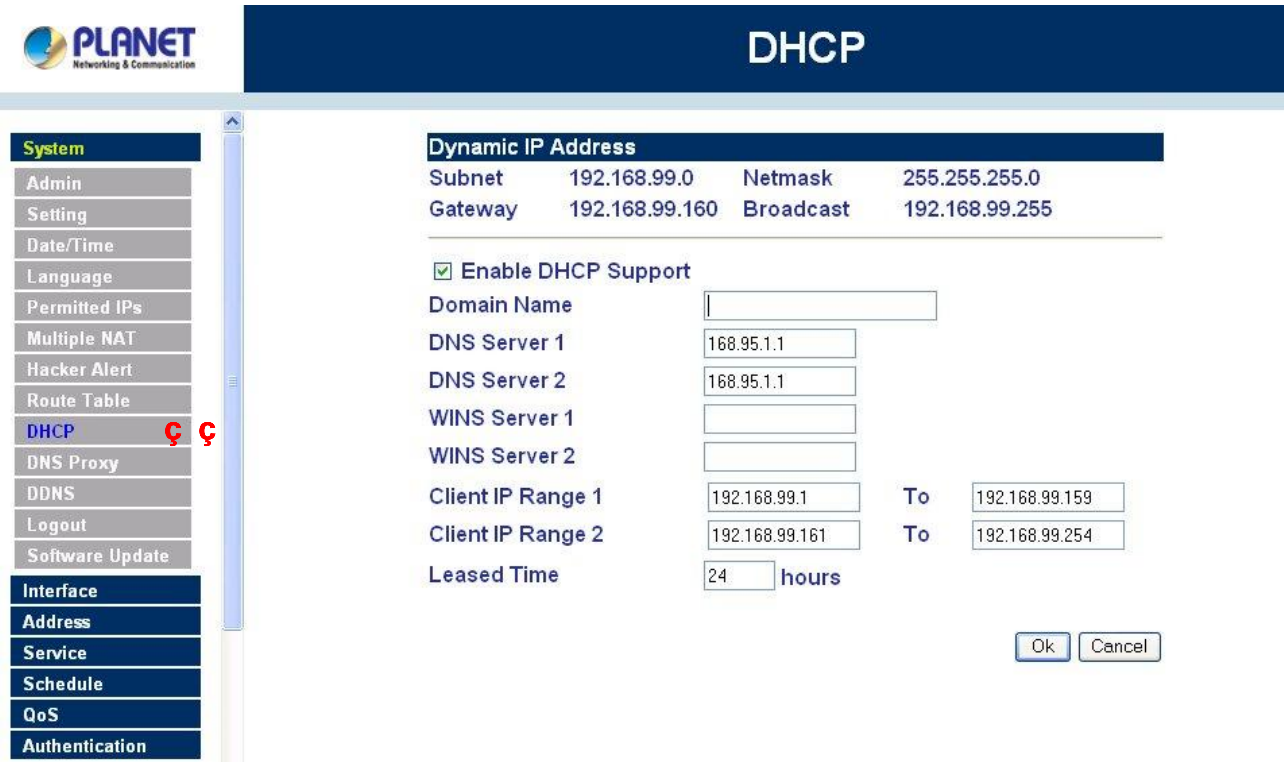
Do you really want to delete?

4.1.9 DHCP

In the section, the Administrator can configure DHCP (Dynamic Host Configuration Protocol) settings for the LAN (LAN) network.

Entering the DHCP window

Click **System** on the left hand side menu bar, then click **DHCP** below it. The DHCP window appears in which current DHCP settings are shown on the screen.



Dynamic IP Address

Subnet	192.168.99.0	Netmask	255.255.255.0
Gateway	192.168.99.160	Broadcast	192.168.99.255

☑ Enable DHCP Support

Domain Name			
DNS Server 1	168.95.1.1		
DNS Server 2	168.95.1.1		
WINS Server 1			
WINS Server 2			
Client IP Range 1	192.168.99.1	To	192.168.99.159
Client IP Range 2	192.168.99.161	To	192.168.99.254
Leased Time	24	hours	

Dynamic IP Address functions

- **Subnet:** LAN network's subnet
- **NetMask:** LAN network's netmask
- **Gateway:** LAN network's gateway IP address
- **Broadcast:** LAN network's broadcast IP address

Enabling DHCP Support

Step 1. In the Dynamic IP Address window, click **Enable DHCP Support**.

Domain Name: The Administrator may enter the name of the LAN network domain if preferred.

DNS Server 1 : Enter the distributed IP address of DNS Server 1.

DNS Server 2 : Enter the distributed IP address of DNS Server 2.

WINS Server 1 : Enter the distributed IP address of WINS Server 1.

WINS Server 2 : Enter the distributed IP address of WINS Server 2.

Client IP Address Range 1: Enter the starting and the ending IP address dynamically assigning to DHCP clients.

Client IP Address Range 2: Enter the starting and the ending IP address dynamically assigning to DHCP clients. (Optional)

Step 2. Click **OK** to enable DHCP support.

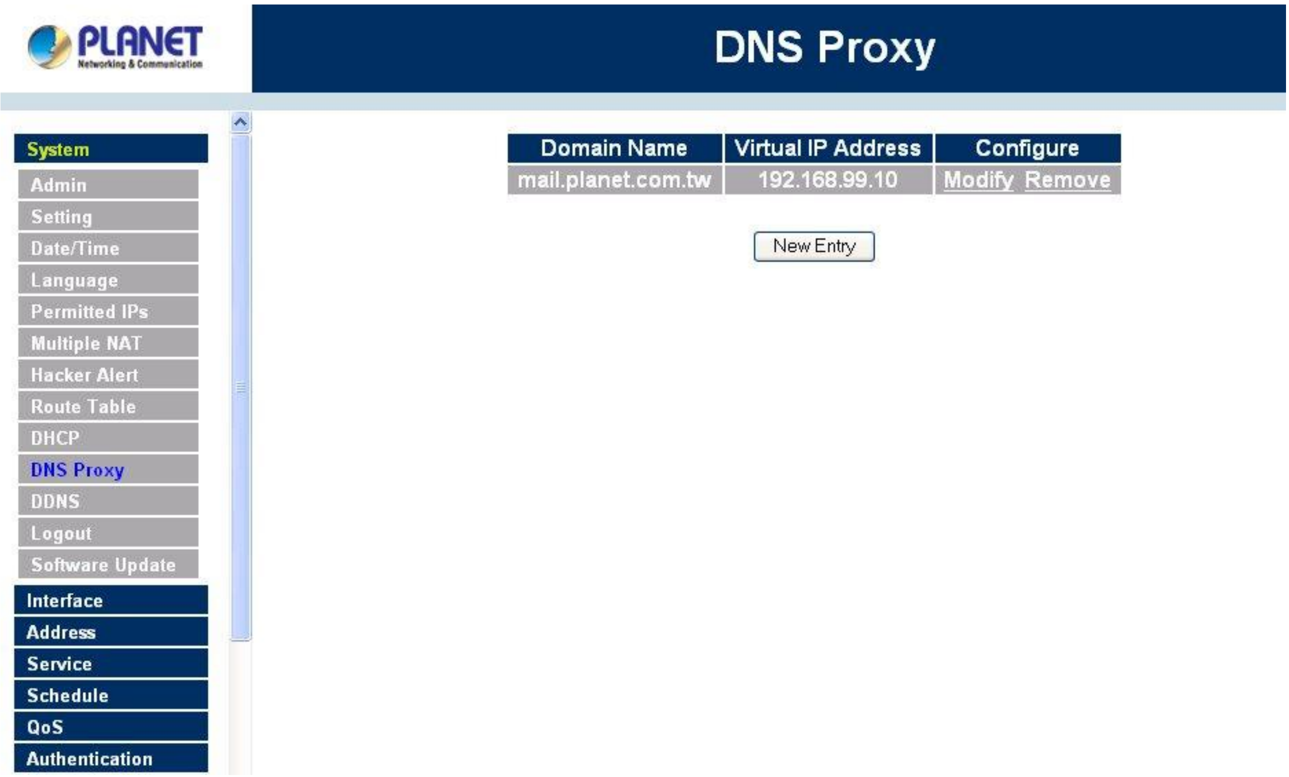
4.1.10 DNS Proxy

The Bandwidth Management Gateway's Administrator may use the DNS Proxy function to make the Bandwidth Management Gateway act as a DNS Server for the LAN and DMZ network. All DNS requests to a specific Domain Name will be routed to the Bandwidth Management Gateway's IP address. For example, let's say an organization has their mail server (i.e., mail.planet.com.tw) in the DMZ network (i.e. 192.168.10.10). The outside Internet world may access the mail server of the organization easily by its domain name, providing that the Administrator has set up Virtual Server or Mapped IP settings correctly. However, for the users in the LAN network, their WAN DNS server will assign them a public IP address for the mail server. So for the LAN network to access the mail server (mail.planet.com.tw, they would have to go out to the Internet, then come back through the Bandwidth Management Gateway to access the mail server. Essentially, the LAN network is accessing the mail server by a real public IP address, while the mail server serves their request by a NAT address and not a real one.

This odd situation occurs when there are servers in the DMZ network and they are bound to real IP addresses. To avoid this, set up DNS Proxy so all the LAN network computers will use the Bandwidth Management Gateway as a DNS server, which acts as the DNS Proxy.

If you want to use the DNS Proxy function of the device, the end user's main DNS server IP address should be the same IP Address as the device.

Click on **System** in the menu bar, then click on **DNS Proxy** below it. The DNS Proxy window will appear.



Domain Name	Virtual IP Address	Configure
mail.planet.com.tw	192.168.99.10	Modify Remove

Below is the information needed for setting up the **DNS Proxy**:

- **Domain Name:** The domain name of the server
- **Virtual IP Address:** The virtual IP address respective to DNS Proxy
- **Configure:** modify or remove each DNS Proxy policy

Adding a new DNS Proxy

Step 1: Click on the **New Entry** button and the **Add New DNS Proxy** window will appear.

Step 2: Fill in the appropriate settings for the domain name and virtual IP address.

Step 3: Click **OK** to save the policy or **Cancel** to cancel.

Modifying a DNS Proxy

Step 1: In the DNS Proxy window, find the policy to be modified and click the corresponding **Modify** option in the **Configure** field.

Step 2: Make the necessary changes needed.

Step 3: Click **OK** to save changes or click on **Cancel** to cancel modifications.

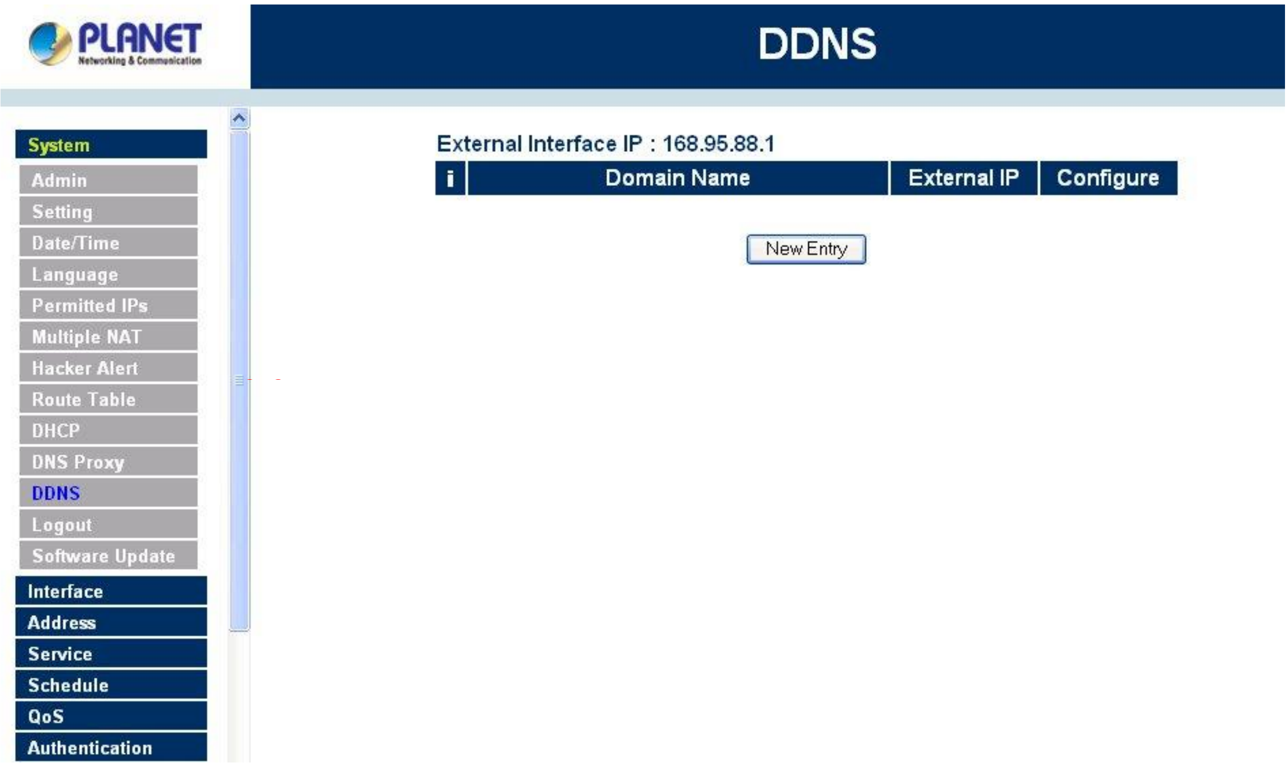
Removing a DNS Proxy

Step 1: In the **DNS Proxy** window, find the policy to be removed and click the corresponding **Remove** option in the **Configure** field.

Step 2: A confirmation pop-up box will appear, click **OK** to remove the DNS Proxy or click **Cancel**.

4.1.11 DDNS

The **Dynamic DNS** (require Dynamic DNS Service) allows you to alias a dynamic IP address to a static hostname, allowing your device to be more easily accessed by specific name. When this function is enabled, the IP address in Dynamic DNS Server will be automatically updated with the new IP address provided by ISP.



External Interface IP : 168.95.88.1

i	Domain Name	External IP	Configure

Click **DDNS** in the **System** menu to enter Dynamic DNS window.

The nouns in Dynamic DNS window:

!: Update Status, Connecting; ✓Update succeed; ✗Update fail; ⚠Unidentified error.

Domain name: Enter the password provided by ISP.

WAN IP Address: IP Address of the WAN port.

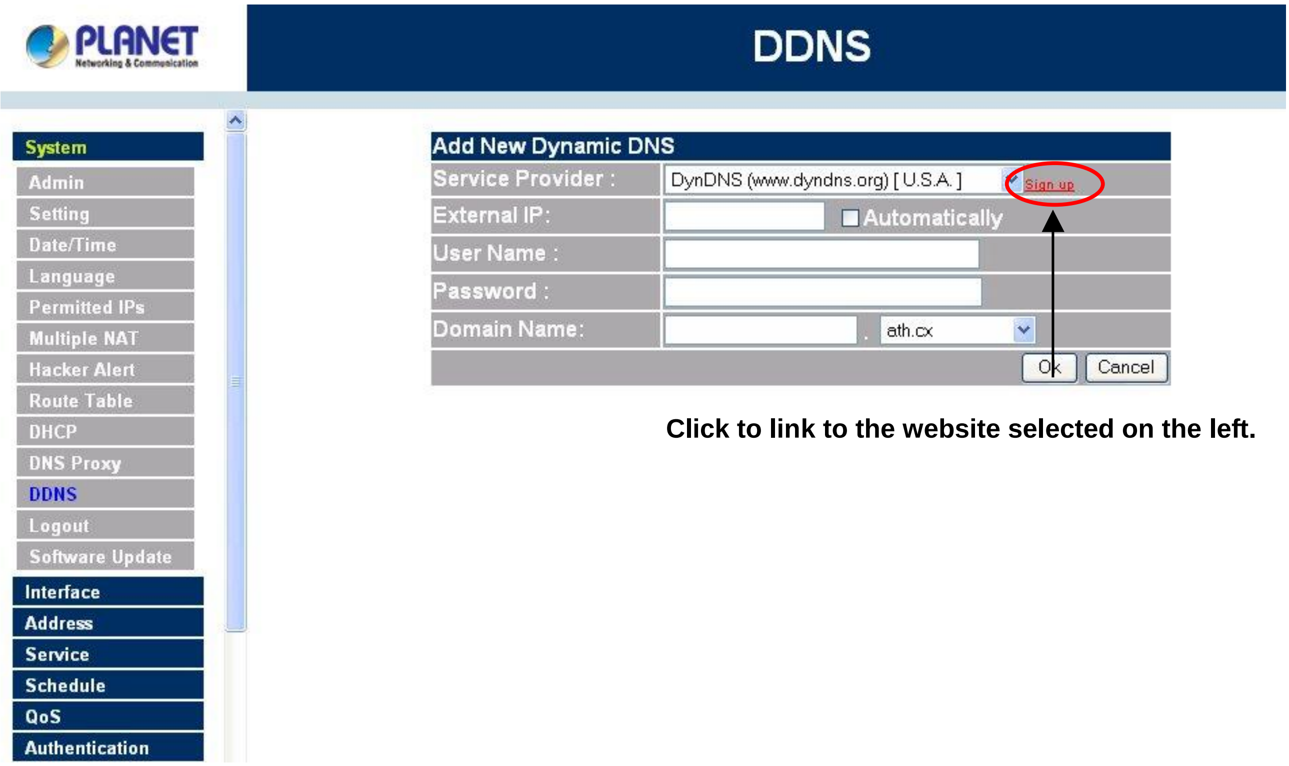
Modify: Modify dynamic DNS settings. Click **Modify** to change the DNS parameters; click Delete to delete the settings.

How to use dynamic DNS:

The Bandwidth Management Gateway provides many service providers, users have to register prior to use this function. For the usage regulations, see the providers' websites.

How to register:

Firstly, Click **Dynamic DNS** in the **System** menu to enter Dynamic DNS window, then click **Add** button，on the right side of the service providers, click **Register**, the service providers' website will appear, please refer to the website for the way of registration.



Add New Dynamic DNS

Service Provider :	DynDNS (www.dyndns.org) [U.S.A.] Sign up
External IP:	□ Automatically
User Name :	
Password :	
Domain Name:	. ath.cx

Click to link to the website selected on the left.

Add Dynamic DNS settings

Step 1. Click **Add** button.

Step 2. Click the information in the column of the new window.

Service providers: Select service providers.

Register: to the service providers' website.

WAN IP Address: IP Address of the WAN port.

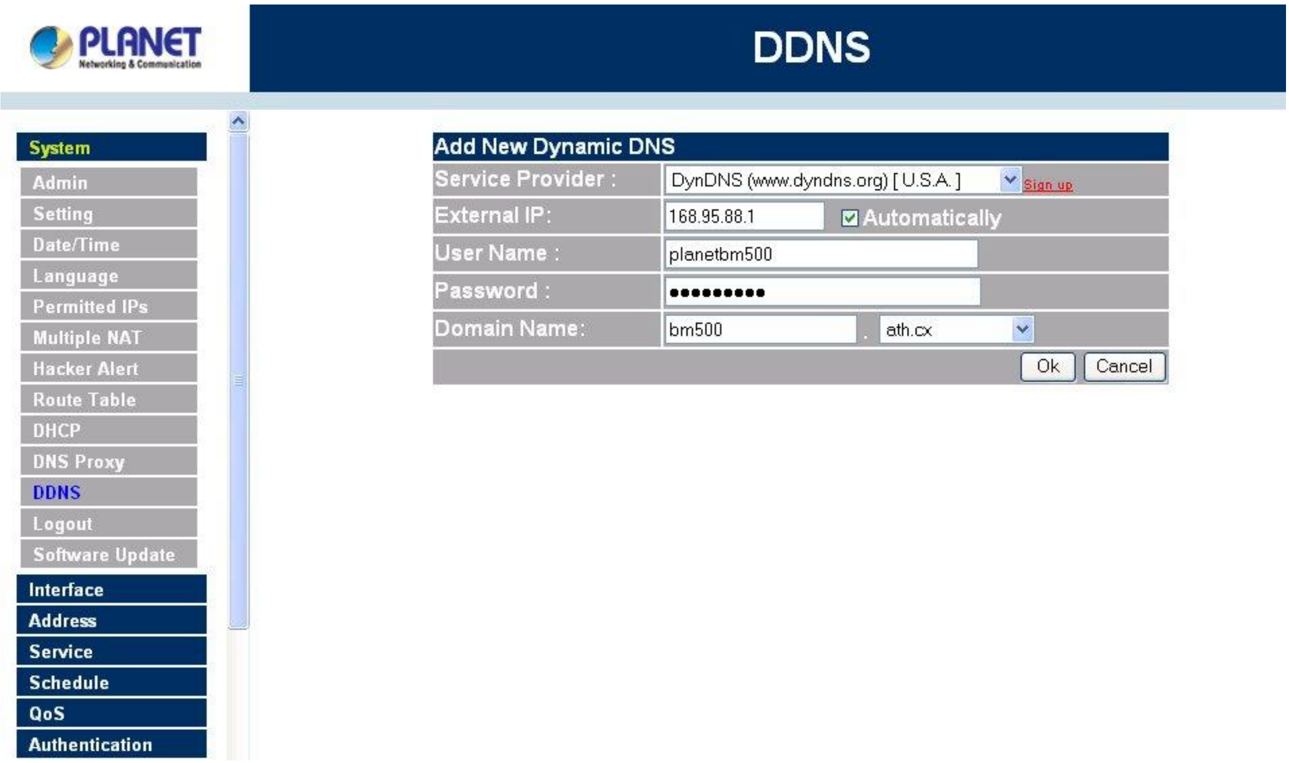
¨ **automatically fill in the WAN IP**: Check to automatically fill in the WAN IP. ◦

User Name: Enter the registered user name.

Password: Enter the password provided by ISP(Internet Service Provider).

Domain name: Your host domain name provided by ISP.

Click **OK** to add dynamic DNS or click **Cancel** to discard changes.



Add New Dynamic DNS

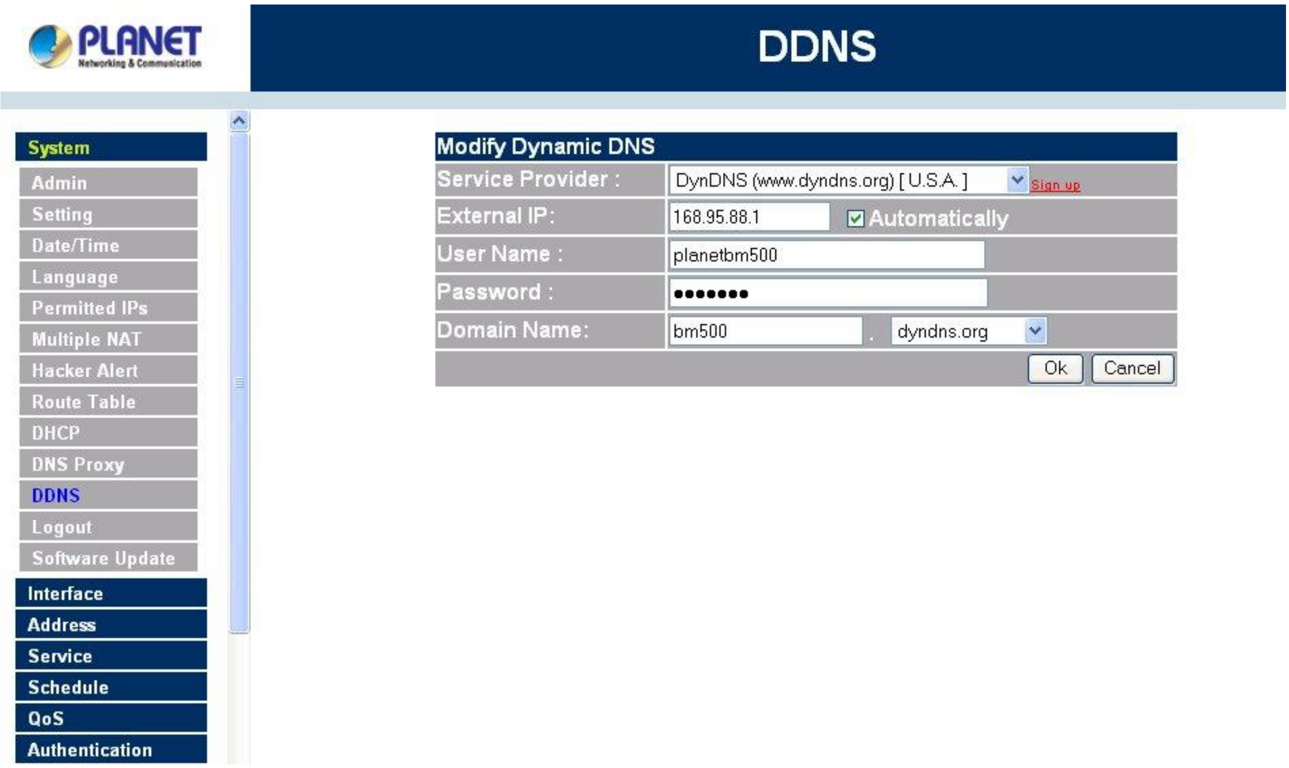
Service Provider :	DynDNS (www.dyndns.org) [U.S.A.] Sign up
External IP:	168.95.88.1 ☑ Automatically
User Name :	planetbm500
Password :	●●●●●●●●●●
Domain Name:	bm500 . ath.cx

Modify dynamic DNS

Step 1. Find the item you want to change and click **Modify**.

Step 2. Enter the new information in the Modify Dynamic DNS window.

Click **OK** to change the settings or click **Cancel** to discard changes. ◦



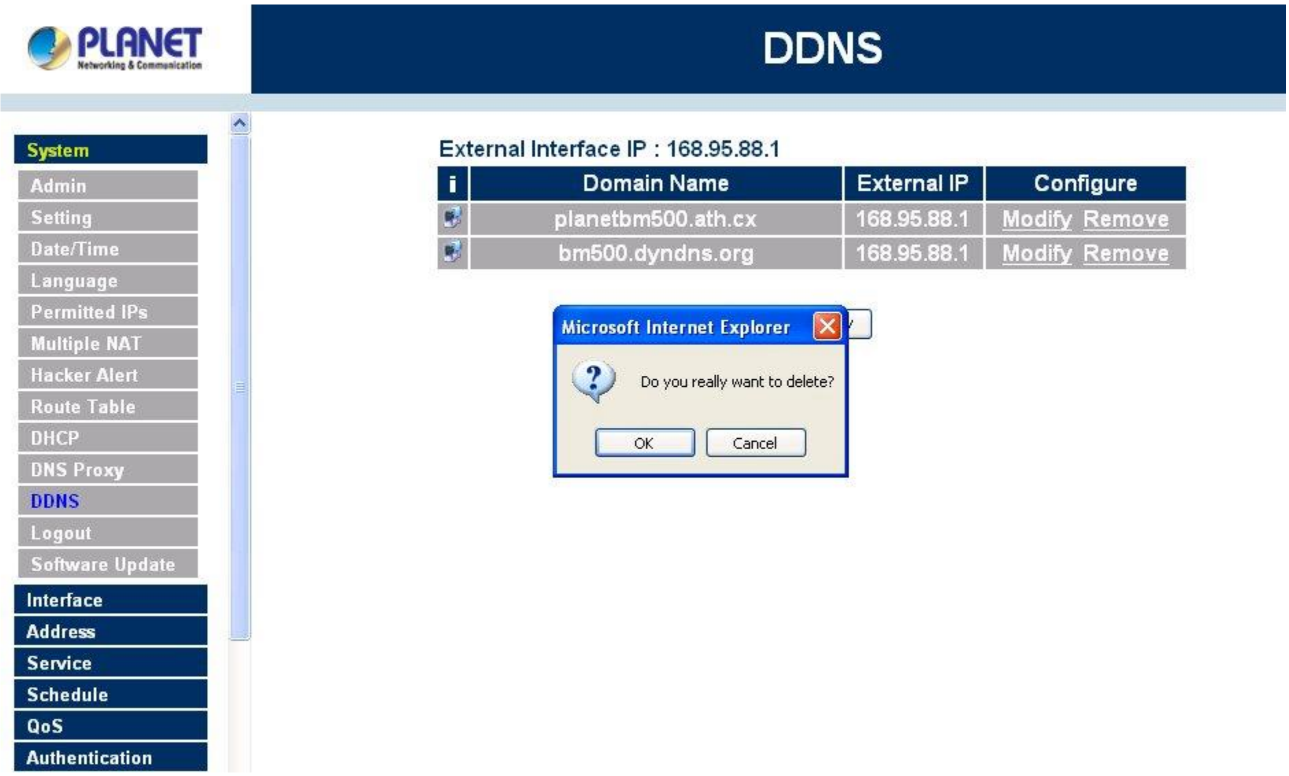
Modify Dynamic DNS

Service Provider :	DynDNS (www.dyndns.org) [U.S.A.]
External IP:	168.95.88.1 ☑ Automatically
User Name :	planetbm500
Password :	●●●●●●●
Domain Name:	bm500 . dyndns.org

Remove Dynamic DNS

Step 1. Find the item you want to change and click **Remove**.

Step 2. A confirmation pop-up box will appear, click OK to delete the settings or click Cancel to discard changes.



External Interface IP : 168.95.88.1

i	Domain Name	External IP	Configure
	planetbm500.ath.cx	168.95.88.1	Modify Remove
	bm500.dyndns.org	168.95.88.1	Modify Remove

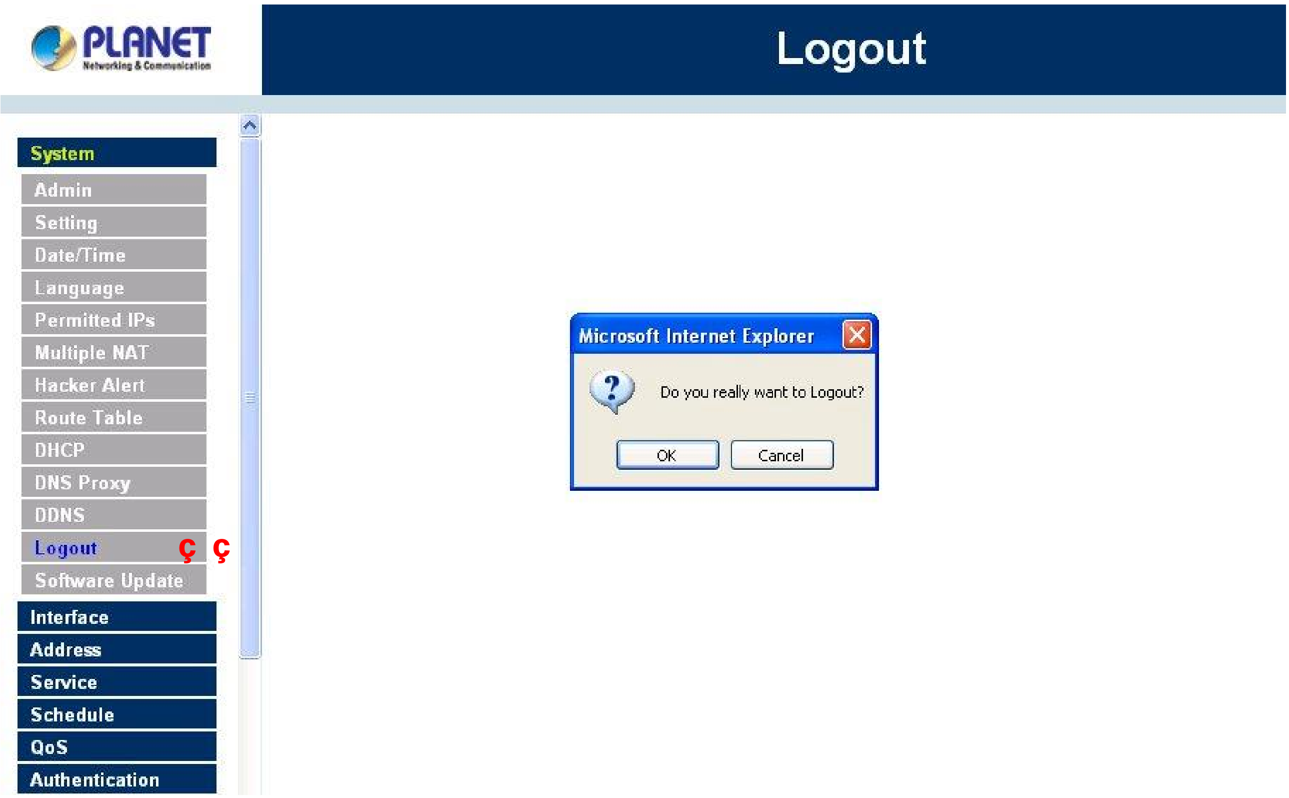
Do you really want to delete?

4.1.12 Logout

Step 1. Select this option to the device's **Logout** the Bandwidth Management Gateway. This function protects your system while you are away.

Step 2. Click Logout the Bandwidth Management Gateway.

Step 3. Click **OK** to logout or click **Cancel** to discard the change.



Do you really want to Logout?

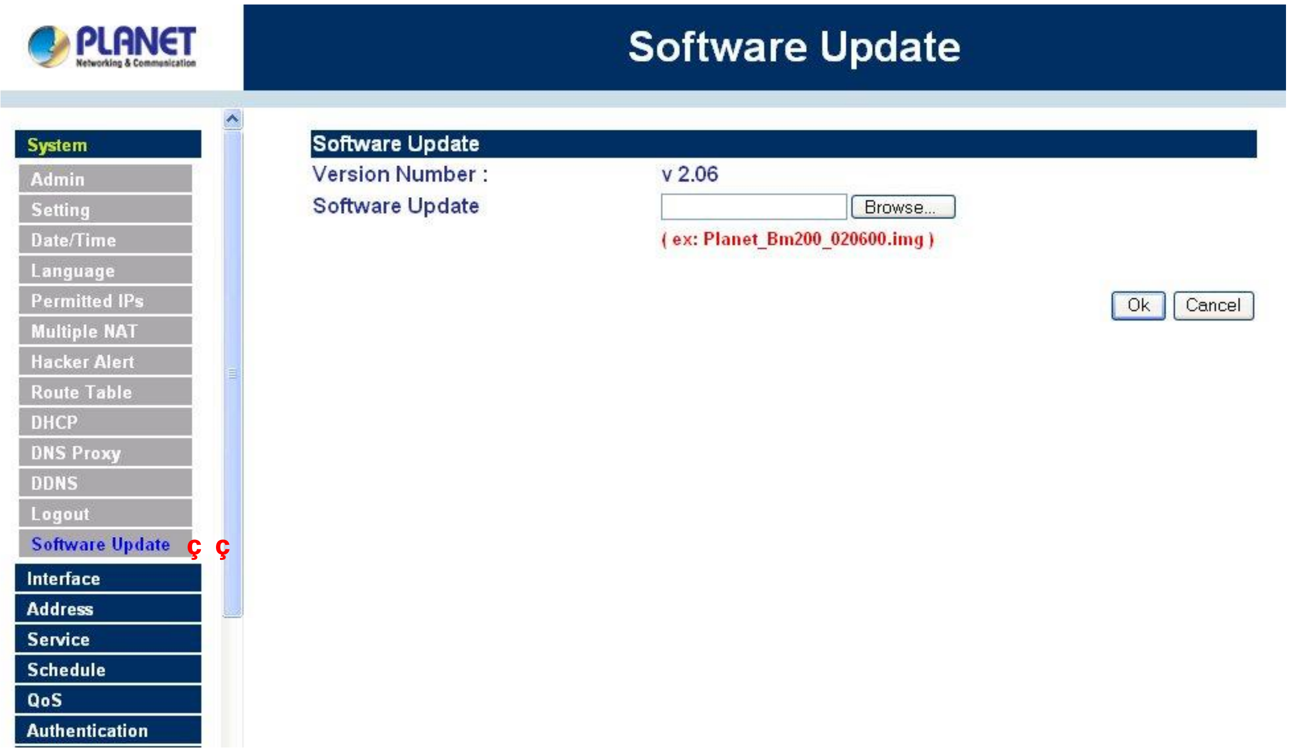
4.1.13 Software Update

Under **Software Update**, the admin may update the device’s software with a newer software.

You may acquire the current version number of software in **Version Number**. Administrators may visit distributor’s web site to download the latest version and save it in server’s hard disc.

Step 1. Click **Browse** to select the latest version of Software.

Step 2. Click **OK** to update software.



Software Update

Version Number : v 2.06

Software Update

(ex: Planet_Bm200_020600.img)

NOTE: It takes three minutes to update the software. The system will restart automatically after updating the software.

4.2 Interface

In this section, the **Administrator** can set up the IP addresses for the office network. The Administrator may configure the IP addresses of the Internal (LAN) network, and the External (WAN) network. The netmask and gateway IP addresses are also configured in this section.

Entering the Interface menu:

Step 1. Click on **Configuration** in the left menu bar.

Step 2. Then click on **Interface** below it. The current settings of the interface addresses will appear on the screen.

LAN Interface

Using the Internal Interface, the Administrator sets up the Internal (LAN) network. The Internal network will use a private IP scheme. The private IP network will not be routable on the Internet.

Transparent Mode: All the IP internetwork uses real IP.

NAT Mode: All the IP Internetwork uses NAT (Network Address Translation), which allows the private IP internetworks use non-registered IP addresses to connect to the Internet.

IP Address: The private IP address of the Firewall's internal network is the IP address of the Internal (LAN) port of the Bandwidth Management Gateway. The default IP address is 192.168.1.1.

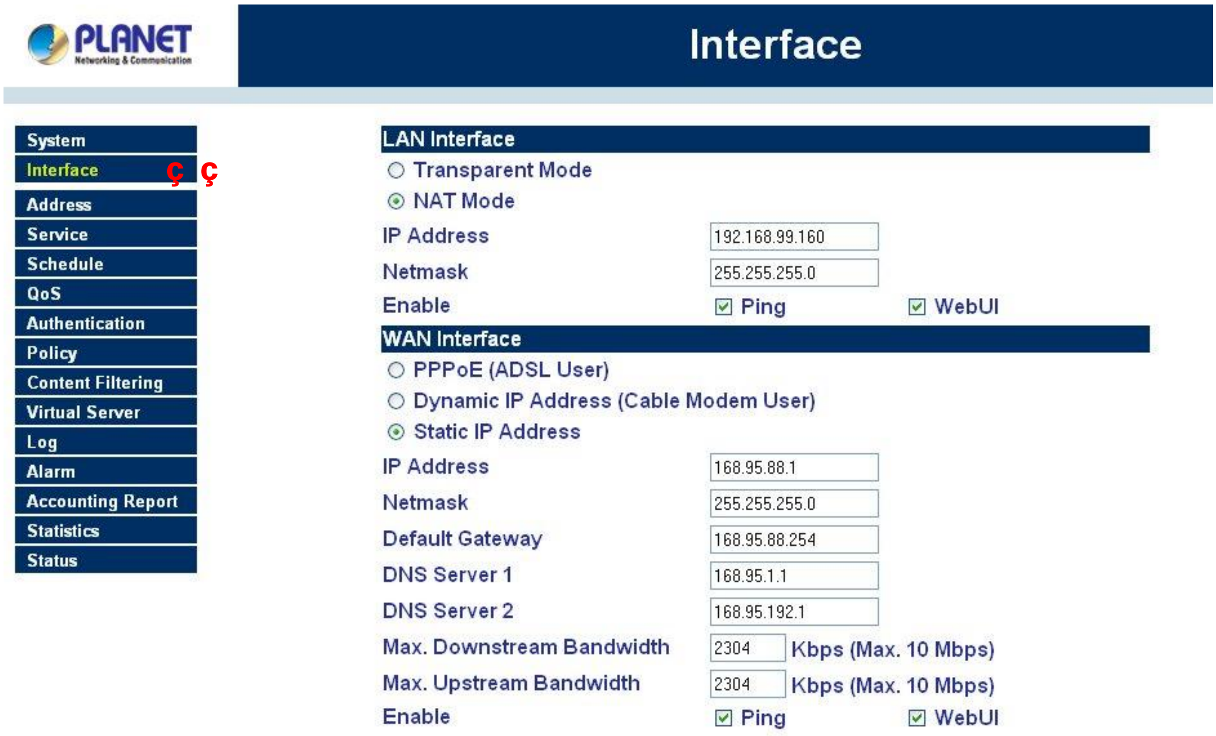
NOTE: The IP Address of Internal Interface and the DMZ Interface is a private IP address only.

If the new Internal IP Address is not 192.168.1.1, the **Administrator** needs to set the IP Address on the computer to be on the same subnet as the Firewall and restart the System to make the new IP address effective. For example, if the Firewall's new Internal IP Address is 172.16.0.1, then enter the new Internal IP Address 172.16.0.1 in the URL field of browser to connect to Firewall.

NetMask: This is the netmask of the internal network. The default netmask of the Bandwidth Management Gateway is 255.255.255.0.

Ping: Select this to allow the internal network to ping the IP Address of the Firewall. If set to enable, the Bandwidth Management Gateway will respond to ping packets from the internal network.

WebUI: Select this to allow the Bandwidth Management Gateway WEBUI to be accessed from the Internal (LAN) network.



LAN Interface

○ Transparent Mode

● NAT Mode

IP Address	192.168.99.160	
Netmask	255.255.255.0	
Enable	☑ Ping	☑ WebUI

WAN Interface

○ PPPoE (ADSL User)

○ Dynamic IP Address (Cable Modem User)

● Static IP Address

IP Address	168.95.88.1	
Netmask	255.255.255.0	
Default Gateway	168.95.88.254	
DNS Server 1	168.95.1.1	
DNS Server 2	168.95.192.1	
Max. Downstream Bandwidth	2304 Kbps (Max. 10 Mbps)	
Max. Upstream Bandwidth	2304 Kbps (Max. 10 Mbps)	
Enable	☑ Ping	☑ WebUI

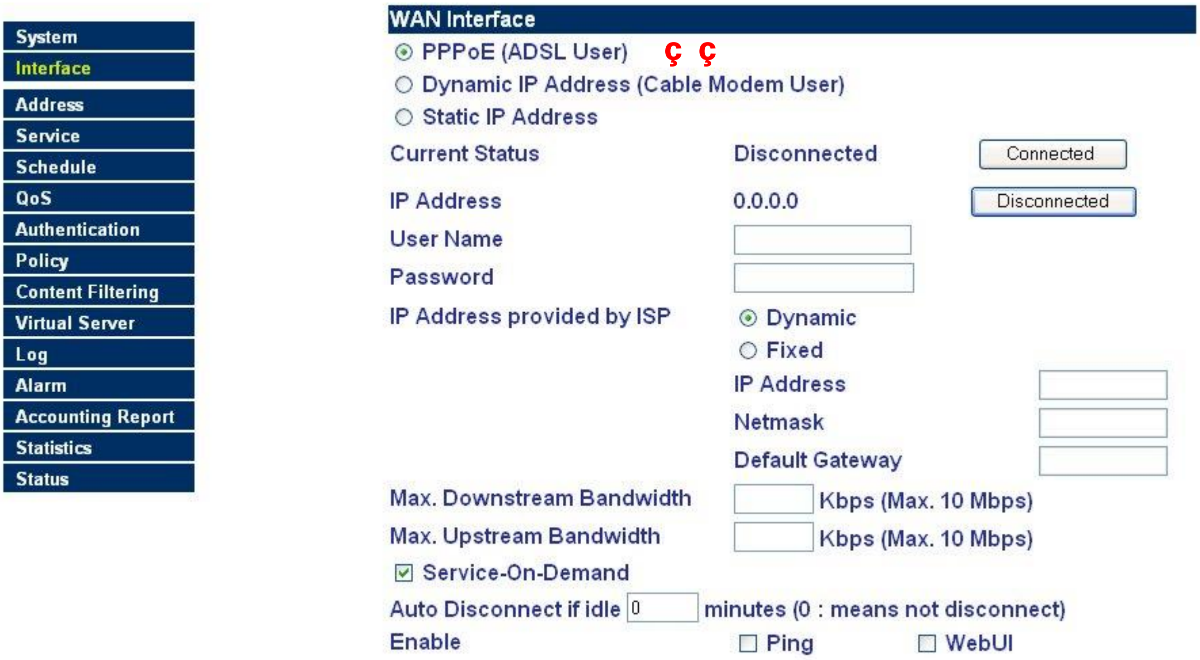
ADSL user Interface setting

PPPoE（External Interface）

Step 1. Select **Interface** function in the menu bar.

Step 2. Check the item **PPPoE (ADSL User)** below **WAN Interface**.

Step 3. Enter each parameter of WAN Interface.



WAN Interface

● PPPoE (ADSL User) ç ç

○ Dynamic IP Address (Cable Modem User)

○ Static IP Address

Current Status	Disconnected	
IP Address	0.0.0.0	
User Name		
Password		
IP Address provided by ISP	● Dynamic	
	○ Fixed	
	IP Address	
	Netmask	
	Default Gateway	
Max. Downstream Bandwidth	Kbps (Max. 10 Mbps)	
Max. Upstream Bandwidth	Kbps (Max. 10 Mbps)	

☑ Service-On-Demand

Auto Disconnect if idle 0 minutes (0 : means not disconnect)

Enable	□ Ping	□ WebUI

For PPPoE (ADSL User): This option is for PPPoE users who are required to enter a username and password in order to connect, such as ADSL users.

Current Status: Displays the current line status of the PPPoE connection.

IP Address: Displays the IP Address of the PPPoE connection

Username: Enter the PPPoE username provided by the ISP.

Password: Enter the PPPoE password provided by the ISP.

IP Address provided by ISP:

Dynamic: Select this if the IP address is automatically assigned by the ISP.

Fixed: Select this if you were given a static IP address. Enter the IP address that is given to you by your ISP.

Upload/Download Bandwidth: The bandwidth your ISP provided. (Maximum bandwidth for Upload/Download Bandwidth is 10Mbps)

Service-On-Demand:

Auto Disconnect: The PPPoE connection will automatically disconnect after a length of idle time (no activities). Enter in the amount of idle minutes before disconnection. Enter '0' if you do not want the PPPoE connection to disconnect at all.

Ping: Select this to allow the external network to ping the IP Address of the Firewall. This will allow people from the Internet to be able to ping the Firewall. If set to enable, the Bandwidth Management Gateway will respond to echo request packets from the external network.

WebUI: Select this to allow the Bandwidth Management Gateway WEBUI to be accessed from the External (WAN) network. This will allow the WebUI to be configured from a user on the Internet. Keep in mind that the Bandwidth Management Gateway always requires a username and password to enter the WebUI.

After completing the setting, click **OK**.

For Dynamic IP Address (Cable Modem User): This option is for users who are automatically assigned an IP address by their ISP, such as cable modem users. The following fields apply:

IP Address: The dynamic IP address obtained by the Firewall from the ISP will be displayed here. This is the IP address of the External (WAN) port of the Bandwidth Management Gateway.

MAC Address: This is the MAC Address of the Bandwidth Management Gateway.

User Name (Some ISPs may require): This is provided by your ISP.

Hostname: This will be the name assign to the Bandwidth Management Gateway. Some cable modem ISP assign a specific hostname in order to connect to their network. Please enter the hostname here. If not required by your ISP, you do not have to enter a hostname.

Max. Upstream/Downstream Bandwidth: The bandwidth provided by ISP. (Upstream/Downstream can be up to 10Mbps)

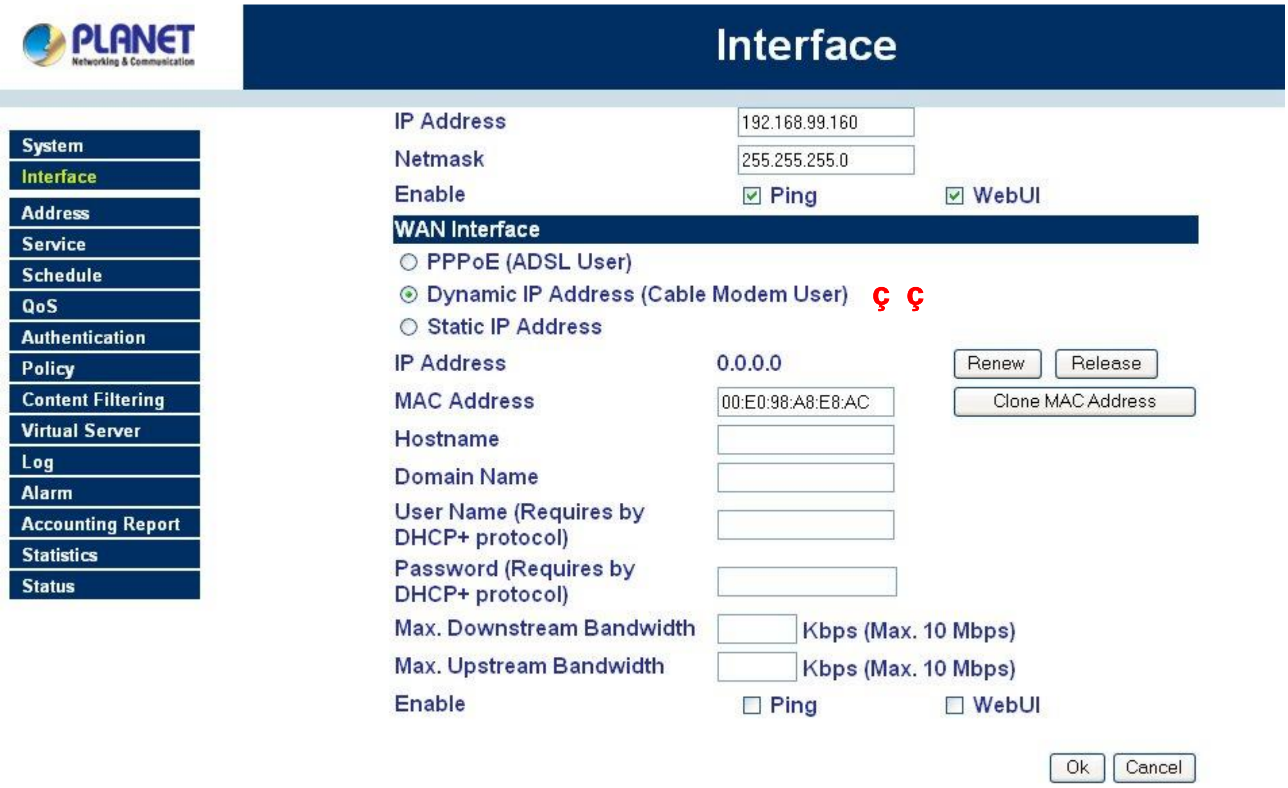
Renew: Requests for receiving the new WAN IP address.

Release: Requests for releasing the obtained WAN IP address.

Ping: Select this to allow the external network to ping the IP Address of the Firewall. This will allow people from the Internet to be able to ping the Firewall. If set to enable, the Bandwidth Management Gateway will respond to echo request packets from the external network.

WebUI: Select this to allow the Bandwidth Management Gateway WEBUI to be accessed from the External (WAN) network. This will allow the WebUI to be configured from a user on the Internet. Keep in mind that the Bandwidth Management Gateway always requires a username and password to enter the WebUI.

After setting all of the parameters, click **OK** button.



IP Address 192.168.99.160
Netmask 255.255.255.0
Enable ☑ Ping ☑ WebUI

WAN Interface
○ PPPoE (ADSL User)
● Dynamic IP Address (Cable Modem User) ç ç
○ Static IP Address

IP Address 0.0.0.0
MAC Address 00:E0:98:A8:E8:AC
Hostname
Domain Name
User Name (Requires by DHCP+ protocol)
Password (Requires by DHCP+ protocol)
Max. Downstream Bandwidth Kbps (Max. 10 Mbps)
Max. Upstream Bandwidth Kbps (Max. 10 Mbps)
Enable ☐ Ping ☐ WebUI

For Static IP Address: This option is for users who are assigned a static IP Address from their ISP. Your ISP will provide all the information needed for this section such as IP Address, Netmask, Gateway, and DNS. Use this option if you have more than one public IP Address assigned to you.

IP Address: Enter the static IP address assigned to you by your ISP. This will be the public IP address of the External (WAN) port of the Bandwidth Management Gateway.

Netmask: This will be the Netmask of the external (WAN) network. (i.e. 255.255.255.0)

Default Gateway: This will be the Gateway IP address.

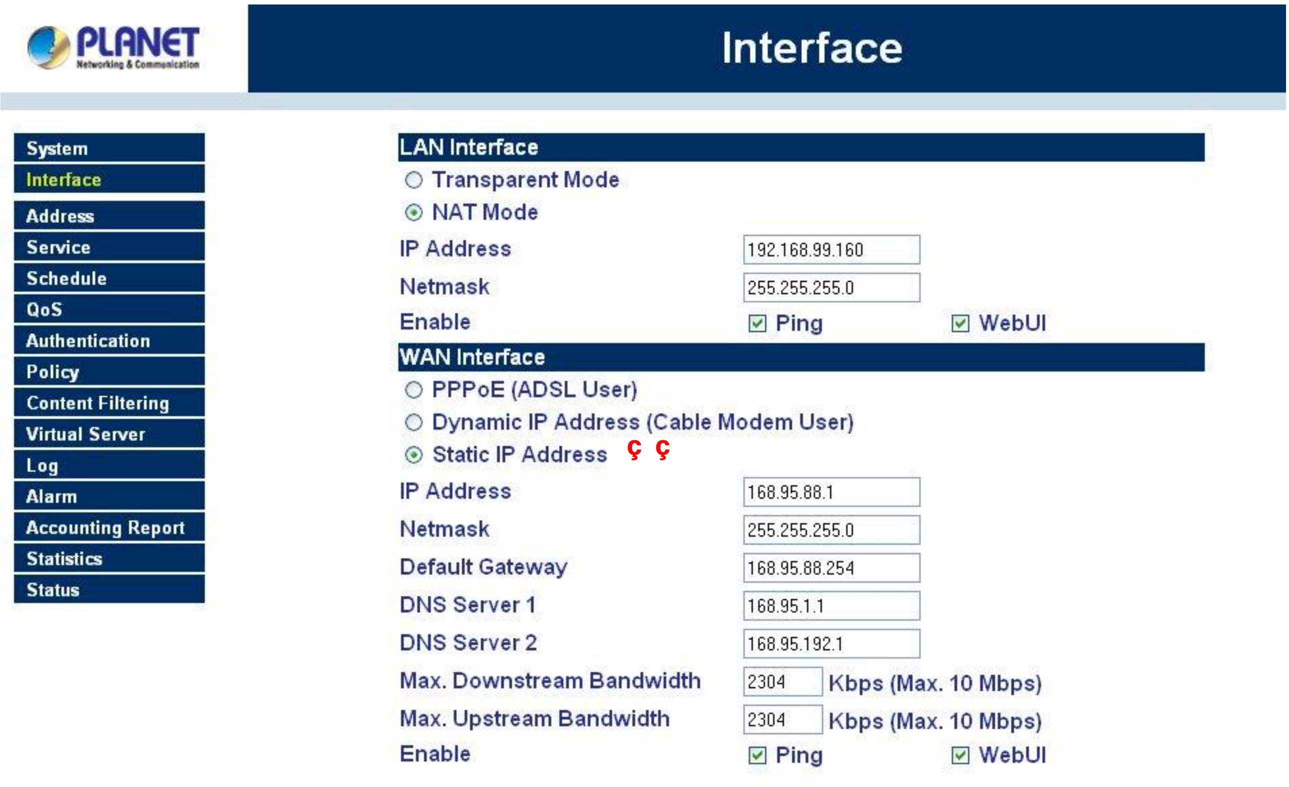
DNS Server 1/2: Enter the DNS 1/2 server provided by ISP. (See *Note.)*

Max. Upstream Bandwidth / Max. Downstream Bandwidth: The bandwidth provided by ISP. (Upstream/Downstream can be up to 10Mbps)

Ping: Select this to allow the external network to ping the IP Address of the Firewall. This will allow people from the Internet to be able to ping the Firewall. If set to enable, the Bandwidth Management Gateway will respond to echo request packets from the external network.

