

# Bandwidth Management

## User's Manual

# Contents

<b>System</b>	<b>1</b>
Admin	<b>3</b>
Setting	<b>7</b>
Date/Time	<b>16</b>
Language	<b>18</b>
Permitted IP	<b>19</b>
Multiple NAT	<b>23</b>
Hack Alert	<b>28</b>
Route Table	<b>31</b>
DHCP	<b>35</b>
Dynamic DNS	<b>37</b>
Logout	<b>42</b>
Software Update	<b>43</b>

<b>Interface</b>	<b>44</b>
<b>Address</b>	<b>53</b>
LAN	<b>54</b>
LAN Group	<b>58</b>
WAN	<b>62</b>
WAN Group	<b>66</b>
<b>Service</b>	<b>70</b>
Pre-defined	<b>71</b>
Custom	<b>72</b>
Group	<b>77</b>
<b>Schedule</b>	<b>81</b>
<b>QoS</b>	<b>86</b>
<b>Policy</b>	<b>91</b>
Outgoing	<b>92</b>
Incoming	<b>99</b>

<b>Content filtering</b>	<b>107</b>
URL Blocking	<b>108</b>
General Blocking	<b>113</b>
<b>Virtual Server</b>	<b>114</b>
Mapped IP	<b>116</b>
Virtual Server	<b>120</b>
<b>LOG</b>	<b>128</b>
Traffic Log	<b>129</b>
Event Log	<b>132</b>
Connection Log	<b>135</b>
Log Backup	<b>138</b>
<b>Alarm</b>	<b>141</b>
Traffic Alarm	<b>142</b>
Event Alarm	<b>145</b>

<b>Accounting Report</b>	<b>148</b>
Outbound	<b>150</b>
Inbound	<b>156</b>
<b>Statistics</b>	<b>162</b>
WAN Statistics	<b>164</b>
Policy Statistics	<b>165</b>
<b>Status</b>	<b>167</b>
Interface Status	<b>168</b>
ARP Table	<b>170</b>
DHCP Clients	<b>171</b>
<b>Setup Examples</b>	<b>172</b>

# System

The Bandwidth Management 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 settings into local files;
3. Set up alerts for Hackers invasion.

## What is System?

“System” is the managing of settings such as the privileges of packets that pass through the Bandwidth Management and monitoring controls. Administrators may manage, monitor, and configure Bandwidth Management 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.

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

**Setting:** The Administrator may use this function to backup Bandwidth Management 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 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 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 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.

**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.

**Hack Alert** When abnormal conditions occur, the Bandwidth Management 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. 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.

## Admin

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



Figure1-1

### Settings of the Administration table

**Administrator Name:** The username of Administrators for the Bandwidth Management. 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.

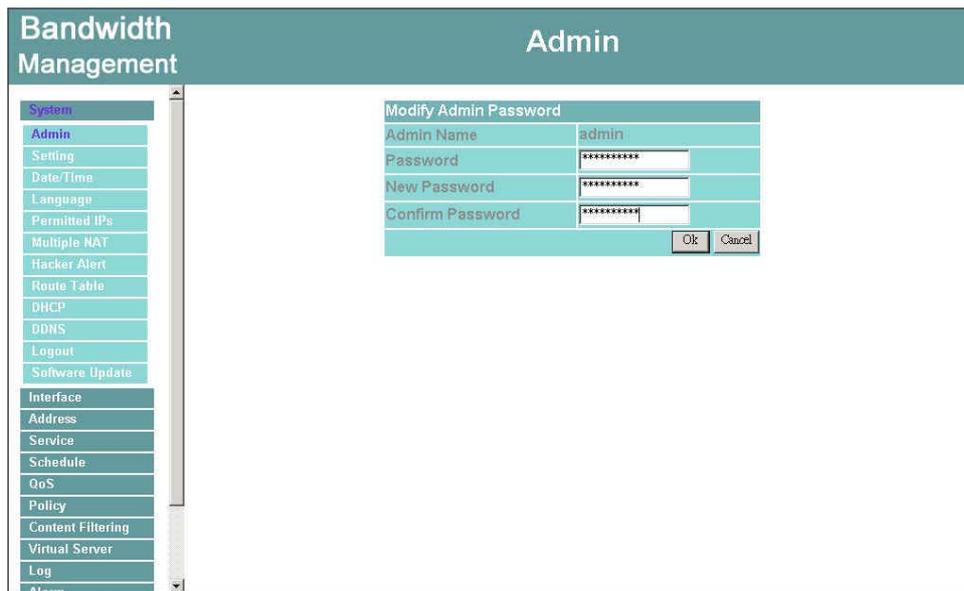


Figure1-2

## 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.

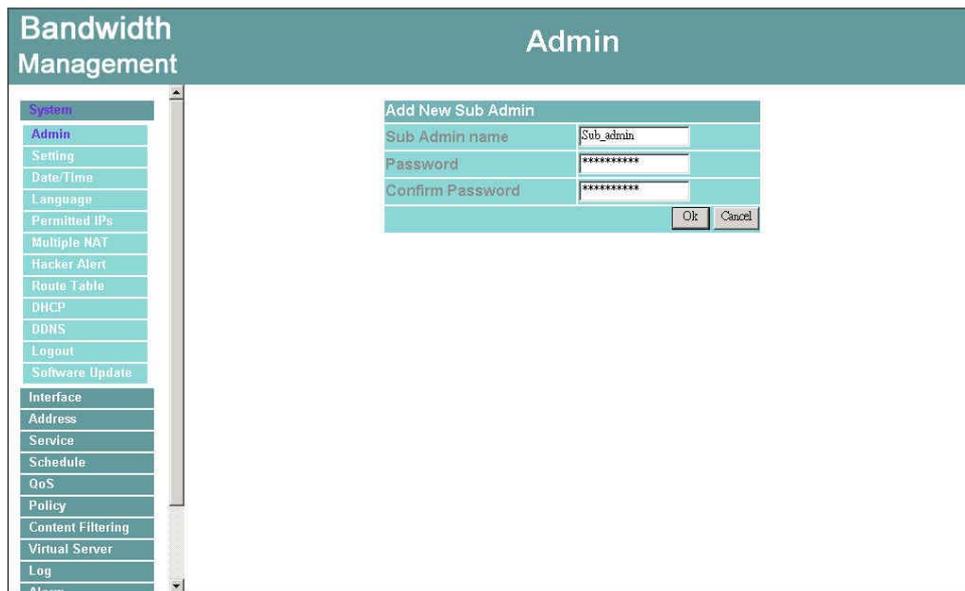


Figure 1-3

## 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.



Figure1-4 Remove Sub Admin

## Settings

The Administrator may use this function to backup Bandwidth Management 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 back to default factory settings.

### Entering the Settings window

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

The screenshot displays the 'Setting' window for Bandwidth Management. On the left, a vertical menu lists various system functions, with 'Setting' highlighted in blue and two black arrows pointing to it. The main content area is titled 'Setting' and contains several configuration sections:

- Bandwidth Management Configuration:** Includes 'Export System Settings to Client' with a 'Download' button, and 'Import System Settings from Client' with a 'Browse...' button and a file name '(ex: bandwidth.conf)'.
- Reset Factory Settings:** A checkbox labeled 'Reset Factory Settings'.
- E-mail Settings:** Includes a checkbox 'Enable E-mail Alert Notification', and input fields for 'Sender Address(Optional)', 'SMTP Server', 'E-mail Address 1', and 'E-mail Address 2'. A 'Mail Test' button is also present.
- Web Management (WAN Interface):** Includes an input field for 'HTTP Port' with the value '80'.
- MTU Setting:** Includes an input field for 'MTU' with the value '1500'.
- To Bandwidth Management Packets Log:** Includes a checked checkbox 'Enable To Bandwidth Management Packets Log'.
- Bandwidth Management Rebooting:** Includes a 'Reboot' button.

At the bottom right of the window, there are 'Ok' and 'Cancel' buttons.