WebUI: Select this to allow the Bandwidth Management Gateway WEBUI to be accessed from the External (WAN) network. This will allow the WebUI to be configured from a user on the Internet. Keep in mind that the Bandwidth Management Gateway always requires a username and password to enter the WebUI.

After setting all of the interface address, click **OK** button.



LAN Interface

○ Transparent Mode

● NAT Mode

IP Address	192.168.99.160	
Netmask	255.255.255.0	
Enable	☑ Ping	☑ WebUI

WAN Interface

○ PPPoE (ADSL User)

○ Dynamic IP Address (Cable Modem User)

● Static IP Address ç ç

IP Address	168.95.88.1	
Netmask	255.255.255.0	
Default Gateway	168.95.88.254	
DNS Server 1	168.95.1.1	
DNS Server 2	168.95.192.1	
Max. Downstream Bandwidth	2304	Kbps (Max. 10 Mbps)
Max. Upstream Bandwidth	2304	Kbps (Max. 10 Mbps)
Enable	☑ Ping	☑ WebUI

If you want to set up DNS Server, you have to go to **Virtual Server** function to map the real IP address from DNS server to the corresponding private IP address of internal DNS server. Enter the mapped IP address of internal server in DNS server address field.

4.3 Address

The Bandwidth Management Gateway allows the Administrator to set addresses of the LAN network, LAN network group, WAN network, WAN group.   These settings are to be used for policy editing.

What is the Address Table?

An IP address in the Address Table can be an address of a computer or a sub network. The Administrator can assign an easily recognized name to an IP address. Based on the network it belongs to, an IP address can be an LAN IP address, WAN IP address. If the Administrator needs to create a control policy for packets of different IP addresses, he can first add a new group in the LAN **Network Group** or the **WAN Network Group** and assign those IP addresses into the newly created group.   Using group addresses can greatly simplify the process of building control policies.

With easily recognized names of IP addresses and names of address groups shown in the address table, the Administrator can use these names as the source address or destination address of control policies. The address table should be built before creating control policies, so that the Administrator can pick the names of correct IP addresses from the address table when setting up control policies.

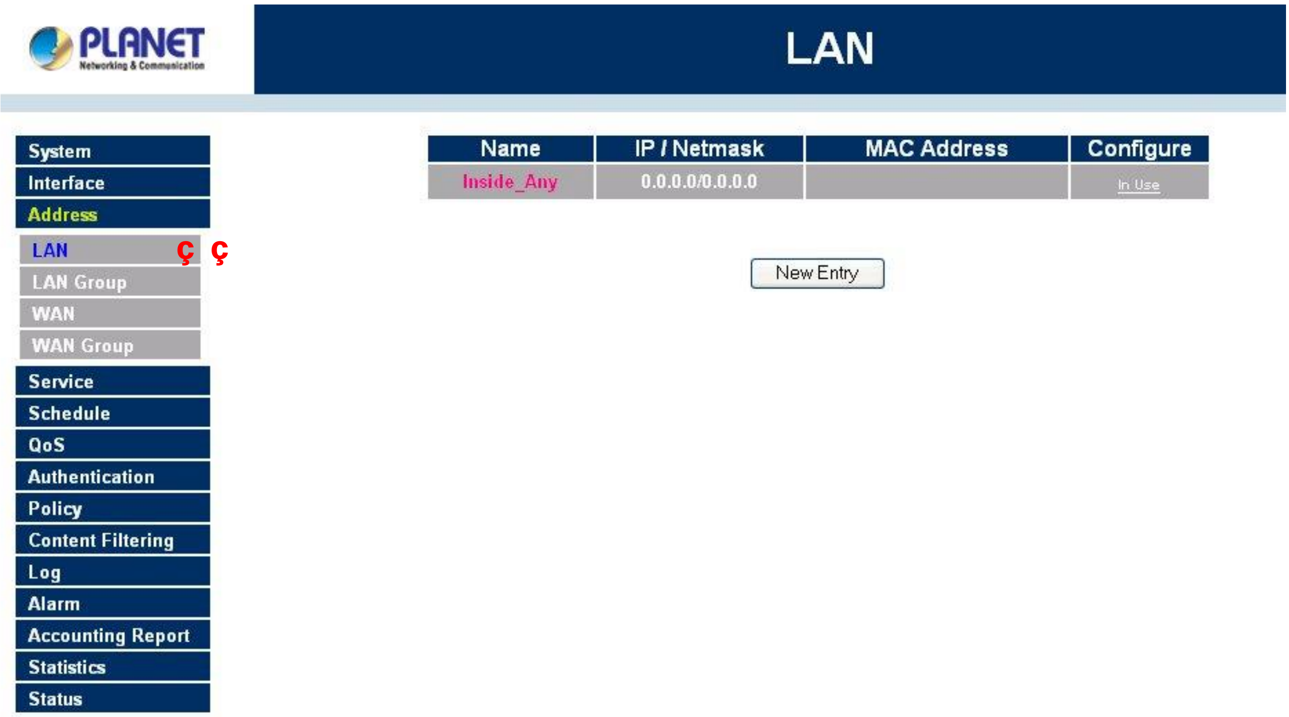
How to use Address Table

With easily recognized names of IP addresses and names of address groups shown in the address table, the Administrator can use these names as the source address or destination address of control policies. The address table should be built before creating control policies, so that the Administrator can pick the names of correct IP addresses from the address table when setting up control policies.

4.3.1 LAN

Entering the LAN window

Step 1. Click LAN under the **Address** menu to enter the LAN window. The current setting information such as the name of the LAN network, IP and Netmask addresses will show on the screen.



Name	IP / Netmask	MAC Address	Configure
Inside_Any	0.0.0.0/0.0.0.0		In Use

Definition

Name: Name of LAN network address.

IP: IP address of LAN network

Netmask: Netmask of LAN network.

MAC Address: MAC address corresponded with LAN IP address.

Configure: You can configure the settings in LAN network. Click **Modify** to change the parameters in LAN network. Click **Remove** to delete the settings.

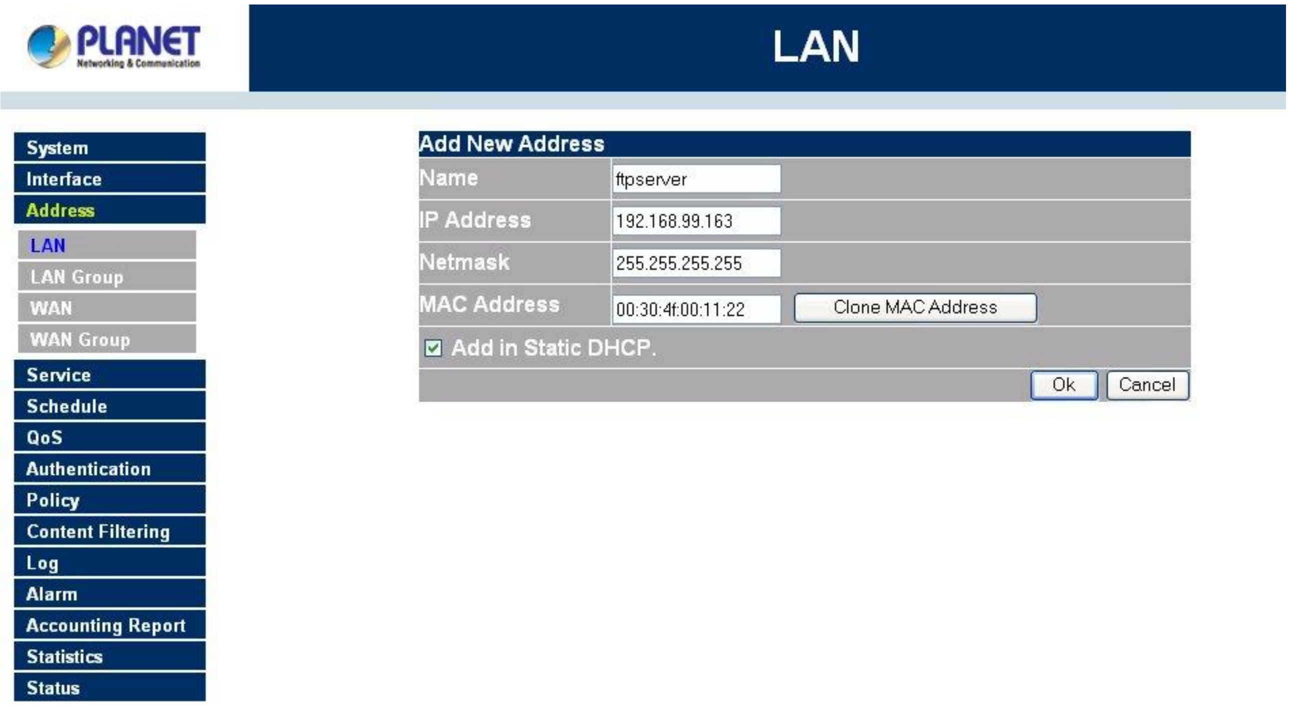
In the **LAN** window, if one of the members has been added to **Policy** or **LAN Group**, the **Configure** column will show the message – **In Use**. In this case, you are not allowed to modify or remove the setting.

Adding a new LAN Address

Step 1. In the LAN window**,** click the **New Entry** button.

Step 2. In the **Add New Address** window, enter the settings of a new LAN network address.

Step 3. Click **OK** to add the specified LAN network or click **Cancel** to cancel the changes.



Add New Address

Name	ftpserver
IP Address	192.168.99.163
Netmask	255.255.255.255
MAC Address	00:30:4f:00:11:22

☑ Add in Static DHCP.

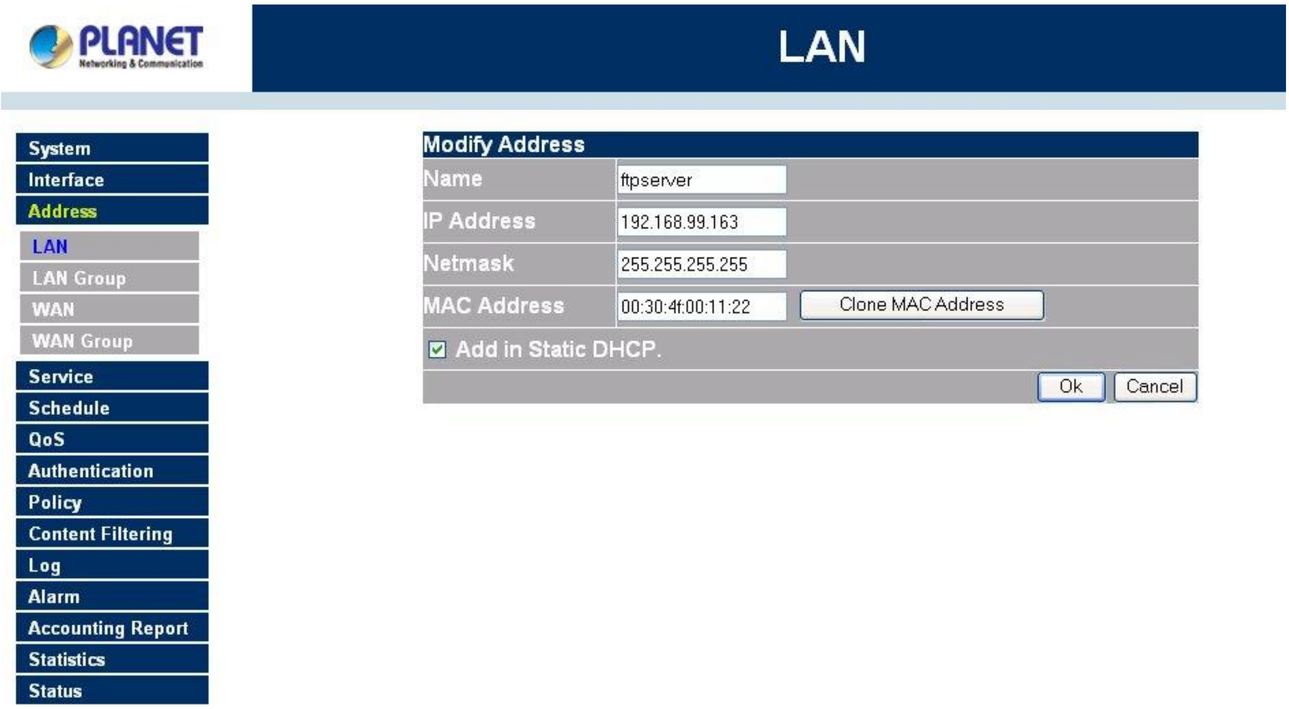
If you want to enable **Add in Static DHCP** function, enter the MAC Address then check the **Add in Static DHCP**.

Modifying an LAN Address

Step 1. In the LAN window, locate the name of the network to be modified. Click the **Modify** option in its corresponding **Configure** field. The **Modify Address** window appears on the screen immediately.

Step 2. In the **Modify Address** window, fill in the new addresses.

Step 3. Click **OK** to save changes or click **Cancel** to discard changes.



Modify Address

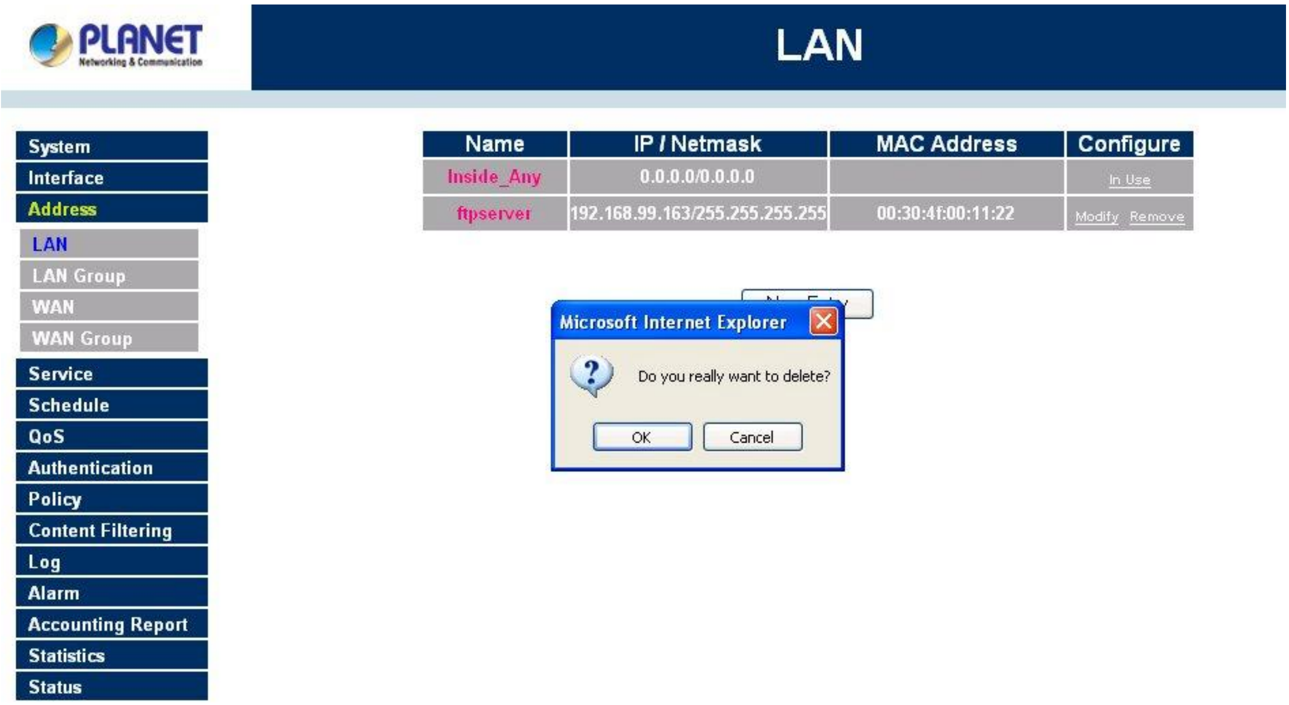
Name	ftpserver
IP Address	192.168.99.163
Netmask	255.255.255.255
MAC Address	00:30:4f:00:11:22

☑ Add in Static DHCP.

Removing a LAN Address

Step 1. In the LAN window, locate the name of the network to be removed. Click the **Remove** option in its corresponding **Configure** field.

Step 2. In the **Remove** confirmation pop-up box, click **OK** to remove the address or click **Cancel** to discard changes.



Name	IP / Netmask	MAC Address	Configure
Inside_Any	0.0.0.0/0.0.0.0		In Use
ftpserver	192.168.99.163/255.255.255.255	00:30:4f:00:11:22	Modify Remove

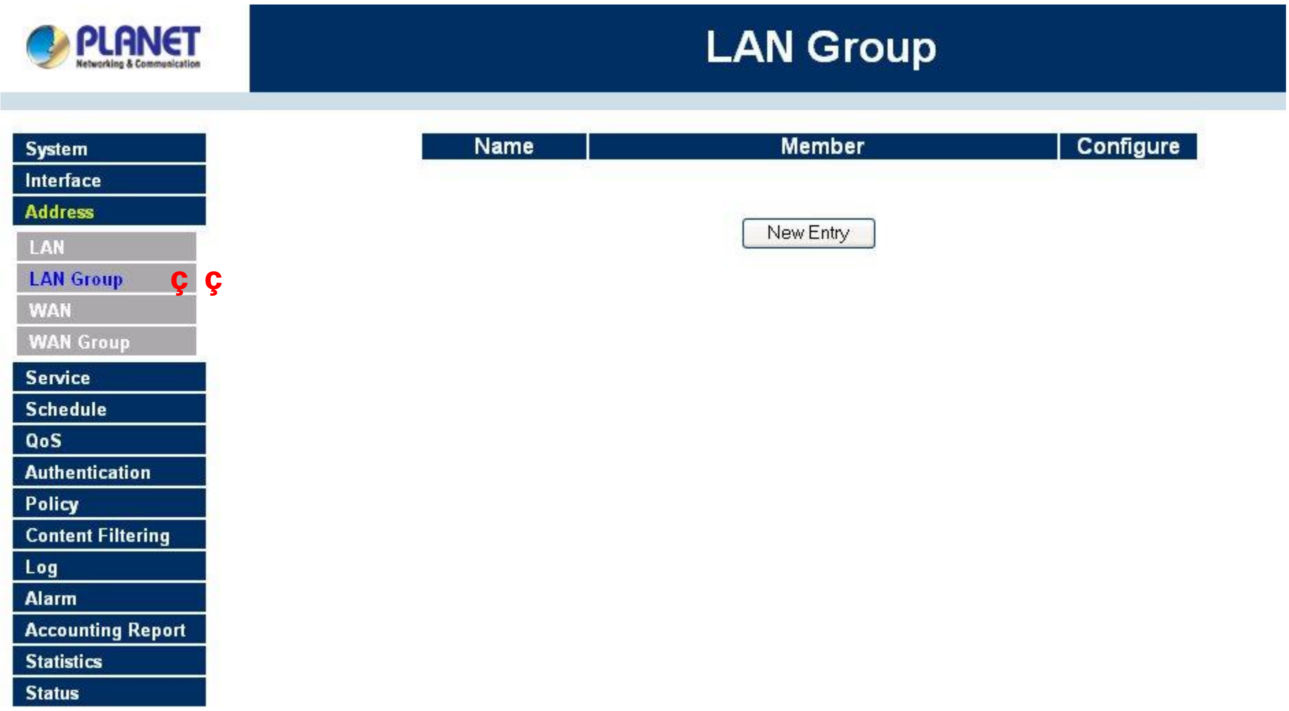
Do you really want to delete?

4.3.2 LAN Group

Entering the LAN Group window

The LAN Addresses may be combined together to become a group.

Step 1. Click LAN **Group** under the **Address** menu to enter the LAN Group window. The current setting information for the LAN network group appears on the screen.



Definitions (LAN group):

Name: Name of the LAN group.

Member: Members of the group.

Configure: Configure the settings of LAN group. Click **Modify** to change the settings of LAN group. Click **Remove** to delete the group.

In the **LAN Group** window, if one of the LAN Group has been added to **Policy**, the **Configure** column will show the message – **In Use**. In this case, you are not allowed to modify or remove the LAN group. You have to delete the Group in **Policy** window, and then you are allowed to configure the LAN Group.

Adding a LAN Group

Step 1. In the LAN **Group** window, click the **New Entry** button to enter the **Add New Address Group** window.

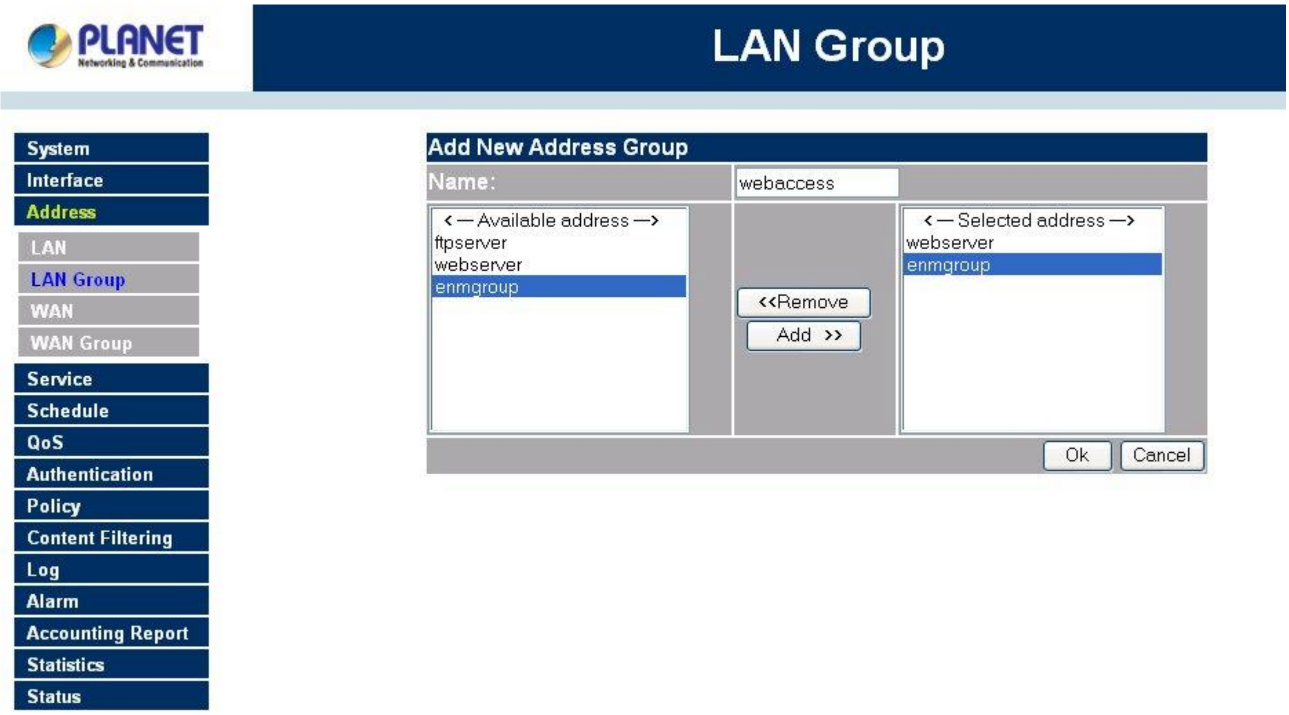
Step 2. In the Add New Address Group window:

- **Available Address:** list the names of all the members of the LAN network.
- **Selected Address:** list the names to be assigned to the new group.
- **Name:** enter the name of the new group in the open field.

Step 3. **Add members:** Select names to be added in Available Address list, and click the **Add>>** button to add them to the Selected Address list.

Step 4. **Remove members:** Select names to be removed in the Selected Address list, and click the **<<Remove** button to remove these members from Selected Address list.

Step 5. Click **OK** to add the new group or click Cancel to discard changes.



Add New Address Group

Name: webaccess

<— Available address —>
ftpserver
webserver
enmgroup

<— Selected address —>
webserver
enmgroup

Modifying a LAN Group

Step 1. In the LAN **Group** window, locate the network group desired to be modified and click its corresponding **Modify** option in the **Configure** field.

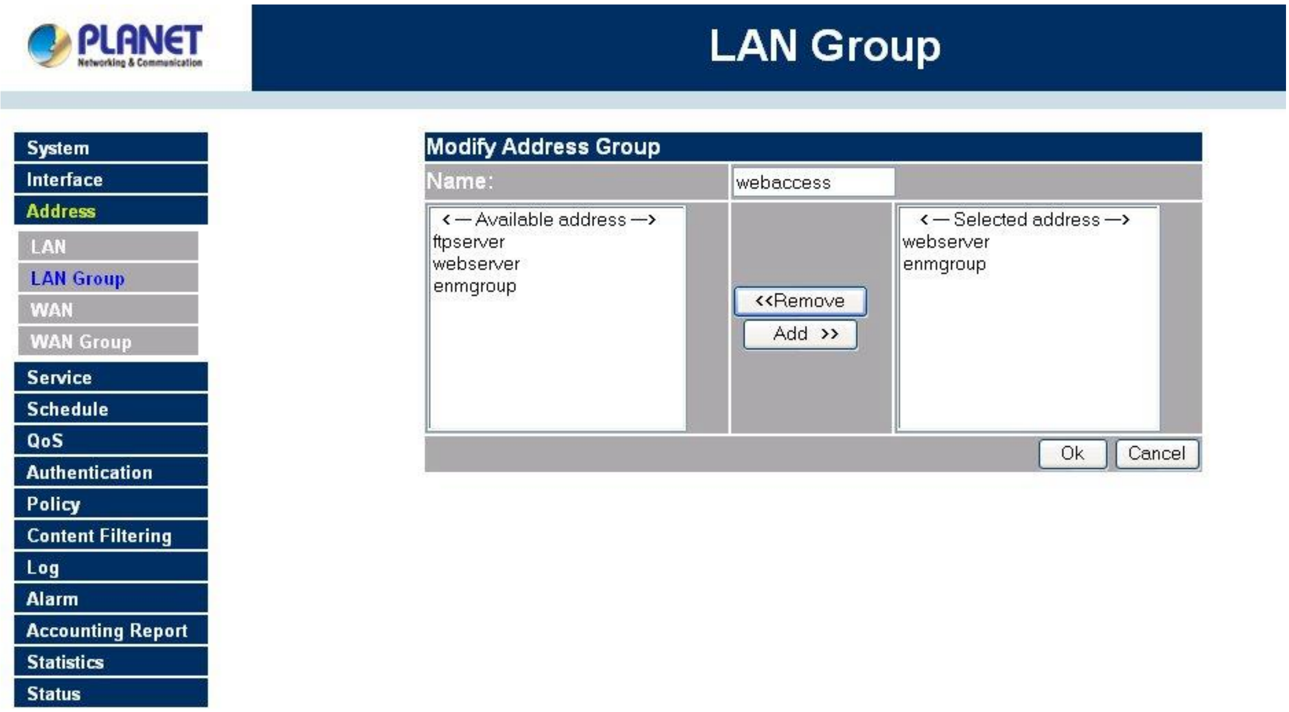
Step 2. A window displaying the information of the selected group appears:

- **Available Address:** list names of all members of the LAN network.
- **Selected Address:** list names of members which have been assigned to this group.

Step 3. **Add members:** Select names in **Available Address** list, and click the **Add>>** button to add them to the **Selected Address** list.

Step 4. **Remove members:** Select names in the **Selected Address** list, and click the **<<Remove** button to remove these members from the **Selected Address** list.

Click **OK** to save changes or click **Cancel** to discard changes.



Modify Address Group

Name: webaccess

<—Available address—>
ftpserver
webserver
enmgroup

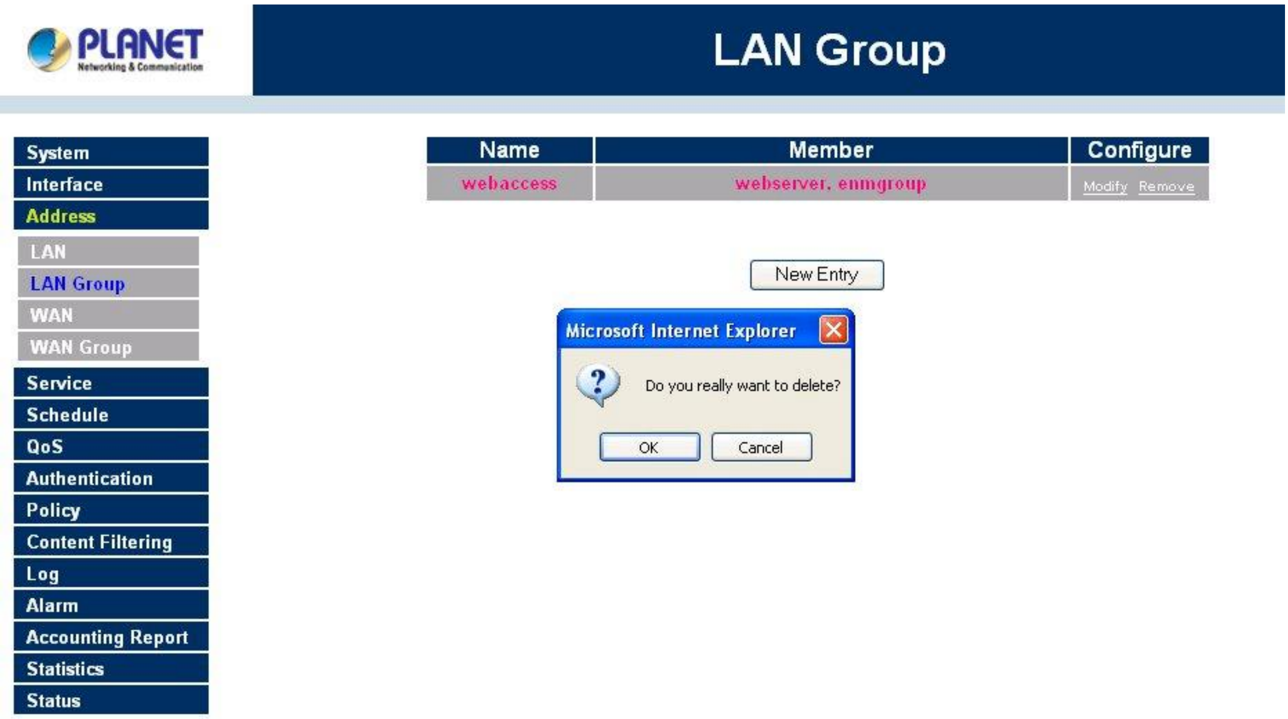
<—Selected address—>
webserver
enmgroup

Figure3-7 Modify LAN Group

Removing a LAN Group

Step 1. In the LAN **Group** window, locate the group to be removed and click its corresponding **Remove** option in the **Configure** field.

Step 2. In the **Remove** confirmation pop-up box, click **OK** to remove the group or click **Cancel** to discard changes.



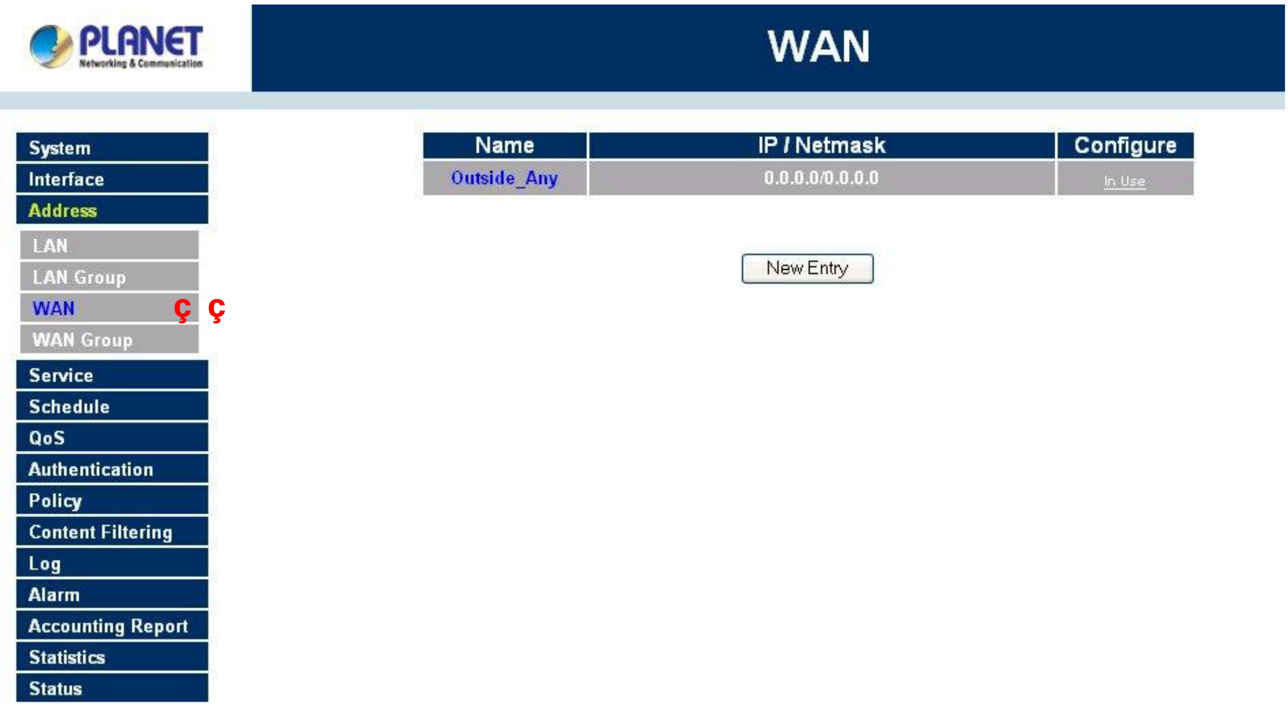
Name	Member	Configure
webaccess	webserver, enmgroup	Modify Remove

Do you really want to delete?

4.3.3 WAN

Entering the WAN window

Step 1. Click **WAN** under the **Address** menu to enter the WAN window. The current setting information, such as the name of the WAN network, IP and Netmask addresses will show on the screen.



Name	IP / Netmask	Configure
Outside_Any	0.0.0.0/0.0.0.0	In Use

Definitions

Name: Name of WAN network address.

IP/Netmask: IP address/Netmask of WAN network.

Configure: Configure the settings of WAN network. Click **Modify** to change the settings of WAN network. Click **Remove** to delete the setting of WAN network.

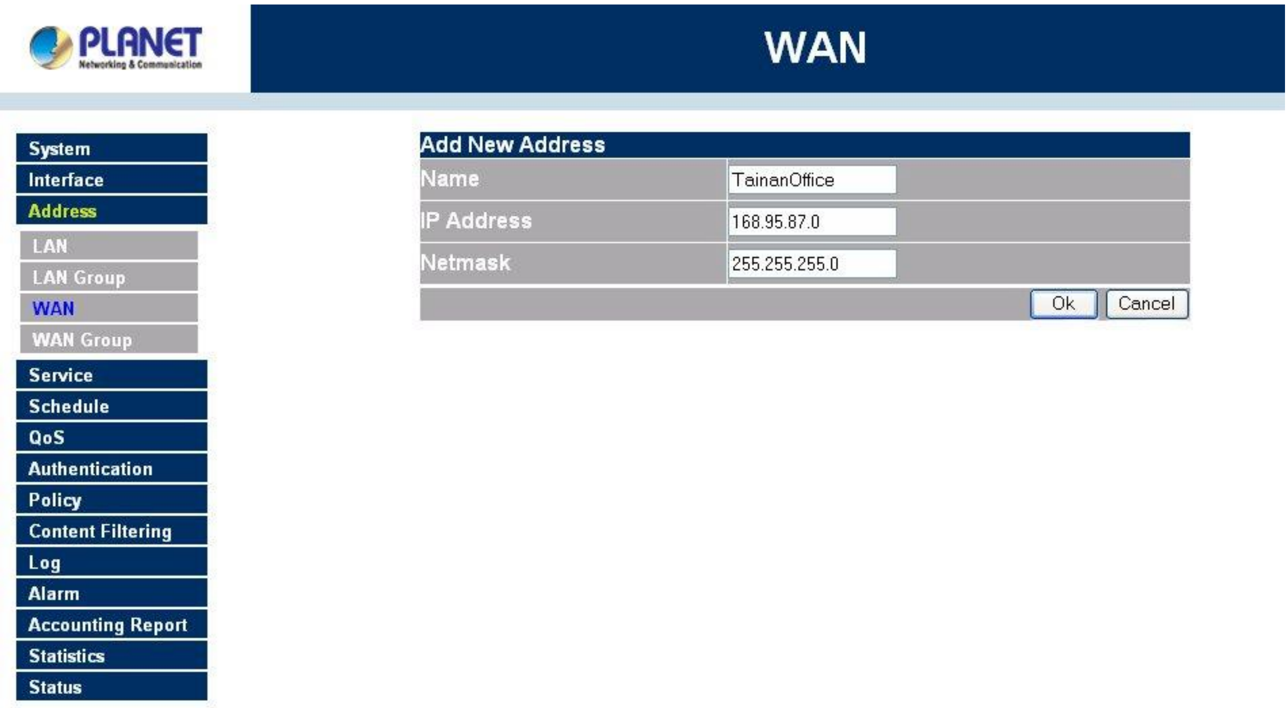
NOTE: In the WAN Network window, if one of the members has been added to **Policy** or **LAN Group**, the **Configure** column will show the message – **In Use**. In this case you are not allowed to modify or remove the settings.

Adding a new WAN Address

Step 1. In the WAN window, click the **New Entry** button.

Step 2. In the **Add New Address** window, enter the settings for a new WAN network address.

Step 3. Click **OK** to add the specified WAN network or click **Cancel** to discard changes.



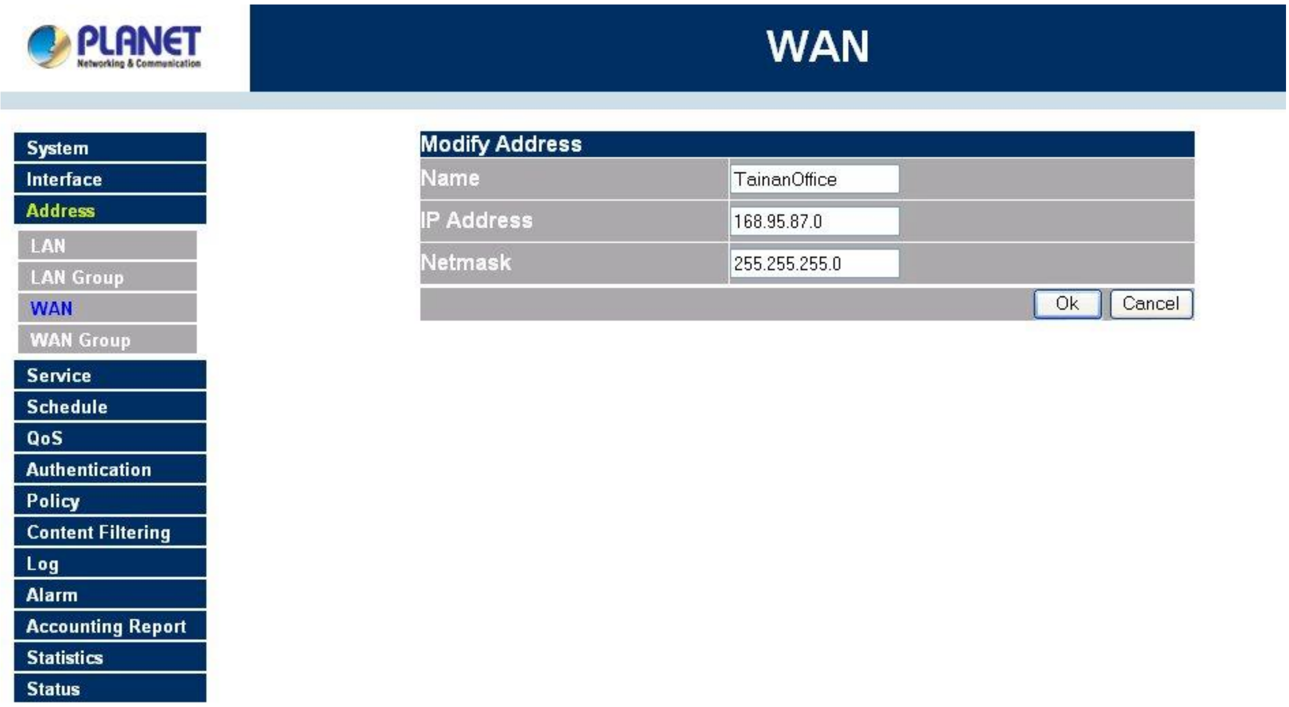
Add New Address	
Name	TainanOffice
IP Address	168.95.87.0
Netmask	255.255.255.0

Modifying an WAN Address

Step 1. In the WAN table, locate the name of the network to be modified and click the **Modify** option in its corresponding **Configure** field.

Step 2. The **Modify Address** window will appear on the screen immediately. In the **Modify Address** window, fill in new addresses.

Step 3. Click **OK** to save changes or click **Cancel** to discard changes.



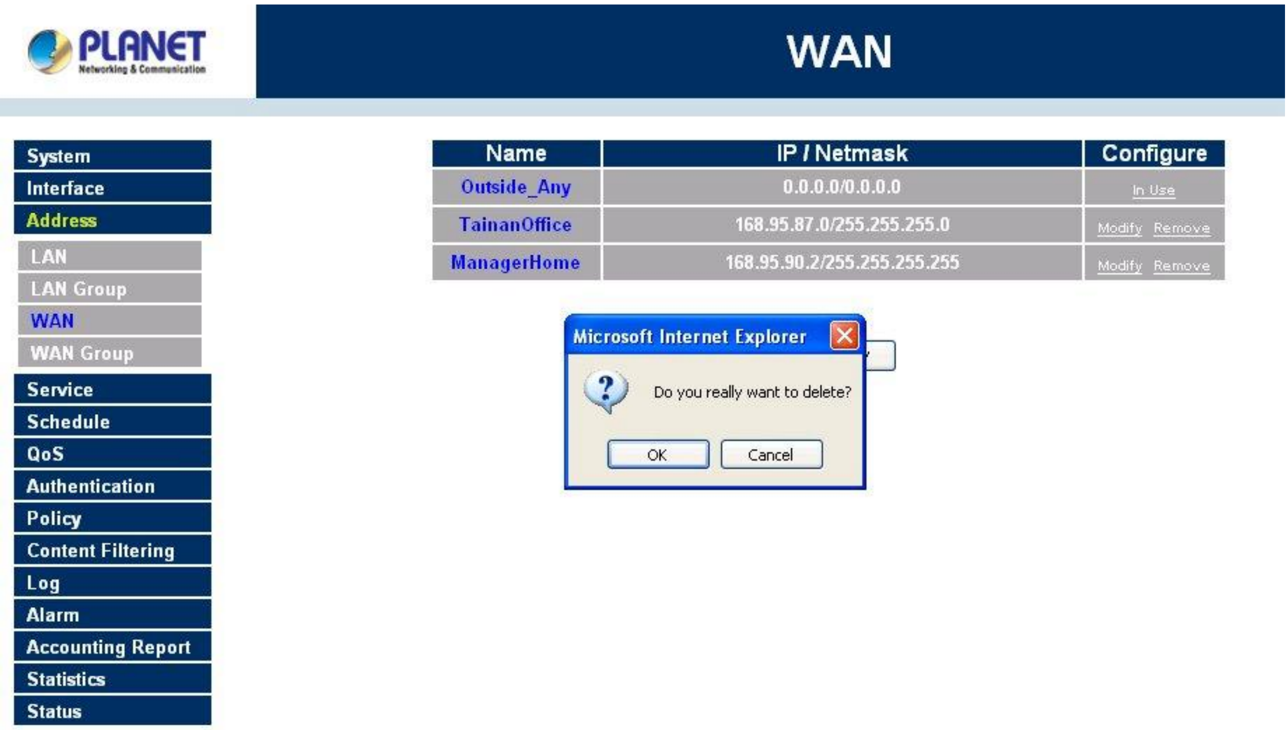
Modify Address

Name	TainanOffice
IP Address	168.95.87.0
Netmask	255.255.255.0

Removing an WAN Address

Step 1. In the WAN table, locate the name of the network to be removed and click the **Remove** option in its corresponding Configure field.

Step 2. In the Remove confirmation pop-up box, click **OK** to remove the address or click **Cancel** to discard changes.



Name	IP / Netmask	Configure
Outside_Any	0.0.0.0/0.0.0.0	In Use
TainanOffice	168.95.87.0/255.255.255.0	Modify Remove
ManagerHome	168.95.90.2/255.255.255.255	Modify Remove

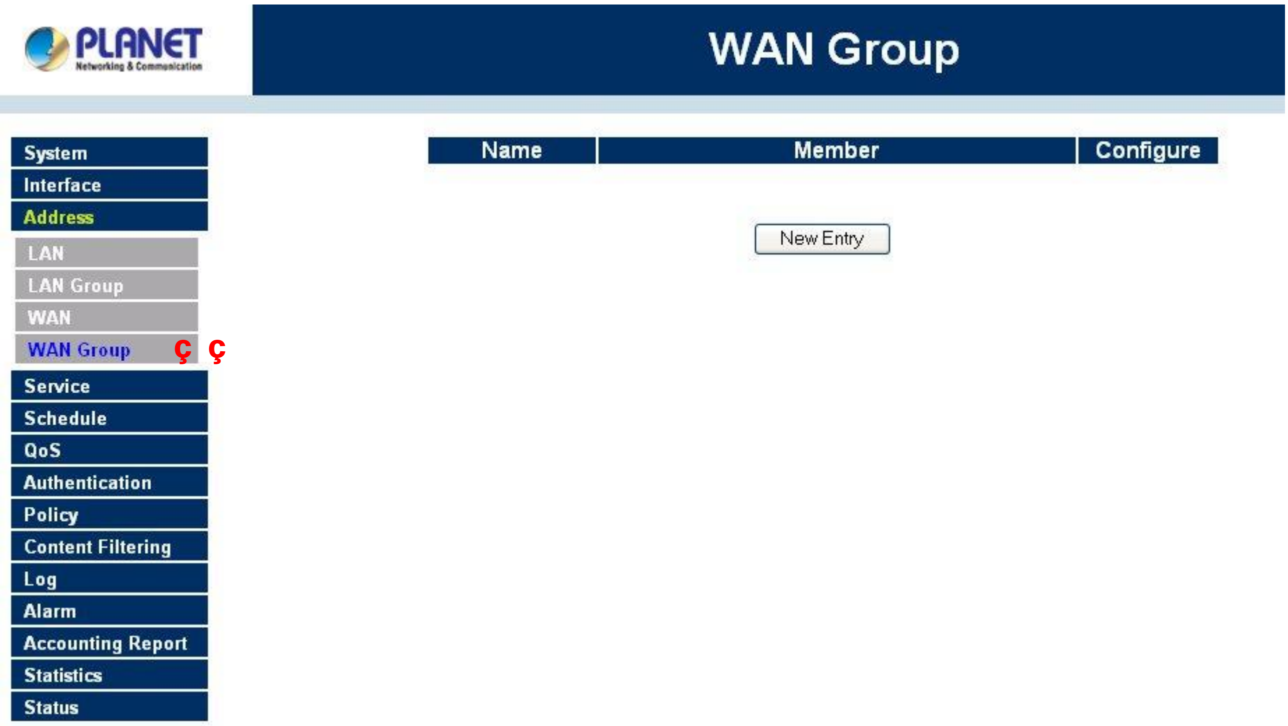
Microsoft Internet Explorer

Do you really want to delete?

4.3.4 WAN Group

Entering the WAN Group window

Step 1. Click the **WAN Group** under the **Address** menu bar to enter the WAN window. The current settings for the WAN network group(s) will appear on the screen.



Name	Member	Configure

Definitions:

Name: Name of the WAN group.

Member: Members of the group.

Configure: Configure the settings of WAN group. Click **Modify** to change the parameters of WAN group Click Remove to delete the selected group.

NOTE: In the **WAN Group** window, if one of the members has been added to the **Policy**, "**In Use**" message will appear in the **Configure** column. You are not allowed to modify or remove the settings. Go to the **Policy** window to remove the setting, and then you can configure.

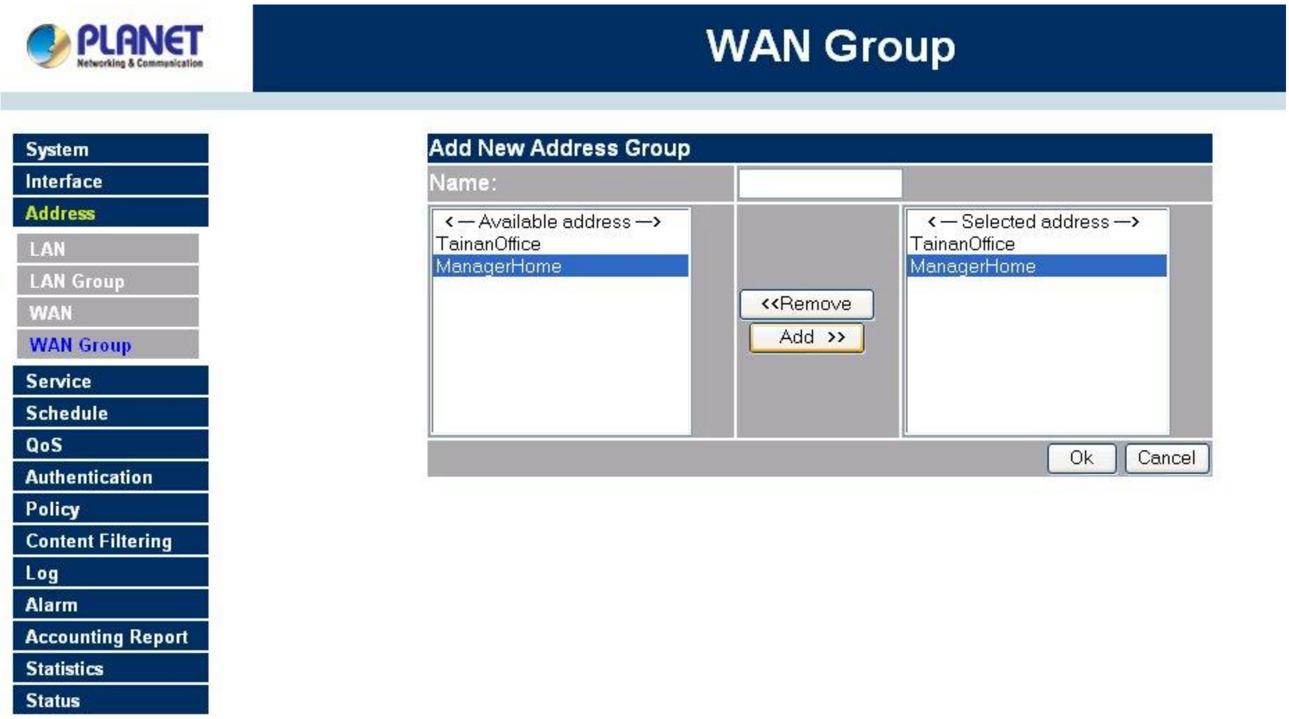
Adding an WAN Group

Step 1. In the **WAN Group** window, click the **New Entry** button and the **Add New Address Group** window will appear.

Step 2. In the **Add New Address Group** window the following fields will appear:

- n **Name:** enter the name of the new group.
- n **Available Address:** List the names of all the members of the WAN network.
- n **Selected Address:** List the names to assign to the new group.
- n **Add members:** Select the names to be added in the **Available Address** list, and click the **Add>>** button to add them to the **Selected Address** list.
- n **Remove members:** Select the names to be removed in the **Selected Address** list, and click the **<<Remove** button to remove them from the **Selected Address** list.

Step 3. Click **OK** to add the new group or click **Cancel** to discard changes.



Modifying a WAN Group

Step 1. In the **WAN Group** window, locate the network group to be modified and click its corresponding **Modify** button in the **Configure** field.

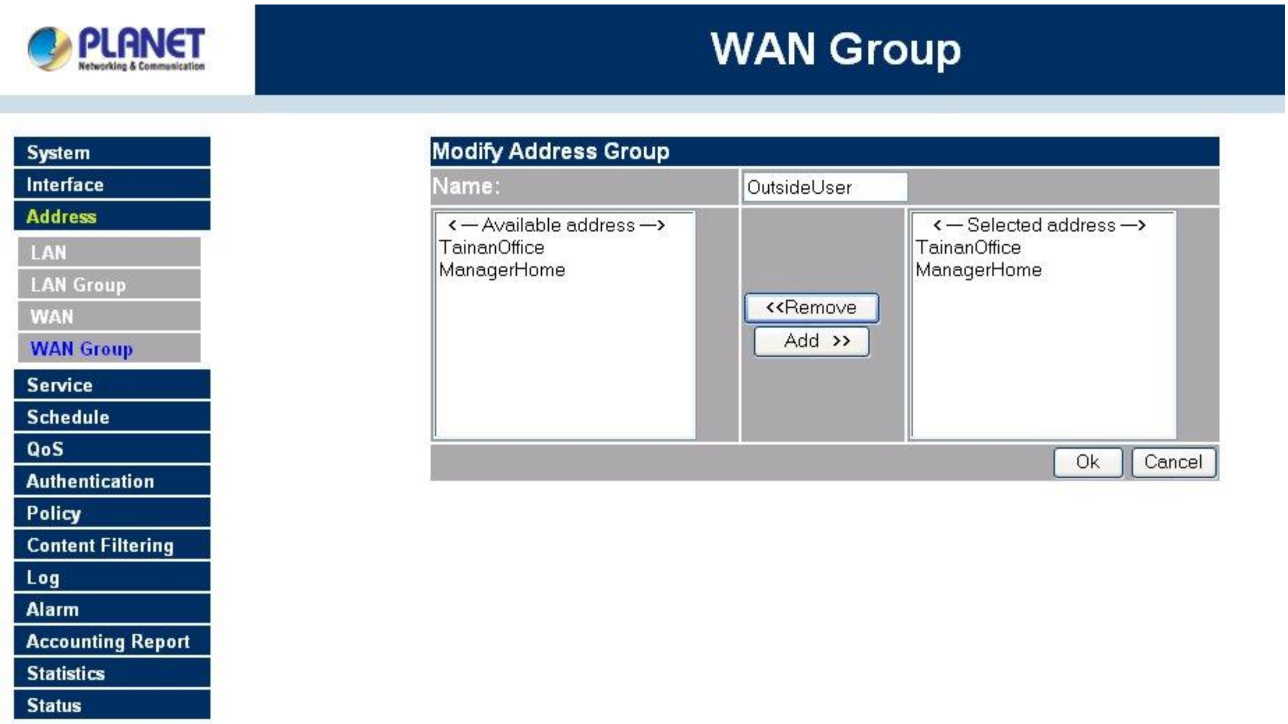
Step 2. A window displaying the information of the selected group appears:

n **Available Address:** list the names of all the members of the WAN network.
n **Selected Address:** list the names of the members that have been assigned to this group.

Step 3. **Add members:** Select the names to be added in the **Available Address** list, and click the **Add>>** button to add them to the **Selected Address** list.

Step 4. **Remove members:** Select the names to be removed in the **Selected Address** list, and click the **<<Remove** button to remove them from the **Selected Address** list.

Step 5. Click **OK** to save changes or click **Cancel** to discard changes.



Modify Address Group

Name: OutsideUser

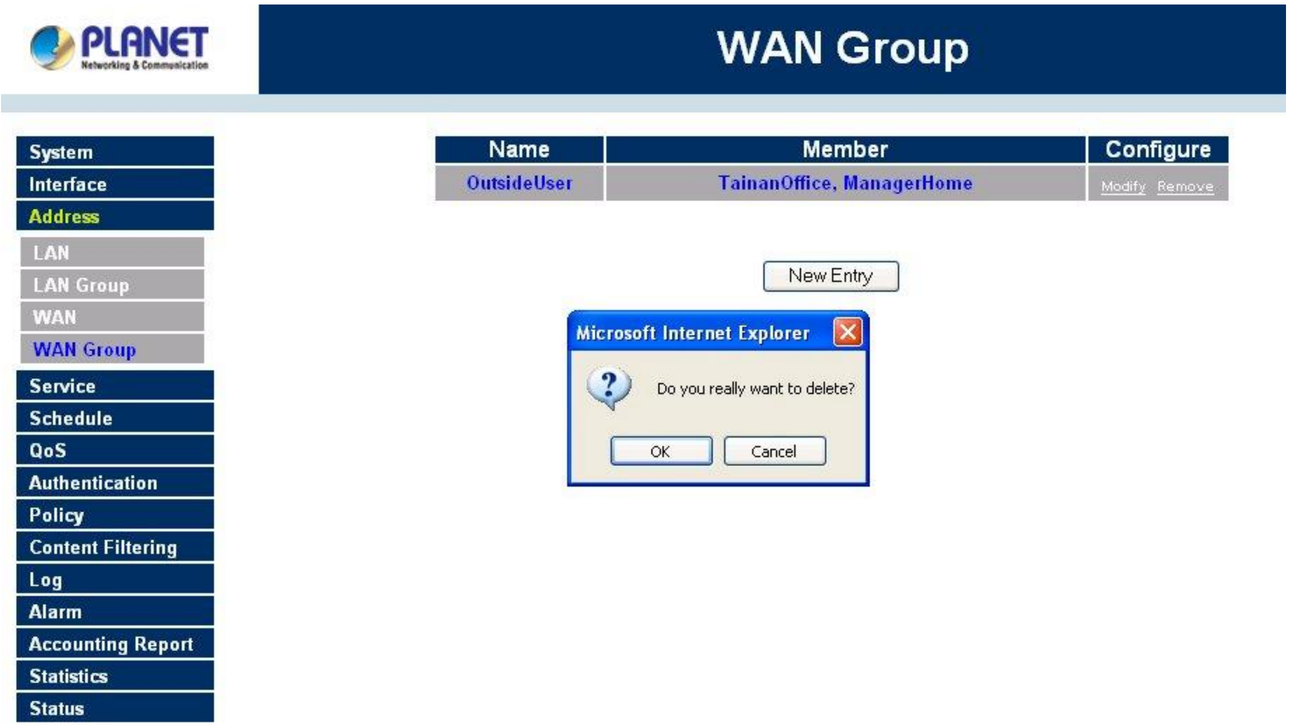
<—Available address—>
TainanOffice
ManagerHome

<—Selected address—>
TainanOffice
ManagerHome

Removing a WAN Group

Step 1. In the **WAN Group** window, locate the group to be removed and click its corresponding **Modify** option in the **Configure** field.

Step 2. In the **Remove confirmation** pop-up box, click **OK** to remove the group or click **Cancel** to discard changes.



Name	Member	Configure
OutsideUser	TainanOffice, ManagerHome	Modify Remove

Do you really want to delete?

4.4 Service

In this section, network services are defined and new network services can be added. There are three sub menus under Service which are: **Pre-defined**, **Custom**, and **Group**. The Administrator can simply follow the instructions below to define the protocols and port numbers for network communication applications. Users then can connect to servers and other computers through these available network services.

What is Service?

TCP and UDP protocols support varieties of services, and each service consists of a TCP Port or UDP port number, such as TELNET(23), SMTP(21), POP3(110),etc. The Bandwidth Management Gateway defines two services: pre-defined service and custom service. The common-use services like TCP and UDP are defined in the pre-defined service and cannot be modified or removed. In the custom menu, users can define other TCP port and UDP port numbers that are not in the pre-defined menu according to their needs. When defining custom services, the client port ranges from 1024 to 65535 and the server port ranges from 0 to 1023.

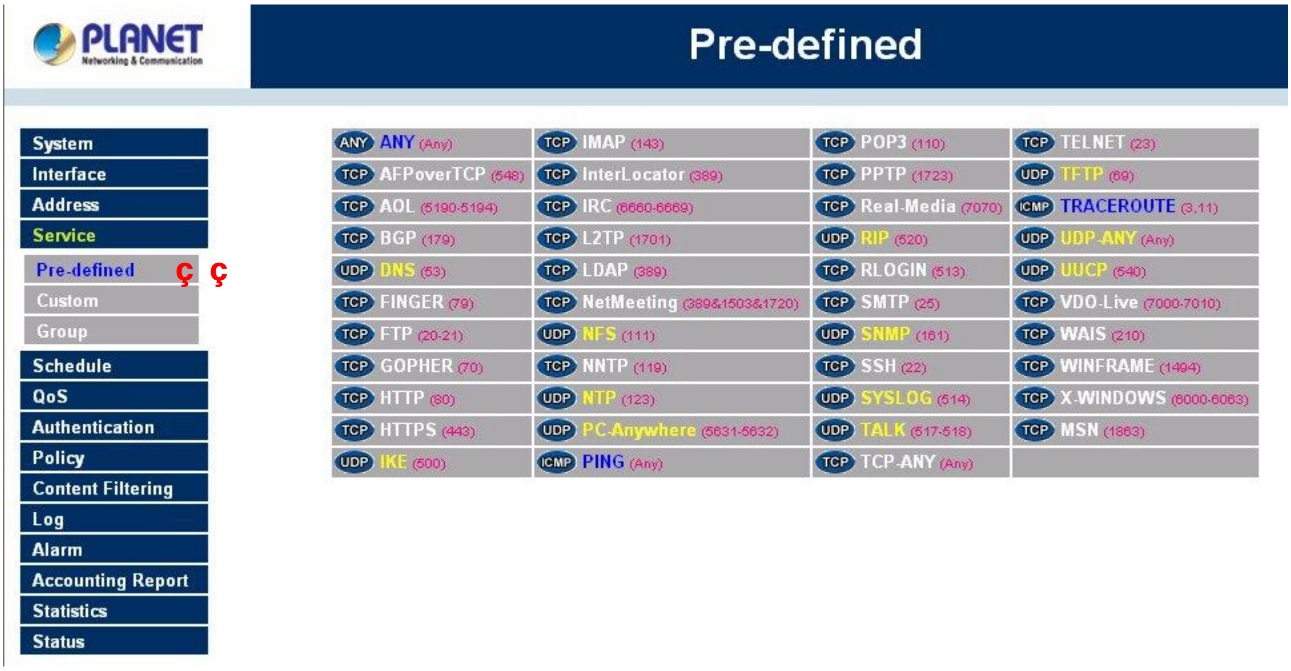
How do I use Service?

The Administrator can add new service group names in the **Group** option under **Service** menu, and assign desired services into that new group. Using service group the Administrator can simplify the processes of setting up control policies. For example, there are 10 different computers that want to access 5 different services on a server, such as HTTP, FTP, SMTP, POP3, and TELNET. Without the help of service groups, the Administrator needs to set up 50 (10x5) control policies, but by applying all 5 services to a single group name in the **service** field, it takes only one control policy to achieve the same effect as the 50 control policies.

4.4.1 Pre-defined

Entering a Pre-defined window

Step 1. Click **Pre-defined** under it. A window will appear with a list of services and their associated IP addresses. This list cannot be modified.



ANY ANY (Any)	TCP IMAP (143)	TCP POP3 (110)	TCP TELNET (23)
TCP AFPoverTCP (548)	TCP InterLocator (389)	TCP PPTP (1723)	UDP TFTP (69)
TCP AOL (5190-5194)	TCP IRC (6660-6669)	TCP Real-Media (7070)	ICMP TRACEROUTE (3,11)
TCP BGP (179)	TCP L2TP (1701)	UDP RIP (520)	UDP UDP-ANY (Any)
UDP DNS (53)	TCP LDAP (389)	TCP RLOGIN (513)	UDP UUCP (540)
TCP FINGER (79)	TCP NetMeeting (389&1503&1720)	TCP SMTP (25)	TCP VDO-Live (7000-7010)
TCP FTP (20-21)	UDP NFS (111)	UDP SNMP (161)	TCP WAIS (210)
TCP GOPHER (70)	TCP NNTP (119)	TCP SSH (22)	TCP WINFRAME (1494)
TCP HTTP (80)	UDP NTP (123)	UDP SYSLOG (514)	TCP X-WINDOWS (6000-6063)
TCP HTTPS (443)	UDP PC-Anywhere (5631-5632)	UDP TALK (517-518)	TCP MSN (1863)
UDP IKE (500)	ICMP PING (Any)	TCP TCP-ANY (Any)	

Icons and Descriptions

Figur	Description
TCP	TCP services, i.g. FTP、FINGER、HTTP、、HTTPS 、IMAP、SMTP、POP3、ANY、AOL、BGP、GOPHER、InterLocator、IRC、L2TP、LDAP、NetMeeting、NNTP、PPTPReal、 Media、RLOGIN、SSH、TCP ANY、TELNET、VDO Live、WAIS 、WINFRAME 、X-WINDOWS, etc.
UDP	UDP services, i.g. IKE 、DNS 、NTP 、IRC 、RIP 、SNMP 、SYSLOG 、TALK 、TFTP 、UDP-ANY 、UUC, etc.
ICMP	ICMP services, i.g. PING 、TRACEROUTE, etc.

4.4.2 Custom

Entering the Custom window

Step 1. Click **Custom** under it. A window will appear with a table showing all services currently defined by the Administrator.

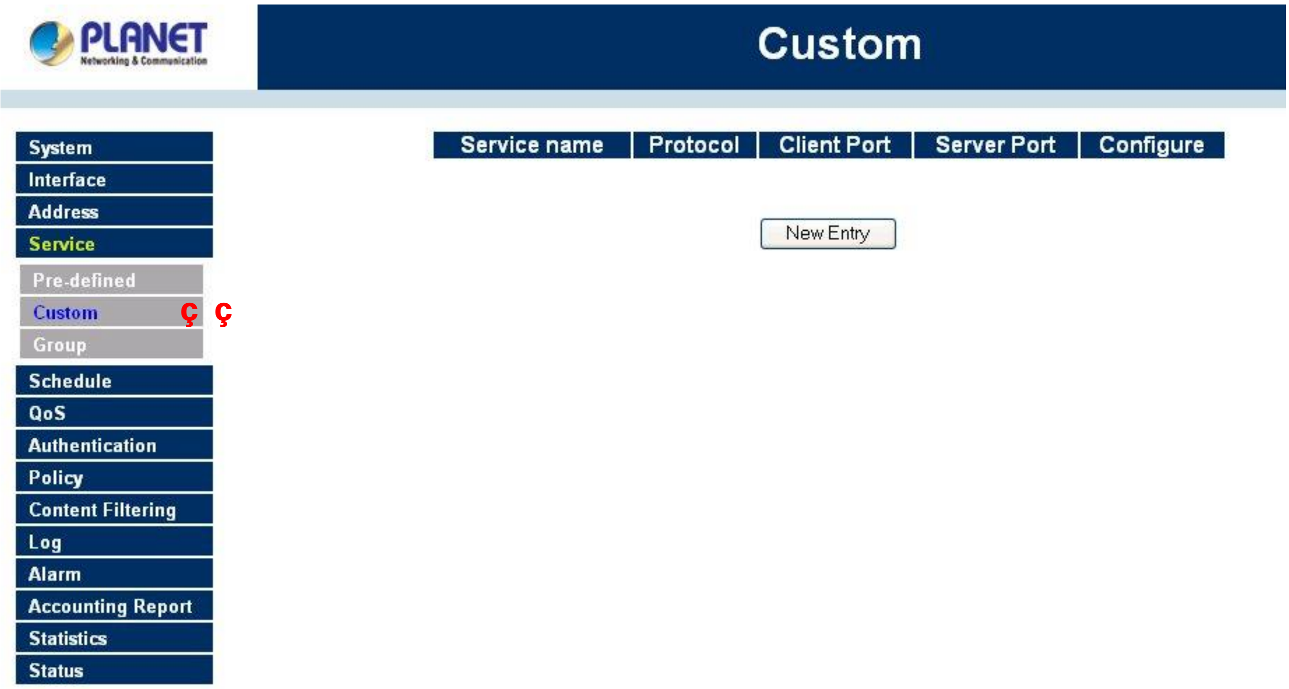


Figure 4-2 Custom Service

Definitions:

Service name: The defined service name.

Protocol: Network protocol used in the basic setting. Such as TCP、UDP or others.

Client port: The range of Client port in defined service.

If the number of ports entered in the two fields of Client port is different, it means that the port numbers between these two numbers are opened. If the number of ports entered in the two fields of Client port is identical, it means that the entered port number is opened.

Service port: The range of Service port in defined service.

If the number of ports entered in the two fields of Service port is different, it means that the port numbers between these two numbers are opened. If the number of ports entered in the two fields of Service port is identical, it means that the entered port number is opened.

Configure: Configure the settings in Service table. Click **Modify** to change the parameters in Service table. Click **Remove** to delete the selected setting.

NOTE: In the **Custom** window, if one of the services has been added to **Policy** or **Group**, "**In Use**" message will appear in the **Configure** column. In this case you are not allowed to modify or remove the settings. Go to the **Policy** or **Group** window to delete the setting, and then you can configure the settings.

Adding a new Service

In the **Custom** window, click the **New Entry** button and a new service table appears.

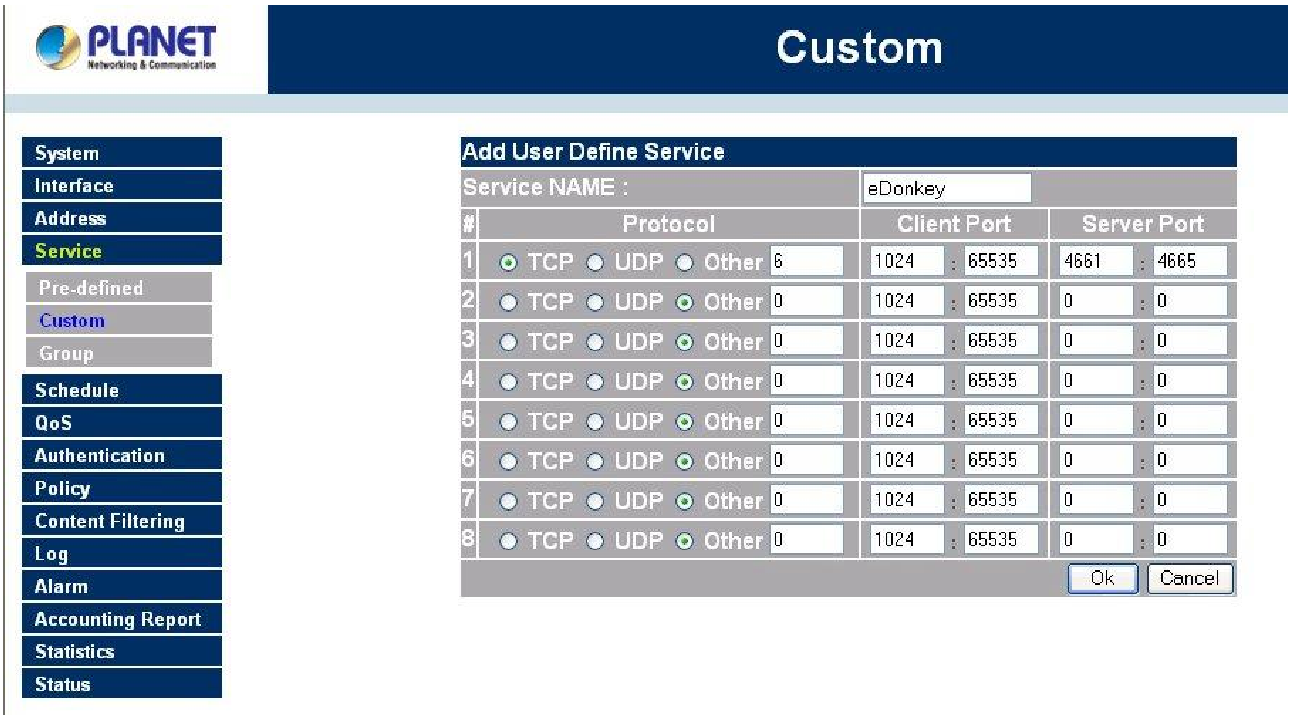
In the new service table:

- New Service Name: This will be the name referencing the new service.
- Protocol: Enter the network protocol type to be used, such as TCP, UDP, or Other (please enter the number for the protocol type).
- Client Port: enter the range of port number of new clients.
- Server Port: enter the range of port number of new servers.

The client port ranges from 1024 to 65535 and the server port ranges from 0 to 1023.

Step 1. Click **OK** to add new services, or click **Cancel** to cancel.

Step 2. Click **OK** to accept editing; or click **Cancel**.



Add User Define Service

Service NAME : eDonkey

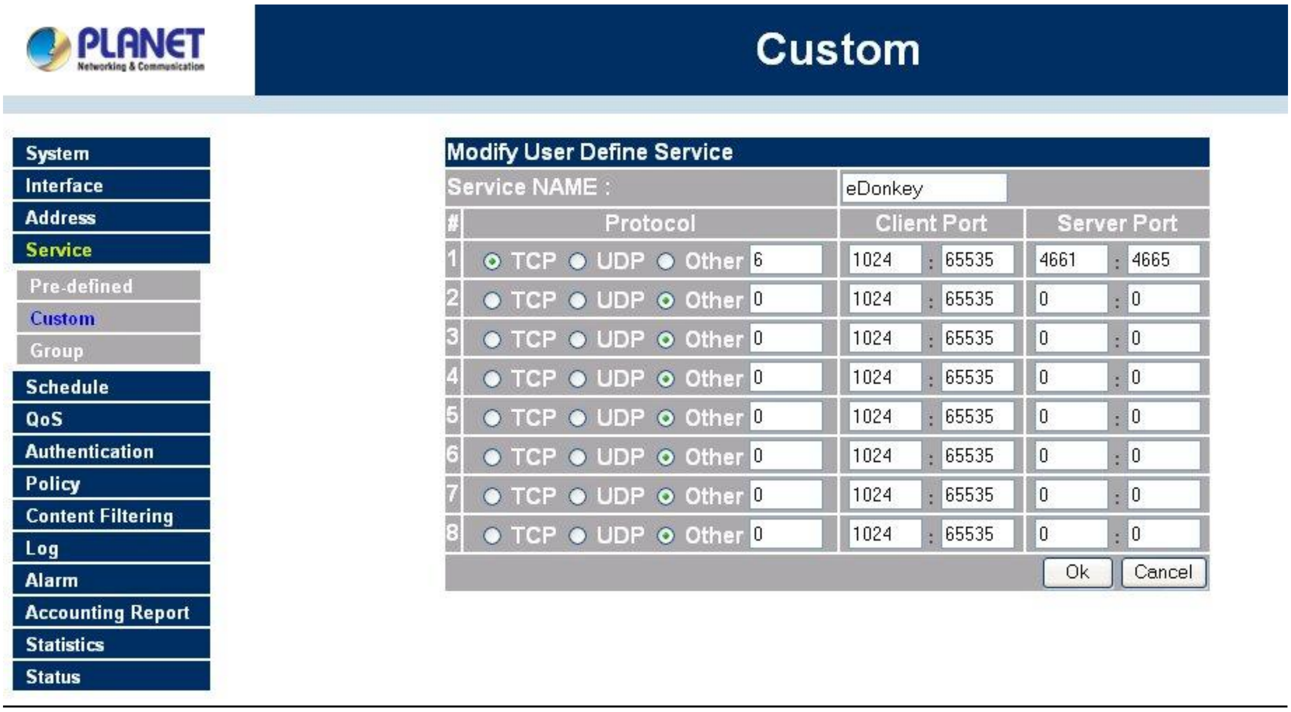
#	Protocol	Client Port	Server Port
1	● TCP ○ UDP ○ Other 6	1024 : 65535	4661 : 4665
2	○ TCP ○ UDP ● Other 0	1024 : 65535	0 : 0
3	○ TCP ○ UDP ● Other 0	1024 : 65535	0 : 0
4	○ TCP ○ UDP ● Other 0	1024 : 65535	0 : 0
5	○ TCP ○ UDP ● Other 0	1024 : 65535	0 : 0
6	○ TCP ○ UDP ● Other 0	1024 : 65535	0 : 0
7	○ TCP ○ UDP ● Other 0	1024 : 65535	0 : 0
8	○ TCP ○ UDP ● Other 0	1024 : 65535	0 : 0

Modifying Custom Services

Step 1. A table showing the current settings of the selected service appears on the screen

Step 2. Enter the new values.

Step 3. Click **OK** to accept editing; or click **Cancel**.



Modify User Define Service

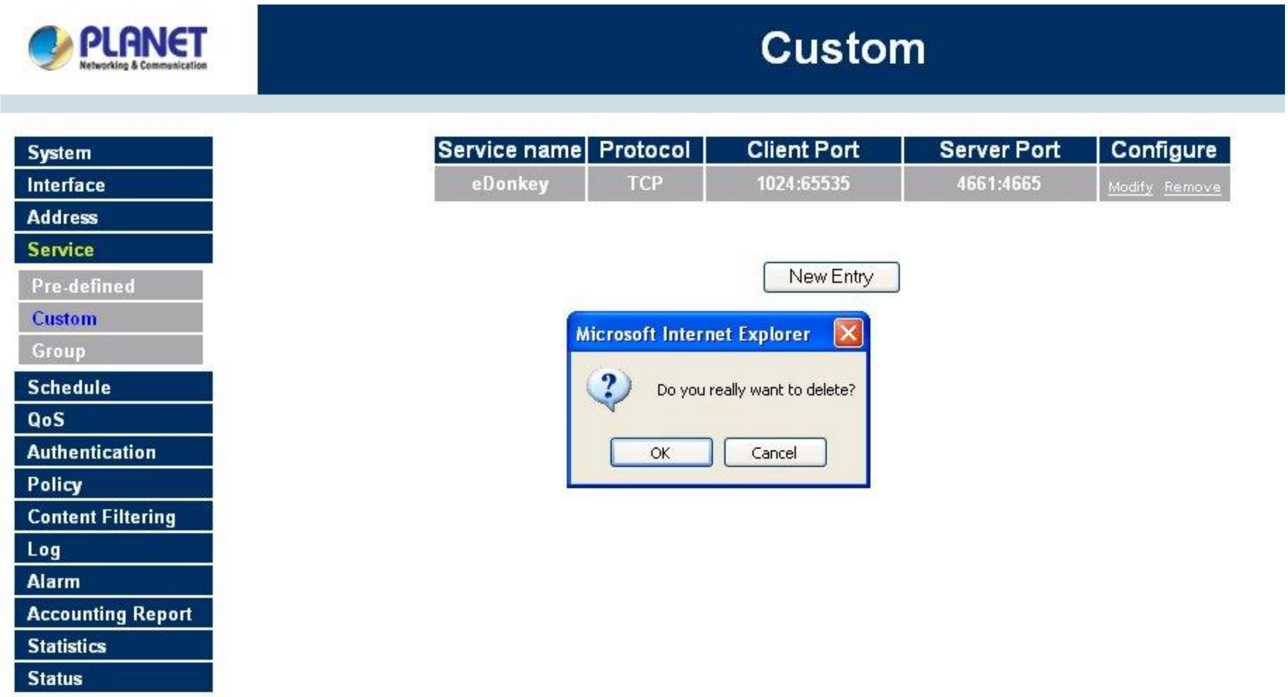
Service NAME : eDonkey

#	Protocol	Client Port	Server Port
1	● TCP ○ UDP ○ Other 6	1024 : 65535	4661 : 4665
2	○ TCP ○ UDP ● Other 0	1024 : 65535	0 : 0
3	○ TCP ○ UDP ● Other 0	1024 : 65535	0 : 0
4	○ TCP ○ UDP ● Other 0	1024 : 65535	0 : 0
5	○ TCP ○ UDP ● Other 0	1024 : 65535	0 : 0
6	○ TCP ○ UDP ● Other 0	1024 : 65535	0 : 0
7	○ TCP ○ UDP ● Other 0	1024 : 65535	0 : 0
8	○ TCP ○ UDP ● Other 0	1024 : 65535	0 : 0

Removing Custom Services

Step 1. Click its corresponding **Remove** option in the **Configure** field.

Step 2. In the **Remove** confirmation pop-up box, click **OK** to remove the selected service or click **Cancel** to cancel action.



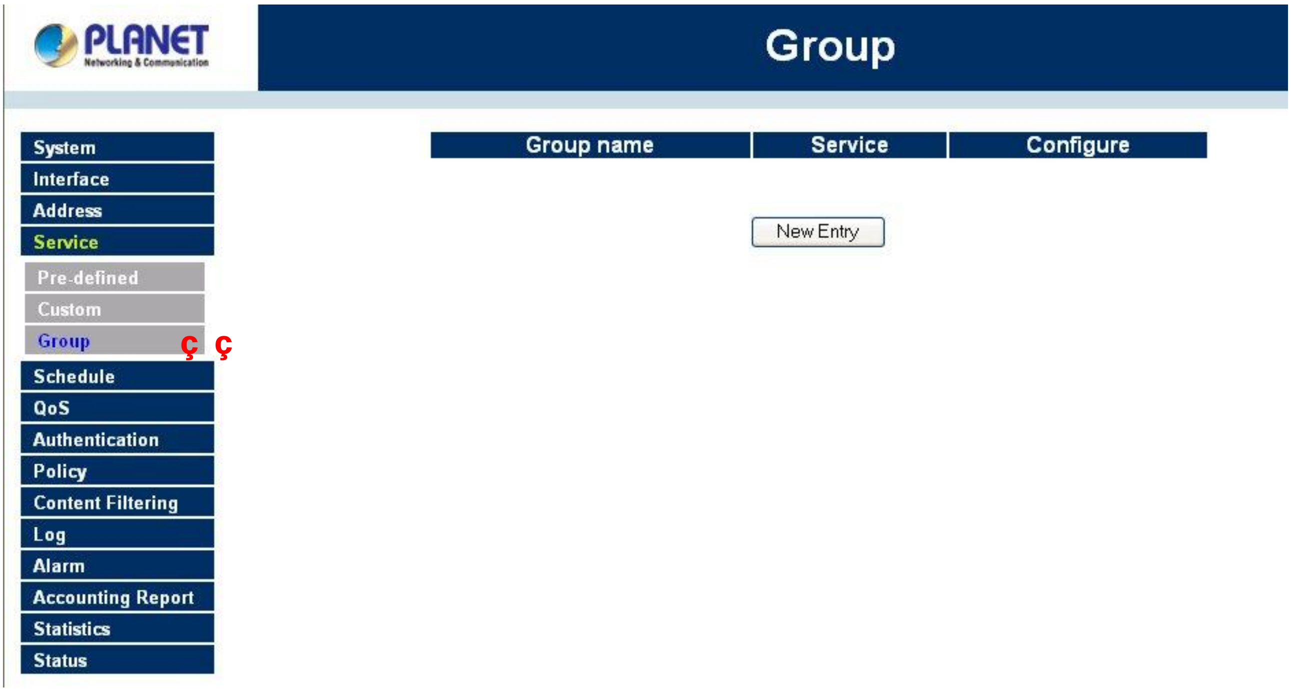
Service name	Protocol	Client Port	Server Port	Configure
eDonkey	TCP	1024:65535	4661:4665	Modify Remove

Do you really want to delete?

4.4.3 Group

Accessing the Group window

Step 1. Click **Group** under it. A window will appear with a table displaying current service group settings set by the Administrator.



Definitions:

Group name: The Group name of the defined Service.

Service: The Service item of the Group.

Configure: Configure the settings of Group. Click **Modify** to change the parameters of the Group. Click Remove to delete the Group.

NOTE: In the **Group** window, if one of the Service Groups has been added to **Policy**. "**In Use**" message will appear in the **Configure** column. You are not allowed to modify or remove the settings. Go to the Policy window, remove the Service group first, and then you are allowed to configure the setting.

Adding Service Groups

Step 1. In the **Group** window, click the **New Entry** button.

Step 2. In the **Add Service Group** window, the following fields will appear:

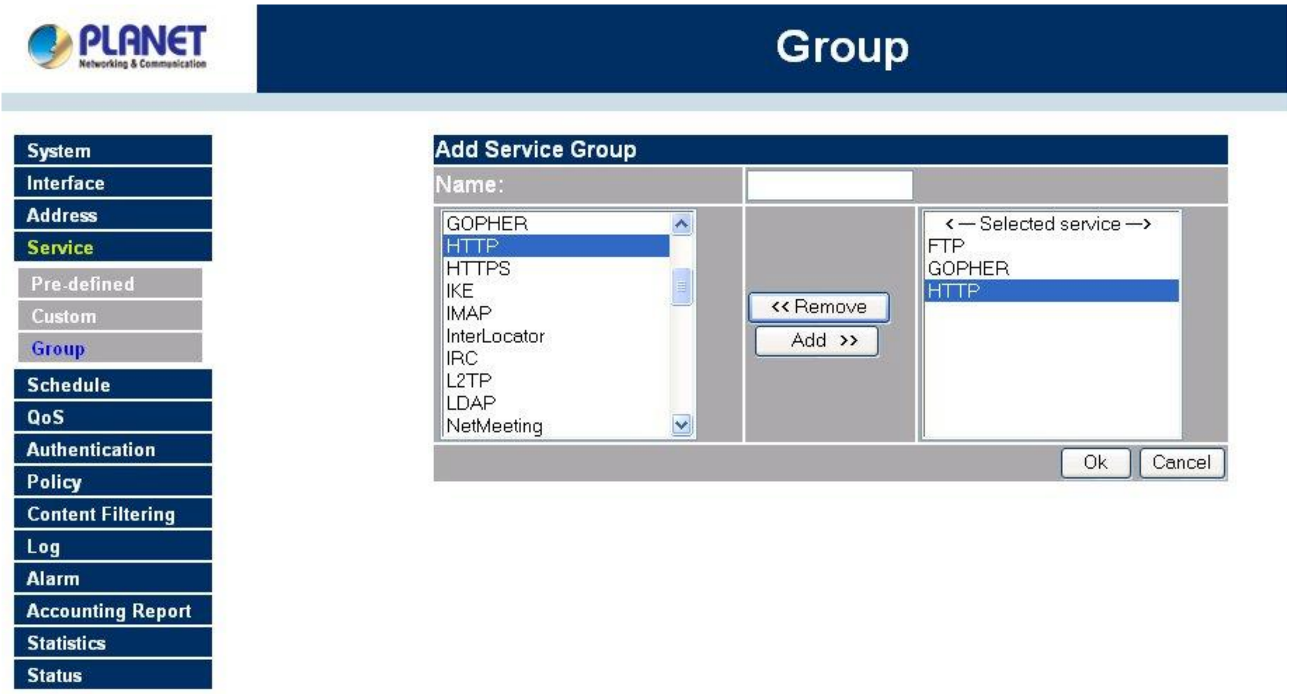
n **Available Services:** list all the available services.
n **Selected Services:** list services to be assigned to the new group.

Step 3. Enter the new group name in the group **Name** field. This will be the name referencing the created group.

Step 4. **To add new services:** Select the services desired to be added in the **Available Services** list and then click the **Add>>** button to add them to the group.

Step 5. **To remove services:** Select services desired to be removed in the **Available Services**, and then click the **<<Remove** button to remove them from the group.

Step 6. Click **OK** to add the new group.



Modifying Service Groups

Step 1. In the Mod (modify) group window the following fields are displayed:

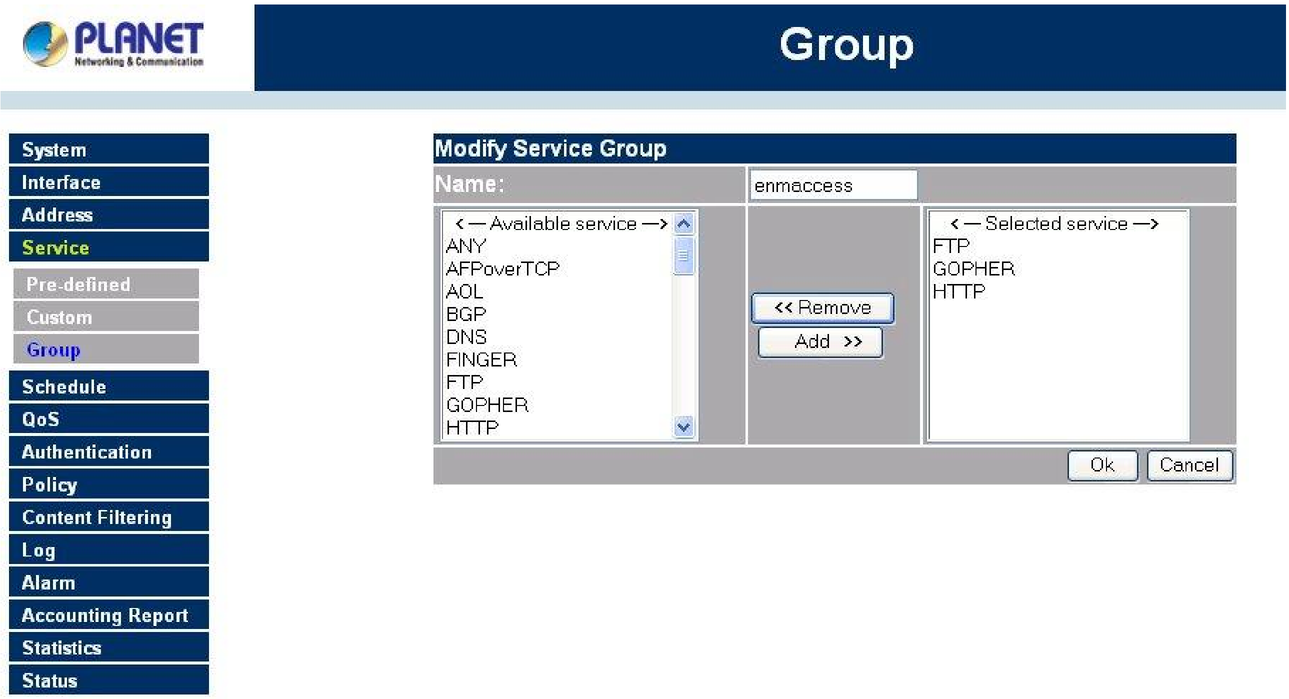
n **Available Services:** lists all the available services.

n **Selected Services:** list services that have been assigned to the selected group.

Step 2. **Add new services:** Select services in the **Available Services** list, and then click the **Add>>** button to add them to the group.

Step 3. **Remove services:** Select services to be removed in the **Selected Services** list, and then click the **<<Remove** button to remove theses services from the group.

Step 4. Click **OK** to save editing changes.



Modify Service Group

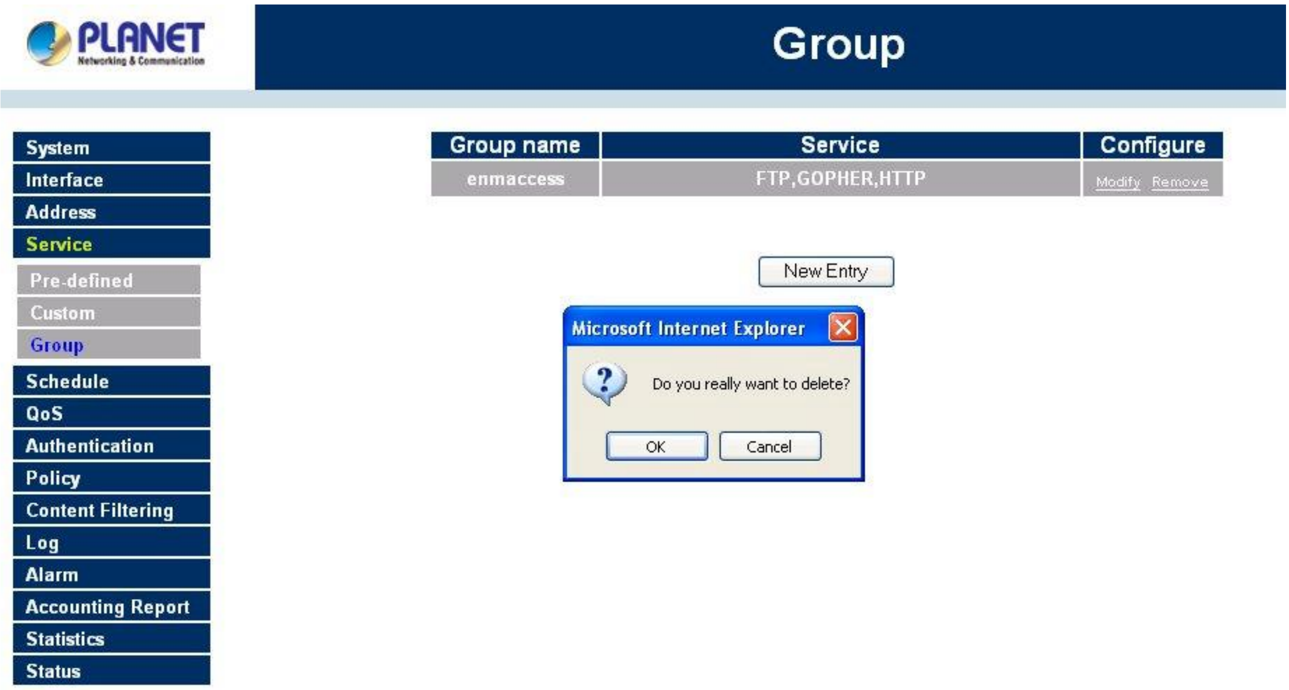
Name: enmaccess

<— Available service —>
ANY
AFPoverTCP
AOL
BGP
DNS
FINGER
FTP
GOPHER
HTTP

<— Selected service —>
FTP
GOPHER
HTTP

Removing Service Groups

In the **Remove** confirmation pop-up box, click **OK** to remove the selected service group or click **Cancel** to cancel removing.



Group name	Service	Configure
enmaccess	FTP,GOPHER,HTTP	Modify Remove

Microsoft Internet Explorer

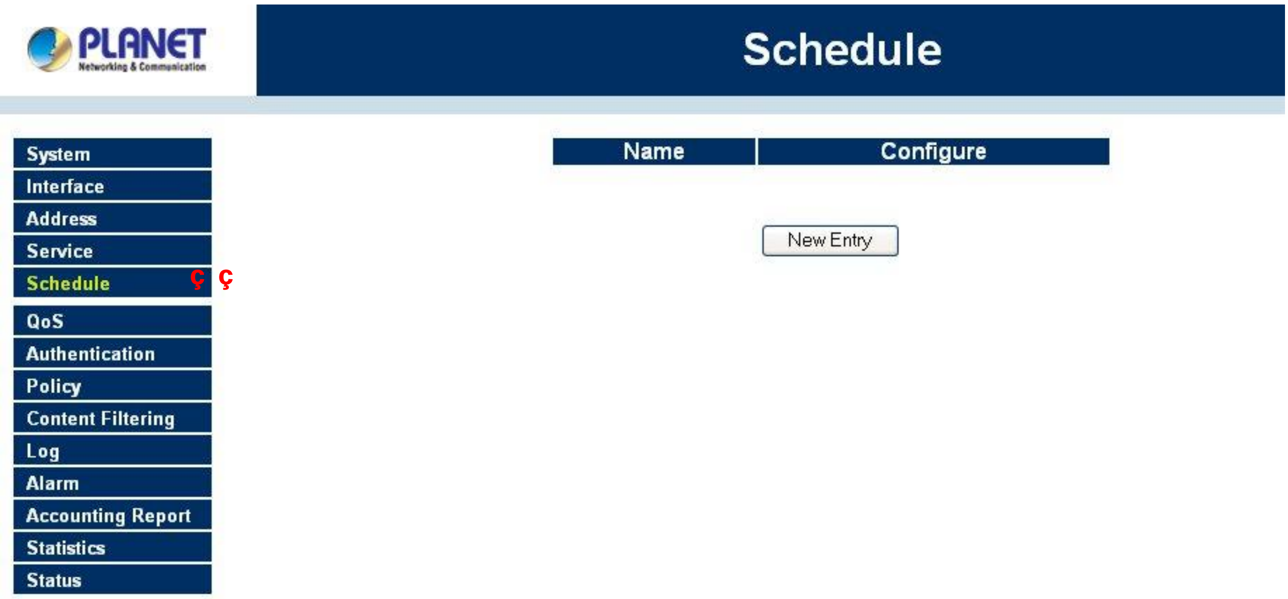
Do you really want to delete?

4.5 Schedule

The Bandwidth Management Gateway allows the Administrator to configure a schedule for policies to take affect. By creating a schedule, the Administrator is allowing the Bandwidth Management Gateway policies to be used at those designated times only. Any activities outside of the scheduled time slot will not follow the Bandwidth Management Gateway policies therefore will likely not be permitted to pass through the Bandwidth Management Gateway. The Administrator can configure the start time and stop time, as well as creating 2 different time periods in a day. For example, an organization may only want the Bandwidth Management Gateway to allow the LAN network users to access the Internet during work hours. Therefore, the Administrator may create a schedule to allow the Bandwidth Management Gateway to work Monday-Friday, 8AM - 5PM only. During the non-work hours, the Bandwidth Management Gateway will not allow Internet access.

Accessing the Schedule window

Step 1. Click on **Schedule** on the menu bar and the schedule window will appear displaying the active schedules.



The following items are displayed in this window:

Name: the name assigned to the schedule

Comment: a short comment describing the schedule

Configure: modify or remove

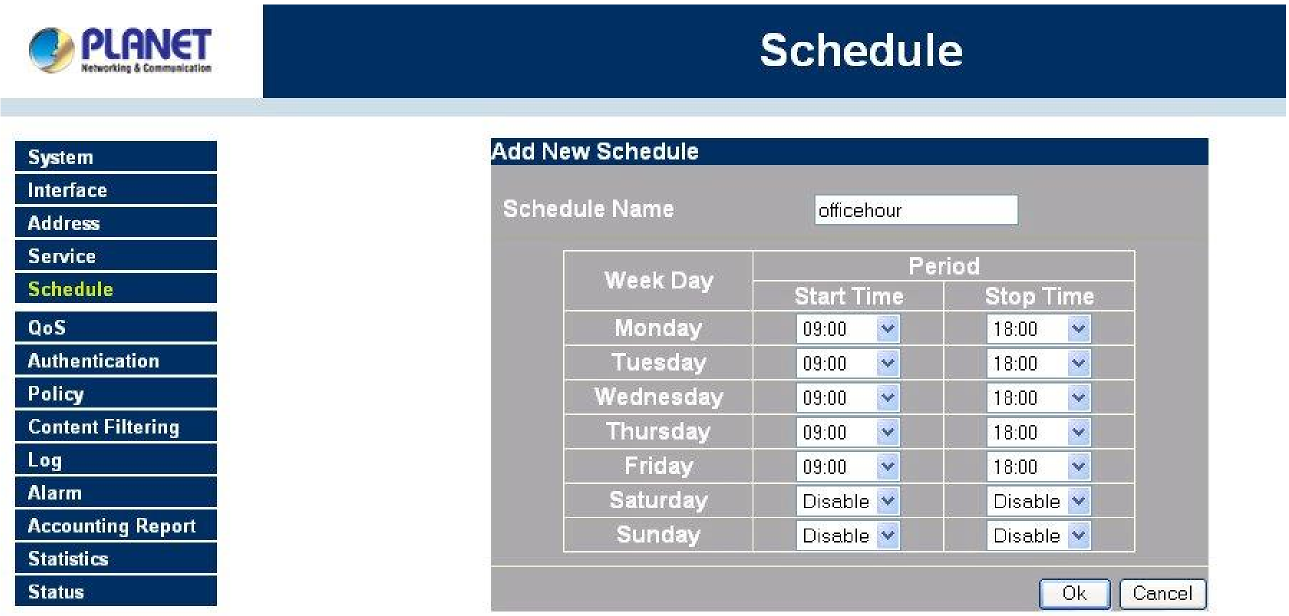
Adding a new Schedule

Step 1. Click on the **New Entry** button and the **Add New Schedule** window will appear.

n **Schedule Name:** Fill in a name for the new schedule.

n **Period 1:** Configure the start and stop time for the days of the week that the schedule will be active.

Step 2. Click **OK** to save the new schedule or click Cancel to cancel adding the new schedule.



Add New Schedule

Schedule Name: officehour

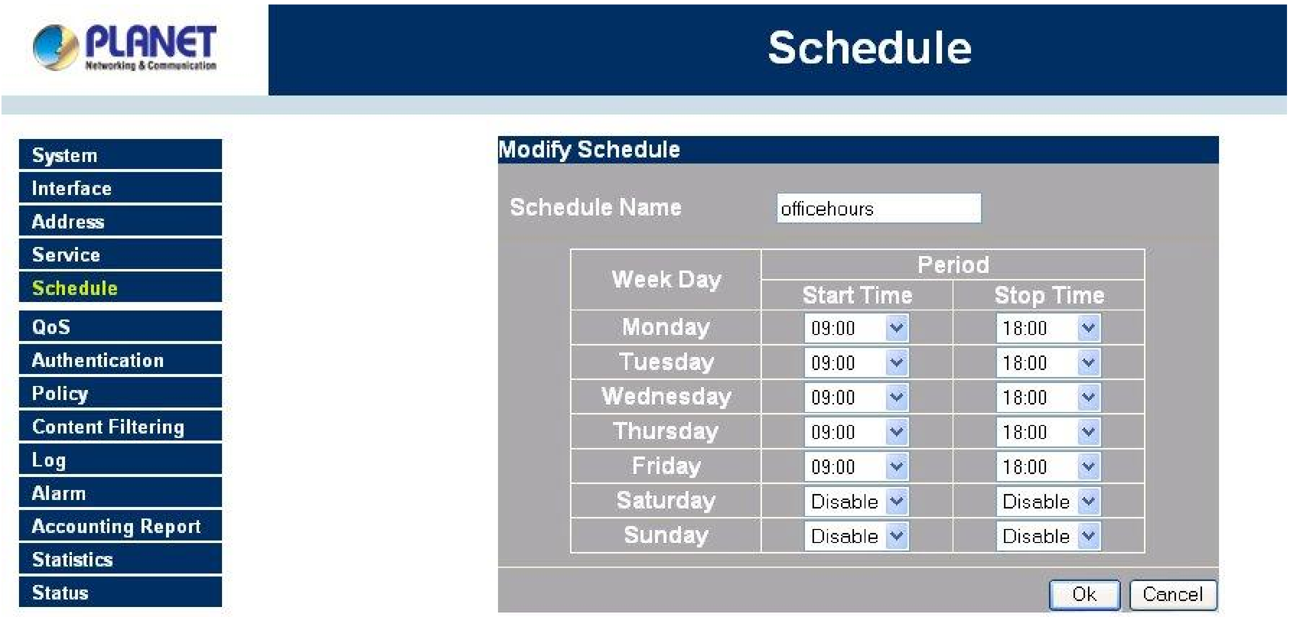
Week Day	Period	
	Start Time	Stop Time
Monday	09:00	18:00
Tuesday	09:00	18:00
Wednesday	09:00	18:00
Thursday	09:00	18:00
Friday	09:00	18:00
Saturday	Disable	Disable
Sunday	Disable	Disable

NOTE: In setting a Schedule, the value in **Start time** must be less than the value in **Stop Time**, or you cannot add or configure the setting.

Modifying a Schedule

Step 1. In the **Schedule** window, find the policy to be modified and click the corresponding **Modify** option in the **Configure** field. Make needed changes.

Step 2. Click **OK** to save changes.



Modify Schedule

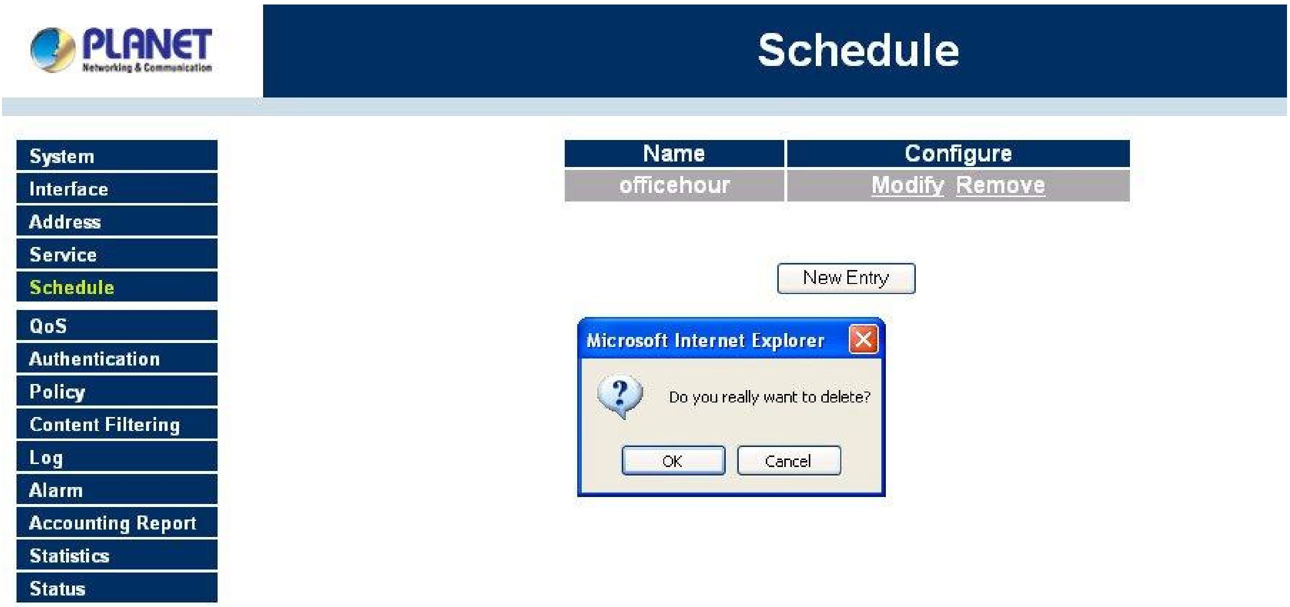
Schedule Name: officehours

Week Day	Period	
	Start Time	Stop Time
Monday	09:00	18:00
Tuesday	09:00	18:00
Wednesday	09:00	18:00
Thursday	09:00	18:00
Friday	09:00	18:00
Saturday	Disable	Disable
Sunday	Disable	Disable

Removing a Schedule

Step 1. In the **Schedule** window, find the policy to be removed and click the corresponding **Remove** option in the **Configure** field.

Step 2. A confirmation pop-up box will appear, click on **OK** to remove the schedule.



Name	Configure
officehour	Modify Remove

Do you really want to delete?

4.6 QoS

By configuring the QoS, you can control the outbound Upstream/downstream Bandwidth.

The administrator can configure the bandwidth according to the WAN bandwidth.

Downstream Bandwidth: To configure the Guaranteed Bandwidth and Maximum Bandwidth.

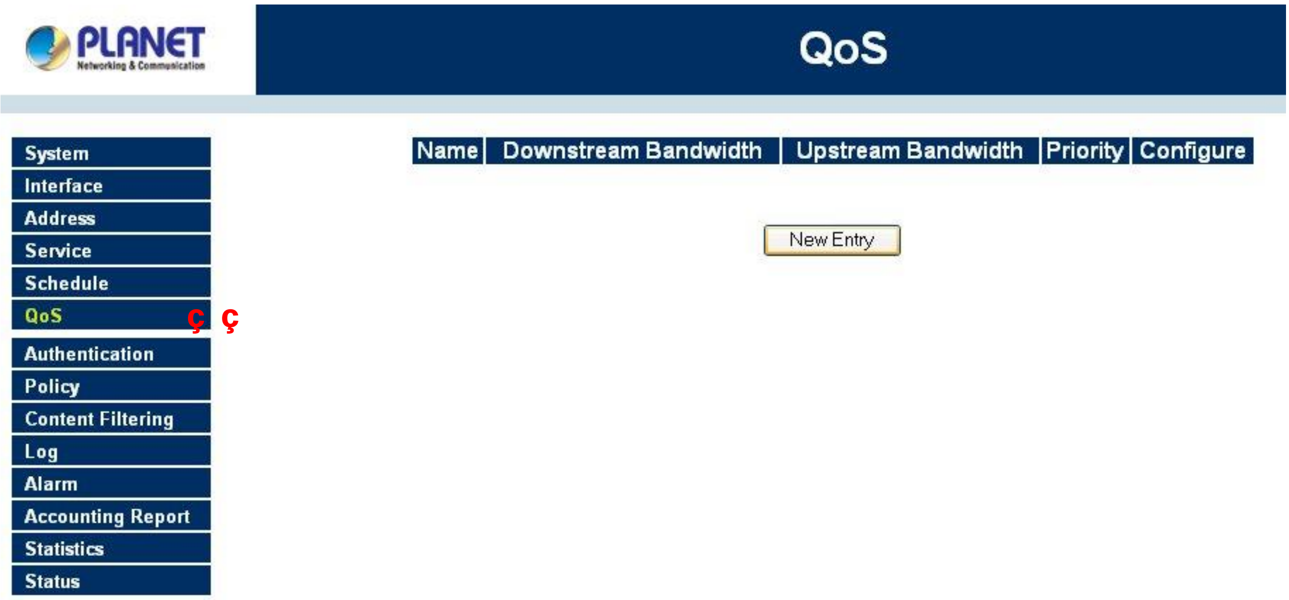
Upstream Bandwidth: To configure the Guaranteed Bandwidth and Maximum Bandwidth.

QoS Priority: To configure the priority of distributing Upstream/Downstream and unused bandwidth.

The Bandwidth Management Gateway configures the bandwidth by different QoS , and selects the suitable QoS through Policy to control and efficiently distribute bandwidth. The Bandwidth Management Gateway also makes it convenient for the administrator to use the Bandwidth Management Gateway with the best Utility.

Configuration of QoS

Click QoS in the menu bar on the left hand side.



Definitions:

Name: The name of the QoS you want to configure.

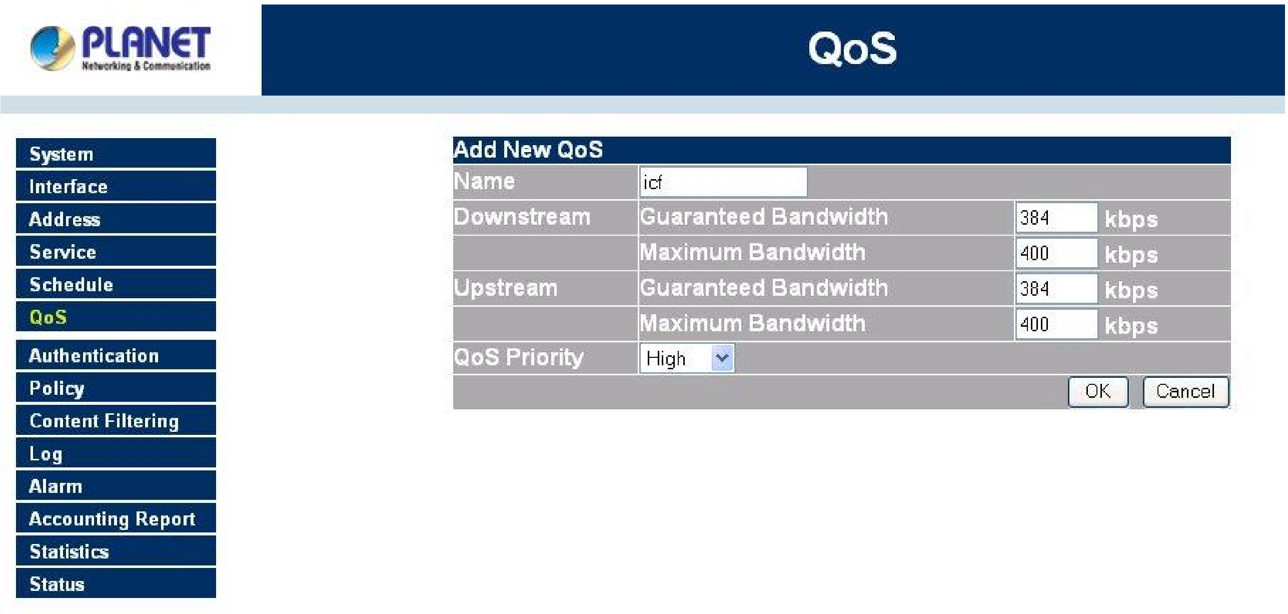
Downstream Bandwidth: To configure the Guaranteed Bandwidth and Maximum Bandwidth.

Upstream Bandwidth: To configure the Guaranteed Bandwidth and Maximum Bandwidth.

QoS Priority: To configure the priority of distributing Upstream/Downstream and unused bandwidth.

Add New QoS

Step 1. Click QoS in the menu bar on the left hand side.



Add New QoS			
Name	icf		
Downstream	Guaranteed Bandwidth	384	kbps
	Maximum Bandwidth	400	kbps
Upstream	Guaranteed Bandwidth	384	kbps
	Maximum Bandwidth	400	kbps
QoS Priority	High		

Step 2. Click the **New Entry** button to add new QoS.

Definition

Name: The name of the QoS you want to configure.

Downstream Bandwidth**: To configure the Guarateed Bandwidth and Maximum Bandwidth.**

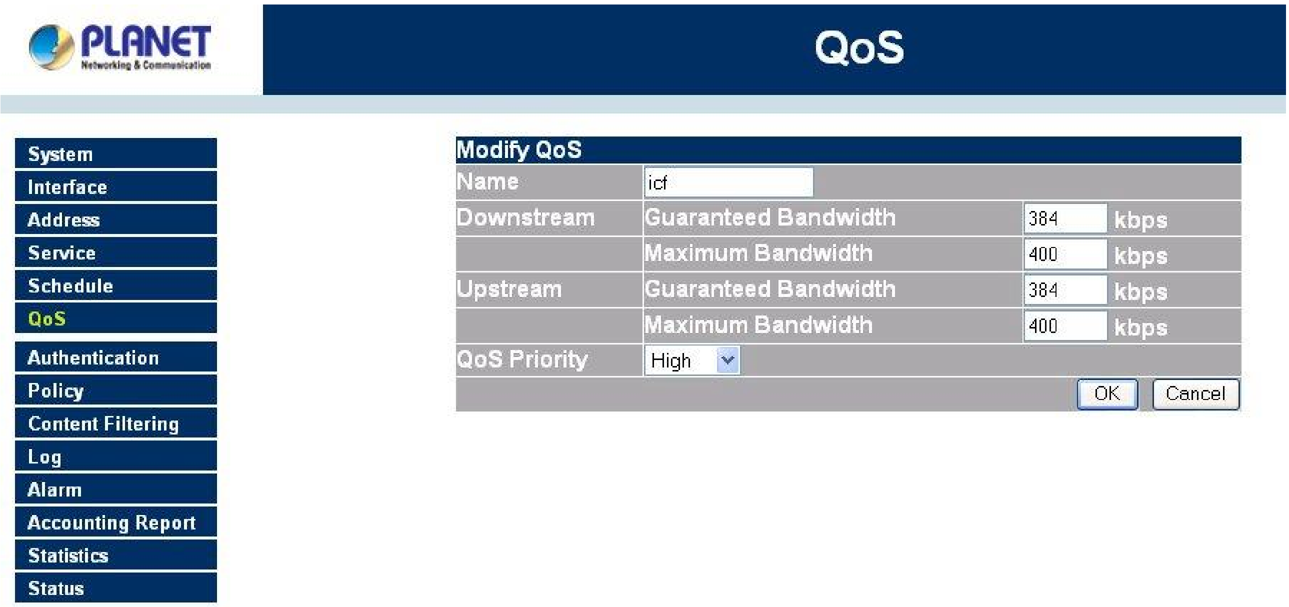
Upstream Bandwidth**: To configure the Guarateed Bandwidth and Maximum Bandwidth.**

QoS Priority**: To configure the priority of distrubuting Upstream/Downstream and unused bandwidth.**

Click the **OK** button to add new QoS.

Modify QoS

Step 1. Click QoS in the menu bar on the left hand side.



Modify QoS

Name	icf		
Downstream	Guaranteed Bandwidth	384	kbps
	Maximum Bandwidth	400	kbps
Upstream	Guaranteed Bandwidth	384	kbps
	Maximum Bandwidth	400	kbps
QoS Priority	High		

Click the Modify button to modify QoS.

Definition:

Name: The name of the QoS you want to configure.

Downstream Bandwidth: To configure the Guarateed Bandwidth and Maximum Bandwidth.

Upstream Bandwidth: To configure the Guarateed Bandwidth and Maximum Bandwidth.

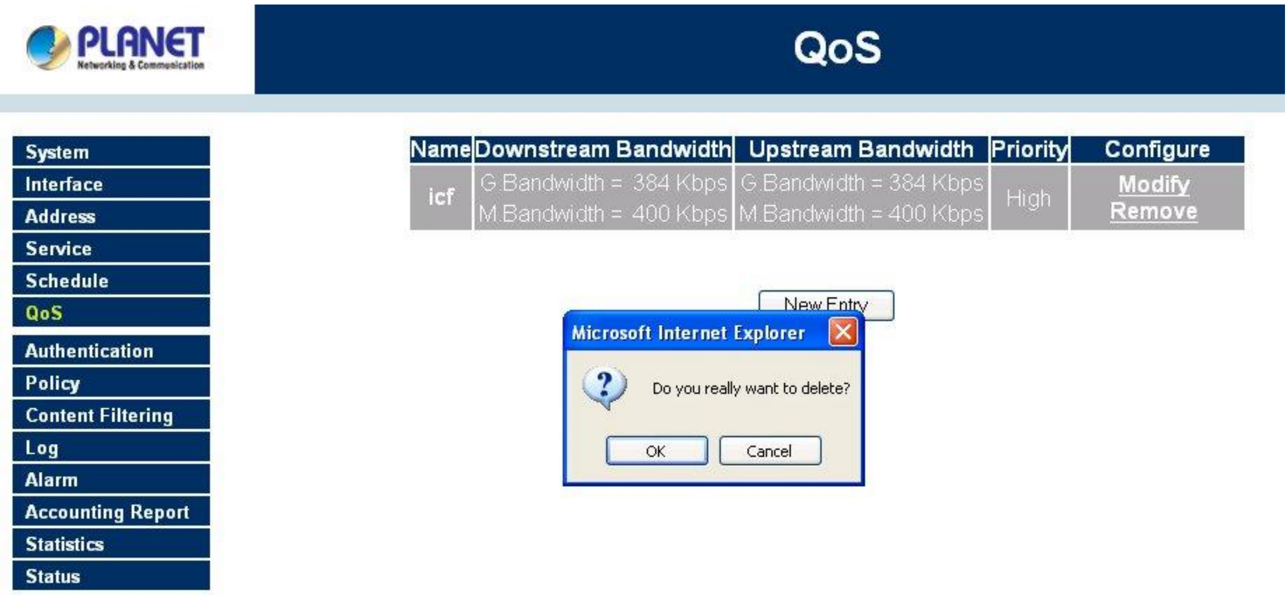
QoS Priority: To configure the priority of distrubuting Upstream/Downstream and unused bandwidth.

Click the **OK** button to modify QoS.

Delete QoS

Step 1. In the QoS window, find the QoS you want to change, and click **Delete** in the Configure column.

Step 2. In the Delete QoS window, click **OK** to delete the QoS or click Cancel to discard the change.



Name	Downstream Bandwidth	Upstream Bandwidth	Priority	Configure

icf	G.Bandwidth = 384 Kbps
	M.Bandwidth = 400 Kbps
		G.Bandwidth = 384 Kbps
		M.Bandwidth = 400 Kbps
			High	Modify
				Remove

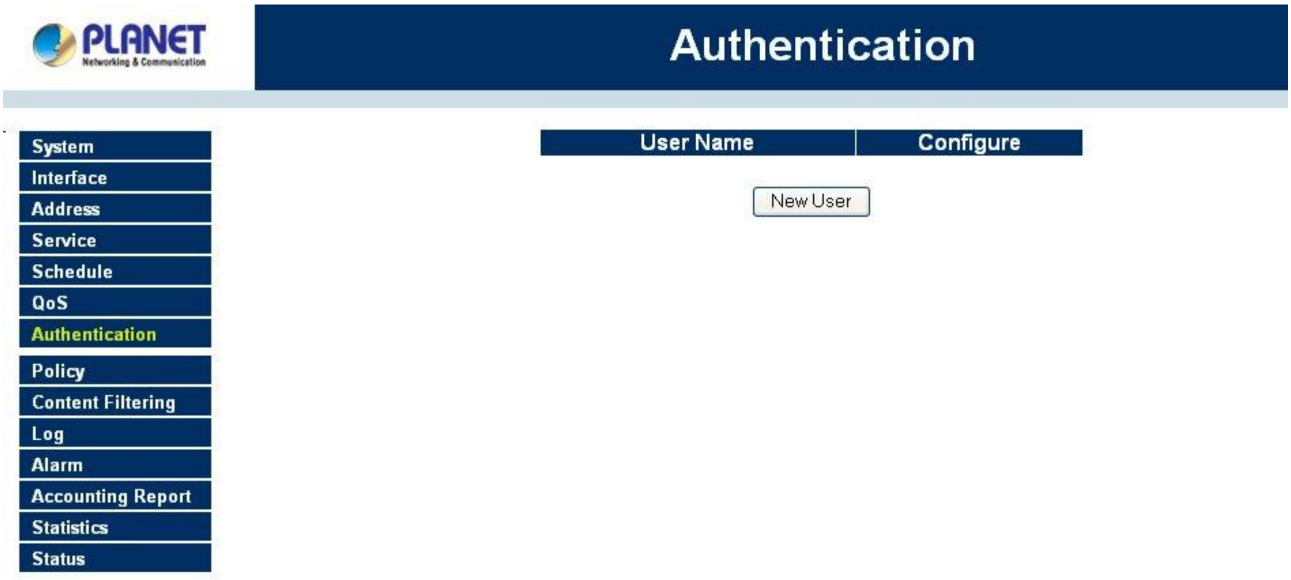
Do you really want to delete?

4.7 Authentication

By configuring the Authentication, you can control the user's access right time of LAN to WAN. The administrator can configure the authentication according to the authentication account and password.
The Bandwidth Management Gateway configures the authentication of LAN's user by setting account and password to identify the privilege.

Configuration of Authentication

Click Authentication in the menu bar on the left hand side.



Definitions:
User Name: The name of the authentication user you want to configure.
Configure: modify settings or remove the user account.

Adding a new Auth User

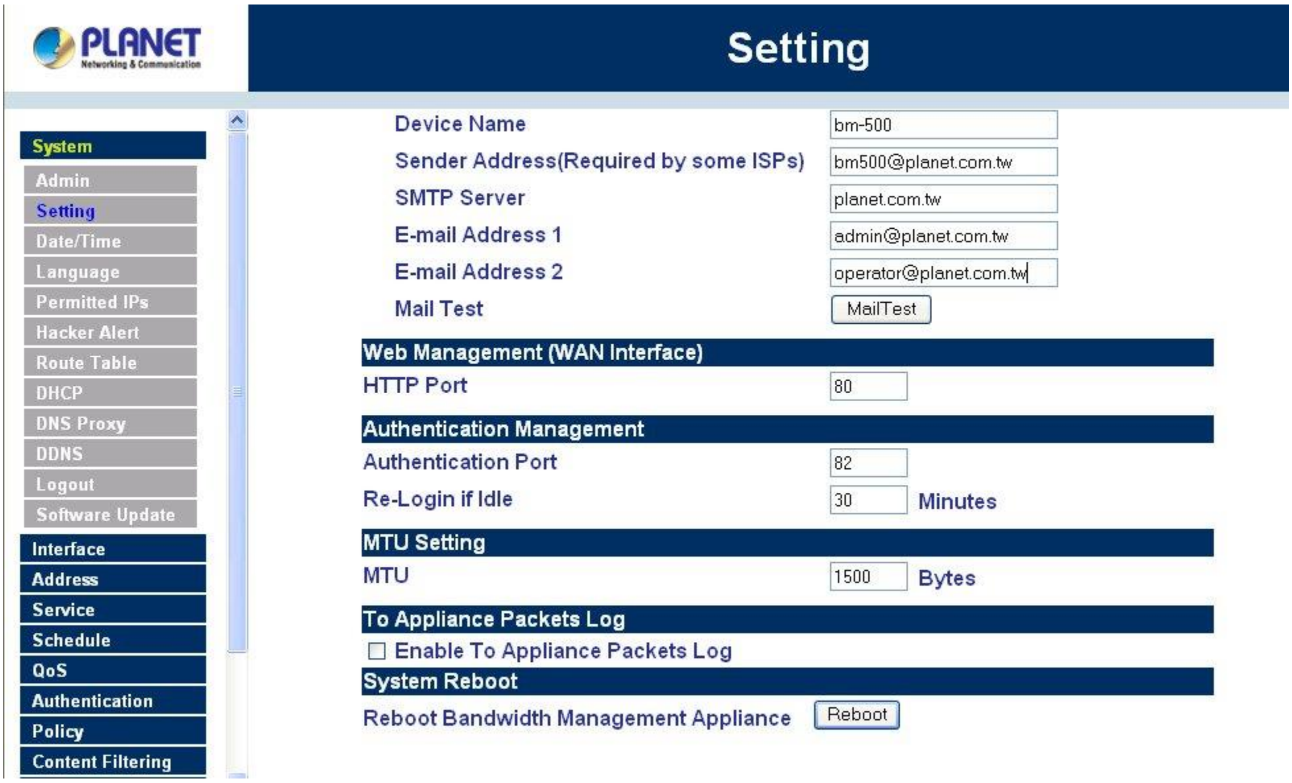
Step 1. In the **Authentication** window, click the **New User** button to create a new **Authentication.**

Step 2. In the **Add New User** window:

- **User Name:** enter the username of new **Authentication.**
- **Password:** enter a password for the new **Authentication.**
- **Confirm Password:** enter the password again.

Step 3. Click **OK** to add the user or click **Cancel** to cancel the addition.

NOTE*:* When the LAN user access to WAN network and do not use for a while, the connection will be time-out. User has to re-login again. The default time is 30 minutes and you can configure this time by "System"-> "Setting" page.



Setting

Device Name: bm-500
Sender Address(Required by some ISPs): bm500@planet.com.tw
SMTP Server: planet.com.tw
E-mail Address 1: admin@planet.com.tw
E-mail Address 2: operator@planet.com.tw
Mail Test: MailTest

Web Management (WAN Interface)
HTTP Port: 80

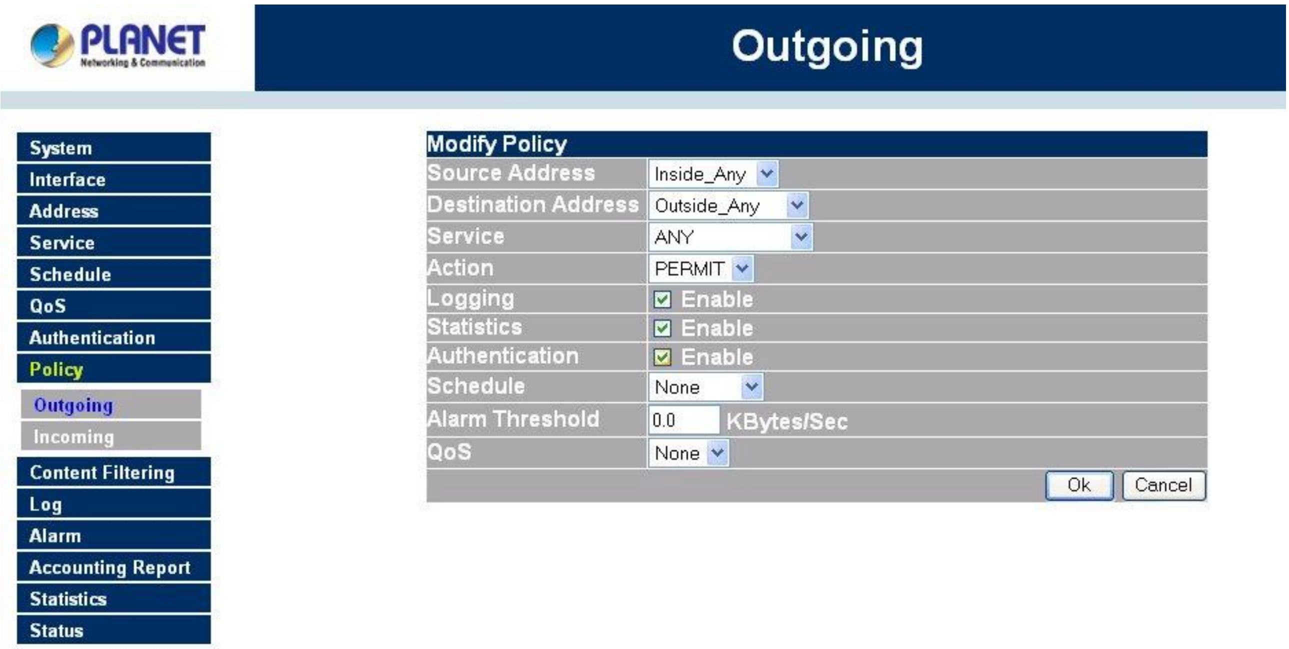
Authentication Management
Authentication Port: 82
Re-Login if Idle: 30 Minutes

MTU Setting
MTU: 1500 Bytes

To Appliance Packets Log
□ Enable To Appliance Packets Log

System Reboot
Reboot Bandwidth Management Appliance: Reboot

In the form of controlling the [Outgoing] Policy, enable the Authentication-User Function.



Outgoing

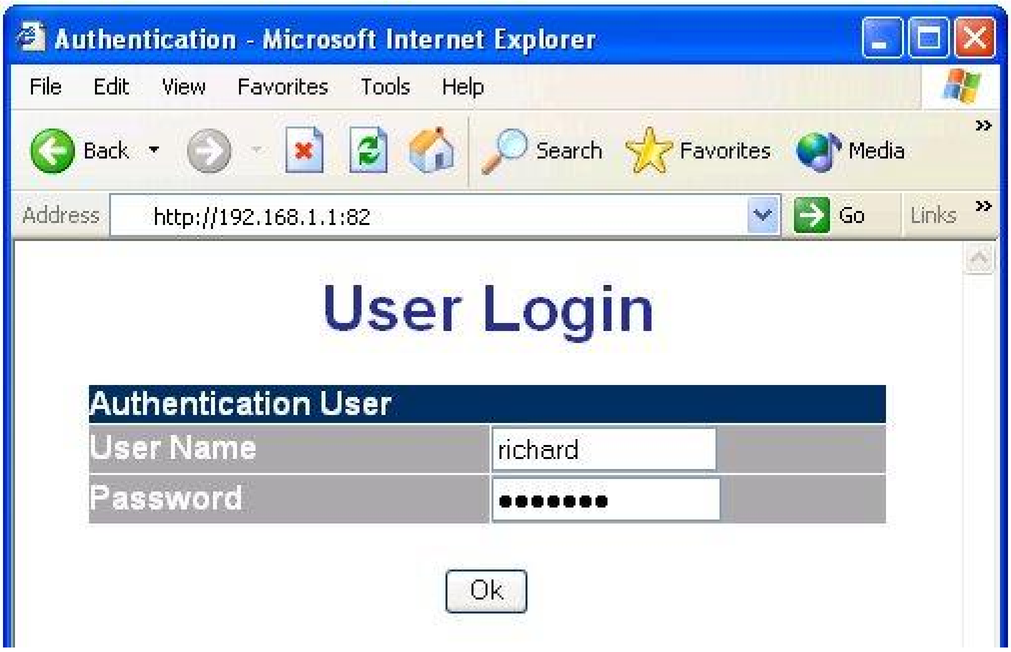
Modify Policy
Source Address: Inside_Any
Destination Address: Outside_Any
Service: ANY
Action: PERMIT
Logging: ☑ Enable
Statistics: ☑ Enable
Authentication: ☑ Enable
Schedule: None
Alarm Threshold: 0.0 KBytes/Sec
QoS: None

When the user's idle time exceed the "Re-Login If Idle" time and the user wan to connect to WAN, the authentication web page will be shown again or user need to manually input the login page. Once user enters the correct user name and password, he can access the WAN resource again.

User Login Page Definitions:

n **User Name**: The name of the Authentication you want to configure.

n **Password**: The input carries on the authentication the password



Address: http://192.168.1.1:82

User Login

Authentication User	
User Name	richard
Password	●●●●●●●●

Ok

Modifying the Authentication User

Step 1. In the **Authentication** window, locate the User name you want to edit, and click on **Modify** in the **Configure** field.

Step 2. The **Modify Auth-User Password** window will appear. Enter in the required information:

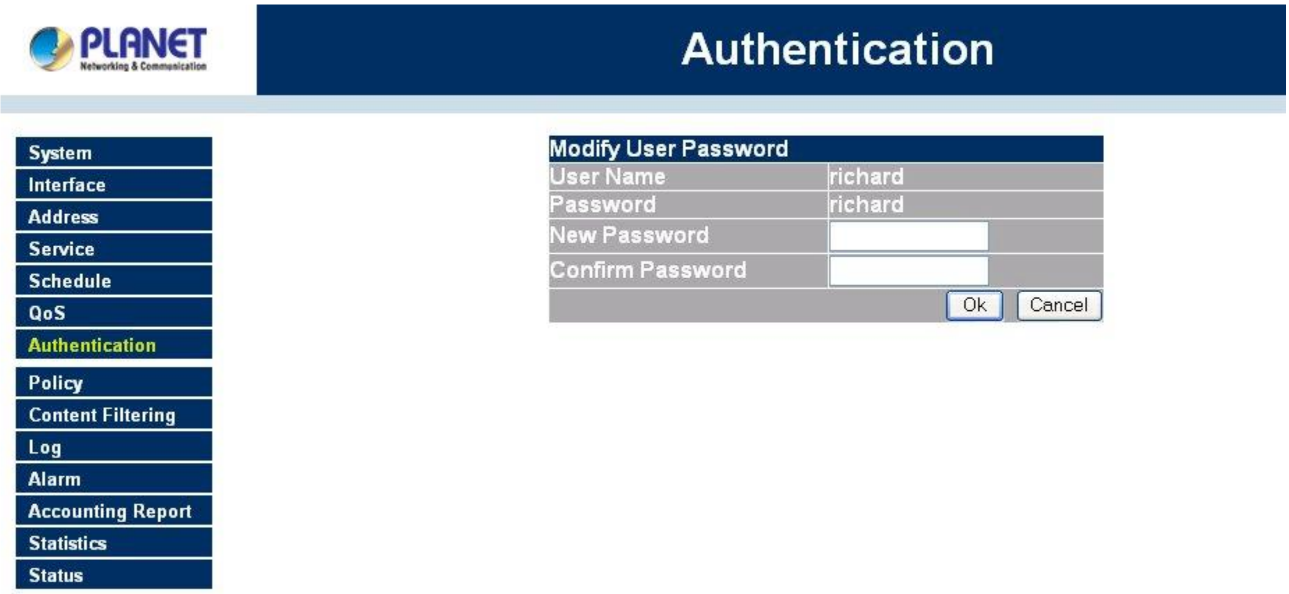
n **Auth-User:** show original authentication user.

n **Password:** show original password.

n **New Password:** enter new password

n **Confirm Password:** enter the new password again.

Step 3. Click **OK** to confirm authentication user change or click **Cancel** to cancel it.



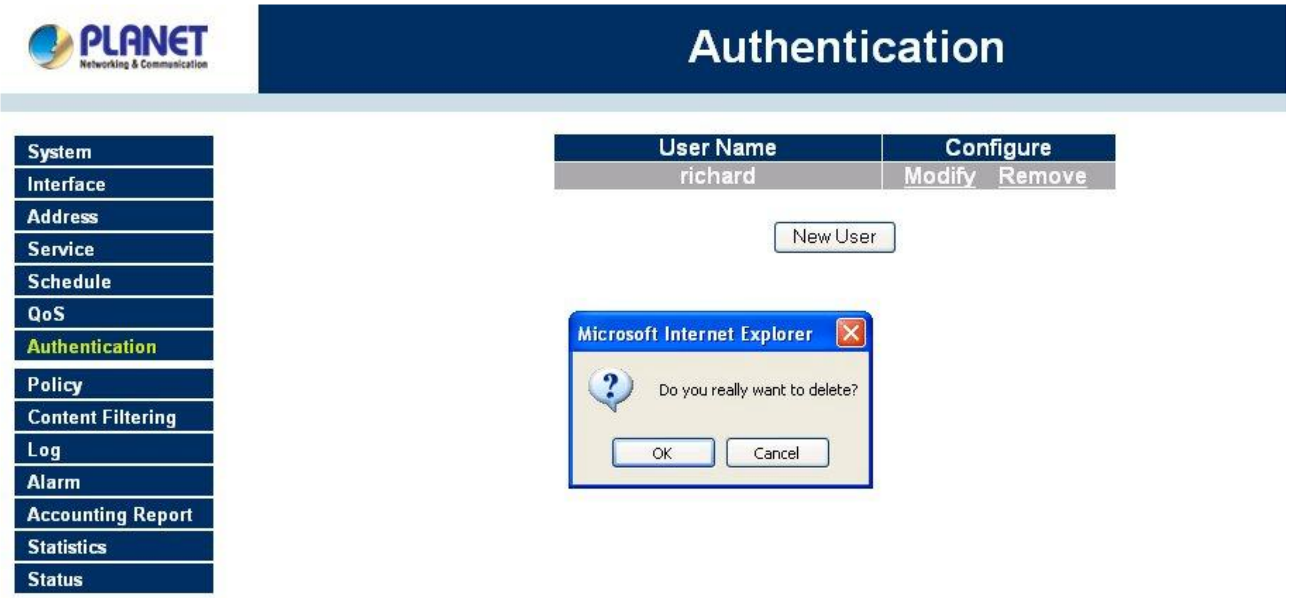
Modify User Password	
User Name	richard
Password	richard
New Password	
Confirm Password	

Removing a Authentication User

Step 1. In the Authentication table, locate the user name you want to remove, and click on the Remove option in the Configure field.

Step 2. The Remove confirmation pop-up box will appear.

Step 3. Click **OK** to remove that Authentication User or click **Cancel** to cancel.



User Name	Configure
richard	Modify Remove

Do you really want to delete?

4.8 Policy

This section provides the Administrator with facilities to sent control policies for packets with different source IP addresses, source ports, destination IP addresses, and destination ports. Control policies decide whether packets from different network objects, network services, and applications are able to pass through the Bandwidth Management Gateway.

What is Policy?

The device uses policies to filter packets. The policy settings are: source address, destination address, services, permission, packet log, packet statistics, and flow alarm. Based on its source addresses, a packet can be categorized into:

(1) Outgoing: a client is in the LAN networks, while a server is in the WAN networks.

(2) Incoming, a client is in the WAN networks, while a server is in the LAN networks.

How do I use Policy?

The policy settings are source addresses, destination addresses, services, permission, log, statistics, and flow alarm. Among them, source addresses, destination addresses and IP mapping addresses have to be defined in the **Address** menu in advance. Services can be used directly in setting up policies, if they are in the Pre-defined Service menu. Custom services need to be defined in the **Custom** menu before they can be used in the policy settings.

If the destination address of an incoming policy is a Mapped IP address or a Virtual Server address, then the address has to be defined in the **Virtual Server** section instead of the **Address** section.

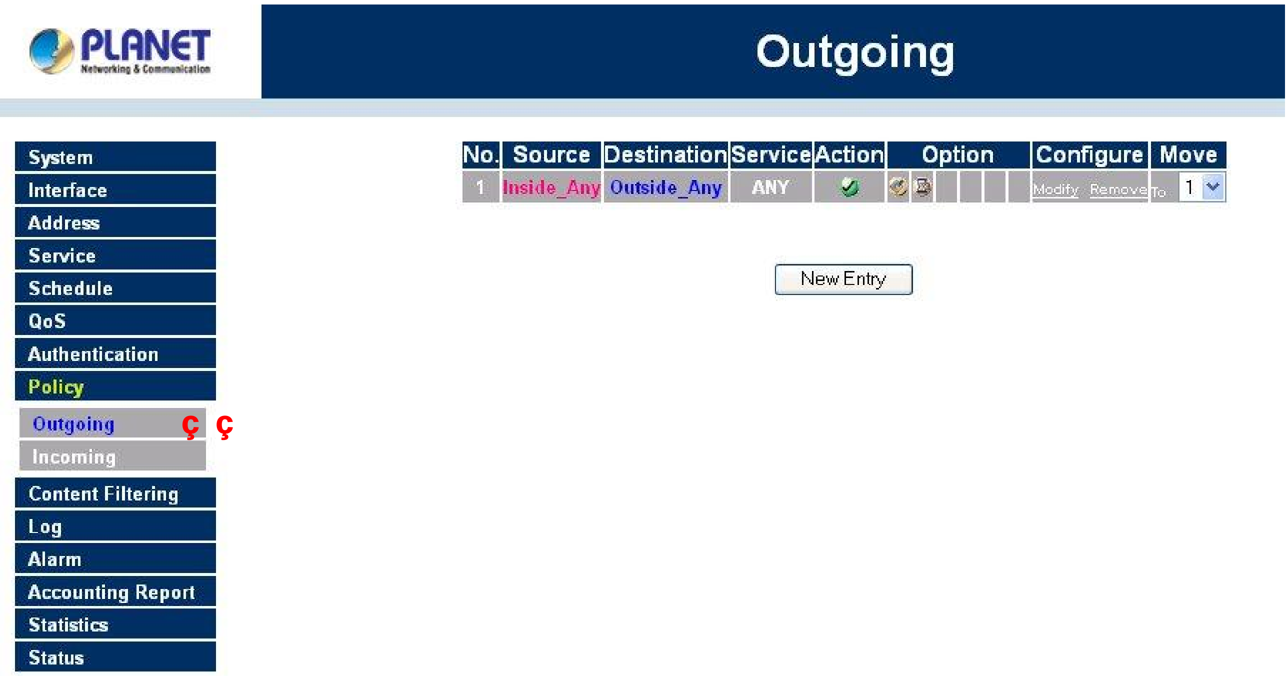
4.8.1 Outgoing

This section describes steps to create policies for packets and services from the LAN network to the WAN network.

Entering the Outgoing window

Step 1. Click **Policy** on the left hand side menu bar,

Step 2. Click **Outgoing** under it. A window will appear with a table displaying currently defined Outgoing policies.



No.	Source	Destination	Service	Action	Option	Configure	Move
1	Inside_Any	Outside_Any	ANY	✓		Modify Remove	To 1

The fields in the Outgoing window are:

n **Source**: source network addresses that are specified in the LAN section of Address menu, or all the LAN network addresses.

n **Destination**: destination network addresses that are specified in the WAN section of the Address menu, or all of the WAN network addresses.

n **Service**: specify services provided by WAN network servers.

n **Action**: control actions to permit or reject/deny packets from LAN networks to WAN network travelling through the Bandwidth Management Gateway.

n **Option**: specify the monitoring functions on packets from LAN networks to WAN networks travelling through the Bandwidth Management Gateway.

n **Configure**: modify settings.

n **Move**: this sets the priority of the policies, number 1 being the highest priority.

Descriptions for **Policy** figures:

Figure	Name	Description
✓	Permit	Permit the specified packets from LAN network to WAN network.
✗	Block	Block the specified packets from LAN network to WAN network.
✎	Log	Traffic and event log function is enabled.
📊	Statistics	Flow statistics function is enabled.
⏰	Schedule	The automatic execution function in Schedule table has been enabled.

	Alarm Threshold	Traffic and event alarm function is enabled.
	QoS	QoS function is enabled.

Remarks:

To view the traffic and event log of the system, click **Log** function in the menu bar on the left hand side.

To view the alarm records of the system, click **Alarm** function in the menu bar on the left hand side.

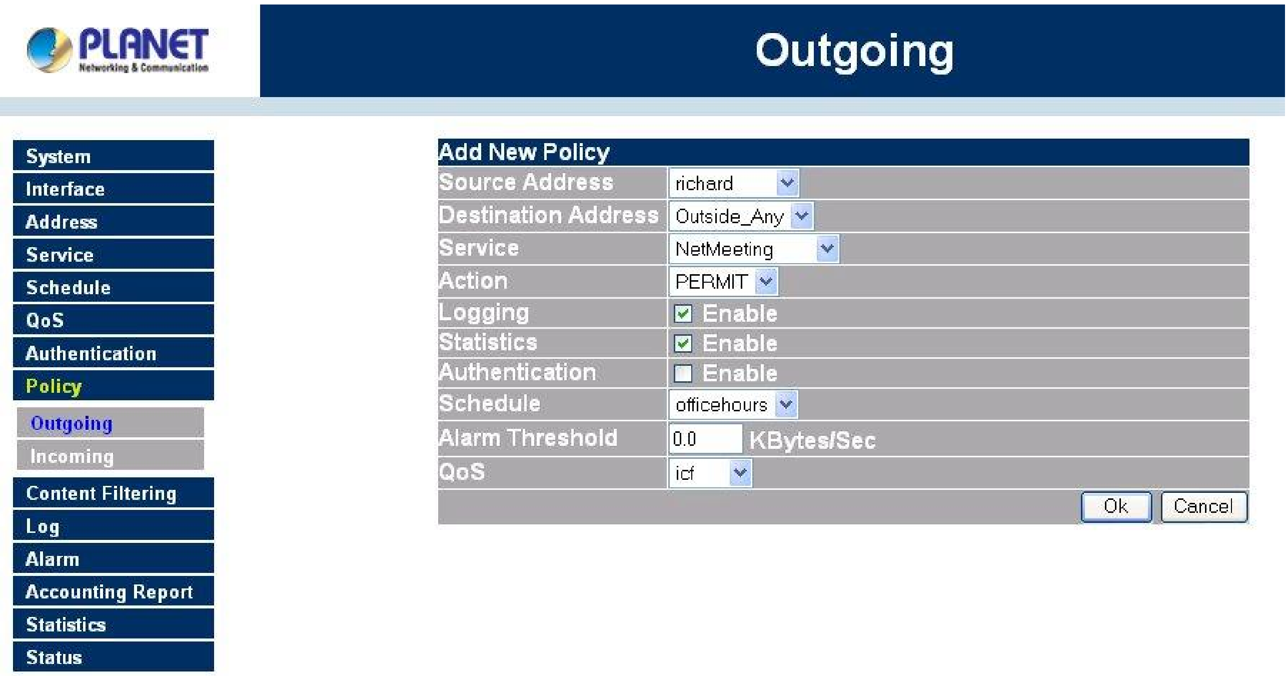
To view the statistics of the system, click **Statistics** function in the menu bar on the left hand side.

Bandwidth Management Gateway can execute the schedule function automatically in a certain time and range. To modify the schedule, click the **Schedule** function in the menu baron the left hand side.

Bandwidth Management Gateway can execute the QoS function function automatically. To modify the QoS, click the **QoS** function in the menu bar on the left hand side.

Adding a new Outgoing Policy

Click on the New Entry button and the Add New Policy window will appear.



Add New Policy

Source Address	richard
Destination Address	Outside_Any
Service	NetMeeting
Action	PERMIT
Logging	☑ Enable
Statistics	☑ Enable
Authentication	□ Enable
Schedule	officehours
Alarm Threshold	0.0 KBytes/Sec
QoS	icf

Source Address: Select the name of the LAN network from the drop down list. The drop down list contains the names of all LAN networks defined in the LAN section of the **Address** menu. To create a new source address, please go to the LAN section under the **Address** menu.

Destination Address: Select the name of the WANnetwork from the drop down list. The drop down list contains the names of all WAN networks defined in the **WAN**section of the **Address** window. To create a new destination address, please go to the **WAN**section under the **Address** menu.

Service: Specified services provided by WANnetwork servers. These are srvices/application that are allowed to pass from the LAN network to the WANnetwork. Choose ANY for all services.

Action: Select Permit or Deny from the drop down list to allow or reject the packets travelling between the source network and the destination network.

Logging: Select Enable to enable flow monitoring.

Statistics: Select Enable to enable flow statistics.

Schedule: Select the pre-defined schedule name from the pull-up menu. The policy will be executed in the specific time slot automatically.

Alarm Threshold: set a maximum flow rate (in Kbytes/Sec). An alarm will be sent if flow rates are higher than the specified value.

QoS: To determine if the QoS function can work in this Policy function.

Click **OK** to add a new outgoing policy; or click **Cancel** to cancel adding a new outgoing policy.

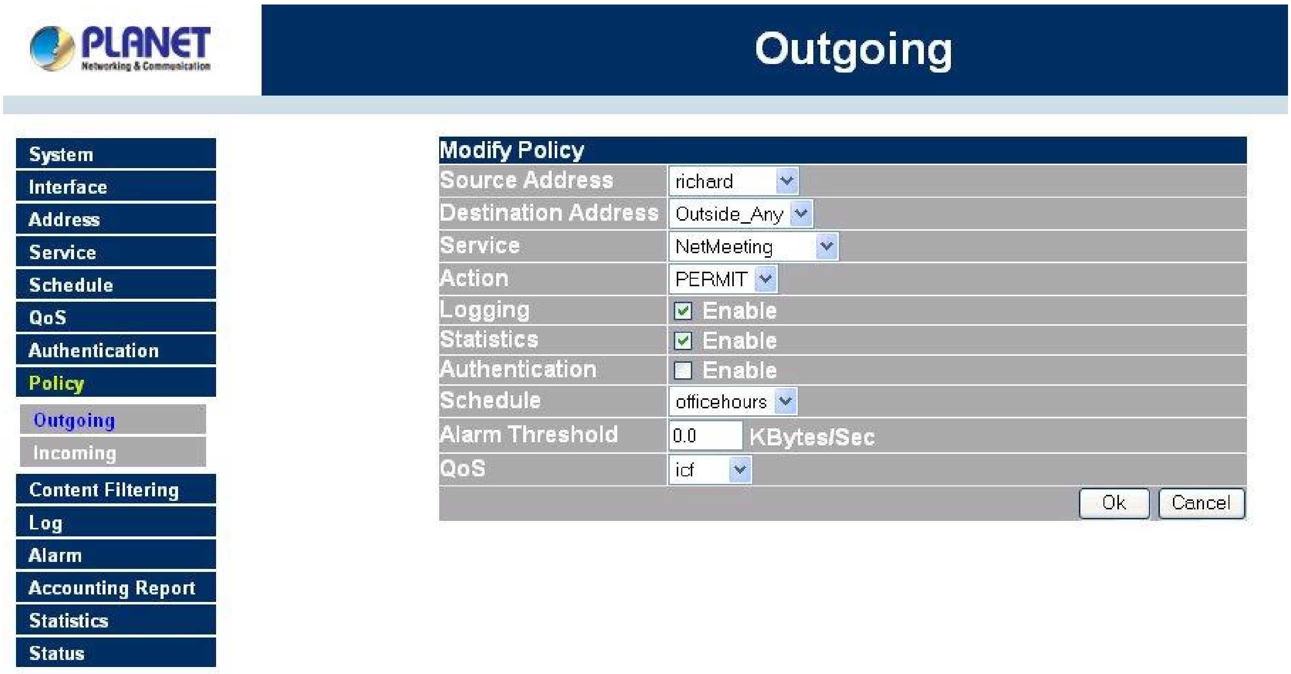
To change the Policy order of **Outgoing**, select the number from the pull-down menu on the right hand side **Move** column

Modifying an Outgoing policy

Step 1. In the **Modify Policy** window, fill in new settings.

NOTE: To change or add selections in the drop-down list for source or destination address, go to the section where the selections are setup. (Source Address→LAN of **Address** menu; Destination Address → WAN of **Address** menu; Service→[Pre-defined],[Custom] or Group under **Service**).

Click **OK** to do confirm modification or click **Cancel** to cancel it.



Modify Policy

Source Address	richard
Destination Address	Outside_Any
Service	NetMeeting
Action	PERMIT
Logging	☑ Enable
Statistics	☑ Enable
Authentication	□ Enable
Schedule	officehours
Alarm Threshold	0.0 KBytes/Sec
QoS	icf

Ok Cancel

Source Address: Select the name of LAN from the pull-down menu.

The names of LAN listed in this pull-down menu are: the Source Addresses that are already set.

Destination Address: Select the name of WAN from the pull-down menu.

The names of WAN listed in this pull-down menu are: the Destination Addresses that are already set IP address of WAN network.

Service: Select the service item from the pull-down menu

Action: Select Permit or Block to allow or reject the specified packets from LAN network to WAN network.

Logging: Select **Enable** to enable the Logging function.

Statistics: Select **Enable** to enable the Statistics function.

Schedule: Select the item listed in the schedule to enable the policy to automatically execute the function in a certain time and range.

Alarm Threshold: To set the maximum value of transmitting and receiving packet, enter the number based on the unit（KBytes/Sec）

QoS: To determine if the QoS function can work in this Policy function.

Click **OK** to execute the new setting or click **Cancel** to discard changes.

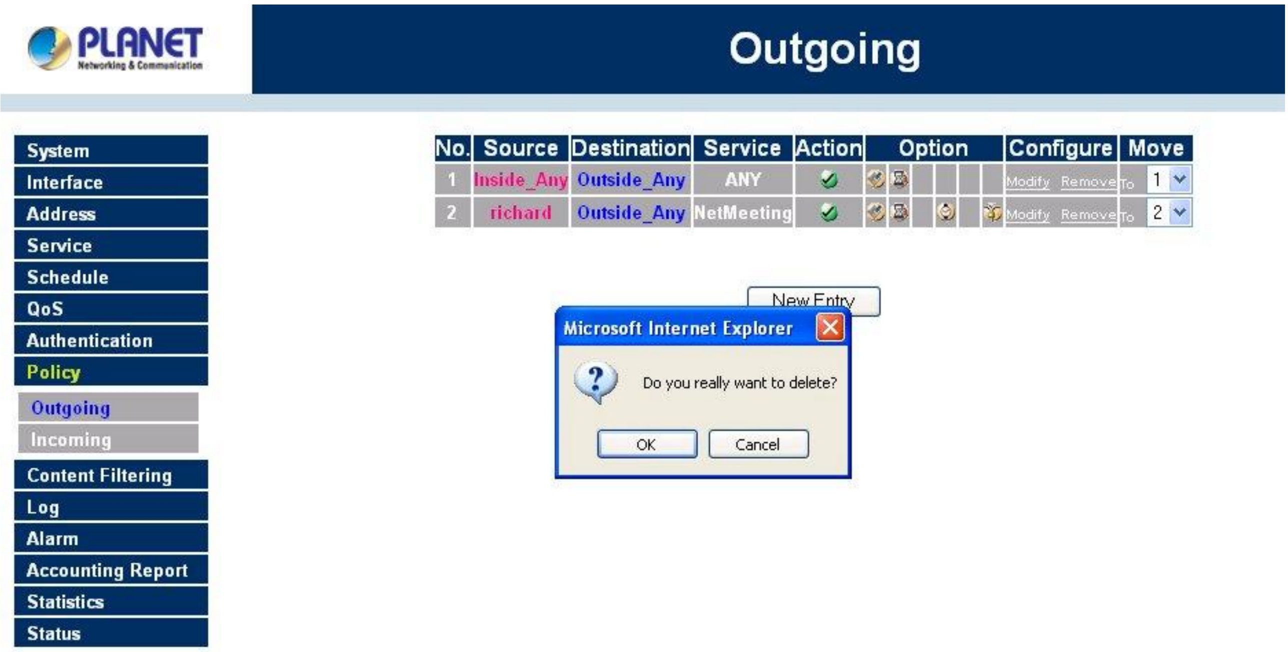
NOTE: If you want to change or add new items in the pull-down menu, go to the corresponding chapter for setup.

Source Address: **LAN** of **Address** menu

Destination Address: **WAN** of **Address** menu

Removing the Outgoing Policy

Step 1. In the **Remove** confirmation dialogue box, click **OK** to remove the policy or click **Cancel** to cancel removing.



No.	Source	Destination	Service	Action	Option	Configure	Move
1	Inside_Any	Outside_Any	ANY	✓		Modify Remove	To 1
2	richard	Outside_Any	NetMeeting	✓		Modify Remove	To 2

Microsoft Internet Explorer

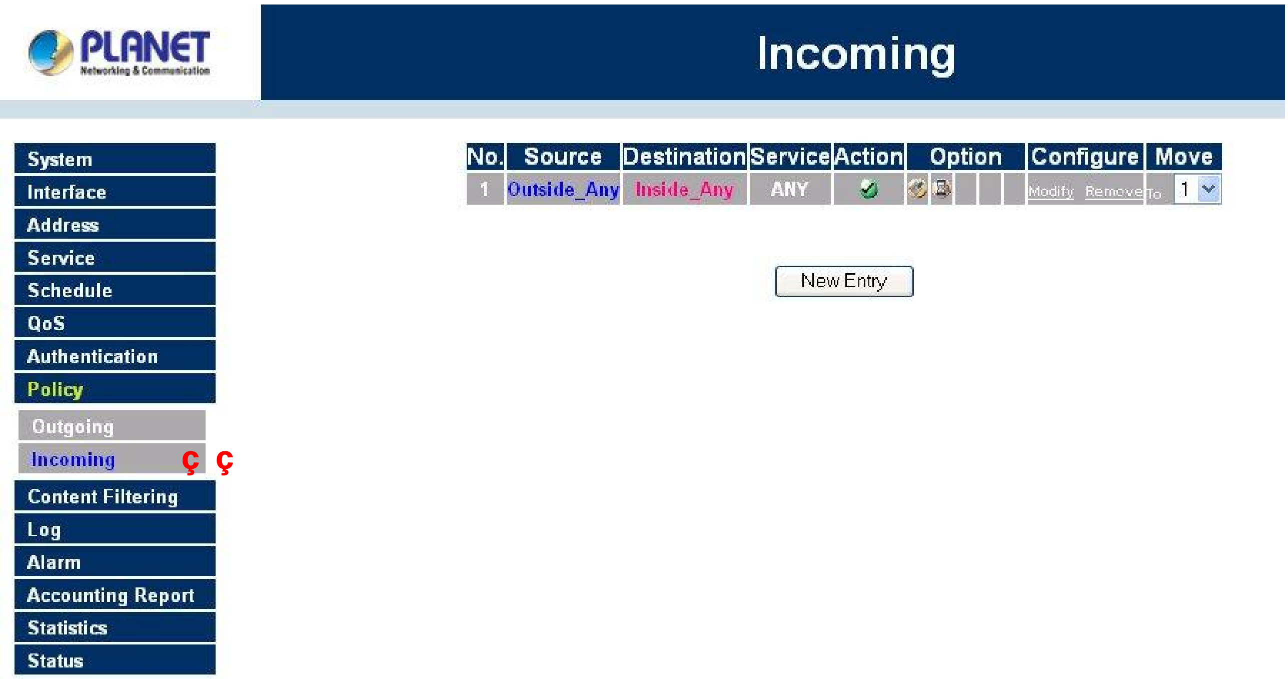
Do you really want to delete?

4.8.2 Incoming

This chapter describes steps to create policies for packets and services from the WAN network to the LAN network including Mapped IP and Virtual Server.

Enter Incoming window

Step 1. Click **Incoming** under the **Policy** menu to enter the Incoming window. The Incoming table will display current defined policies from the WAN network to assigned Mapped IP or Virtual Server.



No.	Source	Destination	Service	Action	Option					Configure		Move
1	Outside_Any	Inside_Any	ANY	✓						Modify	Remove	To 1

Definition (Incoming):

No.: The numbering of the selected Policy, starting with Number 1.

Source Address: The WAN address was selected in WAN function of the Address Table.

Destination Address: The mapped IP or Virtual Server IP configured in the Mapped IP or Virtual Server 1/2/3/4 window under Virtual Server function.

Service: The service item provided by **Virtual Server** (or **Mapped IP**).

Action: Control actions to permit or reject packets from LAN networks to WAN network or Virtual Server (Mapped IP) traveling through the Bandwidth Management Gateway.

Option: Control actions to monitor packets from WAN network or Virtual Server (Mapped IP) traveling through the Bandwidth Management Gateway. The first column is the **logging** function. The second column is the **Statistics** function. The third column is the **Schedule** function. The fourth column is the **Alarm Threshold** function. The fifth column is the **QoS** function. If the figures appear in the column, it means that the function is enabled. On the other hand, if there is no figures appeared in the column, it means that the function is not enabled.

The fields of the **Incoming** window are:

- **Source**: source networks which are specified in the WAN section of the Address menu, or all the WAN network addresses.
- **Destination**: destination networks, which are IP Mapping addresses or Virtual server network addresses created in Virtual Server menu.
- **Service**: services supported by Virtual Servers (or Mapped IP).
- **Action**: control actions to permit or deny packets from WAN networks to Virtual Server/Mapped IP travelling through the device.

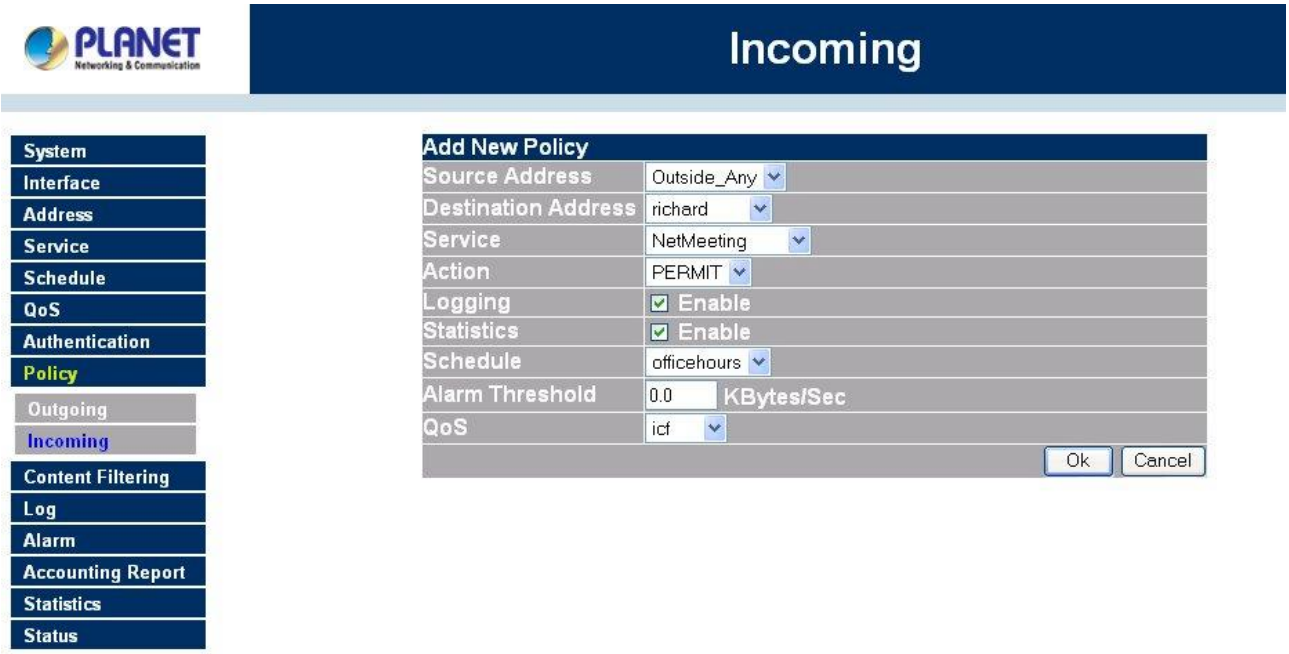
- **Option**: specify the monitoring functions on packets from WAN networks to Virtual Server/Mapped IP travelling through the Bandwidth Management Gateway.
- **Configure**: modify settings or remove incoming policy.
- **Move**: this sets the priority of the policies, number 1 being the highest priority.

Descriptions for **Policy** figures:

Figure	Name	Description
✓	Permit	Permit the specified packets from WAN to LAN.
✗	Block	Block the specified packets from WAN network to LAN network.
	Log	Traffic and event log function is enabled.
	Statistics	Flow statistics function is enabled.
	Schedule	The automatic execution function in Schedule table has been enabled.
	Alarm Threshold	Traffic and event alarm function is enabled.
	QoS	QoS function is enabled.
Remarks: To view the traffic and event log of the system, click **Log** function in the menu bar on the left hand side. To view the alarm records of the system, click **Alarm** function in the menu bar on the left hand side. To view the statistics of the system, click **Statistics** function in the menu bar on the left hand side. Bandwidth Management Gateway can execute the schedule in time slot automatically. To modify the schedule, click the **Schedule** function in the menu bar.		

Adding an Incoming Policy

Under **Incoming** of the **Policy** menu, click the New Entry button.



Add New Policy

Source Address	Outside_Any
Destination Address	richard
Service	NetMeeting
Action	PERMIT
Logging	☑ Enable
Statistics	☑ Enable
Schedule	officehours
Alarm Threshold	0.0 KBytes/Sec
QoS	icf

Source Address: Select the name of WAN from the pull-down menu.

The names of WAN listed in this pull-down menu are: the Source Addresses that are already set. If you want to add new WAN addresses to WAN of address menu, you have to go to WAN function window to configure; you will not be able to add new WAN addresses here.

Source Address: Select the name of WAN from the pull-down menu.

The names of WAN listed in this pull-down menu are: the Source Addresses that are already set. If you want to add new WAN addresses to WAN of address menu, you have to go to WAN function window to configure; you will not be able to add new WAN addresses here.

Destination Address: Select the name of LAN from the pull-down menu.

The names of LAN listed in this pull-down menu are: The Mapped IP or Server Virtual IP configured in the Mapped IP or Virtual Server 1/2/3/4 window under Virtual Server function. To add new items into the pull-down menu, go to Virtual Server window to configure.

Service: Select the service item from the pull-down menu.

Action: Select from the pull-down menu to determine the WAN, Virtual Server(or Mapped IP) packets are permitted or forbidden to pass. Select Permit or Forbid.

Logging: Select Enable to enable the Logging function.

Statistics: Select Enable the enable the Statistics function.

Schedule: Select the item listed in the schedule to enable the policy to automatically execute the function in a certain time and range.

Alarm Threshold: To set the maximum value of transmitting and receiving packet, enter the number based on the unit（KBytes/Sec）

QoS: To determine if the QoS function can work in this Policy function.

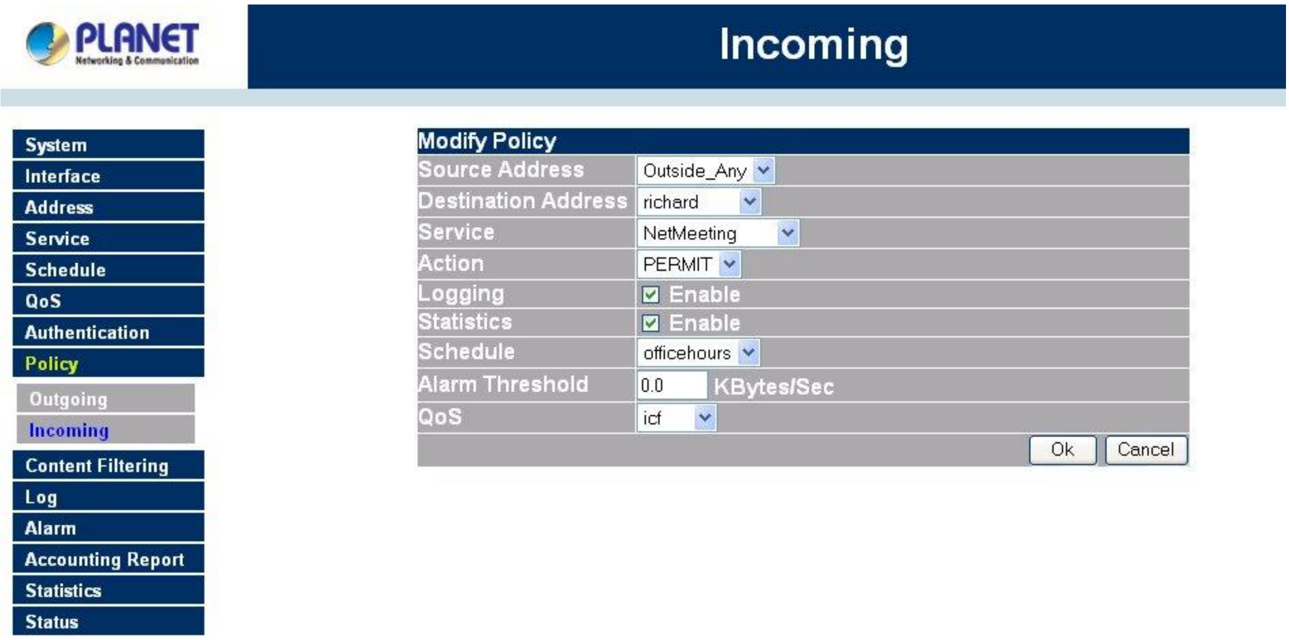
Click **OK** to execute the new setting or click Cancel to discard changes.

NOTE: To change the Policy order of Incoming, select the number from the pull-down menu on the right hand side **Move** column

Modifying Incoming Policy

Step 1. In the Modify Policy window, fill in new settings.

Step 2. Click **OK** to save modifications or click **Cancel** to cancel modifications.



Modify Policy

Source Address	Outside_Any
Destination Address	richard
Service	NetMeeting
Action	PERMIT
Logging	☑ Enable
Statistics	☑ Enable
Schedule	officehours
Alarm Threshold	0.0 KBytes/Sec
QoS	icf

Source Address: Select the name of WAN from the pull-down menu.

The names of WAN listed in this pull-down menu are: the Source Addresses that are already set. If you want to add new WAN addresses to WAN of address menu, you have to go to WAN function window to configure; you will not be able to add new WAN addresses here.

Destination Address: Select the name of LAN from the pull-down menu.

The names of LAN listed in this pull-down menu are: The Mapped IP or Server Virtual IP configured in the Mapped IP or Virtual Server 1/2/3/4 window under Virtual Server function. To add new items into the pull-down menu, go to Virtual Server window to configure.

Service: Select the service item from the pull-down menu.

Action: Select from the pull-down menu to determine the WAN, Virtual Server(or Mapped IP) packets are permitted or forbidden to pass. Select Permit or Forbid.

Logging: Select Enable to enable the Logging function.

Statistics: Select Enable the enable the Statistics function.

Schedule: Select the item listed in the schedule to enable the policy to automatically execute the function in a certain time and range.

Alarm Threshold: To set the maximum value of transmitting and receiving packet, enter the number based on the unit（KBytes/Sec）

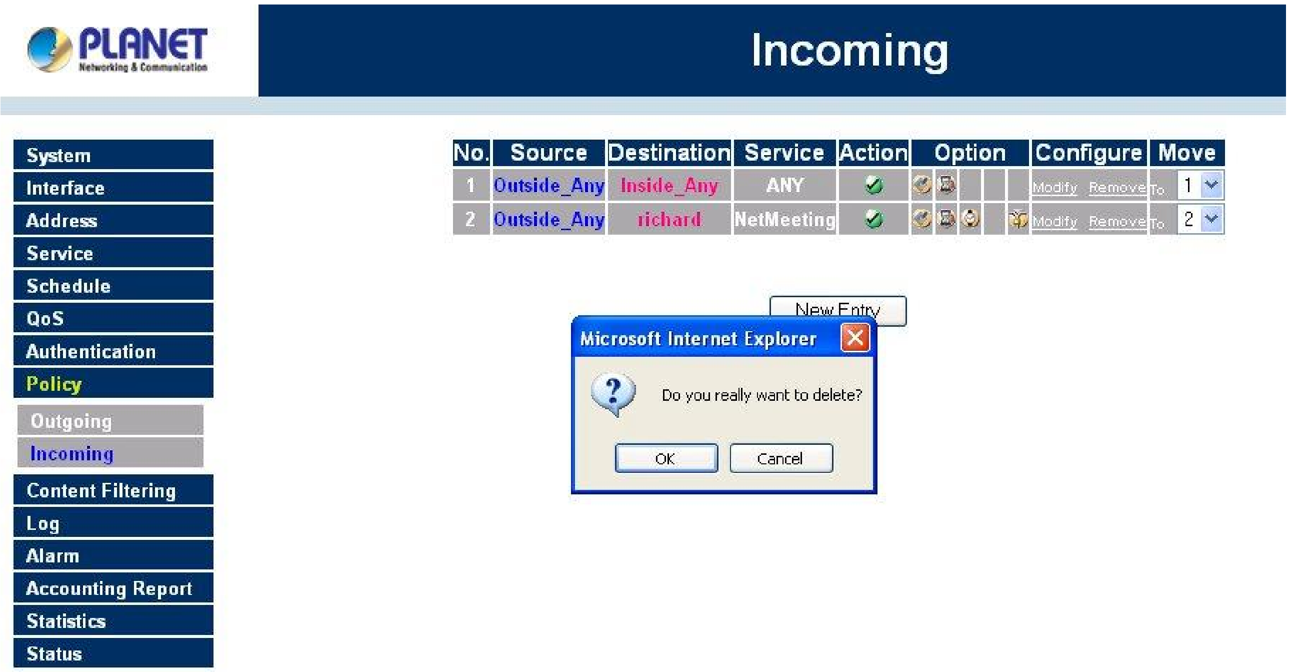
QoS: To determine if the QoS function can work in this Policy function.

Click **OK** to execute the new setting or click Cancel to discard changes.

NOTE: if you want to change or add new items into the pull-down menu, go to the original configuration unit.

Removing an Incoming Policy

Step 1. In the Remove confirmation window, click **Ok** to remove the policy or click **Cancel** to cancel removing.



No.	Source	Destination	Service	Action	Option	Configure	Move
1	Outside_Any	Inside_Any	ANY	✓		Modify Remove	To 1
2	Outside_Any	richard	NetMeeting	✓		Modify Remove	To 2

Microsoft Internet Explorer

Do you really want to delete?

This chapter introduces how to configure the Bandwidth Management Gateway to effectively control your bandwidth usage.

On the top of the Web interface, there is three major menu of the bandwidth Management Gateway:

System Settings: The basic system configurations

Policy Editor: The policy that will be used to manage the bandwidth

Report: The reporting system of the bandwidth Management Gateway base on the system settings and pre-defined policy

The bandwidth Management Gateway will need the three parameters before it operates the bandwidth control: **Host**, (illustrated in section 4.1.6), **Services** (illustrated in section 4.1.7) and **Policy**, (illustrated in section 4.2). However, some of the configurations are also required. Please refer to the related section for the details.

4.9 Content filtering

Content Filtering includes "**URL Blocking**" and "**General Blocking**"

URL Blocking: The administrator can use a complete domain name, key word, " ~ " or " * " to make rules for specific websites.

General Blocking: To let Popup、ActiveX、Java、Cookie in or keep them out.

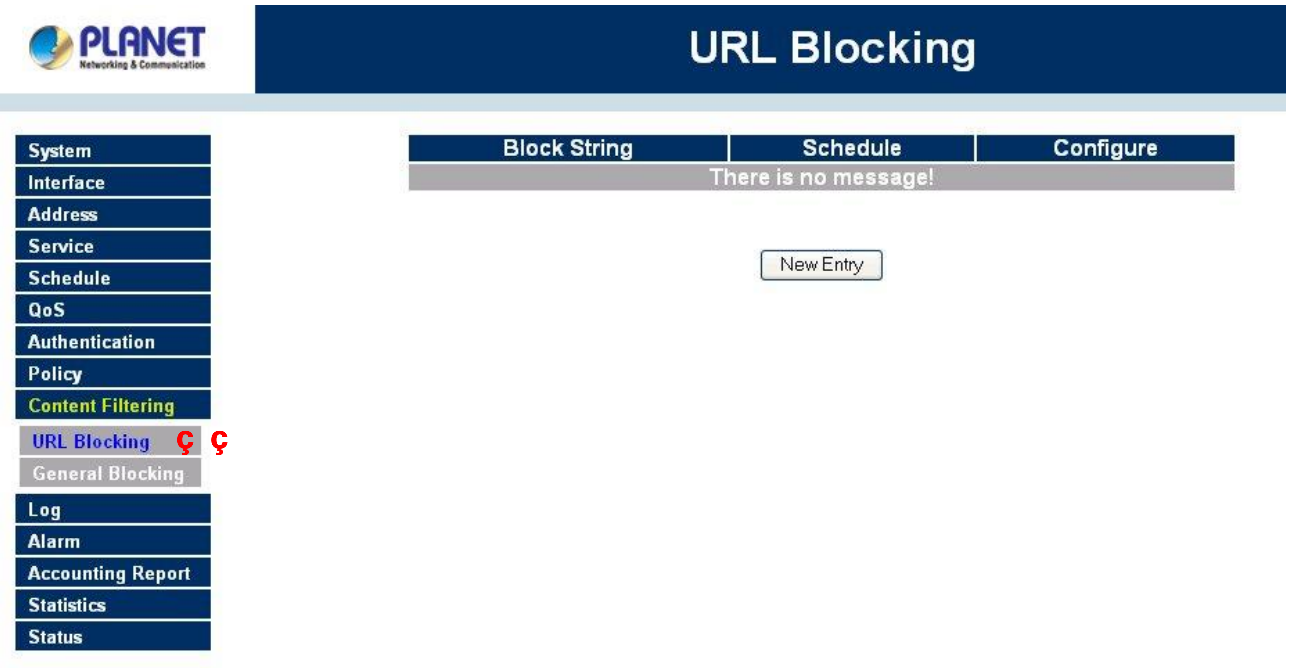
4.9.1 URL Blocking

The Administrator may setup URL Blocking to prevent LAN network users from accessing a specific website on the Internet. Any web request coming from an LAN network computer to a blocked website will receive a blocked message instead of the website.

Entering the URL blocking window

Step 1. Click on **URL Blocking** under the **Configuration** menu bar.

Step 2. Click on **New Entry.**



Block String	Schedule	Configure
There is no message!		

Definition:

Block String: The domain name that is permitted or blocked to enter by Bandwidth Management Gateway.

Schedule: This schedule is used to set the time of permitting or blocking certain websites to enter.

Configuration: To change the settings of URL Blocking, click **Modify** to change the parameters; click **Delete**

to delete the settings.

How to use URL Blocking:

Description of signs: " ~ " means to permit to enter; " * " means wild card.

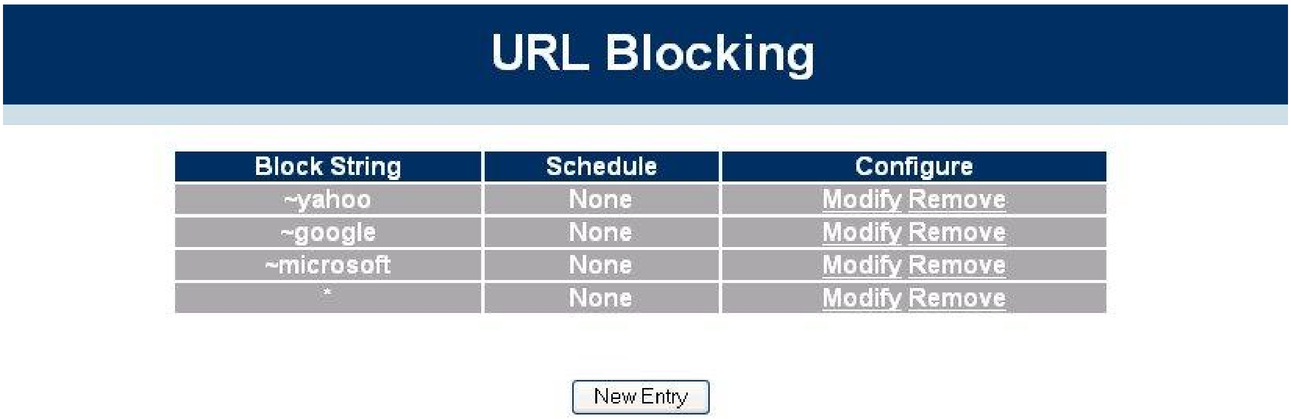
To block certain websites: Enter the complete domain name or key words of the website you want to block in the Block String column. For example, www.yahoo.com or yahoo.

Only permit certain websites to enter:

Enter the complete domain name or key words of the website you permit to enter and add the sign " ~ "in the front.(For example, ~www.yahoo.com or ~yahoo).

After setting all the websites you permit entering, add the sign " * "in front of the last website you want to permit entering. Note: This instruction is always put in front of the last one.

If you want to add new websites to permit entering, you have to remove the instruction of blocking all websites and then key in the new domain name, after that, add the block all instruction.



URL Blocking

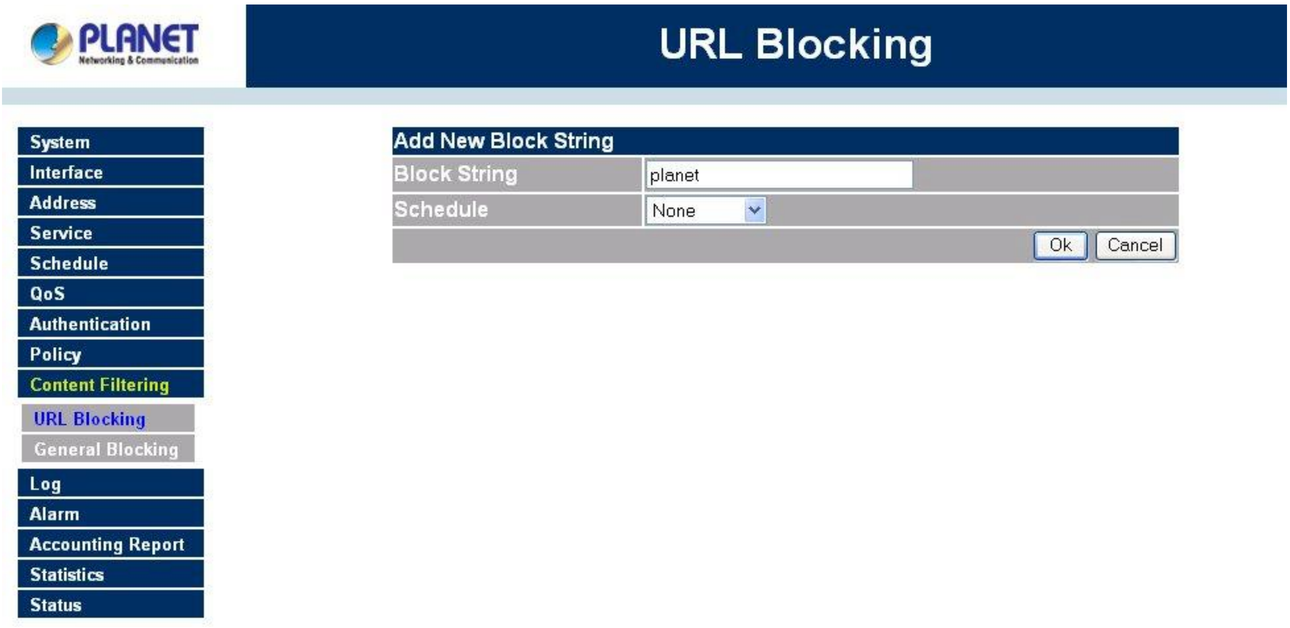
Block String	Schedule	Configure
~yahoo	None	Modify Remove
~google	None	Modify Remove
~microsoft	None	Modify Remove
*	None	Modify Remove

Adding a URL Blocking policy

Step 1. After clicking **New Entry**, the **Add New Block String** window will appear.

Step 2. Enter the URL of the website to be blocked.

Step 3. Click **OK** to add the policy. Click **Cancel** to discard changes.



Add New Block String

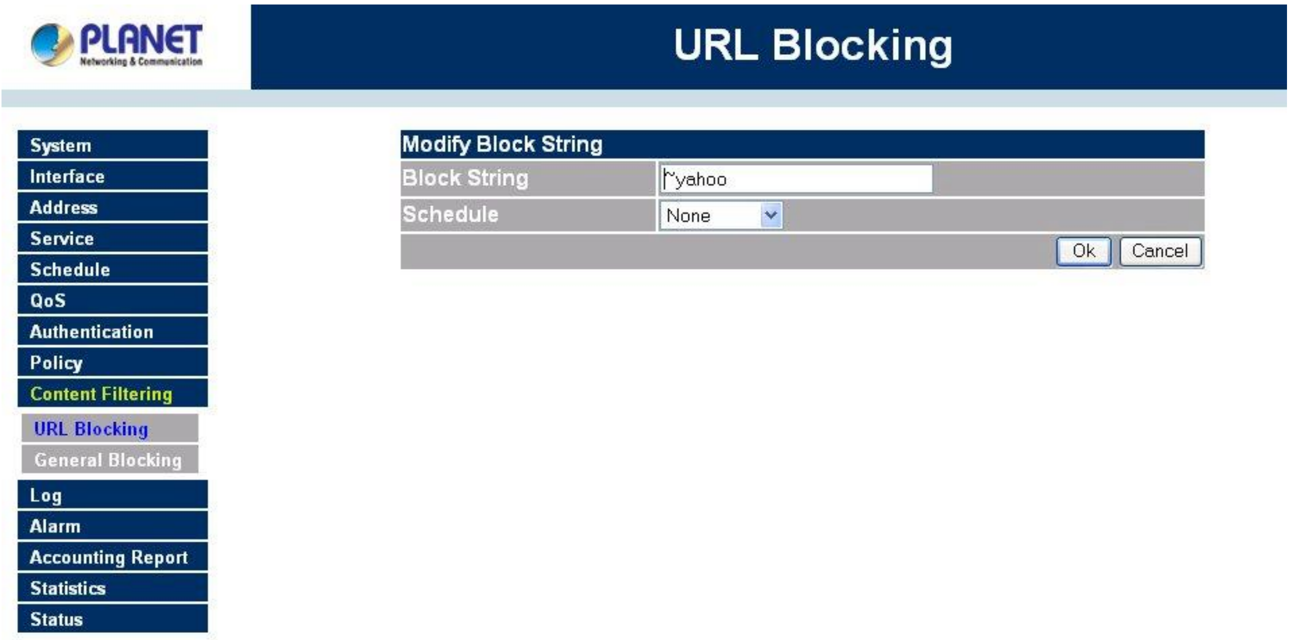
Block String	planet
Schedule	None

Modifying a URL Blocking Policy

Step 1. In the **URL Blocking** window, find the policy to be modified and click the corresponding **Modify** option in the **Configure** field.

Step 2. Make the necessary changes needed.

Step 3. Click on **OK** to save changes or click on **Cancel** to discard changes.



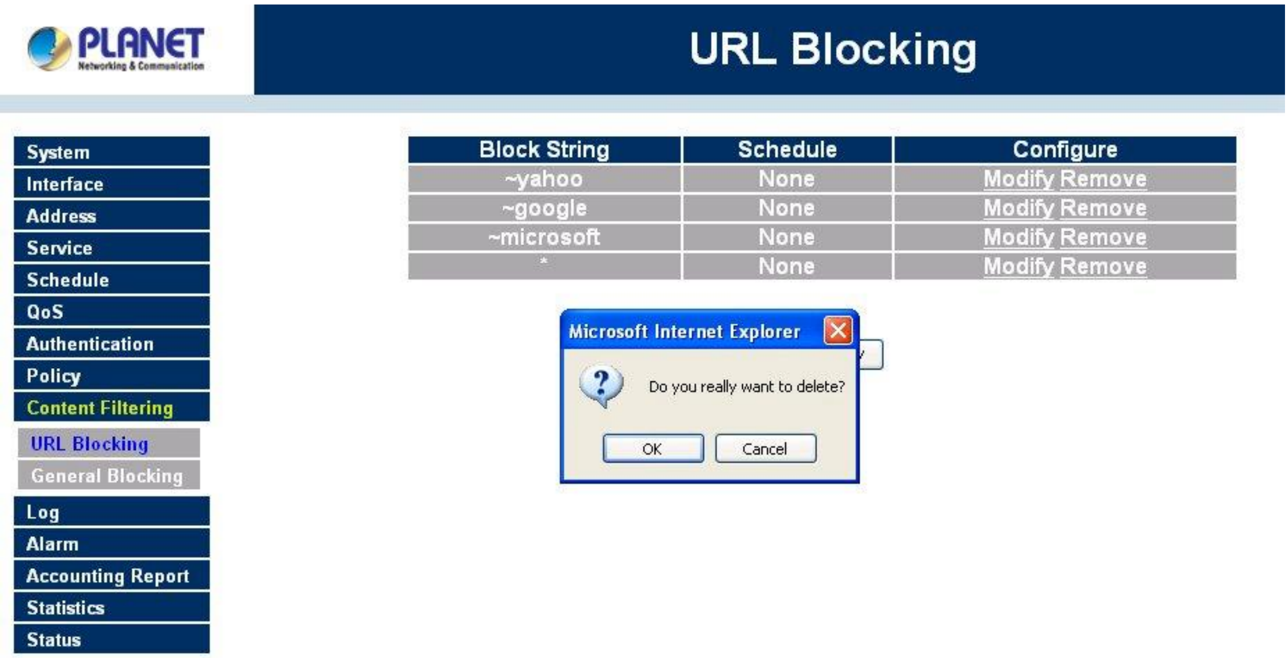
Modify Block String

Block String	~yahoo
Schedule	None

Removing a URL Blocking policy

Step 1. In the **URL Blocking** window, find the policy to be removed and click the corresponding **Remove** option in the **Configure** field.

Step 2. A confirmation pop-up box will appear, click on **OK** to remove the policy or click on **Cancel** to discard changes.



URL Blocking

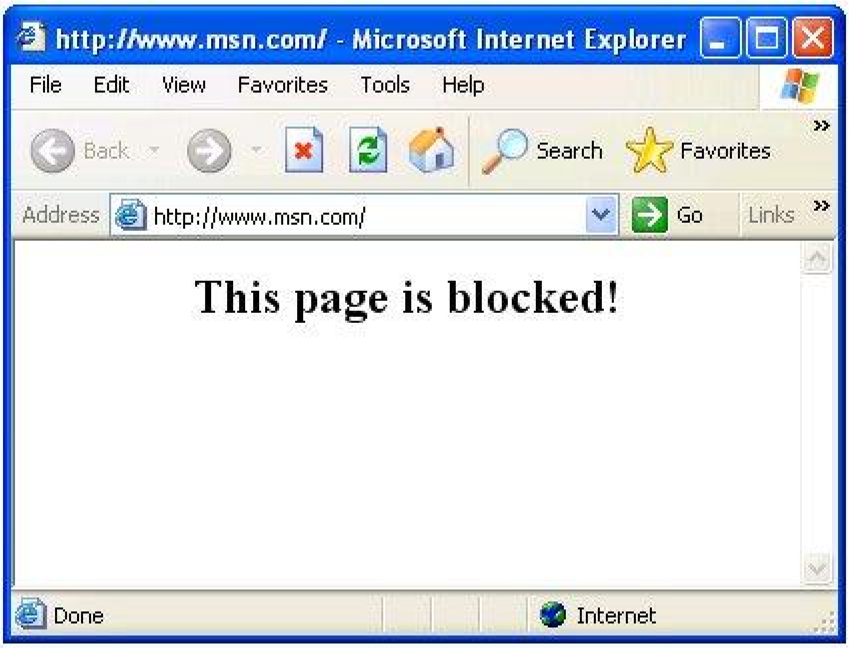
Block String	Schedule	Configure
~yahoo	None	Modify Remove
~google	None	Modify Remove
~microsoft	None	Modify Remove
*	None	Modify Remove

Microsoft Internet Explorer

Do you really want to delete?

Blocked URL site:

When a user from the LAN network tries to access a blocked URL, the error below will appear.



http://www.msn.com/ - Microsoft Internet Explorer

Address http://www.msn.com/

This page is blocked!

Done

4.9.2 General Blocking

To let Popup, ActiveX, Java, or Cookies in or keep them out.

Step 1: Click **Content Filtering** in the menu.

Step 2: **General Blocking** detective functions.

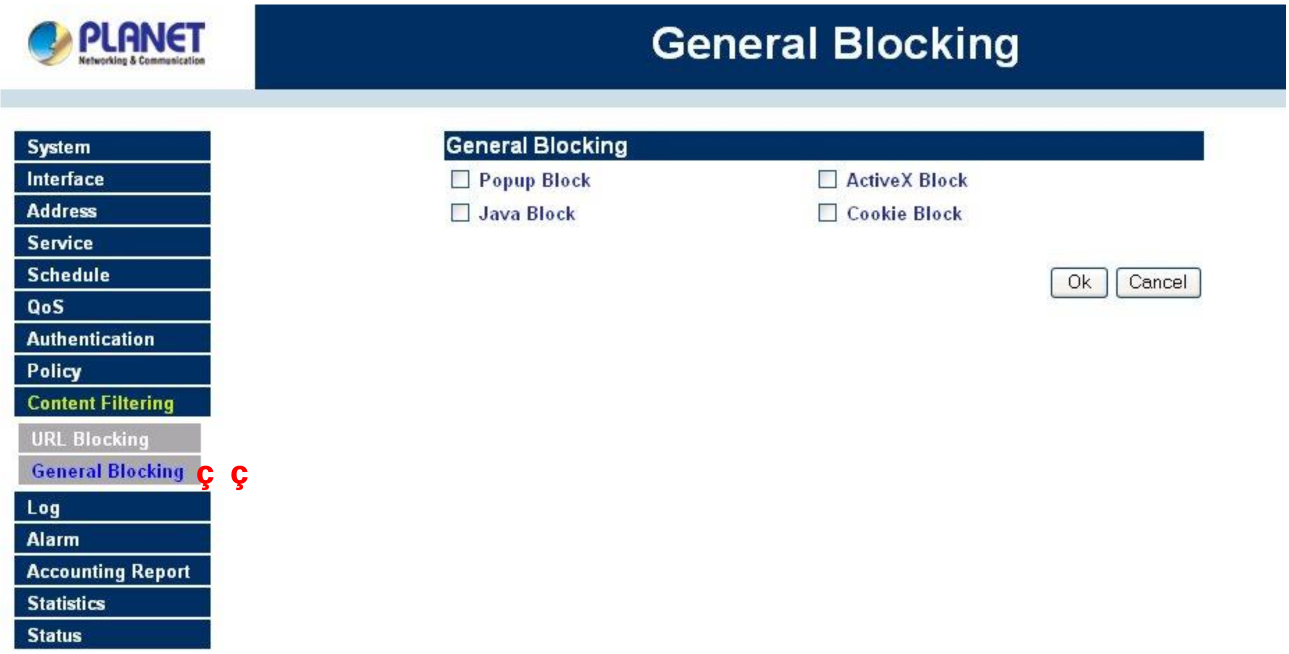
Popup filtering: Prevent pop-up boxes from appearing.

ActiveX filtering: Prevent ActiveX packets.

Java filtering: Prevent Java packets.

Cookie filtering: Prevent Cookie packets.

Step 3: After selecting each function, click the **OK** button below.



General Blocking

□ Popup Block □ ActiveX Block

□ Java Block □ Cookie Block

When the system detects the setting, the Bandwidth Management Gateway will spontaneously work**.**

4.10 Virtual Server

The Bandwidth Management Gateway separates an enterprise's Intranet and Internet into LAN networks and WAN networks respectively. Generally speaking, in order to allocate enough IP addresses for all computers, an enterprise assigns each computer a private IP address, and converts it into a real IP address through Bandwidth Management Gateway's NAT (Network Address Translation) function. If a server providing service to the WAN networks is located in the LAN networks, outside users can't directly connect to the server by using the server's private IP address.

The Bandwidth Management Gateway's Virtual Server can solve this problem. A virtual server has set the real IP address of the Bandwidth Management Gateway's WAN network interface to be the Virtual Server IP. Through the virtual server feature, the Bandwidth Management Gateway translates the virtual server's IP address into the private IP address of physical server in the LAN network. When outside users on the Internet request connections to the virtual server, the request will be forwarded to the private LAN server.

Virtual Server owns another feature known as one-to-many mapping. This is when one virtual server IP address on the WAN interface can be mapped into 4 LAN network server private IP addresses. This option is useful for Load Balancing, which causes the virtual server to distribute data packets to each private IP addresses (which are the real servers). By sending all data packets to all similar servers, this increases the server's efficiency, reduces risks of server crashes, and enhances servers' stability.

How to use Virtual Server and mapped IP

Virtual Server and Mapped IP are part of the IP mapping (also called DMZ, De-Militarization Zone) scheme. By applying the incoming policies, Virtual Server and IP mapping work similarly. They map real IP addresses to the physical servers' private IP addresses (which is opposite to NAT), but there are still some differences:

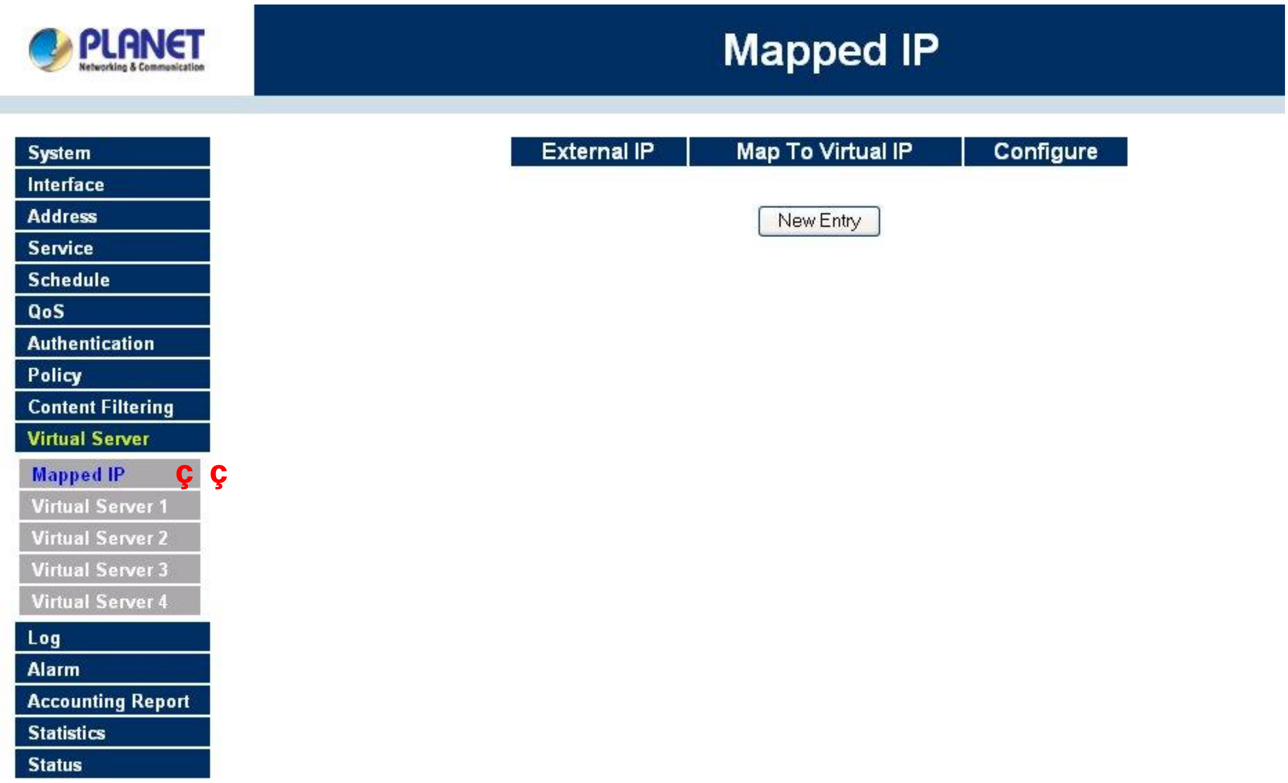
- Virtual Server can map one real IP to several LAN physical servers while Mapped IP can only map one real IP to one LAN physical server (1-to-1 Mapping). The Virtual Servers' load balance feature can map a specific service request to different physical servers running the same services.
- Virtual Server can only map one real IP to one service/port of the LAN physical servers while Mapped IP maps one real IP to all the services offered by the physical server.
- IP mapping and Virtual Server work by binding the IP address of the WAN virtual server to the private LAN IP address of the physical server that supports the services. Therefore users from the WAN network can access servers of the LAN network by requesting the service from the IP address provided by Virtual Server.

4.10.1 Mapped IP

Internal private IP addresses are translated through NAT (Network Address Translation). If a server is located in the LAN network, it has a private IP address, and outside users cannot connect directly to LAN servers' private IP address. To connect to a LAN network server, outside users have to first connect to a real IP address of the WAN network, and the real IP is translated to a private IP of the LAN network. Mapped IP and Virtual Server are the two methods to translate the real IP into private IP. Mapped IP maps IP in one-to-one fashion; that means, all services of one real WAN IP address is mapped to one private LAN IP address.

Entering the Mapped IP window

Step 1. Click **Mapped IP** under the **Virtual Server** menu bar and the Mapped IP configuration window will appear.



Definition:

External IP: WAN IP Address.

Map to Virtual IP: The IP address which WAN maps to the virtual network in the server.

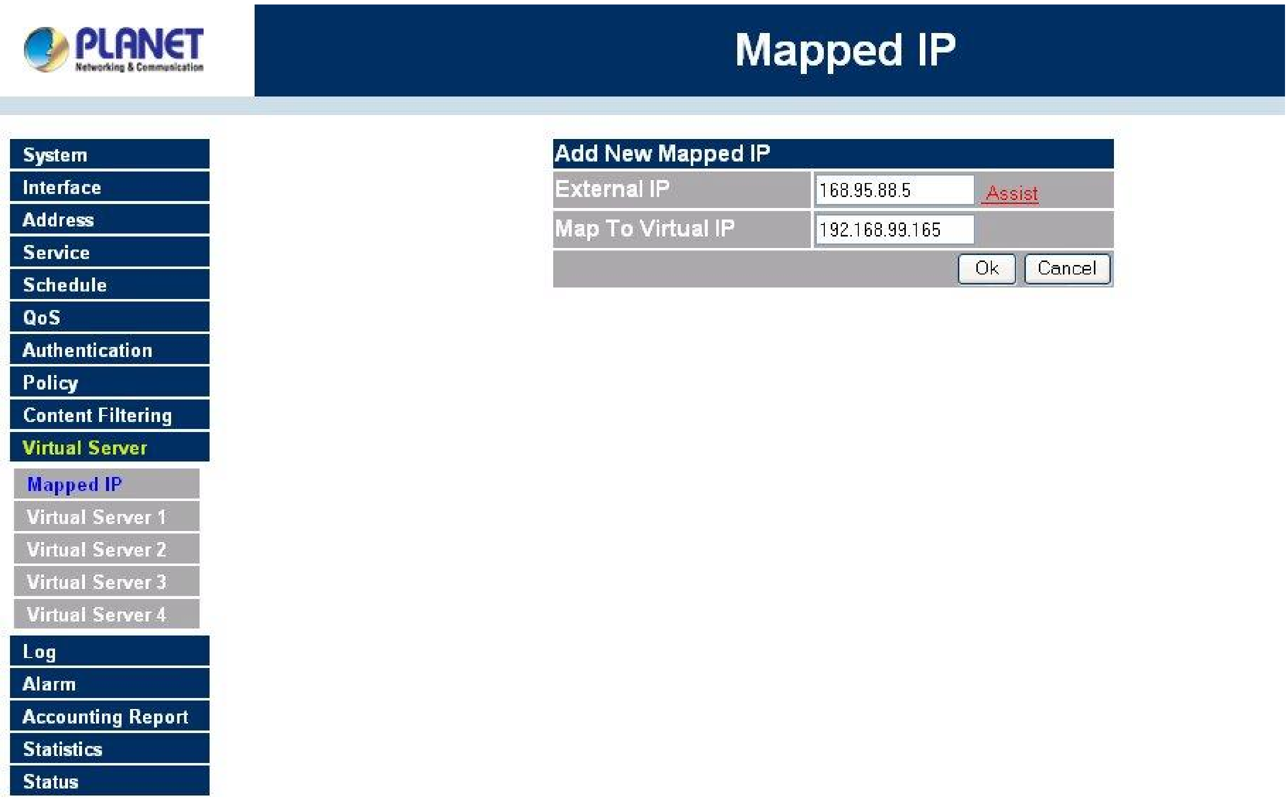
Configure: To change the setting, click Configure to modify the parameters; click delete to delete the setting.

Adding a new IP Mapping

Step 1. In the **Mapped IP** window, click the New Entry button. The Add New Mapped IP window will appear.

- **WAN IP**: select the WAN public IP address to be mapped.
- **Internal IP**: enter the LAN private IP address will be mapped 1-to-1 to the WAN IP address.

Step 2. Click **OK** to add new IP Mapping or click **Cancel** to cancel adding.



Add New Mapped IP

External IP: 168.95.88.5

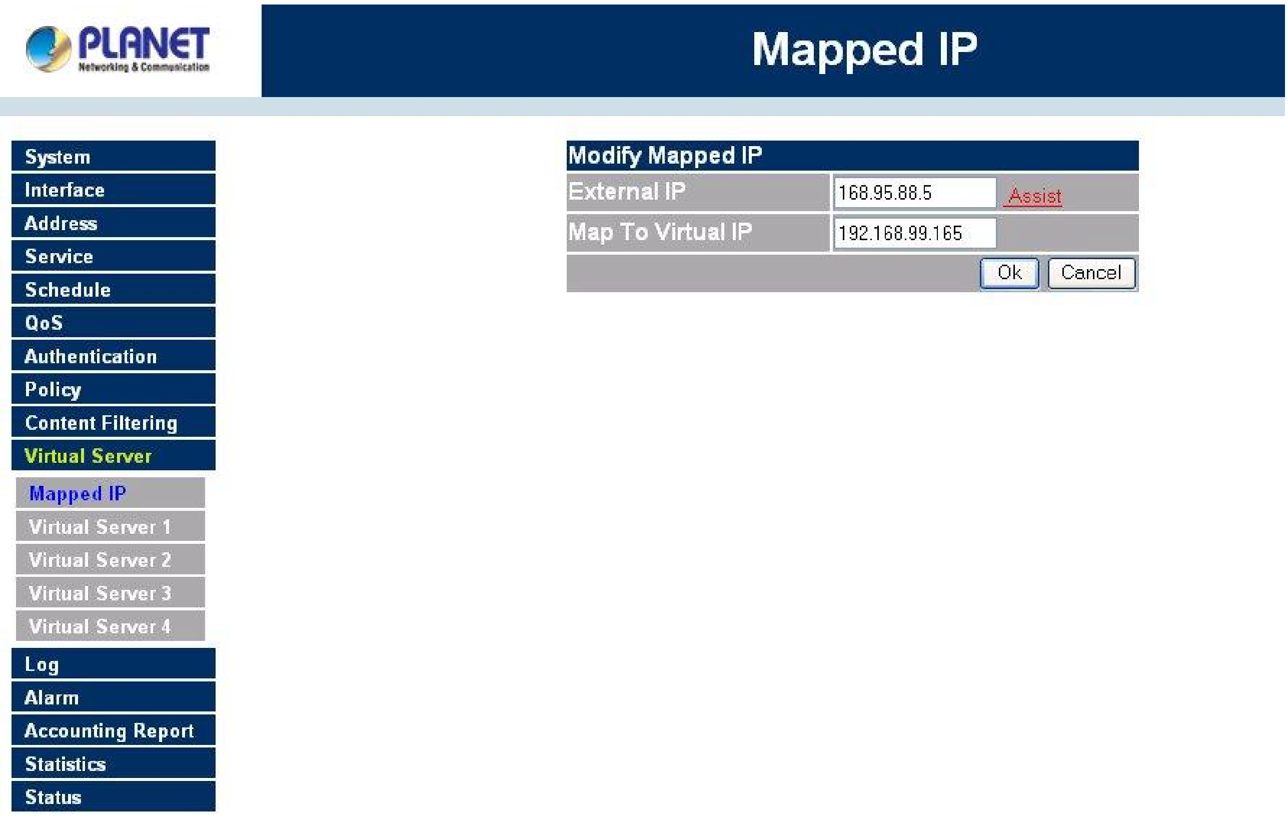
Map To Virtual IP: 192.168.99.165

Modifying a Mapped IP

Step 1. In the **Mapped IP** table, locate the Mapped IP you want it to be modified and click its corresponding Modify option in the Configure field.

Step 2. Enter settings in the Modify Mapped IP window.

Step 3. Click **OK** to save change or click **Cancel** to cancel.



Modify Mapped IP

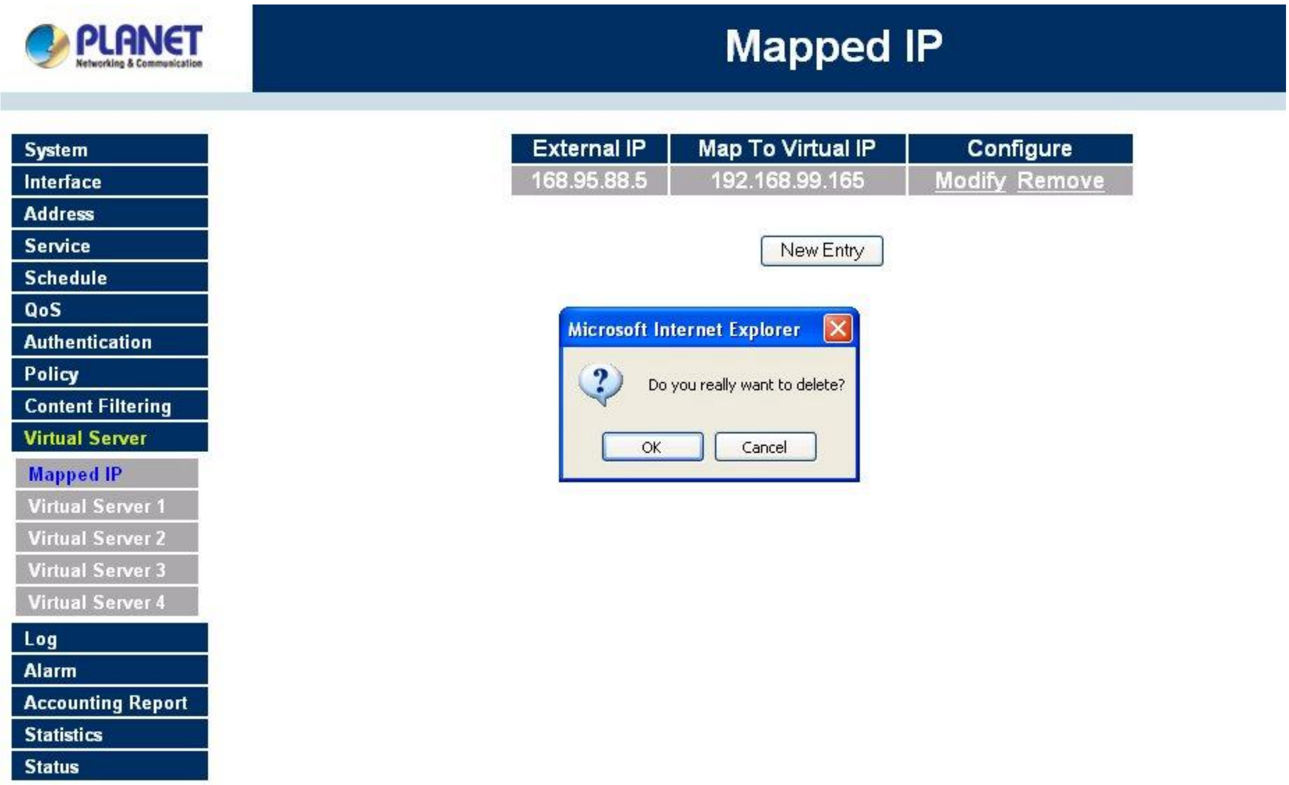
External IP	168.95.88.5
Map To Virtual IP	192.168.99.165

NOTE: A Mapped IP cannot be modified if it has been assigned/used as a destination address of any Incoming policies.

Removing a Mapped IP

Step 1. In the Mapped IP table, locate the Mapped IP desired to be removed and click its corresponding Remove option in the Configure field.

Step 2. In the Remove confirmation pop-up window, click **OK** to remove the Mapped IP or click **Cancel** to cancel.

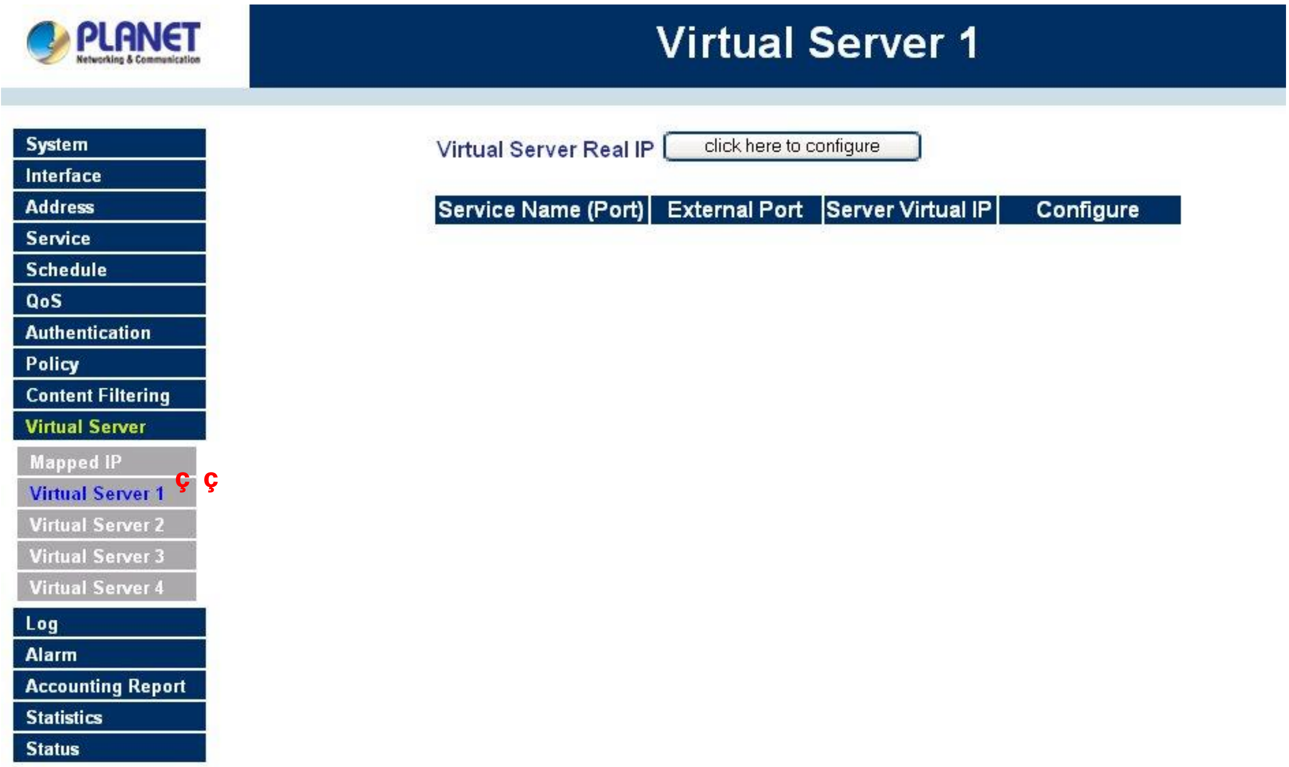


External IP	Map To Virtual IP	Configure
168.95.88.5	192.168.99.165	Modify Remove

Do you really want to delete?

4.10.2 Virtual Server

Virtual server is a one-to-many mapping technique, which maps a real IP address from the WAN interface to private IP addresses of the LAN network. This function provides services or applications defined in the Service menu to enter into the LAN network. Unlike a mapped IP which binds a WAN IP to a LAN IP, virtual server binds WAN IP ports to LAN IP ports.



Service Name (Port)	External Port	Server Virtual IP	Configure

Definition:

Virtual Server IP: The WAN IP address configured by the virtual server. Click "**Click here to configure**" button to add new virtual server address.

Service name: The service names that provided by the virtual server.

Port: The TCP/UDP ports that present the service items provided by the virtual server.

Server Virtual IP: The virtual IP which mapped by the virtual server.

Configure: To change the service configuration, click **Configure** to change the parameters; click **Delete** to delete the configuration.

This virtual server provides four real IP addresses, which means you can setup four virtual servers at most （Setup under the Virtual Server sub-selections Virtual Server 1/2/3/4 in the menu bar on the left hand side.）The administrator can select Virtual Server1/2/3/4 under Virtual Server selection in the menu bar on the left hand side, click **Server Virtual IP** to add or change the virtual server IP address; click **"Click here to configure"** to add or change the virtual server service configuration.

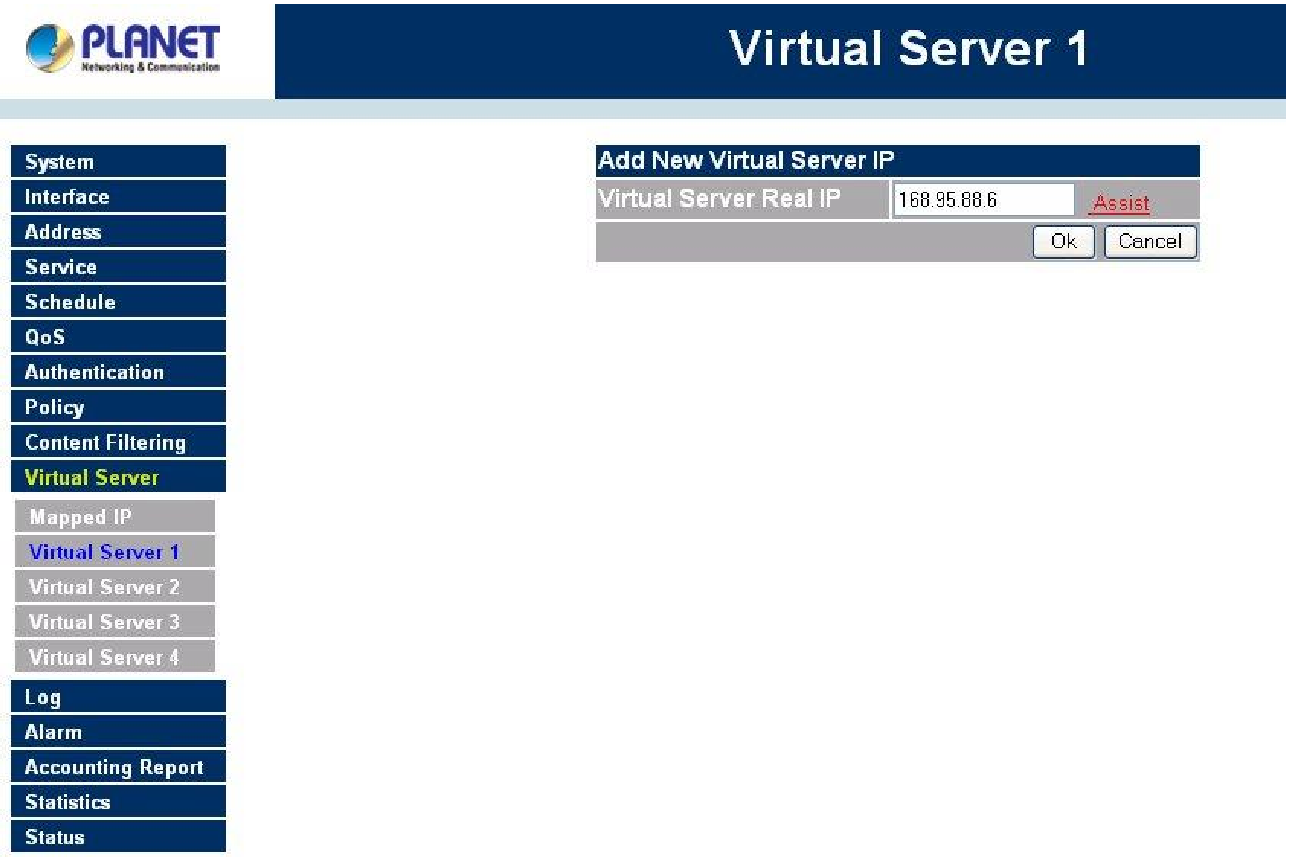
Adding a Virtual Server

Step 1. Click an available virtual server from **Virtual Server** in the **Virtual Server** menu bar to enter the virtual server configuration window. In the following, Virtual Server is assumed to be the chosen option:

Step 2. Click the **click here to configure** button and the Add new Virtual Server IP window appears and asks for an IP address from the WAN network.

Step 3. Select an IP address from the drop-down list of available WAN network IP addresses.

Step 4. Click **OK** to add new Virtual Server or click **Cancel** to cancel adding.



Add New Virtual Server IP

Virtual Server Real IP: 168.95.88.6

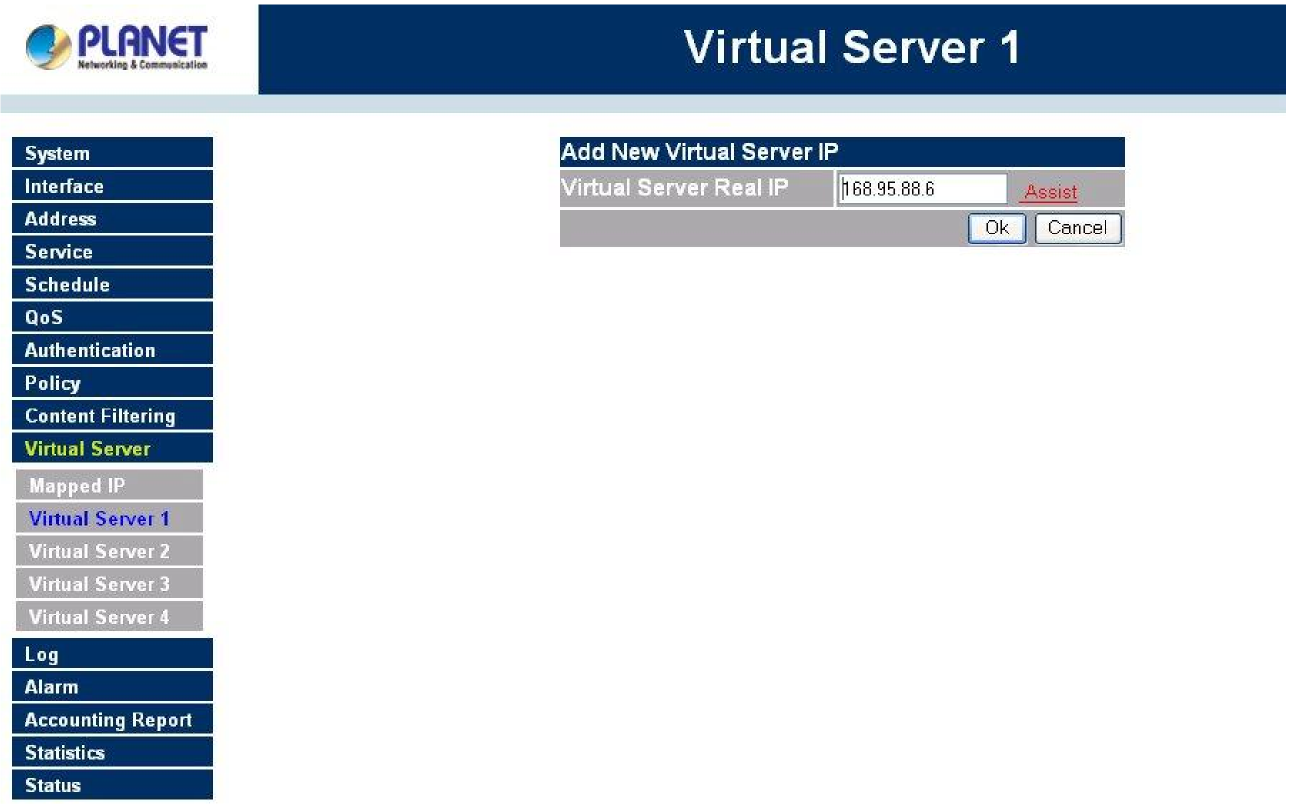
Modifying a Virtual Server IP Address

Step 1. Click the virtual server to be modified Virtual Server under the **Virtual Server** menu bar. A new window appears displaying the IP address and service of the specified virtual server.

Step 2. Click on the Virtual Server's IP Address button at the top of the screen.

Step 3. Choose a new IP address from the drop-down list.

Step 4. Click **OK** to save new IP address or click **Cancel** to discard changes.



Add New Virtual Server IP

Virtual Server Real IP: 168.95.88.6

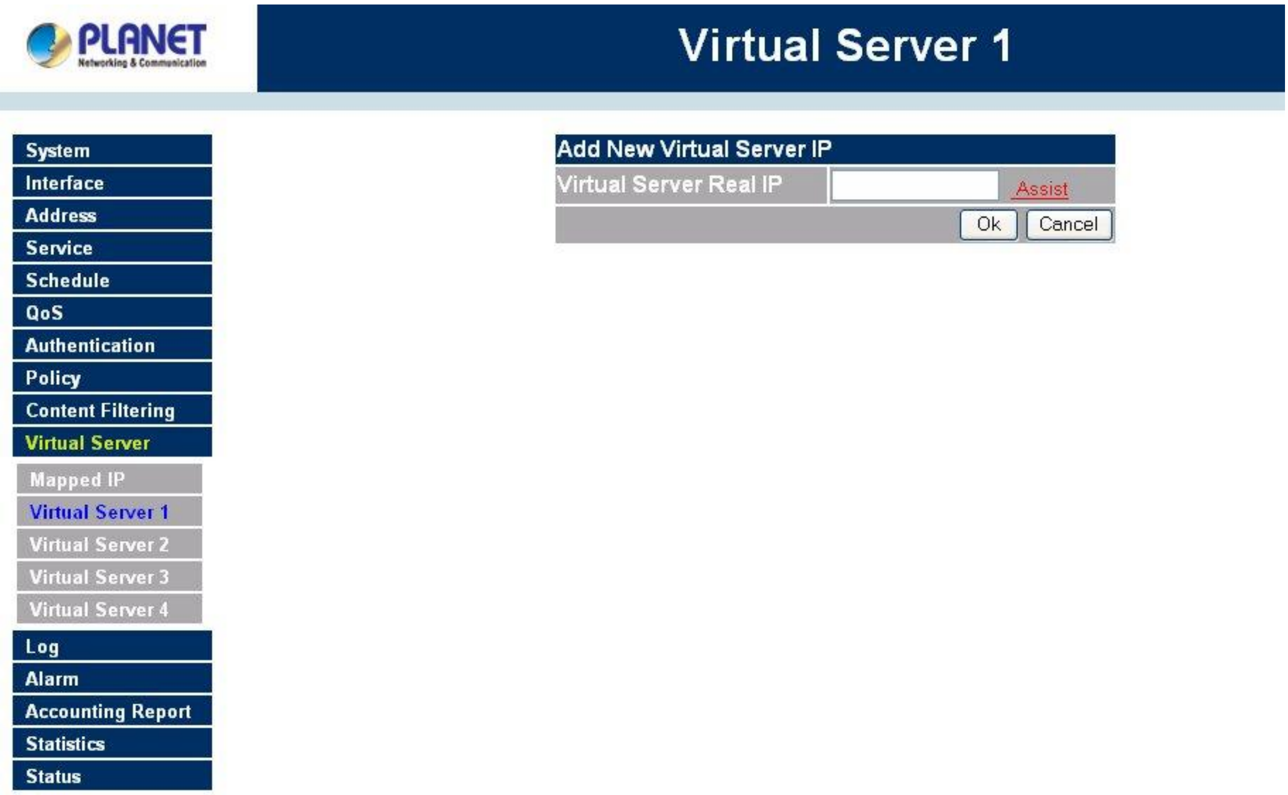
Removing a Virtual Server

Step 1. Click the virtual server to be removed in the corresponding Virtual Server option under the **Virtual Server** menu bar. A new window displaying the virtual server's IP address and service appears on the screen.

Step 2. Click the Virtual Server's IP Address button at the top of the screen.

Step 3. Delete the IP address.

Step 4. Click **OK** to remove the virtual server.



Setting the Virtual Server's services

Step 1. For the Virtual Server which has already been set up with an IP address, click the New Service button in the table.

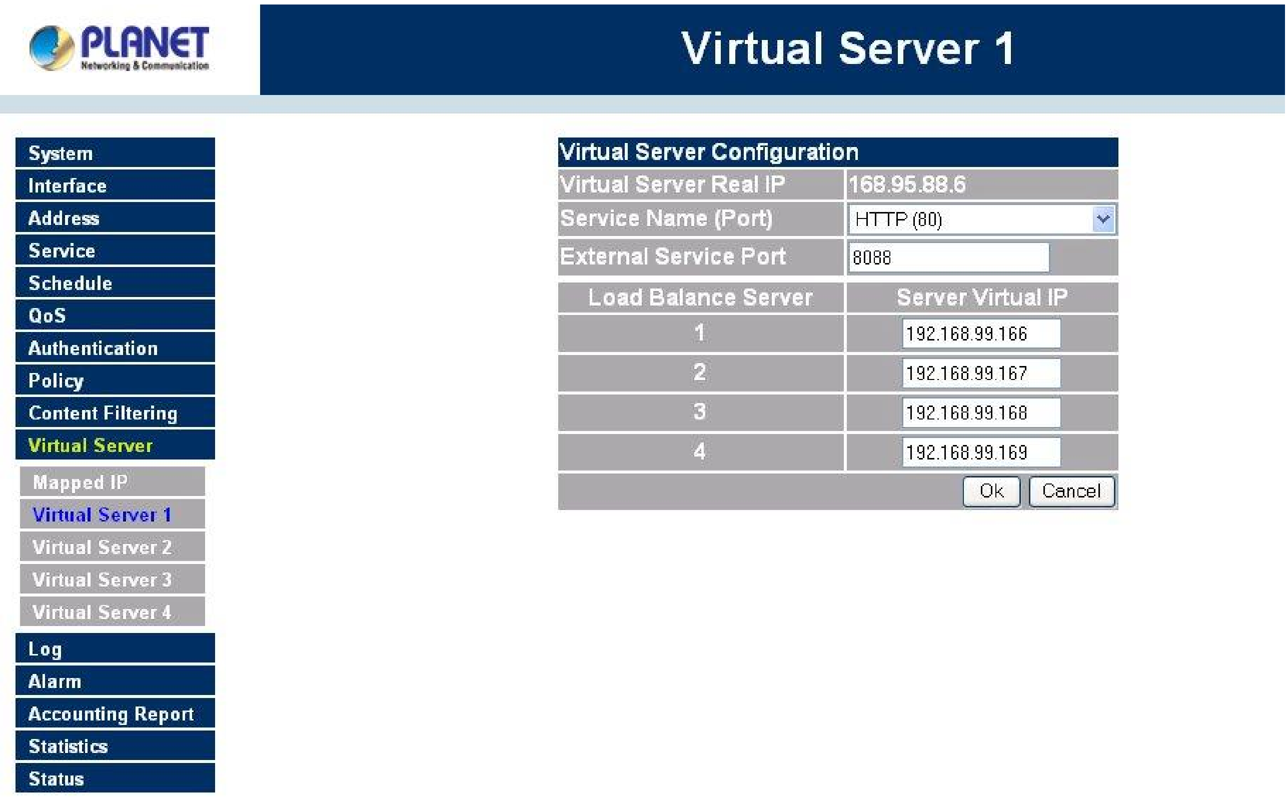
Step 2. In the Virtual Server Configurations window:

- **Virtual Server Real IP:** displays the WAN IP address assigned to the Virtual Server
- **Service Name (Port):** select the service from the pull down list that will be provided by the Real Server (Load Balance Server).
- **External Service Port:** Input the port number that the virtual server will use. Changing the Service will change the port number to match the service.
- **Load Balance Server:** The internal server IP address mapped by the virtual server. Four computer IP addresses can be set at most, and the load can be maintained in a balance by round robin algorithm.

Step 3. Enter the IP address of the LAN network server(s), to which the virtual server will be mapped. Up to four IP addresses can be assigned at most.

Step 4. Click **OK** to save the settings of the Virtual Server.

NOTE: *The services in the drop-down list are all defined in the Pre-defined and Custom section of the* ***Service*** *menu.*



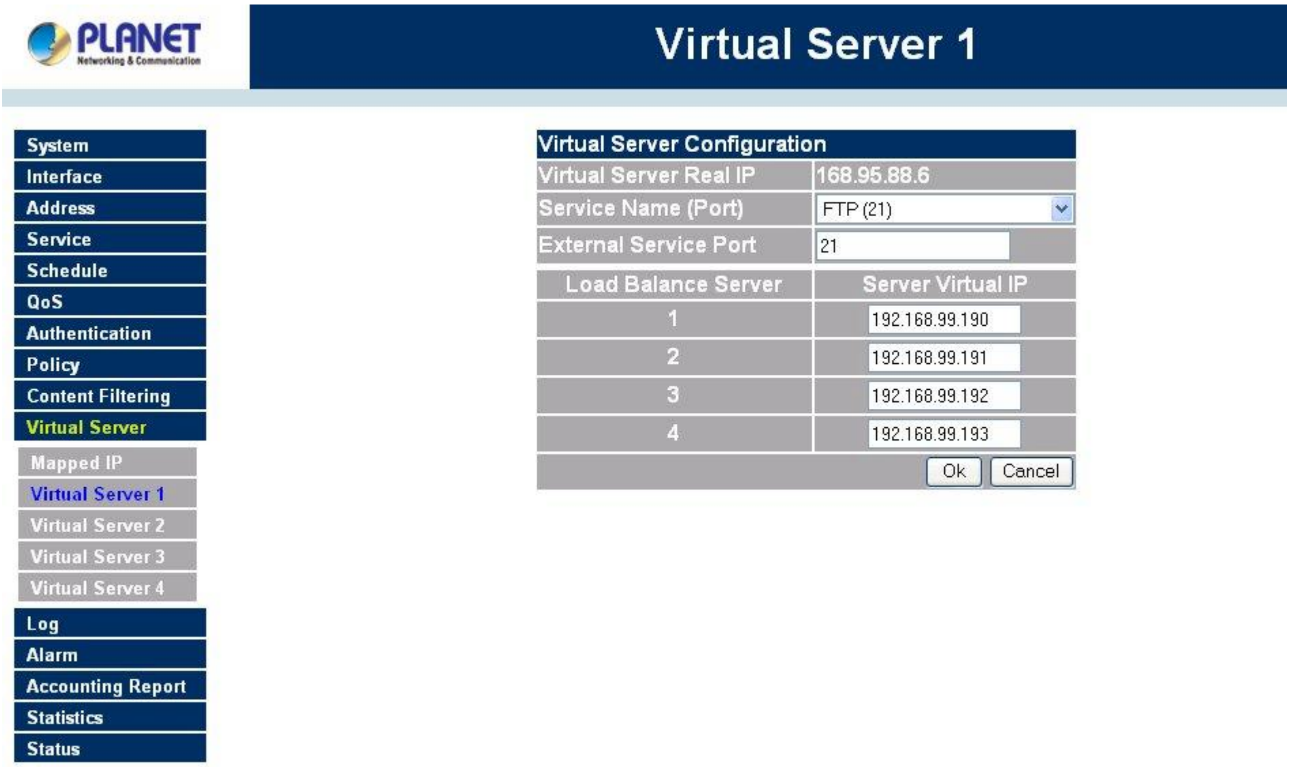
Virtual Server Configuration	
Virtual Server Real IP	168.95.88.6
Service Name (Port)	HTTP (80)
External Service Port	8088
Load Balance Server	Server Virtual IP
1	192.168.99.166
2	192.168.99.167
3	192.168.99.168
4	192.168.99.169

Adding New Virtual Server Service Configuration

Step 1. Select Virtual Server in the menu bar on the left hand side, and then select Virtual Server 1/2/3/4 sub-selections.

Step 2. In Virtual Server 1/2/3/4 Window, click "**New Service**" button.

Step 3. Enter the parameters in the Virtual Server Configuration column.



Virtual Server 1

Virtual Server Configuration	
Virtual Server Real IP	168.95.88.6
Service Name (Port)	FTP (21)
External Service Port	21
Load Balance Server	Server Virtual IP
1	192.168.99.190
2	192.168.99.191
3	192.168.99.192
4	192.168.99.193

n **Virtual Server Real IP:** displays the WAN IP address assigned to the Virtual Server

n **Service Name (Port):** select the service from the pull down list that will be provided by the Real Server (Load Balance Server).

n **External Service Port:** Input the port number that the virtual server will use. Changing the Service will change the port number to match the service.

n **Load Balance Server:** The internal server IP address mapped by the virtual server. Four computer IP addresses can be set at most, and the load can be maintained in a balance by round robin algorithm.

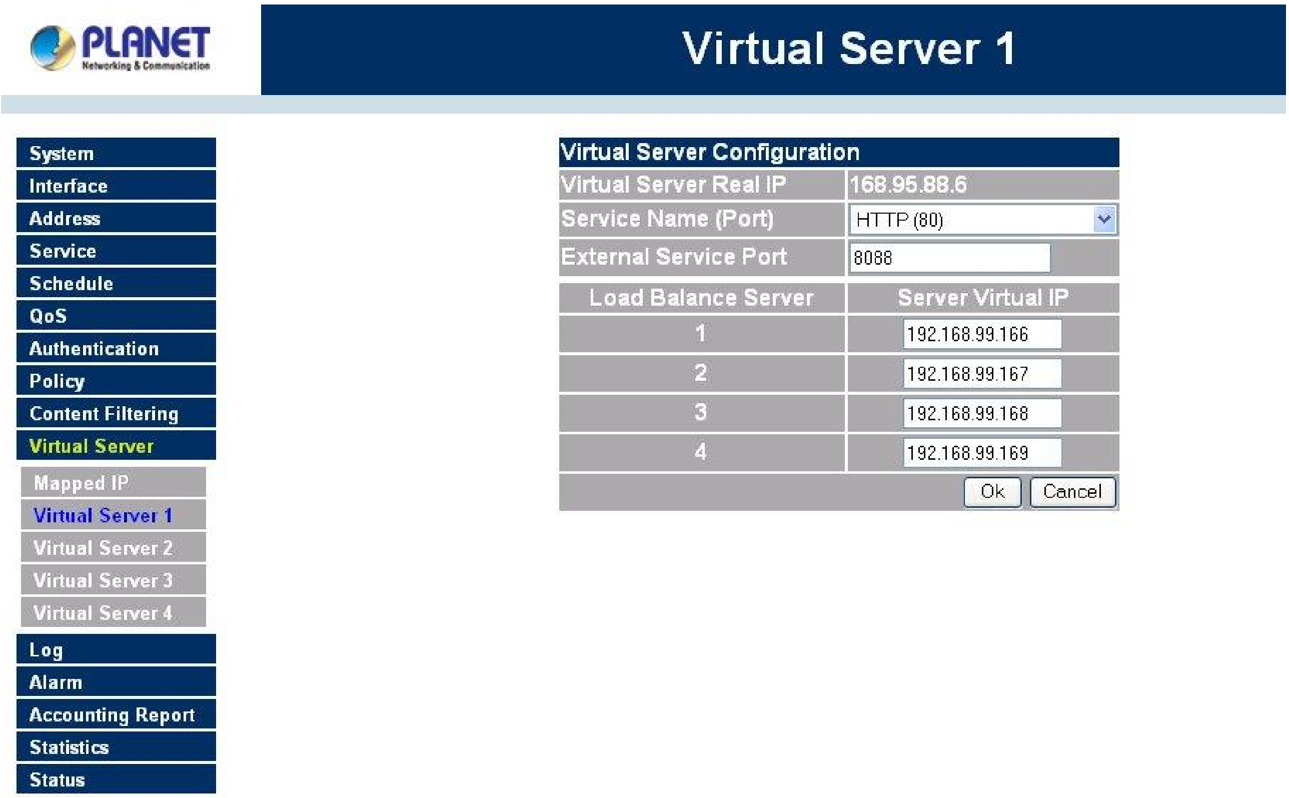
Click **OK** to execute adding new virtual server service, or click **Cancel** to discard adding.
Remember to configure the service items of virtual server before you configure Policy, or the service names will not be shown in Policy.

Modifying the Virtual Server configurations

Step 1. In the Virtual Server window's service table, locate the name of the service desired to be modified and click its corresponding Modify option in the Configure field.

Step 2. In the Virtual Server Configuration window, enter the new settings.

Step 3. Click **OK** to save modifications or click **Cancel** to discard changes.



Virtual Server Configuration	
Virtual Server Real IP	168.95.88.6
Service Name (Port)	HTTP (80)
External Service Port	8088
Load Balance Server	Server Virtual IP
1	192.168.99.166
2	192.168.99.167
3	192.168.99.168
4	192.168.99.169

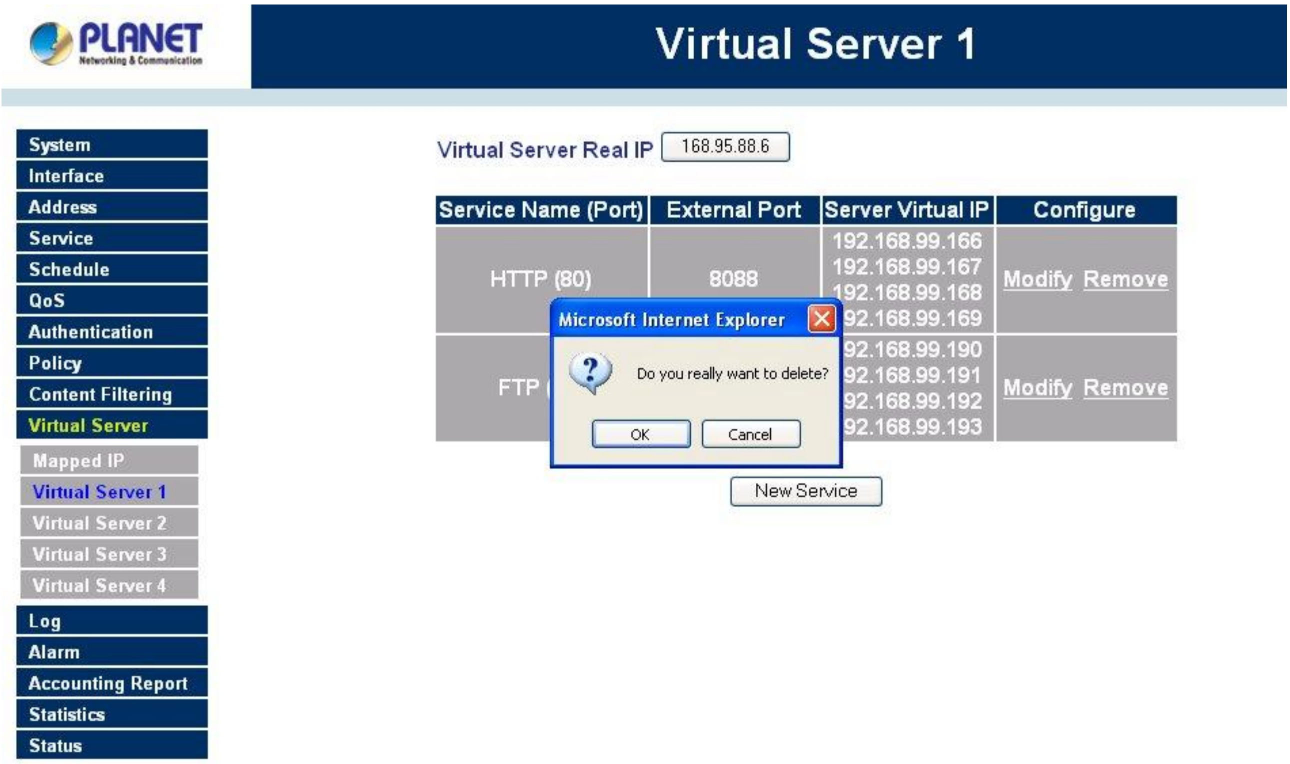
Click **OK** to execute the change of the virtual server, or click **Cancel** to discard changes.

NOTE: If the destination Network in Policy has set a virtual server, it will not be able to change or configure this virtual server, you have to remove this configuration of Policy, and then you can execute the modification or configuration.

Removing the Virtual Server service

Step 1. In the Virtual Server window’s service table, locate the name of the service desired to be removed and click its corresponding Remove option in the Configure field.

Step 2. In the Remove confirmation pop-up box, click **OK** to remove the service or click **Cancel** to cancel removing.



Virtual Server Real IP 168.95.88.6

Service Name (Port)	External Port	Server Virtual IP	Configure
HTTP (80)	8088	192.168.99.166 192.168.99.167 192.168.99.168 92.168.99.169	Modify Remove
FTP (		92.168.99.190 92.168.99.191 92.168.99.192 92.168.99.193	Modify Remove

Do you really want to delete?

NOTE: If the destination Network in Policy has set a virtual server, it will not be able to change or configure this virtual server unless you have already removed this configuration of Policy.

4.11 Log

The Bandwidth Management Gateway supports traffic logging and event logging to monitor and record services, connection times, and the source and destination network address. The Administrator may also download the log files for backup purposes. The Administrator mainly uses the Log menu to monitor the traffic passing through the Bandwidth Management Gateway.

What is Log?

Log records all connections that pass through the Bandwidth Management Gateway's control policies. Traffic log's parameters are setup when setting up control policies. Traffic logs record the details of packets such as the start and stop time of connection, the duration of connection, the source address, the destination address and services requested, for each control policy. Event logs record the contents of System Configuration changes made by the Administrator such as the time of change, settings that change, the IP address used to log on, etc.

How to use the Log

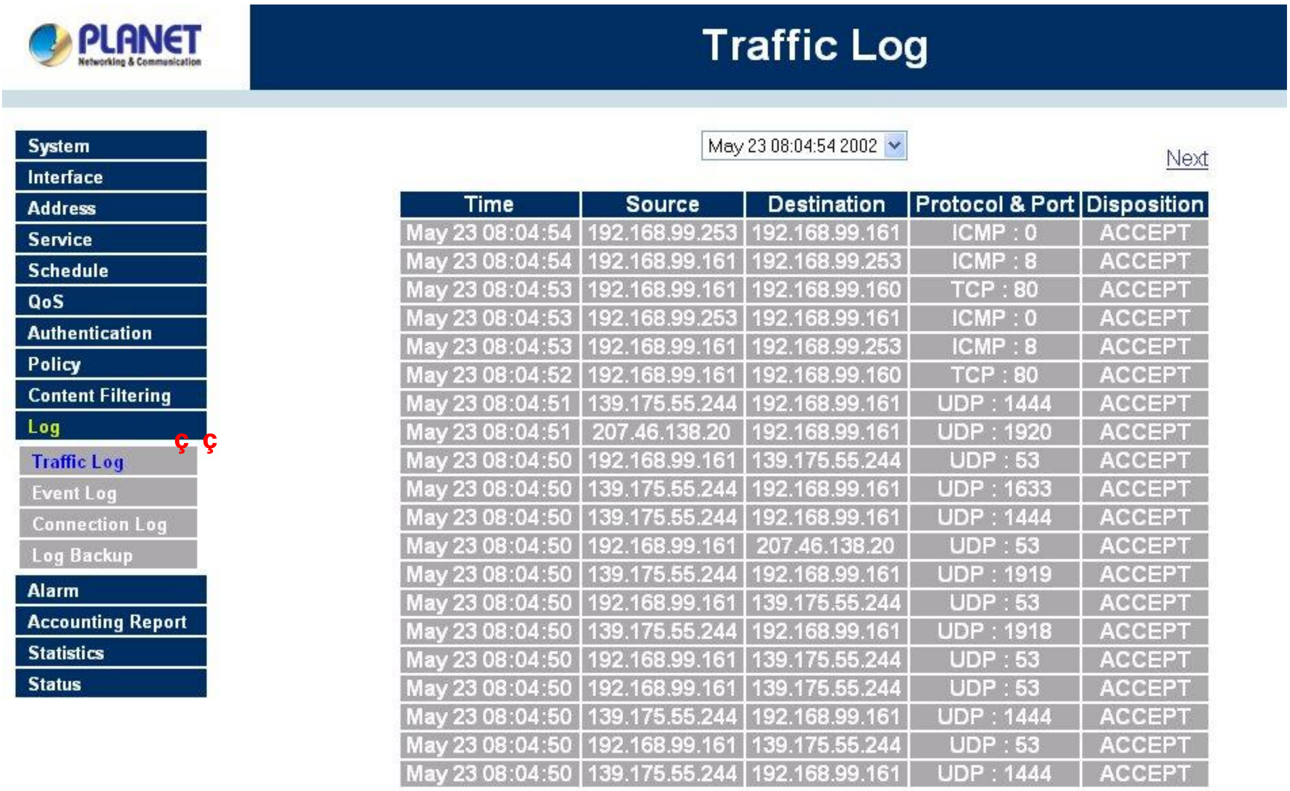
The Administrator can use the log data to monitor and manage the device and the networks. The Administrator can view the logged data to evaluate and troubleshoot the network, such as pinpointing the source of traffic congestions.

4.11.1 Traffic Log

The Administrator queries the Bandwidth Management Gateway for information, such as source address, destination address, start time, and Protocol port, of all connections.

Entering the Traffic Log window

Step 1. Click the **Traffic Log** option under **Log** menu to enter the Traffic Log window.



Time	Source	Destination	Protocol & Port	Disposition
May 23 08:04:54	192.168.99.253	192.168.99.161	ICMP : 0	ACCEPT
May 23 08:04:54	192.168.99.161	192.168.99.253	ICMP : 8	ACCEPT
May 23 08:04:53	192.168.99.161	192.168.99.160	TCP : 80	ACCEPT
May 23 08:04:53	192.168.99.253	192.168.99.161	ICMP : 0	ACCEPT
May 23 08:04:53	192.168.99.161	192.168.99.253	ICMP : 8	ACCEPT
May 23 08:04:52	192.168.99.161	192.168.99.160	TCP : 80	ACCEPT
May 23 08:04:51	139.175.55.244	192.168.99.161	UDP : 1444	ACCEPT
May 23 08:04:51	207.46.138.20	192.168.99.161	UDP : 1920	ACCEPT
May 23 08:04:50	192.168.99.161	139.175.55.244	UDP : 53	ACCEPT
May 23 08:04:50	139.175.55.244	192.168.99.161	UDP : 1633	ACCEPT
May 23 08:04:50	139.175.55.244	192.168.99.161	UDP : 1444	ACCEPT
May 23 08:04:50	192.168.99.161	207.46.138.20	UDP : 53	ACCEPT
May 23 08:04:50	139.175.55.244	192.168.99.161	UDP : 1919	ACCEPT
May 23 08:04:50	192.168.99.161	139.175.55.244	UDP : 53	ACCEPT
May 23 08:04:50	139.175.55.244	192.168.99.161	UDP : 1918	ACCEPT
May 23 08:04:50	192.168.99.161	139.175.55.244	UDP : 53	ACCEPT
May 23 08:04:50	192.168.99.161	139.175.55.244	UDP : 53	ACCEPT
May 23 08:04:50	139.175.55.244	192.168.99.161	UDP : 1444	ACCEPT
May 23 08:04:50	192.168.99.161	139.175.55.244	UDP : 53	ACCEPT
May 23 08:04:50	139.175.55.244	192.168.99.161	UDP : 1444	ACCEPT

Traffic Log Table

The table in the Traffic Log window displays current System statuses:

Definition:

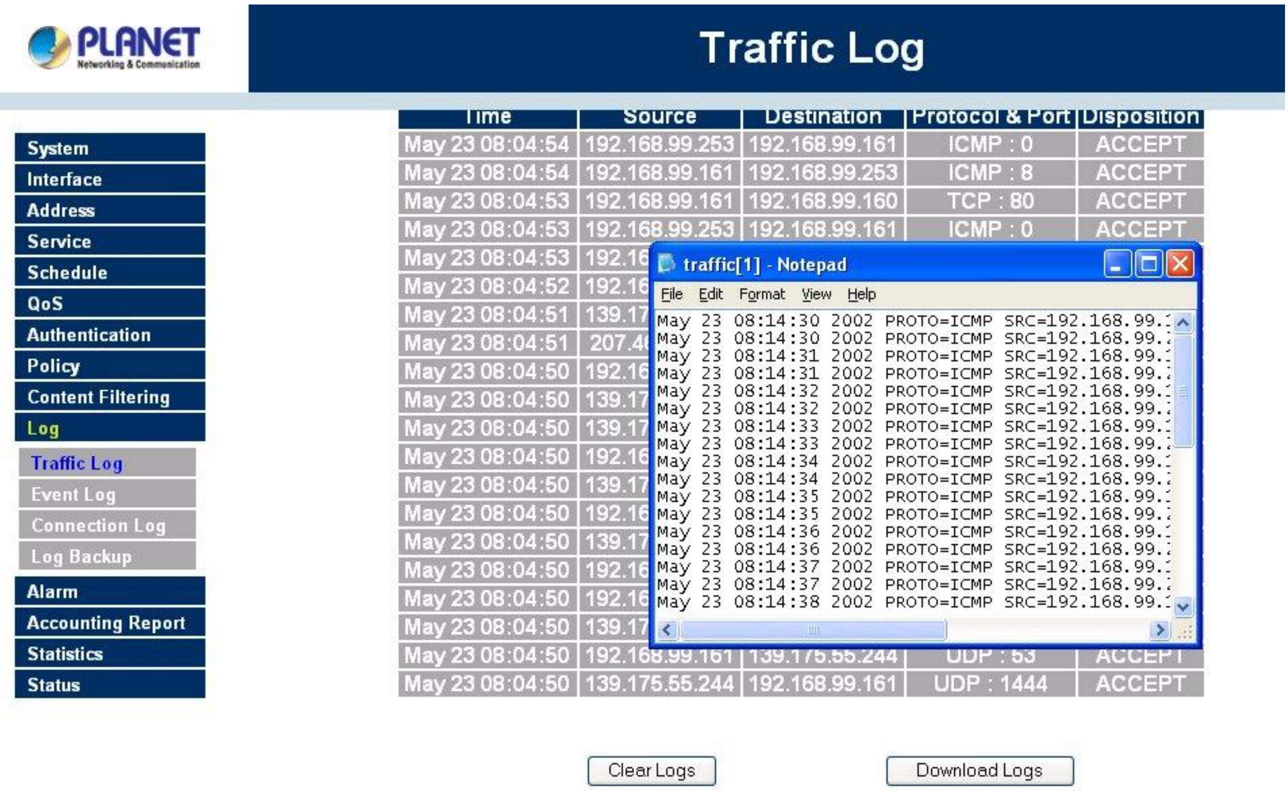
- **Time**: The start time of the connection.
- **Source:** IP address of the source network of the specific connection.
- **Destination:** IP address of the destination network of the specific connection.
- **Protocol & Port:** Protocol type and Port number of the specific connection.
- **Disposition:** Accept or Deny.

Downloading the Traffic Logs

The Administrator can backup the traffic logs regularly by downloading it to the computer.

Step 1. In the Traffic Log window, click the **Download Logs** button at the bottom of the screen.

Step 2. Follow the File Download pop-up window to save the traffic logs into a specified directory on the hard drive.



Time	Source	Destination	Protocol & Port	Disposition
May 23 08:04:54	192.168.99.253	192.168.99.161	ICMP : 0	ACCEPT
May 23 08:04:54	192.168.99.161	192.168.99.253	ICMP : 8	ACCEPT
May 23 08:04:53	192.168.99.161	192.168.99.160	TCP : 80	ACCEPT
May 23 08:04:53	192.168.99.253	192.168.99.161	ICMP : 0	ACCEPT
May 23 08:04:53	192.16			
May 23 08:04:52	192.16			
May 23 08:04:51	139.17			
May 23 08:04:51	207.4			
May 23 08:04:50	192.16			
May 23 08:04:50	139.17			
May 23 08:04:50	139.17			
May 23 08:04:50	192.16			
May 23 08:04:50	139.17			
May 23 08:04:50	192.16			
May 23 08:04:50	139.17			
May 23 08:04:50	192.16			
May 23 08:04:50	192.16			
May 23 08:04:50	139.17			
May 23 08:04:50	192.168.99.161	139.175.55.244	UDP : 53	ACCEPT
May 23 08:04:50	139.175.55.244	192.168.99.161	UDP : 1444	ACCEPT

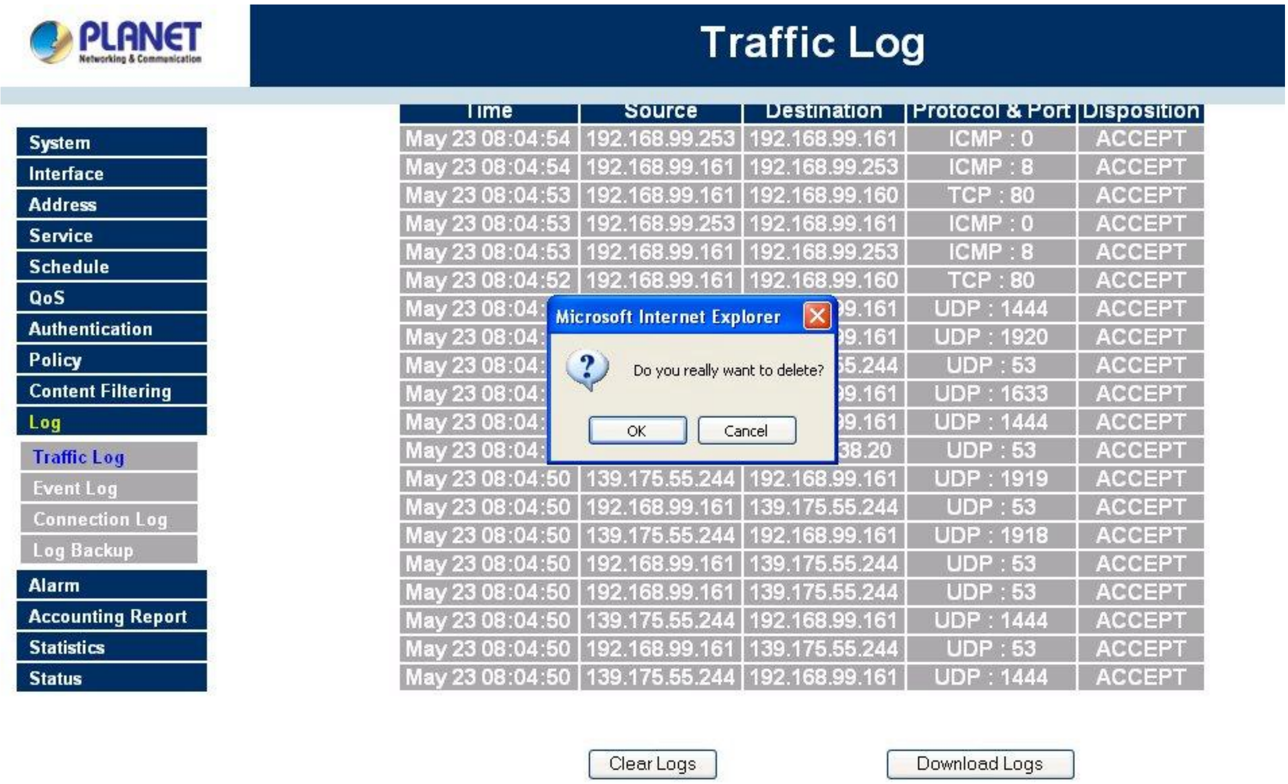
```
May 23 08:14:30 2002 PROTO=ICMP SRC=192.168.99.1
May 23 08:14:30 2002 PROTO=ICMP SRC=192.168.99.2
May 23 08:14:31 2002 PROTO=ICMP SRC=192.168.99.1
May 23 08:14:31 2002 PROTO=ICMP SRC=192.168.99.2
May 23 08:14:32 2002 PROTO=ICMP SRC=192.168.99.1
May 23 08:14:32 2002 PROTO=ICMP SRC=192.168.99.2
May 23 08:14:33 2002 PROTO=ICMP SRC=192.168.99.1
May 23 08:14:33 2002 PROTO=ICMP SRC=192.168.99.2
May 23 08:14:34 2002 PROTO=ICMP SRC=192.168.99.1
May 23 08:14:34 2002 PROTO=ICMP SRC=192.168.99.2
May 23 08:14:35 2002 PROTO=ICMP SRC=192.168.99.1
May 23 08:14:35 2002 PROTO=ICMP SRC=192.168.99.2
May 23 08:14:36 2002 PROTO=ICMP SRC=192.168.99.1
May 23 08:14:36 2002 PROTO=ICMP SRC=192.168.99.2
May 23 08:14:37 2002 PROTO=ICMP SRC=192.168.99.1
May 23 08:14:37 2002 PROTO=ICMP SRC=192.168.99.2
May 23 08:14:38 2002 PROTO=ICMP SRC=192.168.99.1
```

Clearing the Traffic Logs

The Administrator may clear on-line logs to keep just the most updated logs on the screen.

Step 1. In the Traffic Log window, click the **Clear Logs** button at the bottom of the screen.

Step 2. In the Clear Logs pop-up box, click **Ok** to clear the logs or click **Cancel** to cancel it.



Traffic Log

Time	Source	Destination	Protocol & Port	Disposition
May 23 08:04:54	192.168.99.253	192.168.99.161	ICMP : 0	ACCEPT
May 23 08:04:54	192.168.99.161	192.168.99.253	ICMP : 8	ACCEPT
May 23 08:04:53	192.168.99.161	192.168.99.160	TCP : 80	ACCEPT
May 23 08:04:53	192.168.99.253	192.168.99.161	ICMP : 0	ACCEPT
May 23 08:04:53	192.168.99.161	192.168.99.253	ICMP : 8	ACCEPT
May 23 08:04:52	192.168.99.161	192.168.99.160	TCP : 80	ACCEPT
May 23 08:04:		9.161	UDP : 1444	ACCEPT
May 23 08:04:		9.161	UDP : 1920	ACCEPT
May 23 08:04:		5.244	UDP : 53	ACCEPT
May 23 08:04:		9.161	UDP : 1633	ACCEPT
May 23 08:04:		9.161	UDP : 1444	ACCEPT
May 23 08:04:		38.20	UDP : 53	ACCEPT
May 23 08:04:50	139.175.55.244	192.168.99.161	UDP : 1919	ACCEPT
May 23 08:04:50	192.168.99.161	139.175.55.244	UDP : 53	ACCEPT
May 23 08:04:50	139.175.55.244	192.168.99.161	UDP : 1918	ACCEPT
May 23 08:04:50	192.168.99.161	139.175.55.244	UDP : 53	ACCEPT
May 23 08:04:50	192.168.99.161	139.175.55.244	UDP : 53	ACCEPT
May 23 08:04:50	139.175.55.244	192.168.99.161	UDP : 1444	ACCEPT
May 23 08:04:50	192.168.99.161	139.175.55.244	UDP : 53	ACCEPT
May 23 08:04:50	139.175.55.244	192.168.99.161	UDP : 1444	ACCEPT

Microsoft Internet Explorer

Do you really want to delete?

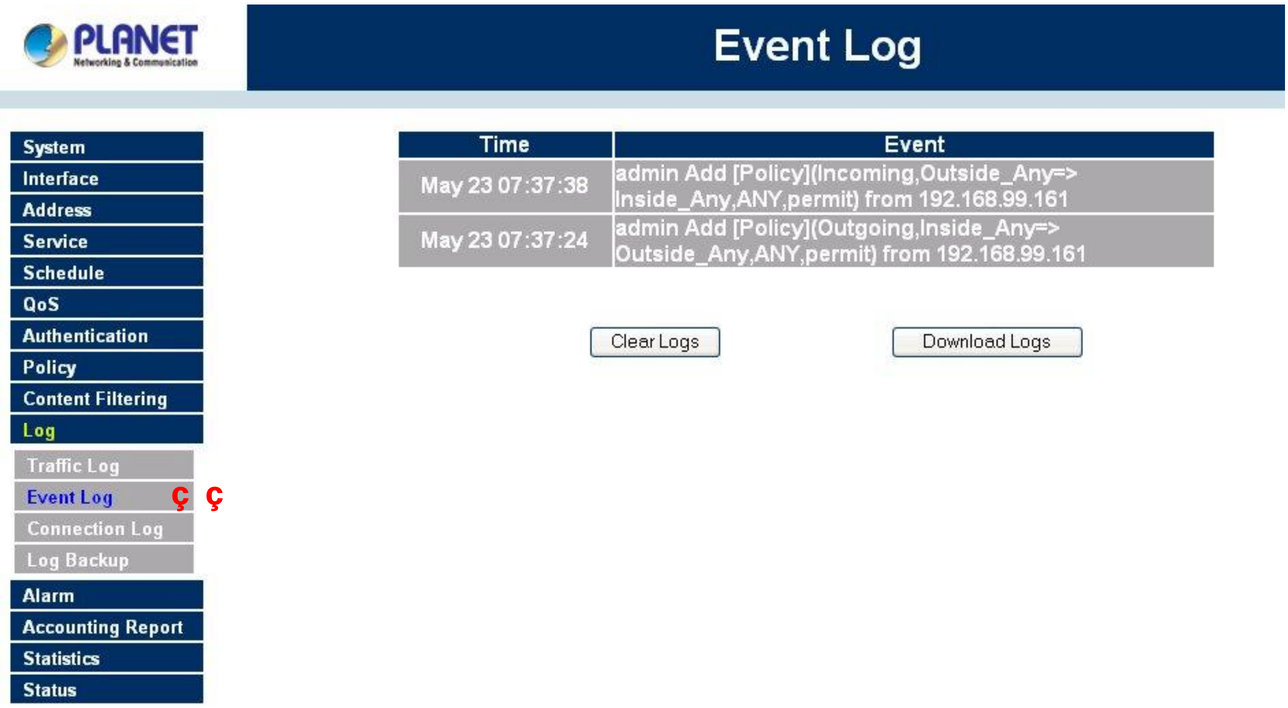
OK Cancel

4.11.2 Event Log

When the Bandwidth Management Gateway WAN detects events, the Administrator can get the details, such as time and description of the events from the Event Logs.

Entering the Event Log window

Step 1. Click the **Event Log** option under the **Log** menu and the Event Log window will appear.



Time	Event
May 23 07:37:38	admin Add [Policy](Incoming,Outside_Any=> Inside_Any,ANY,permit) from 192.168.99.161
May 23 07:37:24	admin Add [Policy](Outgoing,Inside_Any=> Outside_Any,ANY,permit) from 192.168.99.161

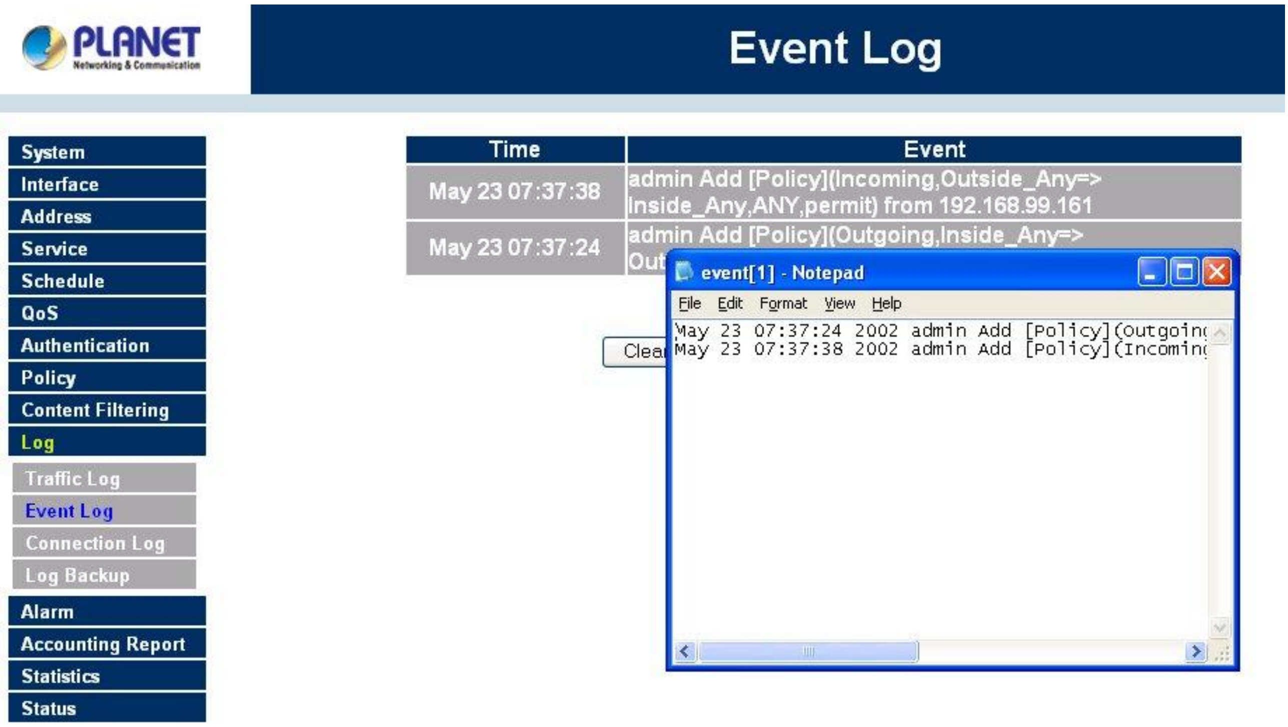
Step 2. The table in the Event Log window displays the time and description of the events.

- **Time:** time when the event occurred.
- **Event:** description of the event.

Downloading the Event Logs

Step 1. In the Event Log window, click the Download Logs button at the bottom of the screen.

Step 2. Follow the File Download pop-up window to save the event logs into a specific directory on the hard drive.



Time	Event
May 23 07:37:38	admin Add [Policy](Incoming,Outside_Any=> Inside_Any,ANY,permit) from 192.168.99.161
May 23 07:37:24	admin Add [Policy](Outgoing,Inside_Any=> Out

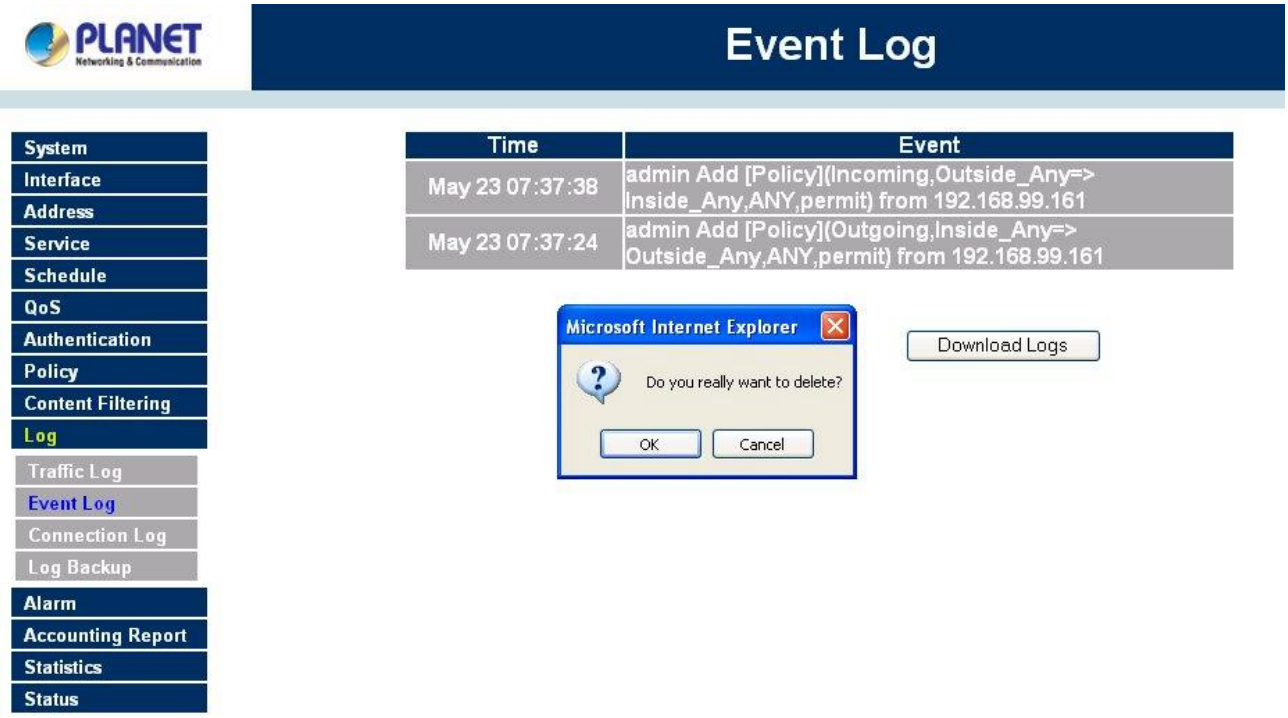
```
May 23 07:37:24 2002 admin Add [Policy](Outgoinc
May 23 07:37:38 2002 admin Add [Policy](Incominc
```

Clearing the Event Logs

The Administrator may clear on-line event logs to keep just the most updated logs on the screen.

Step 1. In the Event Log window, click the Clear Logs button at the bottom of the screen.

Step 2. In the Clear Logs pop-up box, click **OK** to clear the logs or click **Cancel** to cancel it.

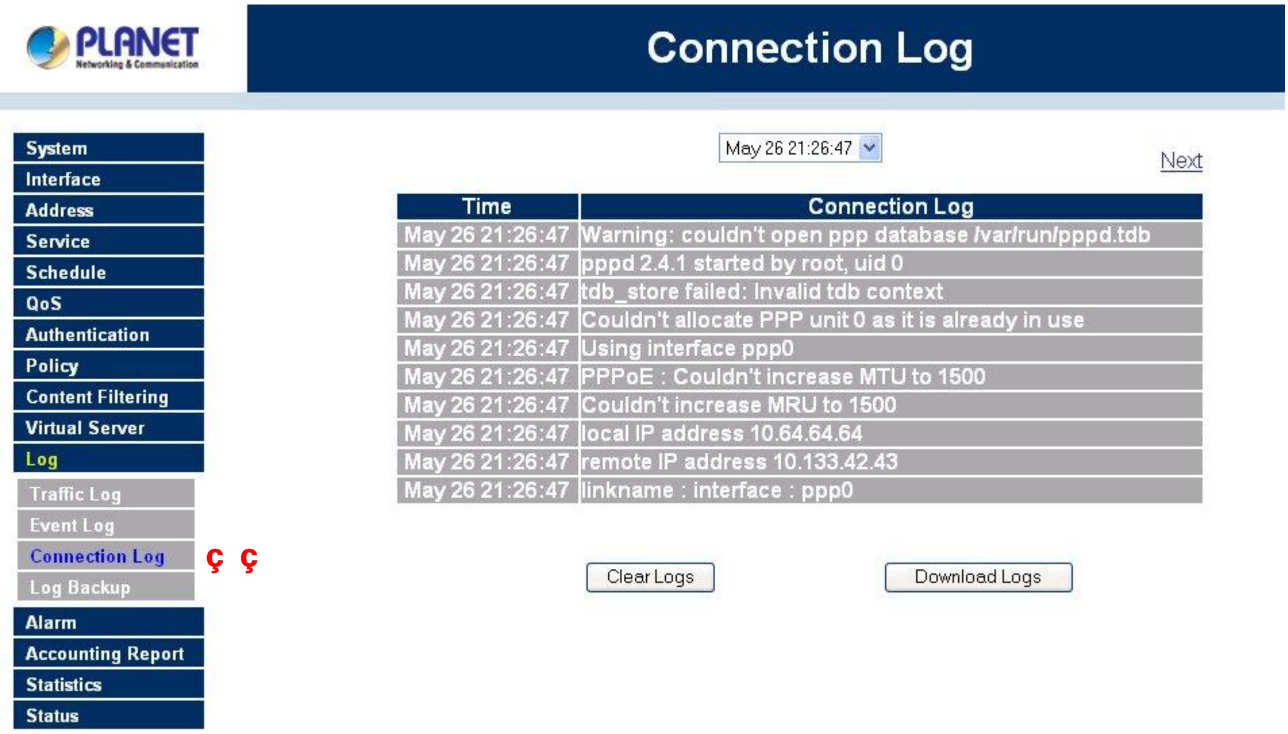


Time	Event
May 23 07:37:38	admin Add [Policy](Incoming,Outside_Any=> Inside_Any,ANY,permit) from 192.168.99.161
May 23 07:37:24	admin Add [Policy](Outgoing,Inside_Any=> Outside_Any,ANY,permit) from 192.168.99.161

Do you really want to delete?

4.11.3 Connection Log

Click Log in the menu bar on the left hand side, and then select the sub-selection Connection Log.



Time	Connection Log
May 26 21:26:47	Warning: couldn't open ppp database /var/run/pppd.tdb
May 26 21:26:47	pppd 2.4.1 started by root, uid 0
May 26 21:26:47	tdb_store failed: Invalid tdb context
May 26 21:26:47	Couldn't allocate PPP unit 0 as it is already in use
May 26 21:26:47	Using interface ppp0
May 26 21:26:47	PPPoE : Couldn't increase MTU to 1500
May 26 21:26:47	Couldn't increase MRU to 1500
May 26 21:26:47	local IP address 10.64.64.64
May 26 21:26:47	remote IP address 10.133.42.43
May 26 21:26:47	linkname : interface : ppp0

Definition:

Time: The start and end time of connection.

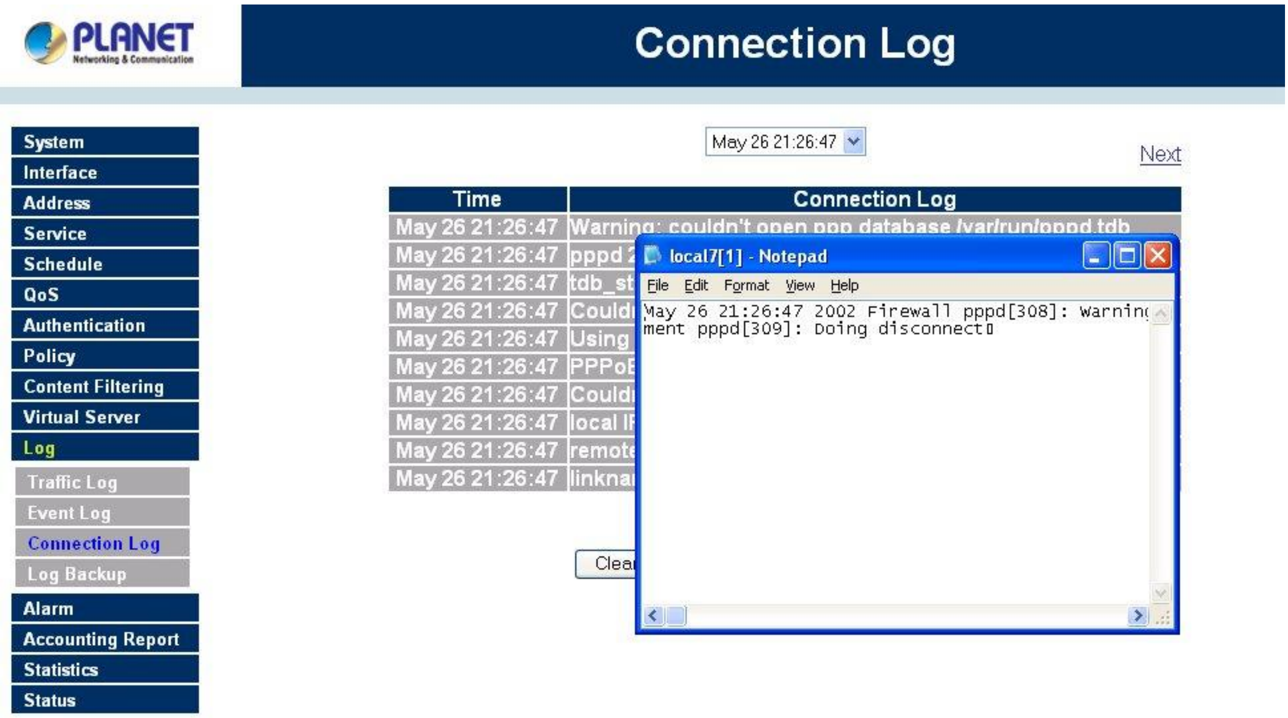
Connection Log: Event description during connection.

Download Logs

Step 1. Click **Log** in the menu bar on the left hand side and then select the sub-selection **Connection Log**.

Step 2. In Connection Log window, click the **Download Logs** button.

Step 3. In the Download Logs window, save the logs to the specified location.



Time	Connection Log
May 26 21:26:47	Warning: couldn't open ppp database /var/run/pppd.tdb
May 26 21:26:47	pppd 2
May 26 21:26:47	tdb_st
May 26 21:26:47	Couldi
May 26 21:26:47	Using
May 26 21:26:47	PPPoE
May 26 21:26:47	Couldi
May 26 21:26:47	local IF
May 26 21:26:47	remote
May 26 21:26:47	linknar

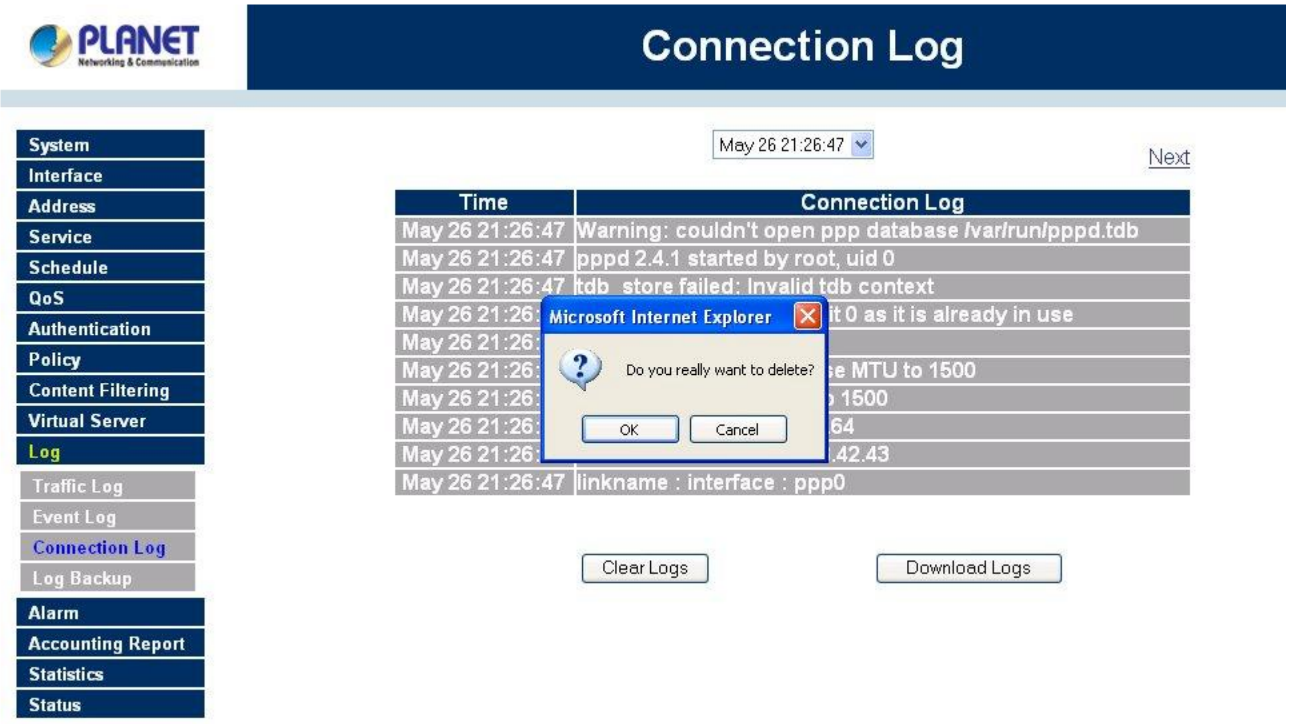
```
May 26 21:26:47 2002 Firewall pppd[308]: Warnin(
ment pppd[309]: Doing disconnect□
```

Clear Logs

Step 1. Click **Log** in the menu bar on the left hand side, and then select the sub-selection **Connection Logs**.

Step 2. In Connection Log window, click the **Clear Logs** button.

Step 3. In Clear Logs window, click **OK** to clear the logs or click **Cancel** to discard changes.



Time	Connection Log
May 26 21:26:47	Warning: couldn't open ppp database /var/run/pppd.tdb
May 26 21:26:47	pppd 2.4.1 started by root, uid 0
May 26 21:26:47	tdb_store failed: Invalid tdb context
May 26 21:26	t 0 as it is already in use
May 26 21:26	
May 26 21:26	e MTU to 1500
May 26 21:26	1500
May 26 21:26	64
May 26 21:26	.42.43
May 26 21:26:47	linkname : interface : ppp0

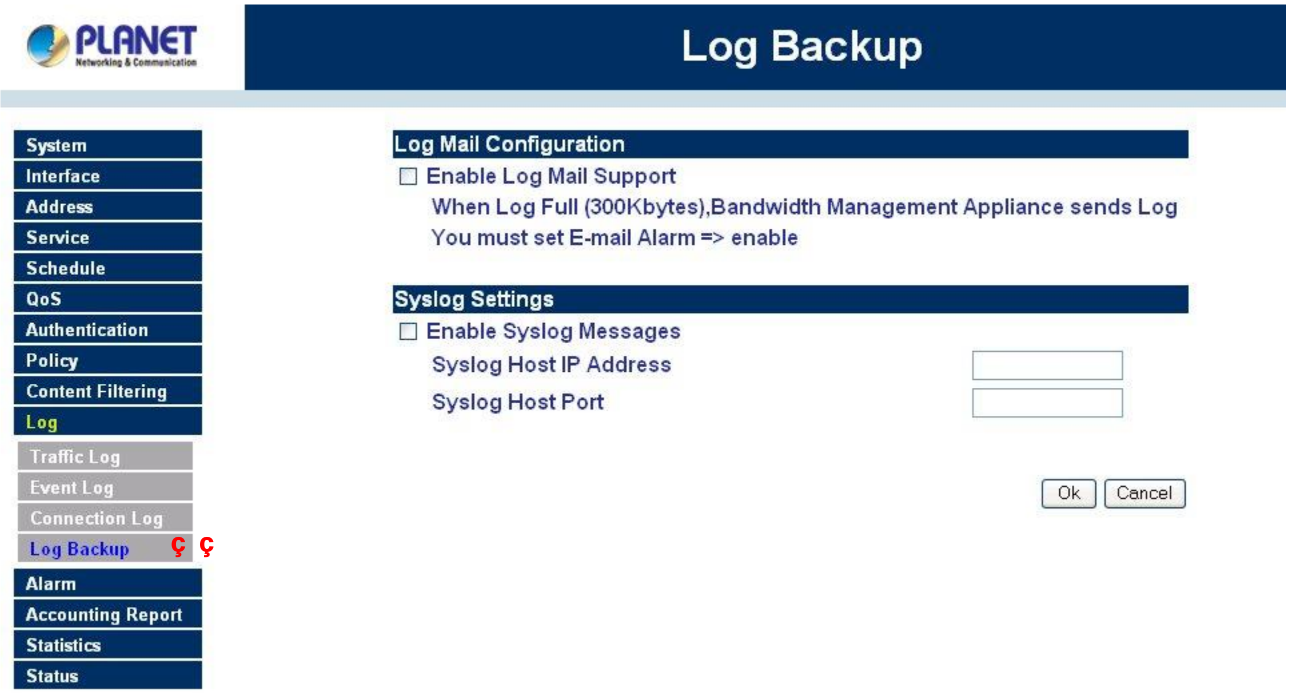
Microsoft Internet Explorer

Do you really want to delete?

OK Cancel

4.11.4 Log Backup

Step 1. Click **Log à Log Backup**.



Log Mail Configuration

□ Enable Log Mail Support

When Log Full (300Kbytes),Bandwidth Management Appliance sends Log

You must set E-mail Alarm => enable

Syslog Settings

□ Enable Syslog Messages

Syslog Host IP Address

Syslog Host Port

Log Mail Configuration: When the Log Mail files accumulated up to 300Kbytes, router will notify administrator by email with the traffic log and event log.

NOTE: Before enabling this function, you have to configure E-mail Settings in System -> Settings.

Syslog Settings: If you enable this function, system will transmit the Traffic Log and the Event Log simultaneously to the server which supports Syslog function.

NOTE: To restart Connection Log, click the **Refresh** button on the right hand side in Log window.

Enable Log Mail Support & Syslog Message

Log Mail Configuration /Enable Log Mail Support

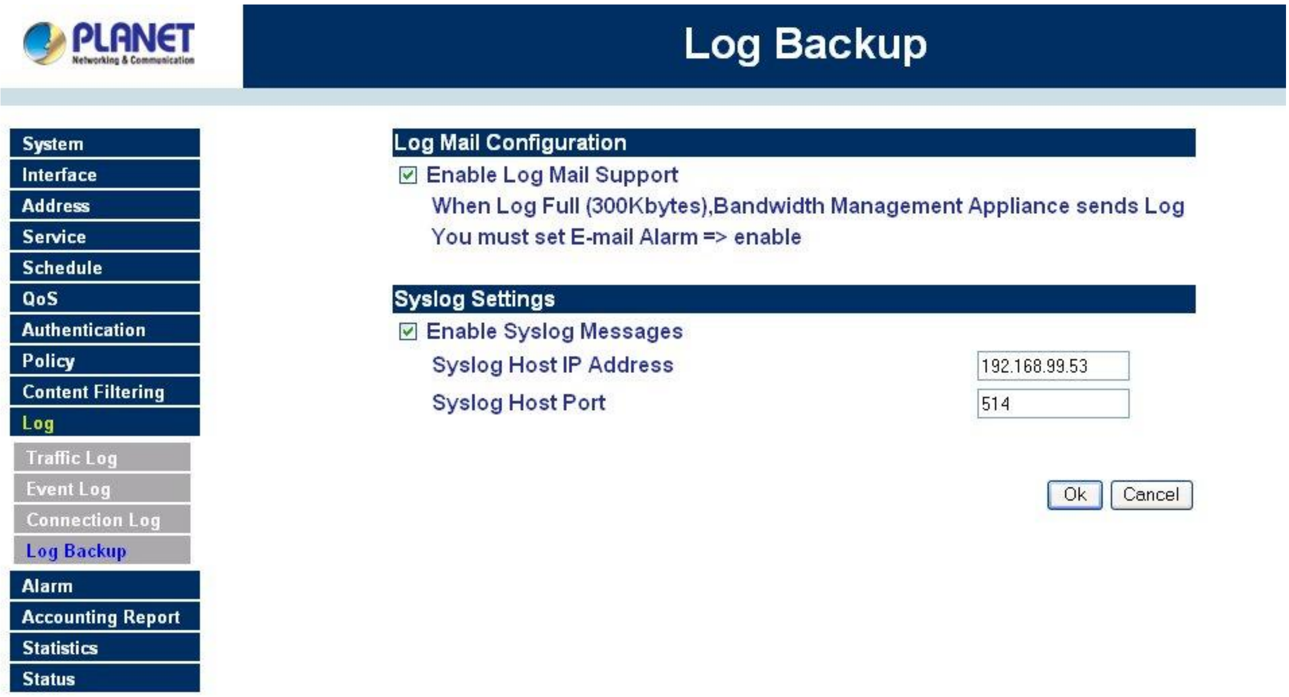
Step 1. Firstly, go to **Admin** –Select **Enable E-mail Alert Notification** under **E-Mail Settings**. Enter the e-mail address to receive the alarm notification. Click **OK**.

Step 2. Go to **LOG àLog Backup.** Check to enable **Log Mail Support.** Click **OK.**

System Settings/Enable Syslog Message

Step 1. Check to enable Syslog Message. Enter the Host IP Address and Host Port number to receive the Syslog message.

Step 2. Click **OK**.



Log Backup

Log Mail Configuration

☑ Enable Log Mail Support

When Log Full (300Kbytes),Bandwidth Management Appliance sends Log

You must set E-mail Alarm => enable

Syslog Settings

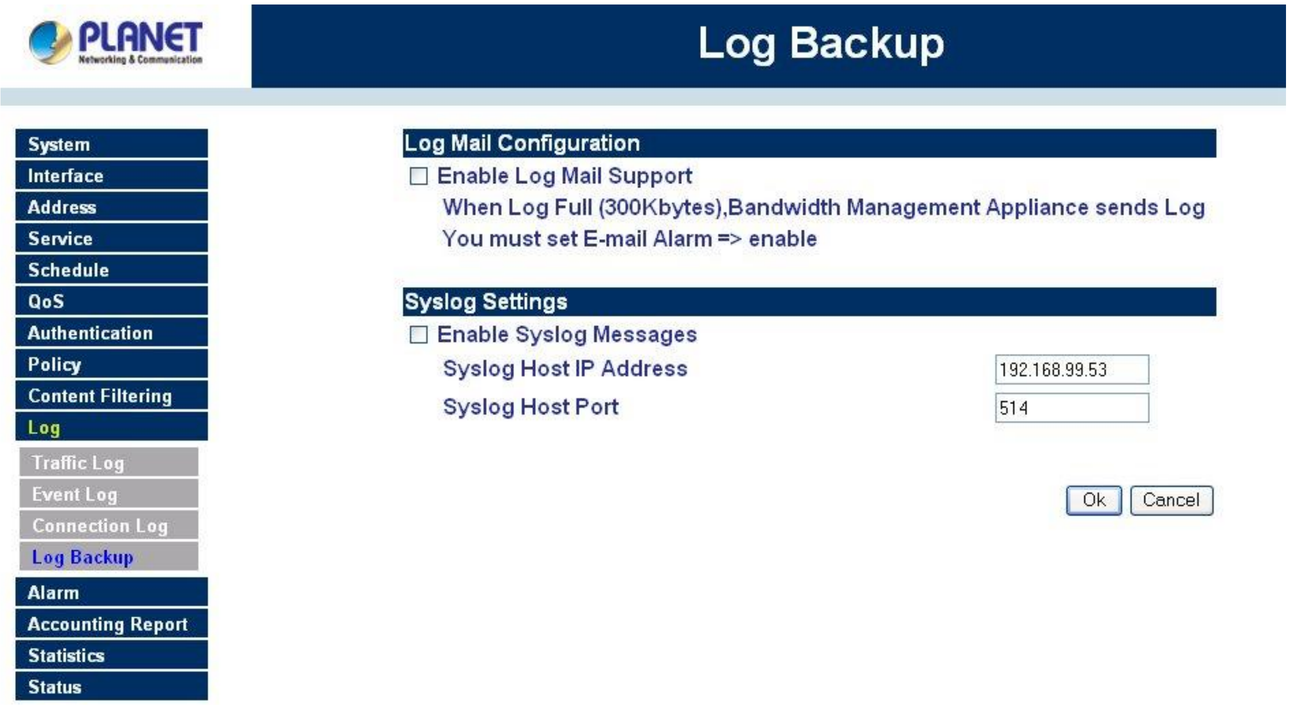
☑ Enable Syslog Messages

Syslog Host IP Address	192.168.99.53
Syslog Host Port	514

Disable Log Mail Support & Syslog Message

Step 1. Go to **LOG àLog Backup**. Uncheck to disable Log Mail Support. Click **OK**.

Step 2. Go to **LOG à Log Backup**. Uncheck to disable Settings Message. Click **OK**.



Log Mail Configuration

☐ Enable Log Mail Support

When Log Full (300Kbytes),Bandwidth Management Appliance sends Log

You must set E-mail Alarm => enable

Syslog Settings

☐ Enable Syslog Messages

Syslog Host IP Address: 192.168.99.53

Syslog Host Port: 514

4.12 Alarm

In this chapter, the Administrator can view traffic alarms and event alarms that occur and the Bandwidth Management Gateway has logged.
Bandwidth Management Gateway has two alarms: **Traffic Alarm** and **Event Alarm**.

Traffic alarm:

In control policies, the Administrator set the threshold value for traffic alarm. The System regularly checks whether the traffic for a policy exceeds its threshold value and adds a record to the traffic alarm file if it does.

Event alarm:

When Bandwidth Management Gateway detects attacks from hackers, it writes attacking data in the event alarm file and sends an e-mail alert to the Administrator to take emergency steps.

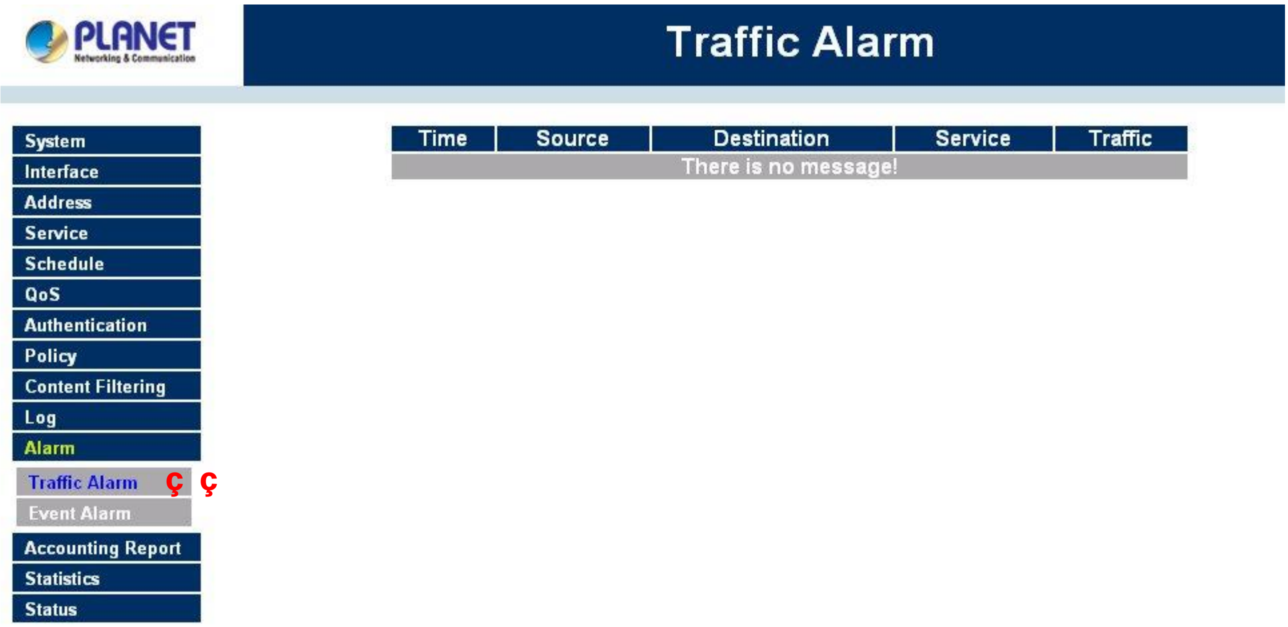
4.12.1 Traffic Alarm

How to apply Traffic Alarm

The administrator can use Traffic Alarm to track the Source Address, Destination Address, network service and the status of network. The administrator can save Traffic Logs and Event Logs for a pre-determined time and then delete them to keep the newest log.
In control policies, the Administrator set the threshold value for traffic alarm. The System regularly checks whether the traffic for a policy exceeds its threshold value and adds a record to the traffic alarm file if it does.

Entering the Traffic Alarm window

Step 1. Click the **Traffic Alarm** option below **Alarm** menu to enter the Traffic Alarm window.



Time	Source	Destination	Service	Traffic
There is no message!				

Step 2. The table in the Traffic Alarm window displays the current traffic alarm logs for connections.

- **Time:** The start and stop time of the specific connection.
- **Source:** Name of the source network of the specific connection.
- **Destination:** Name of the destination network of the specific connection.
- **Service:** Service of the specific connection.
- **Traffic:** Traffic (in Kbytes/Sec) of the specific connection.

Downloading the Traffic Alarm Logs

The Administrator can back up traffic alarm logs regularly and download it to a file on the computer.

Step 1. In the Traffic Alarm window, click the **Download Logs** button on the bottom of the screen.

Step 2. Follow the File Download pop-up box to save the traffic alarm logs into specific directory on the hard drive.

Clearing the Traffic Alarm Logs

Step 1. In the Traffic Alarm window, click the **Clear Logs** button at the bottom of the screen.

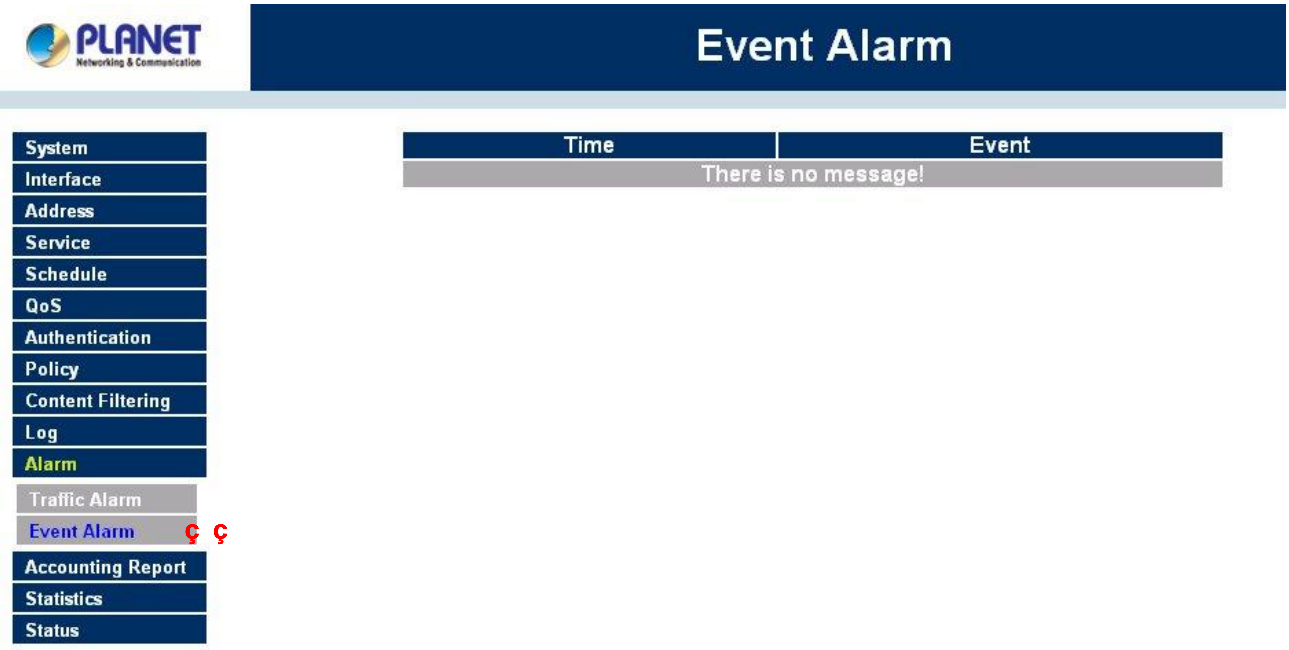
Step 2. In the Clear Logs pop-up box, click **Ok** to clear the logs or click **Cancel** to cancel.

4.12.2 Event Alarm

When Bandwidth Management Gateway detects attacks from hackers, it writes attacking data in the event alarm file and sends an e-mail alert to the Administrator to take emergency steps.

Entering the Event Alarm window

Step 1. Click the **Event Alarm** option below the **Alarm** menu to enter the Event Alarm window.



Time	Event
There is no message!	

The table in Event Alarm window displays current traffic alarm logs for connections.

- **Time:** log time.
- **Event:** event descriptions.

Downloading the Event Alarm Logs

The Administrator can back up event alarm logs regularly by downloading it to a file on the computer.

Step 1. In the Event Alarm window, click the **Download Logs** button at the bottom of the screen.

Step 2. Follow the File Download pop-up box to save the event alarm logs into specific directory on the hard drive.

Clearing Event Alarm Logs

The Administrator may clear on-line logs to keep the most updated logs on the screen.

Step 1. In the Event Alarm window, click the Clear Logs button at the bottom of the screen.

Step 2. In the Clear Logs pop-up box, click **OK**.

4.13 Accounting Report

Accounting Report can be divided into two parts, one is Outbound Accounting Report, and the other is Inbound Accounting Report.

Outbound Accounting Report is the statistics of the downstream and upstream of the LAN, WAN and all kinds of communication services.

Source IP: the IP address used by LAN users who use Bandwidth Management Gateway

Destination IP: The IP address used by WAN service server which uses Bandwidth Management Gateway.

Service: The communication service which listed in the pull-down menu when LAN users use bandwidth Management Gateway to connect to WAN service server.

Inbound Accounting Report is the statistics of downstream/upstream for all kinds of communication services; the Inbound Accounting report will be shown when WAN user uses Bandwidth Management Gateway to connect to LAN Service Server.

Source IP: the IP address used by WAN users who use Bandwidth Management Gateway

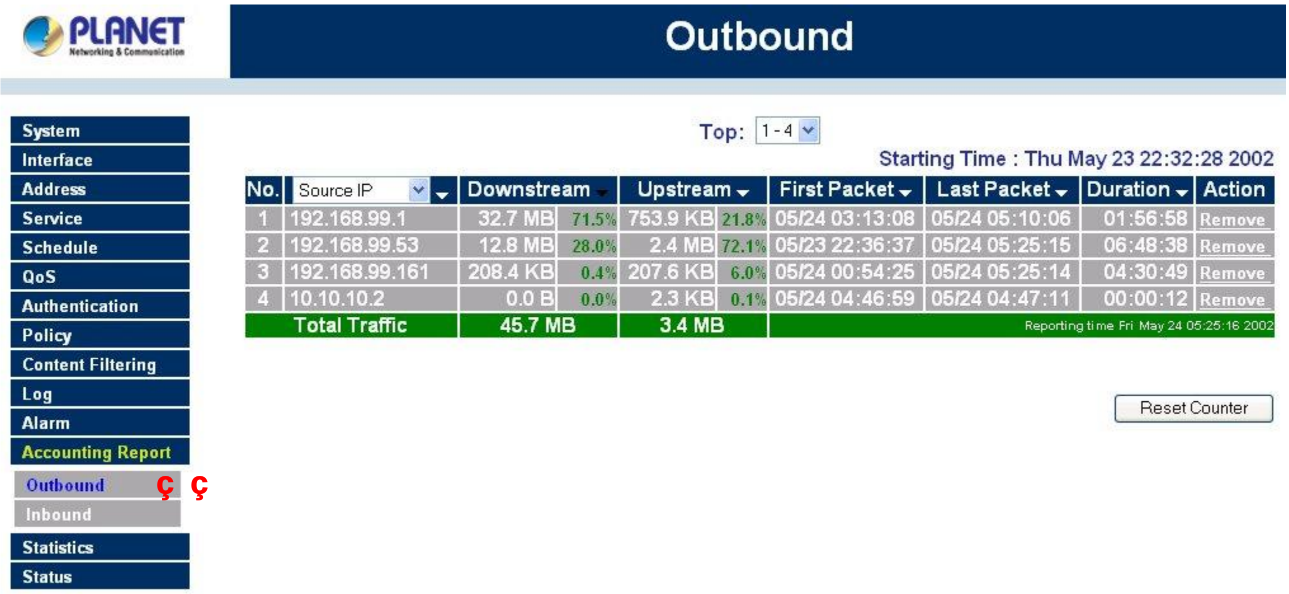
Destination IP: the IP address used by LAN service server who use Bandwidth Management Gateway

Service: The communication service which listed in the pull-down menu when WAN users use bandwidth Management Gateway to connect to LAN Service server..

Administrator can use this Accounting Report to inquire the LAN IP users and WAN IP users, and to gather the statistics of Downstream/Upstream, First packet/Last packet/Duration and the service of all the user's IP that passes the Bandwidth Management Gateway.

4.13.1 Outbound Accounting Report

Step 1. Click the **Accounting Report** function, and then select **Outbound**.



Top: 1 - 4

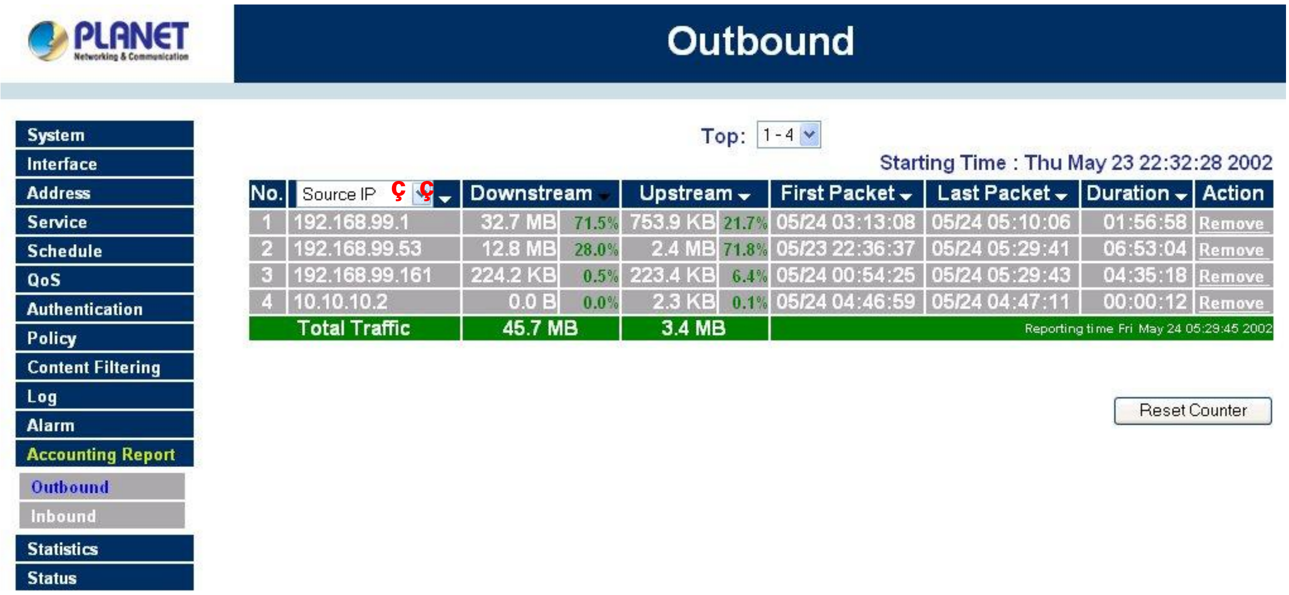
Starting Time : Thu May 23 22:32:28 2002

No.	Source IP	Downstream		Upstream		First Packet	Last Packet	Duration	Action
1	192.168.99.1	32.7 MB	71.5%	753.9 KB	21.8%	05/24 03:13:08	05/24 05:10:06	01:56:58	Remove
2	192.168.99.53	12.8 MB	28.0%	2.4 MB	72.1%	05/23 22:36:37	05/24 05:25:15	06:48:38	Remove
3	192.168.99.161	208.4 KB	0.4%	207.6 KB	6.0%	05/24 00:54:25	05/24 05:25:14	04:30:49	Remove
4	10.10.10.2	0.0 B	0.0%	2.3 KB	0.1%	05/24 04:46:59	05/24 04:47:11	00:00:12	Remove
Total Traffic		45.7 MB		3.4 MB		Reporting time Fri May 24 05:25:16 2002			

Reset Counter

Outbound source IP Accounting Report

When LAN users use Bandwidth Management Gateway to connect to WAN service server, all of the Downstream/Upstream/First Packet/Last Packet/Duration log of the source IP will be recorded.



Top: 1 - 4

Starting Time : Thu May 23 22:32:28 2002

No.	Source IP	Downstream		Upstream		First Packet	Last Packet	Duration	Action
1	192.168.99.1	32.7 MB	71.5%	753.9 KB	21.7%	05/24 03:13:08	05/24 05:10:06	01:56:58	Remove
2	192.168.99.53	12.8 MB	28.0%	2.4 MB	71.8%	05/23 22:36:37	05/24 05:29:41	06:53:04	Remove
3	192.168.99.161	224.2 KB	0.5%	223.4 KB	6.4%	05/24 00:54:25	05/24 05:29:43	04:35:18	Remove
4	10.10.10.2	0.0 B	0.0%	2.3 KB	0.1%	05/24 04:46:59	05/24 04:47:11	00:00:12	Remove
Total Traffic		45.7 MB		3.4 MB		Reporting time Fri May 24 05:29:45 2002			

Reset Counter

Definitions:

TOP: Select the data you want to view, it presents 10 results in one page.

Pull-down menu selection

Source IP: The IP address used by LAN users who use Bandwidth Management gateway to connect to WAN service server.

Downstream: The percentage of downstream and the value of each WAN service server which uses

Bandwidth Management Gateway to LAN user.

Upstream: The percentage of upstream and the value of each LAN user who uses Bandwidth Management Gateway to WAN service server

First Packet: When the first packet is sent to WAN service server from LAN user, the sent time will be recorded by the Bandwidth Management Gateway.

Last Packet: When the last packet sent from WAN service server is received by the LAN user, the sent time will be recorded by the Bandwidth Management Gateway.

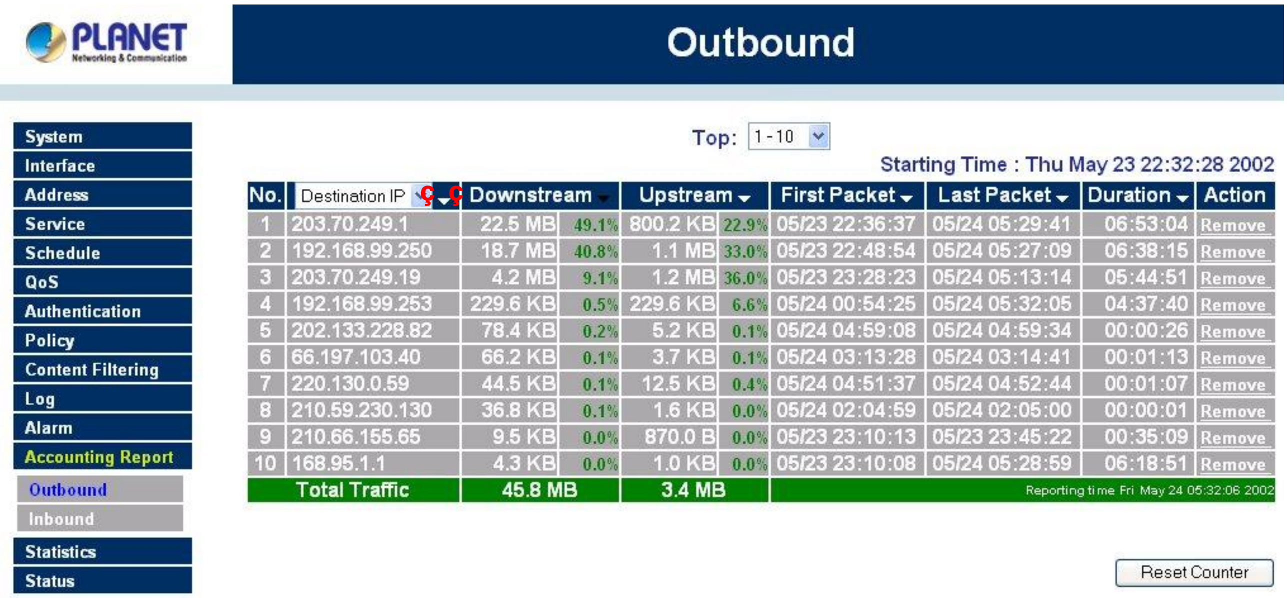
Duration: The period of time which starts from the first packet to the last packet to be recorded.

Total Traffic: The Bandwidth Management Gateway will record the sum of packet sent/receive time and show the percentage of each LAN user's upstream/downstream to WAN service server.

Reset Counter: Click **Reset Counter** button to refresh Accounting Report.

Outbound Destination IP Accounting Report

When WAN service server uses Bandwidth Management Gateway to connect to LAN user, all of the Downstream/Upstream/First Packet/Last Packet/Duration log of the Destination IP will be recorded.



Outbound

Top: 1-10

Starting Time : Thu May 23 22:32:28 2002

No.	Destination IP	Downstream		Upstream		First Packet	Last Packet	Duration	Action
1	203.70.249.1	22.5 MB	49.1%	800.2 KB	22.9%	05/23 22:36:37	05/24 05:29:41	06:53:04	Remove
2	192.168.99.250	18.7 MB	40.8%	1.1 MB	33.0%	05/23 22:48:54	05/24 05:27:09	06:38:15	Remove
3	203.70.249.19	4.2 MB	9.1%	1.2 MB	36.0%	05/23 23:28:23	05/24 05:13:14	05:44:51	Remove
4	192.168.99.253	229.6 KB	0.5%	229.6 KB	6.6%	05/24 00:54:25	05/24 05:32:05	04:37:40	Remove
5	202.133.228.82	78.4 KB	0.2%	5.2 KB	0.1%	05/24 04:59:08	05/24 04:59:34	00:00:26	Remove
6	66.197.103.40	66.2 KB	0.1%	3.7 KB	0.1%	05/24 03:13:28	05/24 03:14:41	00:01:13	Remove
7	220.130.0.59	44.5 KB	0.1%	12.5 KB	0.4%	05/24 04:51:37	05/24 04:52:44	00:01:07	Remove
8	210.59.230.130	36.8 KB	0.1%	1.6 KB	0.0%	05/24 02:04:59	05/24 02:05:00	00:00:01	Remove
9	210.66.155.65	9.5 KB	0.0%	870.0 B	0.0%	05/23 23:10:13	05/23 23:45:22	00:35:09	Remove
10	168.95.1.1	4.3 KB	0.0%	1.0 KB	0.0%	05/23 23:10:08	05/24 05:28:59	06:18:51	Remove
	Total Traffic	45.8 MB		3.4 MB		Reporting time Fri May 24 05:32:06 2002			

Reset Counter

Definition:

TOP: Select the data you want to view, it presents 10 results in one page.

Pull-down menu selection

Destination IP: The IP address used by WAN service server which uses Bandwidth Management Gateway.

Downstream: The percentage of downstream and the value of each WAN service server which uses Bandwidth Management Gateway to LAN user.

Upstream: The percentage of upstream and the value of each LAN user who uses Bandwidth Management Gateway to WAN service server.

First Packet: When the first packet is sent from WAN service server to LAN users, the sent time will be recorded by the Bandwidth Management Gateway.

Last Packet: When the last packet from LAN user is sent to WAN service server, the sent time will be recorded by the Bandwidth Management Gateway.

Duration: The period of time which starts from the first packet to the last packet to be recorded.

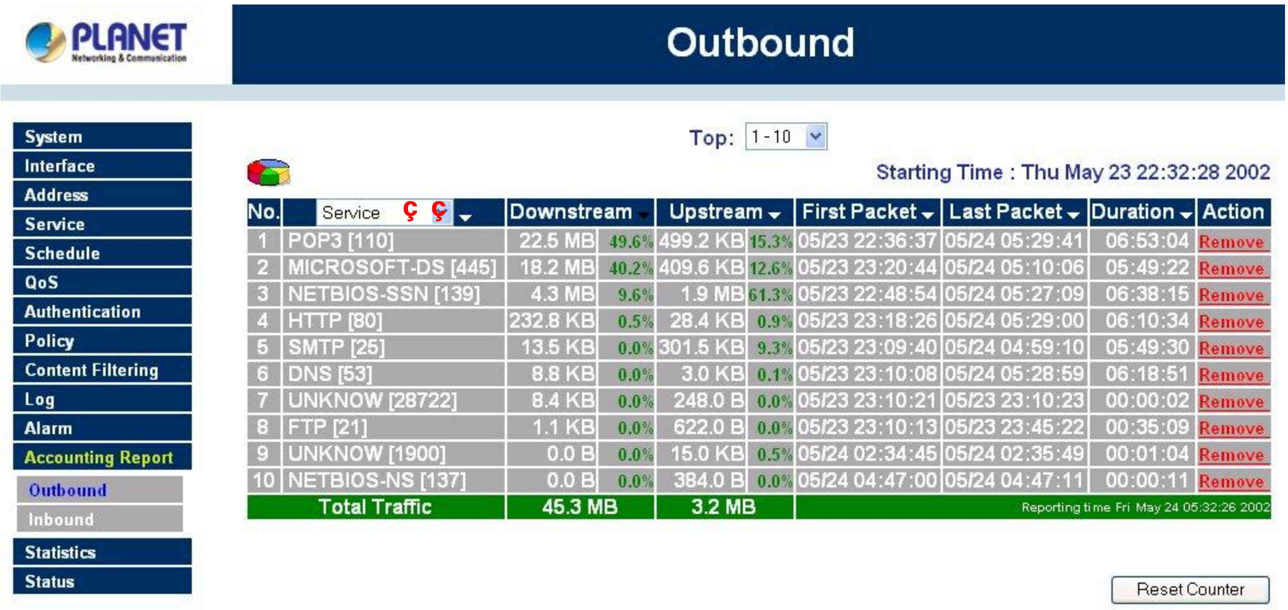
Total Traffic: The Bandwidth Management Gateway will record the sum of time and show the percentage of each WAN service server's upstream/downstream to LAN user.

Reset Counter: Click **Reset Counter** button to refresh Accounting Report.

Outbound Service Accounting Report

When LAN users use Bandwidth Management Gateway to connect to WAN Service Server, all of the Downstream / Upstream / First Packet / Last Packet / Duration log of the Communication Service will be recorded.

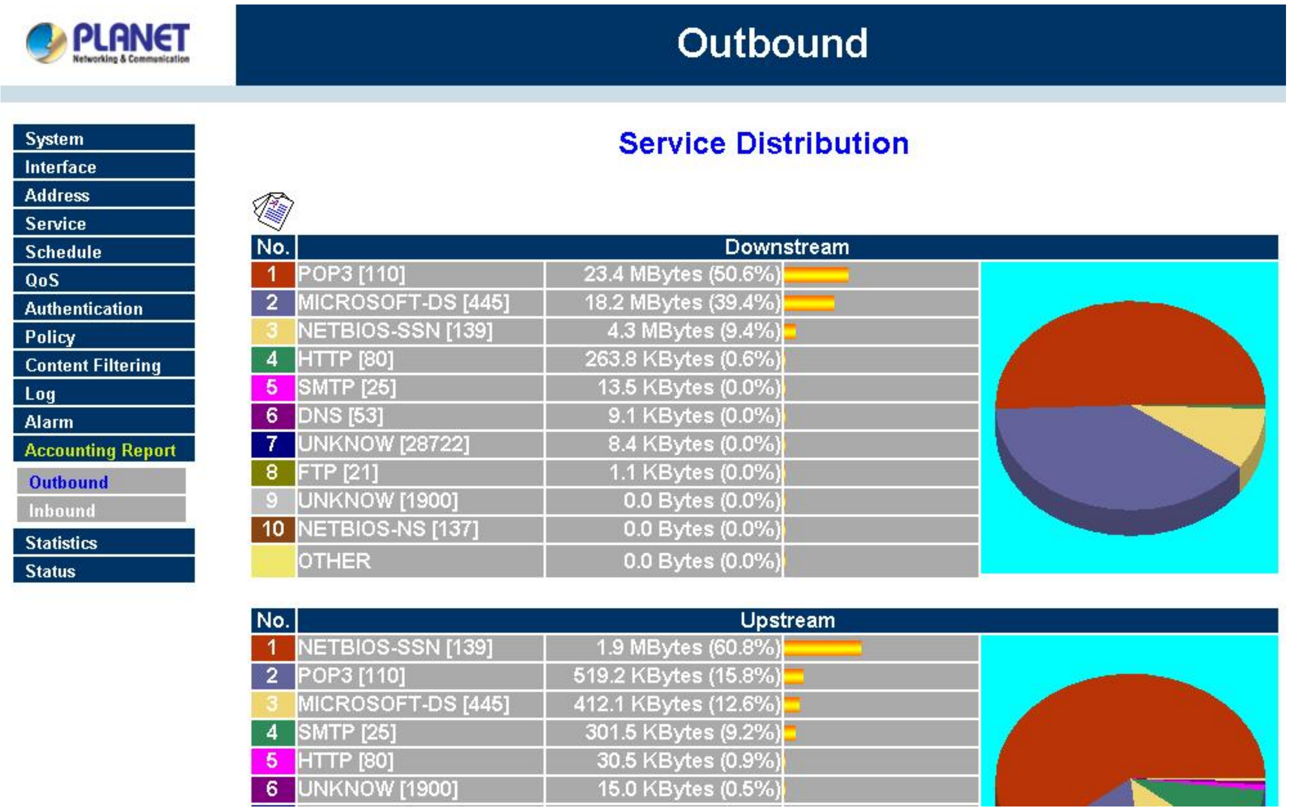
NOTE: To correctly display the pizza chart, please install the latest java VM for http://www.java.com.



Top: 1 - 10

Starting Time : Thu May 23 22:32:28 2002

No.	Service	Downstream		Upstream		First Packet	Last Packet	Duration	Action
1	POP3 [110]	22.5 MB	49.6%	499.2 KB	15.3%	05/23 22:36:37	05/24 05:29:41	06:53:04	Remove
2	MICROSOFT-DS [445]	18.2 MB	40.2%	409.6 KB	12.6%	05/23 23:20:44	05/24 05:10:06	05:49:22	Remove
3	NETBIOS-SSN [139]	4.3 MB	9.6%	1.9 MB	61.3%	05/23 22:48:54	05/24 05:27:09	06:38:15	Remove
4	HTTP [80]	232.8 KB	0.5%	28.4 KB	0.9%	05/23 23:18:26	05/24 05:29:00	06:10:34	Remove
5	SMTP [25]	13.5 KB	0.0%	301.5 KB	9.3%	05/23 23:09:40	05/24 04:59:10	05:49:30	Remove
6	DNS [53]	8.8 KB	0.0%	3.0 KB	0.1%	05/23 23:10:08	05/24 05:28:59	06:18:51	Remove
7	UNKNOW [28722]	8.4 KB	0.0%	248.0 B	0.0%	05/23 23:10:21	05/23 23:10:23	00:00:02	Remove
8	FTP [21]	1.1 KB	0.0%	622.0 B	0.0%	05/23 23:10:13	05/23 23:45:22	00:35:09	Remove
9	UNKNOW [1900]	0.0 B	0.0%	15.0 KB	0.5%	05/24 02:34:45	05/24 02:35:49	00:01:04	Remove
10	NETBIOS-NS [137]	0.0 B	0.0%	384.0 B	0.0%	05/24 04:47:00	05/24 04:47:11	00:00:11	Remove
Total Traffic		45.3 MB		3.2 MB		Reporting time Fri May 24 05:32:26 2002			



Outbound

Service Distribution

No.	Downstream	
1	POP3 [110]	23.4 MBytes (50.6%)
2	MICROSOFT-DS [445]	18.2 MBytes (39.4%)
3	NETBIOS-SSN [139]	4.3 MBytes (9.4%)
4	HTTP [80]	263.8 KBytes (0.6%)
5	SMTP [25]	13.5 KBytes (0.0%)
6	DNS [53]	9.1 KBytes (0.0%)
7	UNKNOW [28722]	8.4 KBytes (0.0%)
8	FTP [21]	1.1 KBytes (0.0%)
9	UNKNOW [1900]	0.0 Bytes (0.0%)
10	NETBIOS-NS [137]	0.0 Bytes (0.0%)
	OTHER	0.0 Bytes (0.0%)

No.	Upstream	
1	NETBIOS-SSN [139]	1.9 MBytes (60.8%)
2	POP3 [110]	519.2 KBytes (15.8%)
3	MICROSOFT-DS [445]	412.1 KBytes (12.6%)
4	SMTP [25]	301.5 KBytes (9.2%)
5	HTTP [80]	30.5 KBytes (0.9%)
6	UNKNOW [1900]	15.0 KBytes (0.5%)

Definitions:

TOP: Select the data you want to view. It presents 10 results in one page. According to the downstream / upstream report of the selected TOP numbering to draw the Protocol Distribution chart.

or : toggle between two display mode.

Pull-down menu selection

Service: The report of Communication Service when LAN users use the Bandwidth Management Gateway to connect to WAN service server.

Downstream: The percentage of downstream and the value of each WAN service server who uses Bandwidth Management Gateway to connect to LAN user.

Upstream: The percentage of upstream and the value of each LAN user who uses Bandwidth Management Gateway to WAN service server.

First Packet: When the first packet is sent to the WAN Service Server, the sent time will be recorded by the Bandwidth Management Gateway.

Last Packet: When the last packet is sent from the WAN Service Server, the sent time will be recorded by the Bandwidth Management Gateway

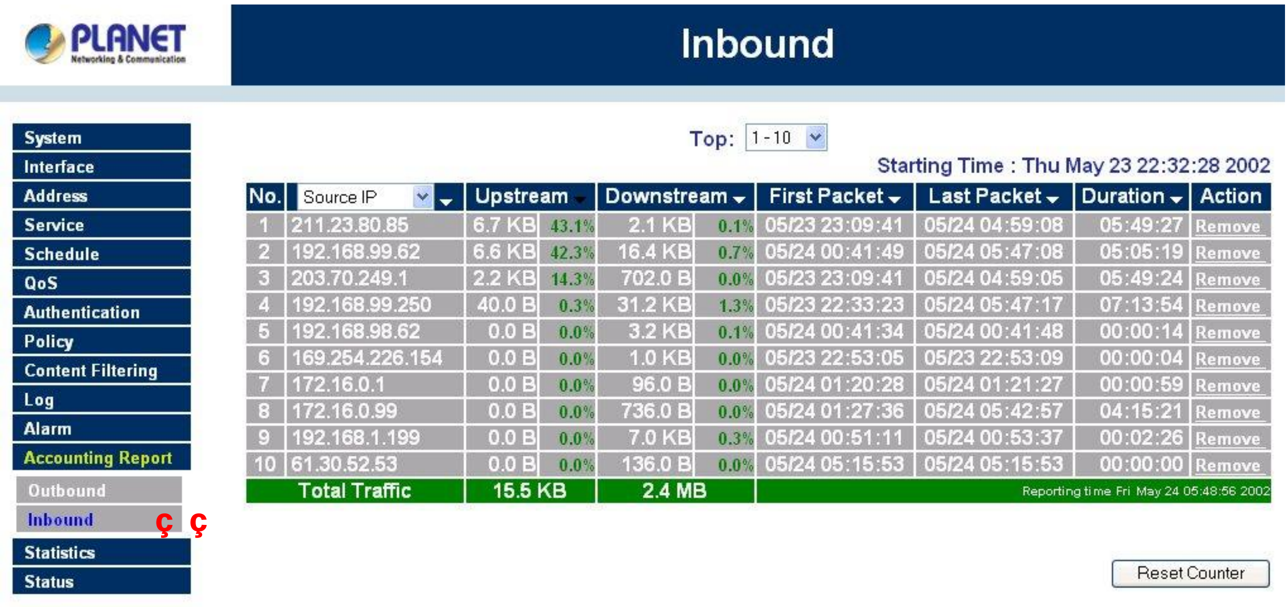
Duration: The period of time starts from the first packet to the last packet to be recorded.

Total Traffic: The Bandwidth Management Gateway will record the sum of time and show the percentage of each Communication Service's upstream/downstream to WAN service server..

Reset Counter: Click the Reset Counter button to refresh the Accounting Report.

4.13.2 Inbound

Click **Service** in the menu bar on the left hand side of the window. Click **Group** under it.

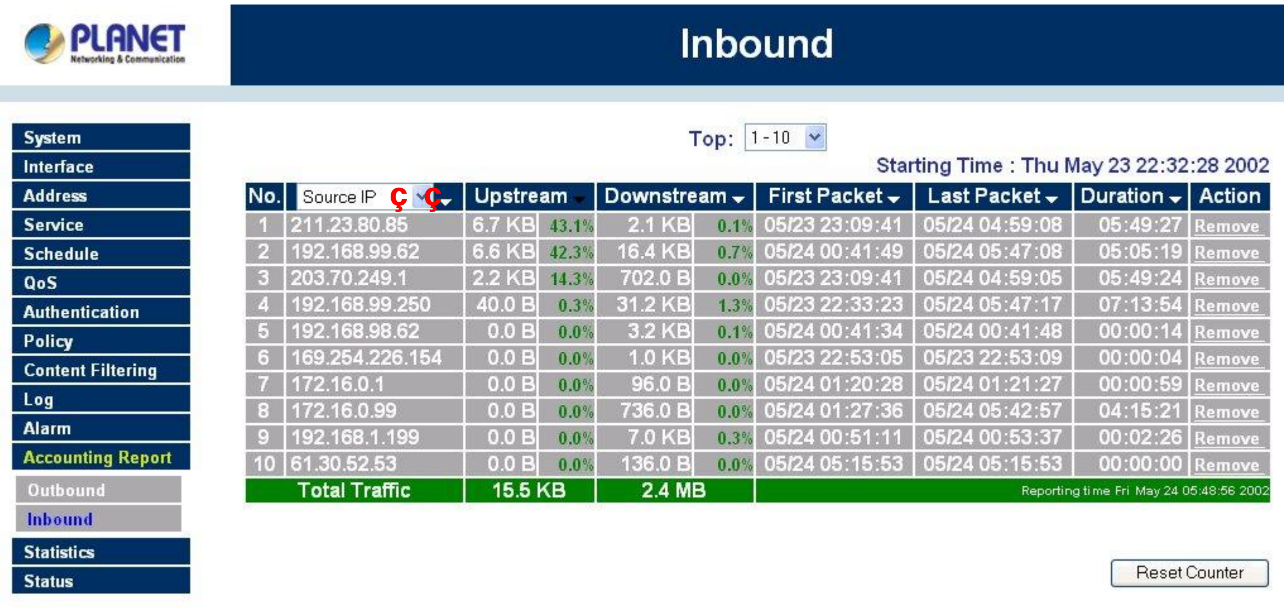


Top: 1 - 10

Starting Time : Thu May 23 22:32:28 2002

No.	Source IP	Upstream		Downstream		First Packet	Last Packet	Duration	Action
1	211.23.80.85	6.7 KB	43.1%	2.1 KB	0.1%	05/23 23:09:41	05/24 04:59:08	05:49:27	Remove
2	192.168.99.62	6.6 KB	42.3%	16.4 KB	0.7%	05/24 00:41:49	05/24 05:47:08	05:05:19	Remove
3	203.70.249.1	2.2 KB	14.3%	702.0 B	0.0%	05/23 23:09:41	05/24 04:59:05	05:49:24	Remove
4	192.168.99.250	40.0 B	0.3%	31.2 KB	1.3%	05/23 22:33:23	05/24 05:47:17	07:13:54	Remove
5	192.168.98.62	0.0 B	0.0%	3.2 KB	0.1%	05/24 00:41:34	05/24 00:41:48	00:00:14	Remove
6	169.254.226.154	0.0 B	0.0%	1.0 KB	0.0%	05/23 22:53:05	05/23 22:53:09	00:00:04	Remove
7	172.16.0.1	0.0 B	0.0%	96.0 B	0.0%	05/24 01:20:28	05/24 01:21:27	00:00:59	Remove
8	172.16.0.99	0.0 B	0.0%	736.0 B	0.0%	05/24 01:27:36	05/24 05:42:57	04:15:21	Remove
9	192.168.1.199	0.0 B	0.0%	7.0 KB	0.3%	05/24 00:51:11	05/24 00:53:37	00:02:26	Remove
10	61.30.52.53	0.0 B	0.0%	136.0 B	0.0%	05/24 05:15:53	05/24 05:15:53	00:00:00	Remove
Total Traffic		15.5 KB		2.4 MB		Reporting time Fri May 24 05:48:56 2002			

Inbound Source IP Accounting Report



Top: 1 - 10

Starting Time : Thu May 23 22:32:28 2002

No.	Source IP	Upstream		Downstream		First Packet	Last Packet	Duration	Action
1	211.23.80.85	6.7 KB	43.1%	2.1 KB	0.1%	05/23 23:09:41	05/24 04:59:08	05:49:27	Remove
2	192.168.99.62	6.6 KB	42.3%	16.4 KB	0.7%	05/24 00:41:49	05/24 05:47:08	05:05:19	Remove
3	203.70.249.1	2.2 KB	14.3%	702.0 B	0.0%	05/23 23:09:41	05/24 04:59:05	05:49:24	Remove
4	192.168.99.250	40.0 B	0.3%	31.2 KB	1.3%	05/23 22:33:23	05/24 05:47:17	07:13:54	Remove
5	192.168.98.62	0.0 B	0.0%	3.2 KB	0.1%	05/24 00:41:34	05/24 00:41:48	00:00:14	Remove
6	169.254.226.154	0.0 B	0.0%	1.0 KB	0.0%	05/23 22:53:05	05/23 22:53:09	00:00:04	Remove
7	172.16.0.1	0.0 B	0.0%	96.0 B	0.0%	05/24 01:20:28	05/24 01:21:27	00:00:59	Remove
8	172.16.0.99	0.0 B	0.0%	736.0 B	0.0%	05/24 01:27:36	05/24 05:42:57	04:15:21	Remove
9	192.168.1.199	0.0 B	0.0%	7.0 KB	0.3%	05/24 00:51:11	05/24 00:53:37	00:02:26	Remove
10	61.30.52.53	0.0 B	0.0%	136.0 B	0.0%	05/24 05:15:53	05/24 05:15:53	00:00:00	Remove
Total Traffic		15.5 KB		2.4 MB		Reporting time Fri May 24 05:48:56 2002			

Source IP: When WAN users use Bandwidth Management Gateway to connect to LAN service server, all of the Downstream/Upstream/First Packet/Last Packet/Duration log of the source IP will be recorded.

Definitions:

TOP: Select the data you want to view. It presents 10 pages in one page.

Select from the Pull-down menu

Source IP: The IP address used by WAN users who use Bandwidth Management Gateway.

Downstream: The percentage of Downstream and the value of each WAN user who uses Bandwidth Management Gateway to LAN service server.

Upstream: The percentage of Upstream and the value of each LAN service server who uses Bandwidth Management Gateway to WAN users.

First Packet: When the first packet is sent from WAN users to LAN service server, the sent time will be recorded by the Bandwidth Management Gateway.

Last Packet: When the last packet is sent from LAN service server to WAN users, the sent time will be recorded by the Bandwidth Management Gateway..

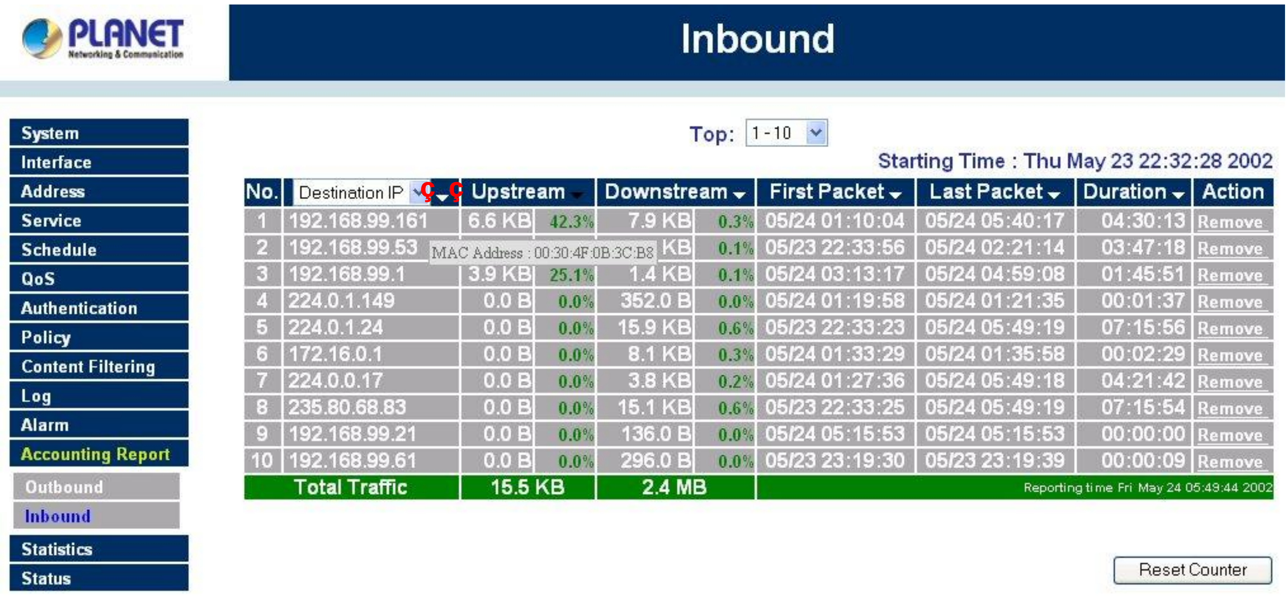
Duration: The period of time starts from the first packet to the last packet to be recorded.

Total Traffic: The Bandwidth Management Gateway will record the sum of time and show the percentage of each WAN user’s upstream/downstream to LAN service server.

Reset Counter: Click the **Reset Counter** button to refresh the Accounting Report.

Inbound Destination IP Accounting Report

When WAN users use Bandwidth Management Gateway to connect to LAN service server, all of the Downstream/Upstream/First Packet/Last Packet/Duration log of the Destination IP will be recorded.



Inbound

Top: 1 - 10

Starting Time : Thu May 23 22:32:28 2002

No.	Destination IP	Upstream		Downstream		First Packet	Last Packet	Duration	Action
1	192.168.99.161	6.6 KB	42.3%	7.9 KB	0.3%	05/24 01:10:04	05/24 05:40:17	04:30:13	Remove
2	192.168.99.53	MAC Address : 00:30:4F:0B:3C:B8		KB	0.1%	05/23 22:33:56	05/24 02:21:14	03:47:18	Remove
3	192.168.99.1	3.9 KB	25.1%	1.4 KB	0.1%	05/24 03:13:17	05/24 04:59:08	01:45:51	Remove
4	224.0.1.149	0.0 B	0.0%	352.0 B	0.0%	05/24 01:19:58	05/24 01:21:35	00:01:37	Remove
5	224.0.1.24	0.0 B	0.0%	15.9 KB	0.6%	05/23 22:33:23	05/24 05:49:19	07:15:56	Remove
6	172.16.0.1	0.0 B	0.0%	8.1 KB	0.3%	05/24 01:33:29	05/24 01:35:58	00:02:29	Remove
7	224.0.0.17	0.0 B	0.0%	3.8 KB	0.2%	05/24 01:27:36	05/24 05:49:18	04:21:42	Remove
8	235.80.68.83	0.0 B	0.0%	15.1 KB	0.6%	05/23 22:33:25	05/24 05:49:19	07:15:54	Remove
9	192.168.99.21	0.0 B	0.0%	136.0 B	0.0%	05/24 05:15:53	05/24 05:15:53	00:00:00	Remove
10	192.168.99.61	0.0 B	0.0%	296.0 B	0.0%	05/23 23:19:30	05/23 23:19:39	00:00:09	Remove
Total Traffic		15.5 KB		2.4 MB		Reporting time Fri May 24 05:49:44 2002			

Definitions:

TOP: Select the data you want to view. It presents 10 pages in one page.

Pull-down menu selection

Destination IP: The IP address used by WAN users who uses Bandwidth Management Gateway.

Downstream: The percentage of Downstream and the value of each WAN user who uses Bandwidth Management Gateway to LAN service server.

Upstream: The percentage of Upstream and the value of each LAN service server who uses Bandwidth Management Gateway to WAN users.

First Packet: When the first packet is sent from WAN users to LAN service server, the sent time will be recorded by the Bandwidth Management Gateway.

Last Packet: When the last packet is sent from LAN service server to WAN users, the sent time will be recorded by the Bandwidth Management Gateway..

Duration: The period of time starts from the first packet to the last packet to be recorded.

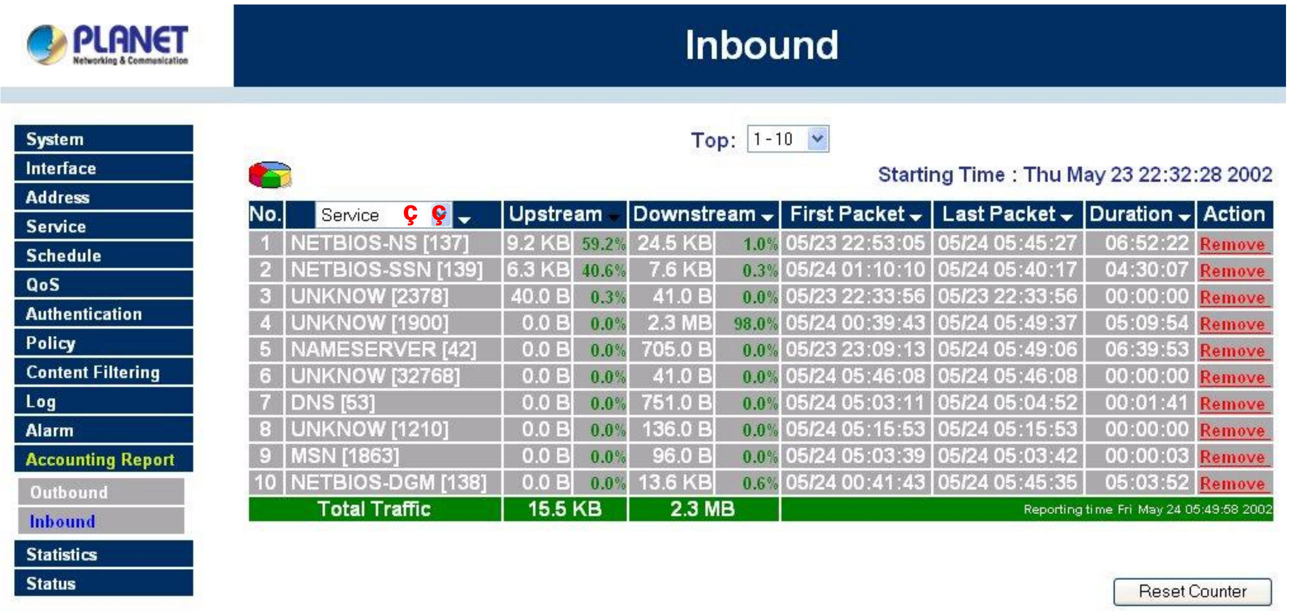
Total Traffic: The Bandwidth Management Gateway will record the sum of time and show the percentage of each WAN user's upstream/downstream to LAN service server.

Reset Counter: Click the **Reset Counter** button to refresh the Accounting Report.

Inbound Service Accounting Report

When WAN users use Bandwidth Management Gateway to connect to LAN Service Server, all of the Downstream/Upstream/First Packet/Last Packet/Duration log of the Communication Service will be recorded.

NOTE: To correctly display the pizza chart, please install the latest java VM for http://www.java.com.



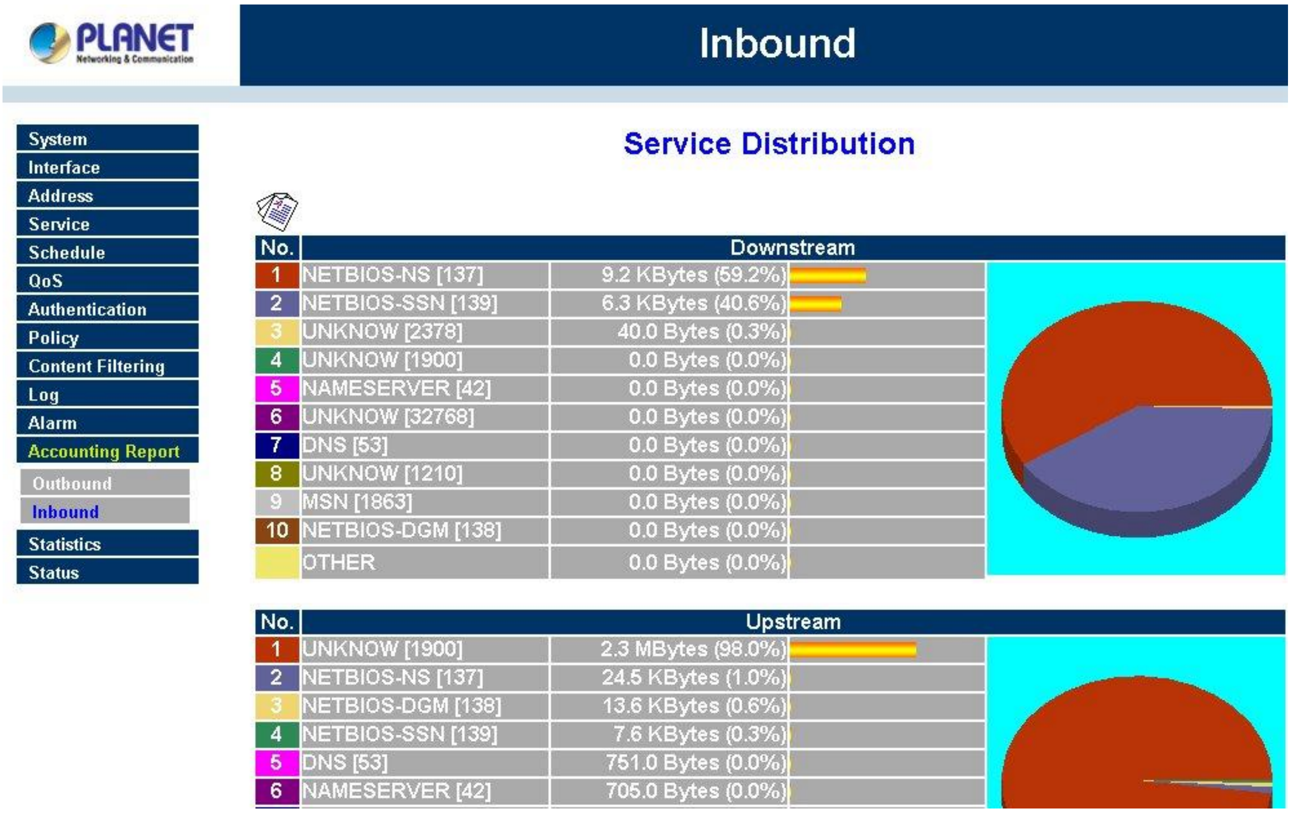
Inbound

Top: 1-10

Starting Time : Thu May 23 22:32:28 2002

No.	Service	Upstream		Downstream		First Packet	Last Packet	Duration	Action
1	NETBIOS-NS [137]	9.2 KB	59.2%	24.5 KB	1.0%	05/23 22:53:05	05/24 05:45:27	06:52:22	Remove
2	NETBIOS-SSN [139]	6.3 KB	40.6%	7.6 KB	0.3%	05/24 01:10:10	05/24 05:40:17	04:30:07	Remove
3	UNKNOW [2378]	40.0 B	0.3%	41.0 B	0.0%	05/23 22:33:56	05/23 22:33:56	00:00:00	Remove
4	UNKNOW [1900]	0.0 B	0.0%	2.3 MB	98.0%	05/24 00:39:43	05/24 05:49:37	05:09:54	Remove
5	NAMESERVER [42]	0.0 B	0.0%	705.0 B	0.0%	05/23 23:09:13	05/24 05:49:06	06:39:53	Remove
6	UNKNOW [32768]	0.0 B	0.0%	41.0 B	0.0%	05/24 05:46:08	05/24 05:46:08	00:00:00	Remove
7	DNS [53]	0.0 B	0.0%	751.0 B	0.0%	05/24 05:03:11	05/24 05:04:52	00:01:41	Remove
8	UNKNOW [1210]	0.0 B	0.0%	136.0 B	0.0%	05/24 05:15:53	05/24 05:15:53	00:00:00	Remove
9	MSN [1863]	0.0 B	0.0%	96.0 B	0.0%	05/24 05:03:39	05/24 05:03:42	00:00:03	Remove
10	NETBIOS-DGM [138]	0.0 B	0.0%	13.6 KB	0.6%	05/24 00:41:43	05/24 05:45:35	05:03:52	Remove
Total Traffic		15.5 KB		2.3 MB		Reporting time Fri May 24 05:49:58 2002			

Reset Counter



Inbound

Service Distribution

No.	Downstream	
1	NETBIOS-NS [137]	9.2 KBytes (59.2%)
2	NETBIOS-SSN [139]	6.3 KBytes (40.6%)
3	UNKNOW [2378]	40.0 Bytes (0.3%)
4	UNKNOW [1900]	0.0 Bytes (0.0%)
5	NAMESERVER [42]	0.0 Bytes (0.0%)
6	UNKNOW [32768]	0.0 Bytes (0.0%)
7	DNS [53]	0.0 Bytes (0.0%)
8	UNKNOW [1210]	0.0 Bytes (0.0%)
9	MSN [1863]	0.0 Bytes (0.0%)
10	NETBIOS-DGM [138]	0.0 Bytes (0.0%)
	OTHER	0.0 Bytes (0.0%)

No.	Upstream	
1	UNKNOW [1900]	2.3 MBytes (98.0%)
2	NETBIOS-NS [137]	24.5 KBytes (1.0%)
3	NETBIOS-DGM [138]	13.6 KBytes (0.6%)
4	NETBIOS-SSN [139]	7.6 KBytes (0.3%)
5	DNS [53]	751.0 Bytes (0.0%)
6	NAMESERVER [42]	705.0 Bytes (0.0%)

Definitions:

TOP: Select the data you want to view. It presents 10 results in one page. According to the downstream/upstream report of the selected TOP numbering to draw the Protocol Distribution chart.

or **:** toggle between two display mode.

Pull-down menu selection

Service: The report of Communication Service when WAN users use the Bandwidth Management Gateway to connect to LAN service server.

Downstream: The percentage of downstream and the value of each WAN user who uses Bandwidth Management Gateway to LAN service server.

Upstream: The percentage of upstream and the value of each LAN service server who uses Bandwidth Management Gateway to WAN user.

First Packet: When the first packet is sent to the LAN Service Server, the sent time will be recorded by the Bandwidth Management Gateway.

Last Packet: When the last packet is sent from the LAN Service Server, the sent time will be recorded by the Bandwidth Management Gateway

Duration: The period of time starts from the first packet to the last packet to be recorded.

Total Traffic: The Bandwidth Management Gateway will record the sum of time and show the percentage of each Communication Service's upstream/downstream to LAN service server..

Reset Counter: Click the **Reset Counter** button to refresh the Accounting Report.

4.14 Statistics

In this chapter, the Administrator queries the Bandwidth Management Gateway for statistics of packets and data which passes across the Bandwidth Management Gateway. The statistics provides the Administrator with information about network traffics and network loads.

What is Statistics

Statistics are the statistics of packets that pass through the Bandwidth Management Gateway by control policies setup by the Administrator.

How to use Statistics

The Administrator can get the current network status from statistics, and use the information provided by statistics as a basis to mange networks.

How to apply WAN Statistics

The Administrator needs to go to Policy to set the network IP addresses that you want to gather statistics, in this way, the administrator can handle the whole network condition and takes it as a basis of managing the network.

The administrator needs to go to the Policy to set the network IP of the WAN statistics. By the Wan statistics you can obtain the status of the network.

4.14.1 WAN Statistics

Step 1. Click Statistics in the menu bar on the left hand side, and then select WAN Statistics.

Step 2. The WAN Statistics will be displayed.

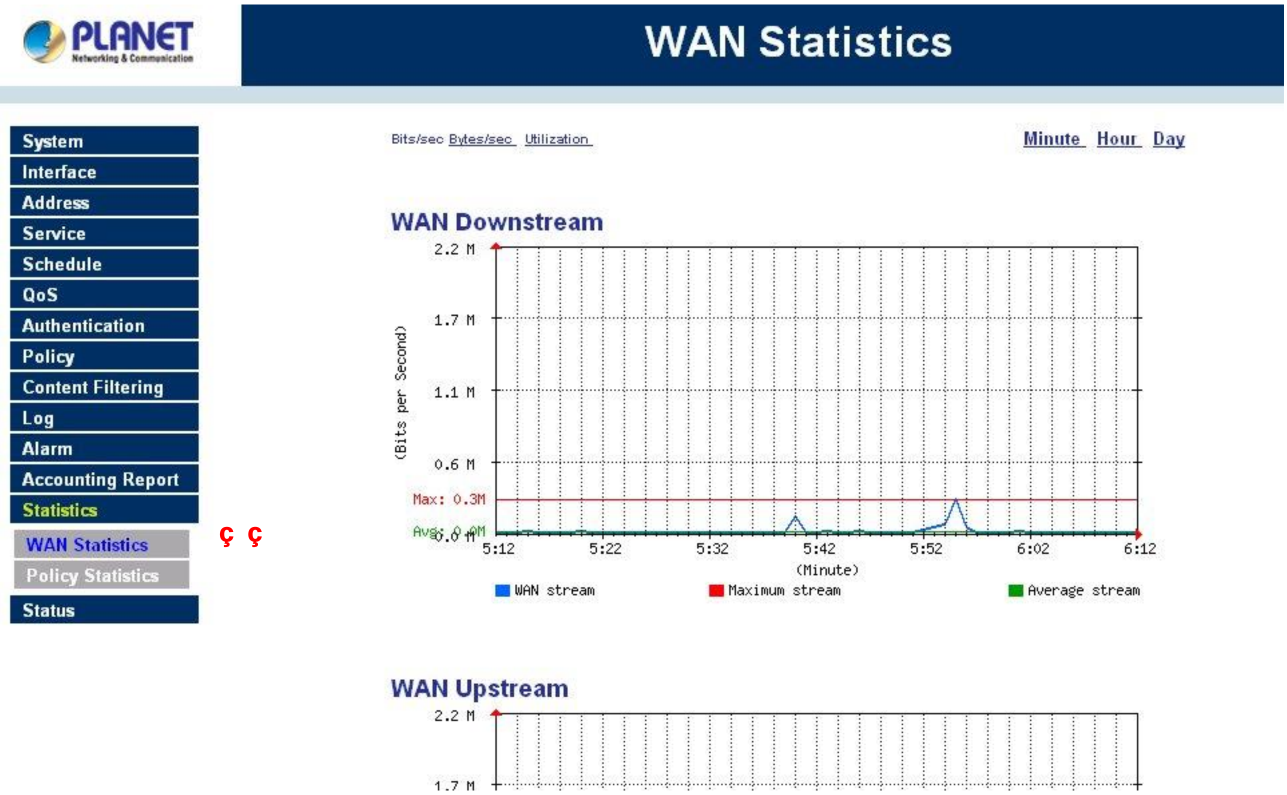


Figure13-1 WAN Statistics

This statistics provide three figure: WAN Downstream, WAN Upstream, WAN Receive Packets, WAN Transmit Packets.

Time: The statistics based on the units of minute (60 minutes), hour (24 hours) and day (30 days).

WAN Statistics

Step 1. Click **Statistics** in the menu bar on the left hand side, and then select **WAN Statistics**.

Step 2. In Statistics window, find the domain name you want to view.

Step 3. In the Statistics window, find the network you want to view and click Minute on the right hand side, and then you will be able to view the Statistics figure of past 60 minutes; click Hour to view the Statistics figure of past 24 hour; click Day to view the Statistics figure or past 30 days.

Y-Coordinate: Network Traffic（Kbytes/Sec）.

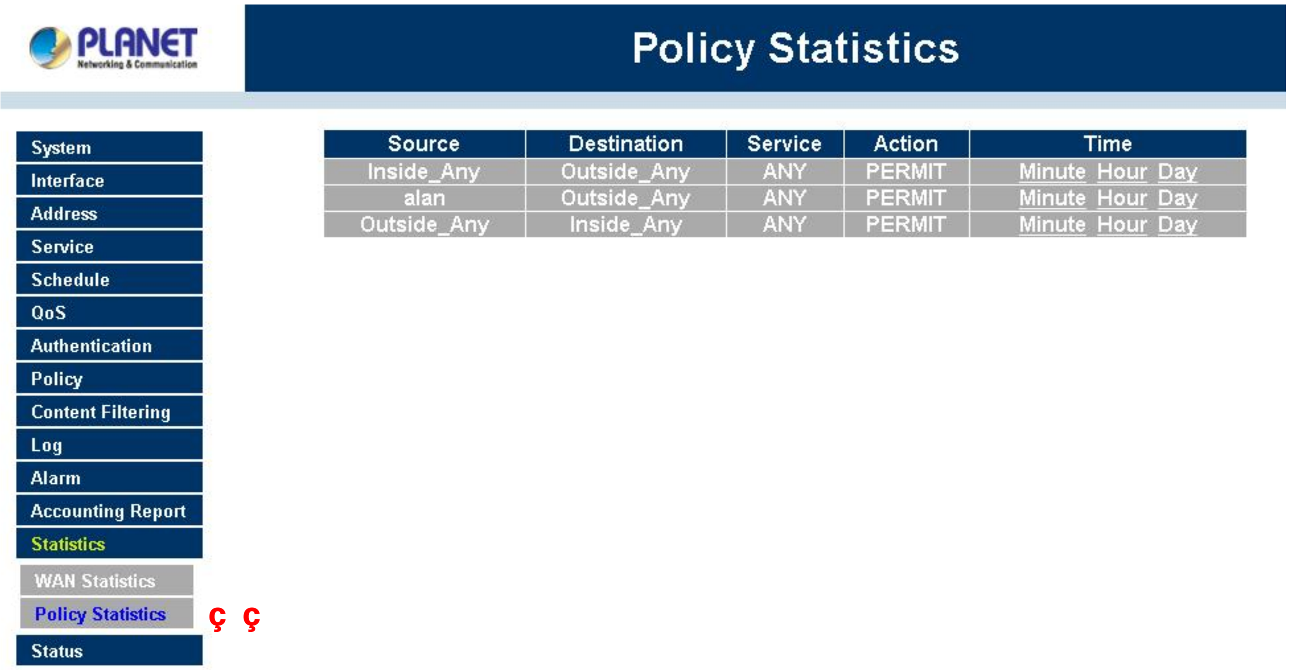
X-Coordinate: Time（Hour/Minute/Day）.

4.14.2 Policy Statistics

Entering the Statistics window

The Statistics window displays the statistics of current network connections.

- n **Source:** the name of source address.
- n **Destination:** the name of destination address.
- n **Service:** the service requested.
- n **Action:** permit or deny
- n **Time:** viewable by minutes, hours, or days



Source	Destination	Service	Action	Time
Inside_Any	Outside_Any	ANY	PERMIT	Minute Hour Day
alan	Outside_Any	ANY	PERMIT	Minute Hour Day
Outside_Any	Inside_Any	ANY	PERMIT	Minute Hour Day

NOTE: To use Statistics, the administrator needs to go to Policy to enable Statistics function.

Entering the Policy Statistics

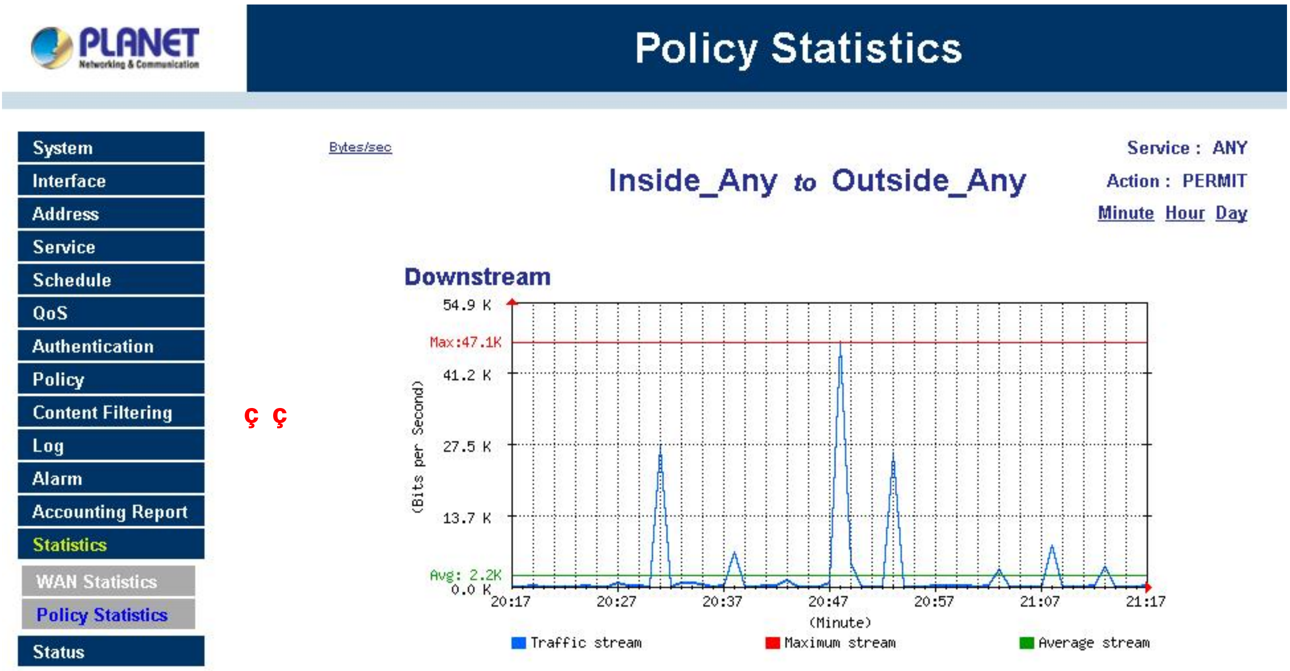
Step 1. Click **Statistics** in the menu bar on the left hand side, and then select **WAN Statistics**.

Step 2. In Statistics window, find the domain name you want to view

Step 3. In the Statistics window, find the network you want to view and click Minute on the right hand side, and then you will be able to view the Statistics figure every minute; click Hour to view the Statistics figure every hour; click Day to view the Statistics figure every day.

Y-Coordinate: Network Traffic (Kbytes/Sec).

X-Coordinate: Time (Hour/Minute/Day).



Policy Statistics

Inside_Any to Outside_Any

Service : ANY

Action : PERMIT

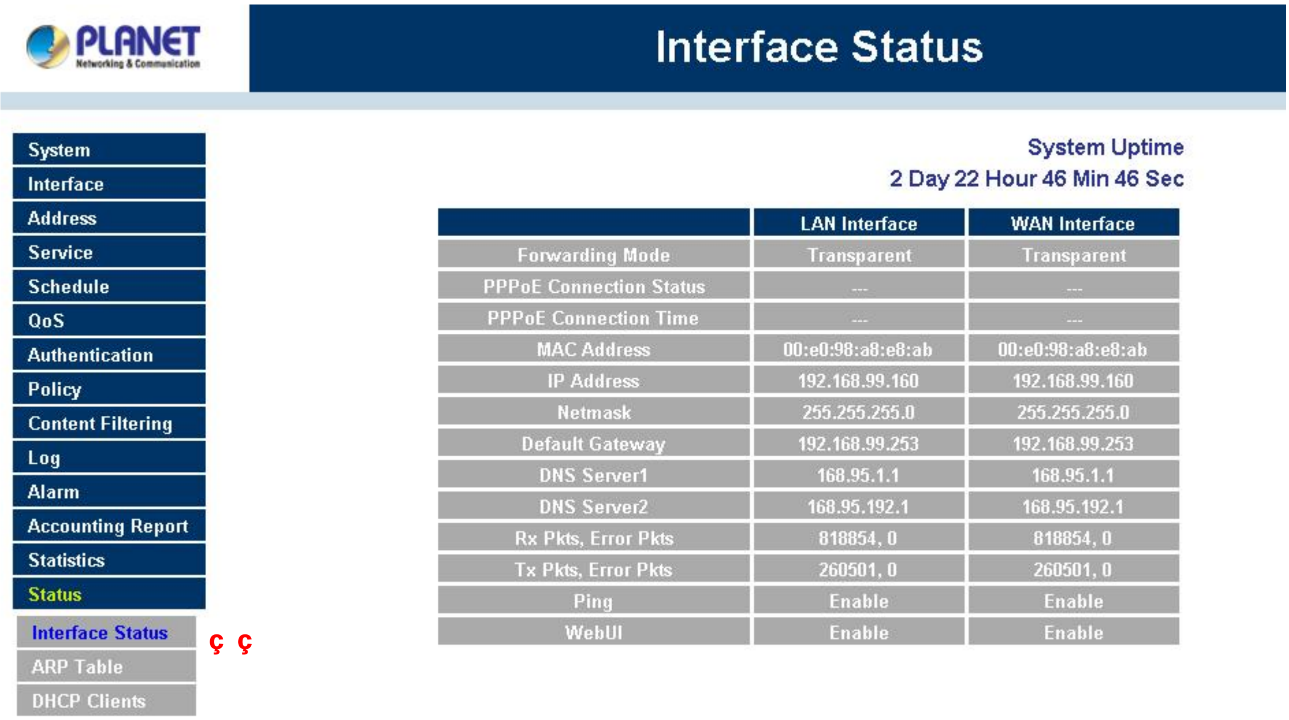
ç ç

4.15 Status

In this section, the device displays the status information about the Bandwidth Management Gateway. Status will display the network information from the Configuration menu. The Administrator may also use Status to check the DHCP lease time and MAC addresses for computers connected to the Bandwidth Management Gateway.

4.15.1 Interface Status

Entering the Interface Status window



System Uptime
2 Day 22 Hour 46 Min 46 Sec

	LAN Interface	WAN Interface
Forwarding Mode	Transparent	Transparent
PPPoE Connection Status	---	---
PPPoE Connection Time	---	---
MAC Address	00:e0:98:a8:e8:ab	00:e0:98:a8:e8:ab
IP Address	192.168.99.160	192.168.99.160
Netmask	255.255.255.0	255.255.255.0
Default Gateway	192.168.99.253	192.168.99.253
DNS Server1	168.95.1.1	168.95.1.1
DNS Server2	168.95.192.1	168.95.192.1
Rx Pkts, Error Pkts	818854, 0	818854, 0
Tx Pkts, Error Pkts	260501, 0	260501, 0
Ping	Enable	Enable
WebUI	Enable	Enable

Internal Interface

In Internet Interface window: The interface IP will be displayed.

System Uptime: The time of booting the Bandwidth Management Gateway.

Forwarding Mode: NAT mode or Transparent mode.

MAC Address: The serial number of the network card.

IP Address/Netmask: Internal IP Address/Internal Netmask.

Rx Pkts, Error Pkts: The received packets and the error received packets will be shown.

Tx Pkts, Error Pkts: The transmit packets and the error transmit packets will be shown.

ADSL Static IP or Cable Modem users

Forwarding Mode: NAT mode or Transparent mode.

Connection Status: Displays the connection status of LAN network.

Connection Time: Displays the connection time of LAN network.

MAC Address: The serial number of the network card.

IP Address/Netmask: external IP Address/external Netmask

Default Gateway: Displays the WAN Gateway address.

Rx Pkts, Error Pkts: The received packets and the error received packets will be shown.

Tx Pkts, Error Pkts: The transmit packets and the error transmit packets will be shown.

DNS Server 1: Displays the using DNS Server 1

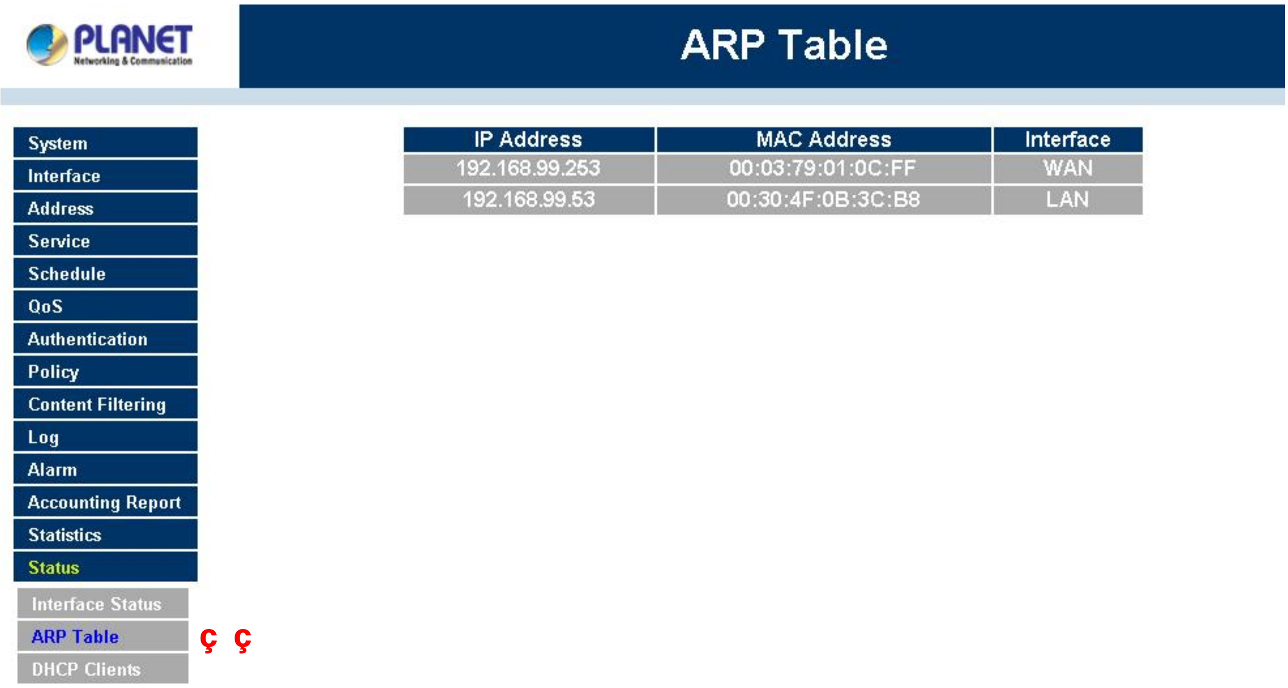
DNS Server 2: Displays the using DNS Server 2.

4.15.2 ARP Table

Entering the ARP Table window

Step 1. Click on **Status** in the menu bar, then click **ARP Table** below it.

Step 2. A window will appear displaying a table with IP addresses and their corresponding MAC addresses. For each computer on the LAN, WAN network that replies to an ARP packet, the device will list them in this ARP table.



IP Address	MAC Address	Interface
192.168.99.253	00:03:79:01:0C:FF	WAN
192.168.99.53	00:30:4F:0B:3C:B8	LAN

IP Address: The IP address of the host computer

MAC Address: The MAC address of that host computer

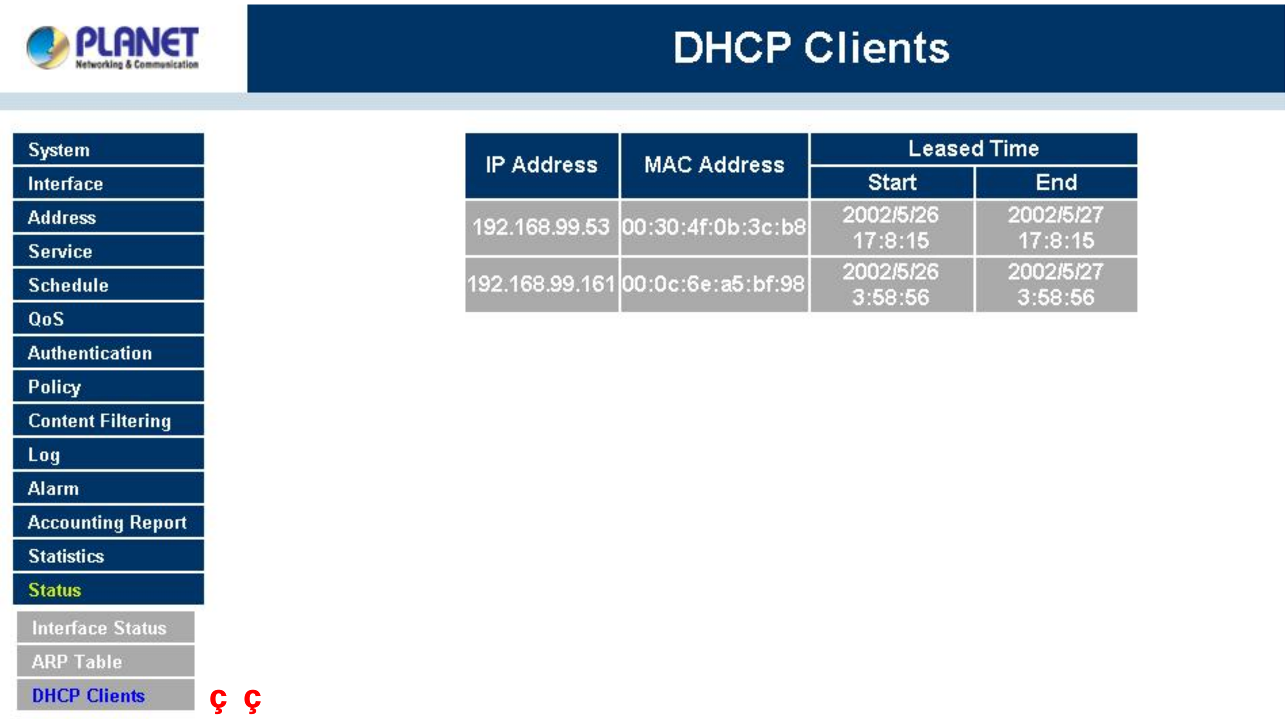
Interface: The port that the host computer is connected to (LAN, WAN)

4.15.3 DHCP Clients

Entering the DHCP Clients window

Step 1. Click on **Status** in the menu bar, then click on **DHCP Clients** below it.

Step 2. A window will appear displaying the table of DHCP clients that are connected to the device. The table will list host computers on the LAN network that obtain its IP address from the Bandwidth Management Gateway’s DHCP server function.



IP Address	MAC Address	Leased Time	
		Start	End
192.168.99.53	00:30:4f:0b:3c:b8	2002/5/26 17:8:15	2002/5/27 17:8:15
192.168.99.161	00:0c:6e:a5:bf:98	2002/5/26 3:58:56	2002/5/27 3:58:56

IP Address: the IP address of the LAN host computer

MAC Address: MAC address of the LAN host computer