Figure1-5 Setting

## Exporting Bandwidth Management 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.

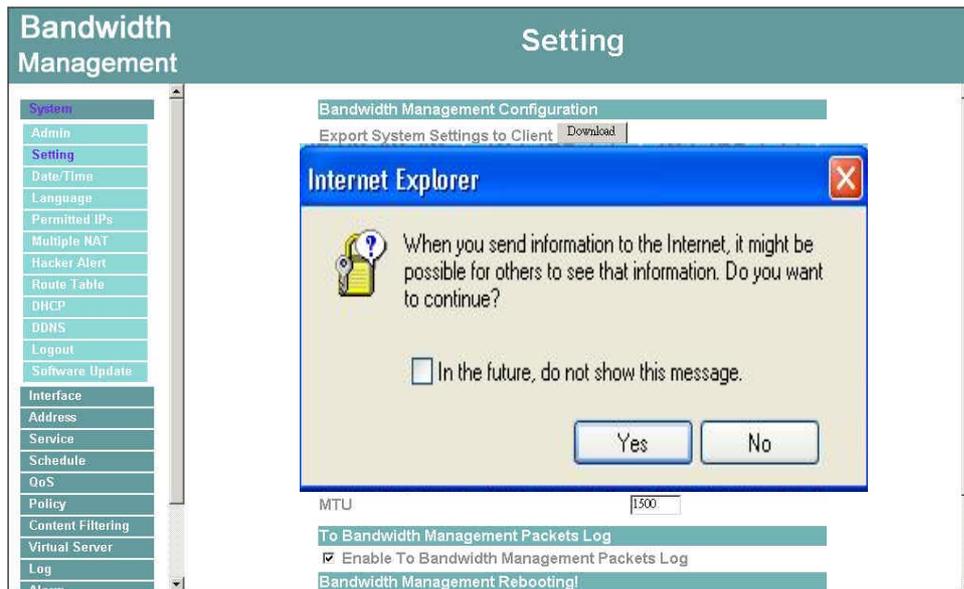


Figure1-6 Select the location where the exported files to be saved

## Importing Bandwidth Management settings

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

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

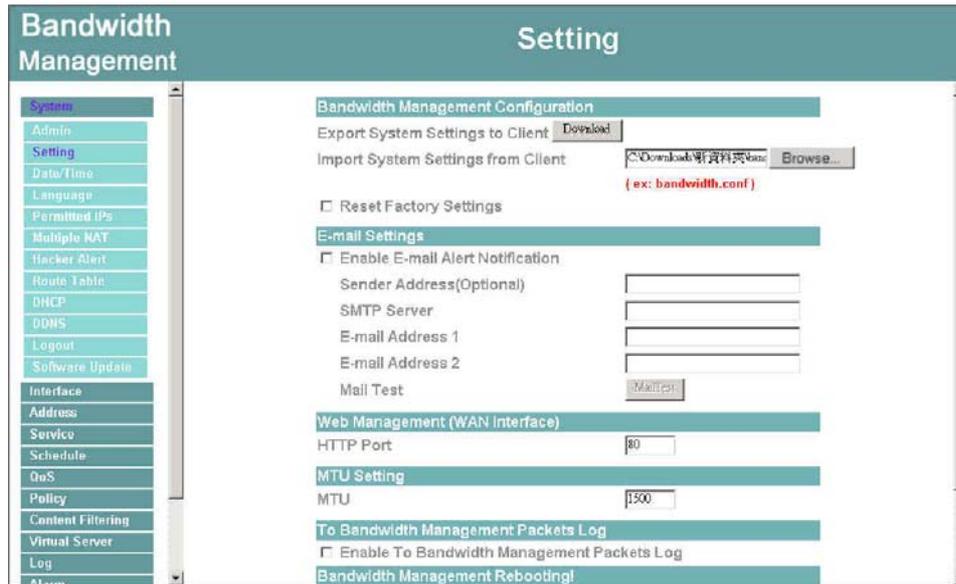


Figure1-7 Location and filename for saving imported file

# 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.

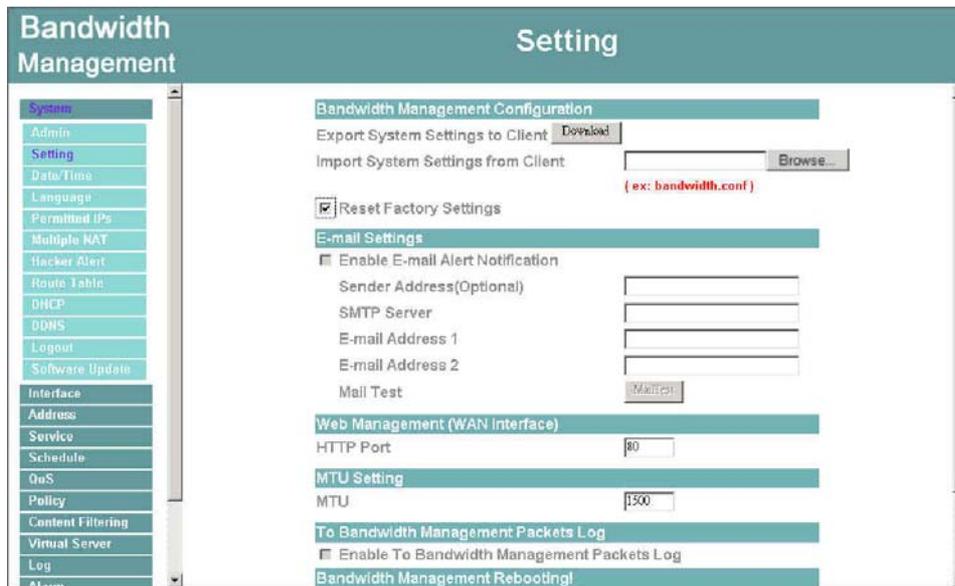


Figure1-8 Select Reset Factory Settings

## Enabling E-mail Alert Notification

**Step 1.** Select **Enable E-mail Alert Notification** under **E-Mail Settings**. This function will enable the Bandwidth Management 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.

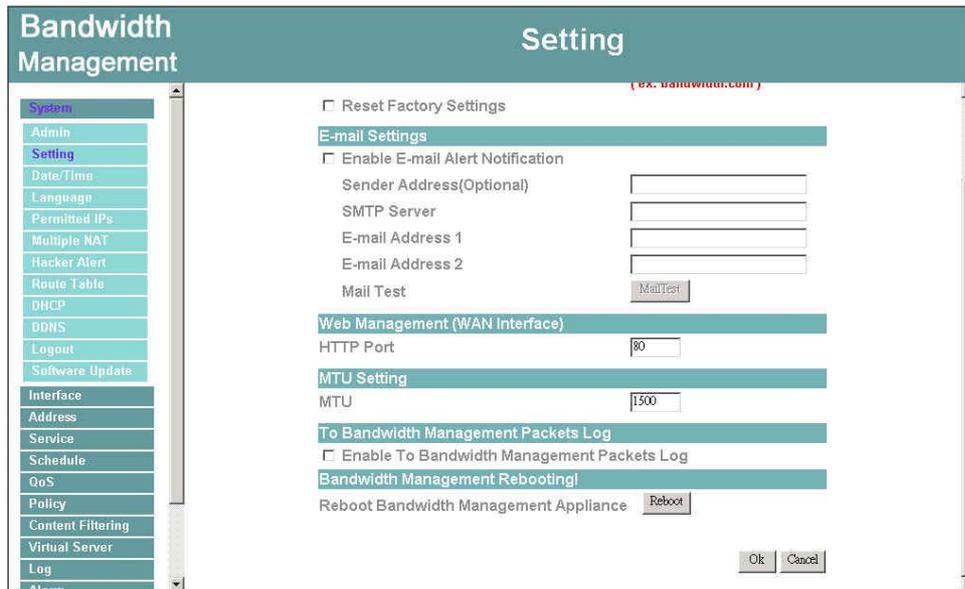
The screenshot displays the 'Bandwidth Management Setting' window. On the left is a navigation menu with options: System, Admin, Setting, Data/Time, Language, Permitted IPs, Multiple NAT, Hacker Alert, Route Table, DHCP, DDNS, Logout, Software Update, Interface, Address, Service, Schedule, QoS, and Policy. The 'Setting' section is active. The main content area is titled 'Bandwidth Management Configuration' and includes: 'Export System Settings to Client' with a 'Download' button; 'Import System Settings from Client' with a text input field and a 'Browse...' button, with '( ex: bandwidth.conf )' below it; an unchecked checkbox for 'Reset Factory Settings'; an 'E-mail Settings' section with a checked checkbox for 'Enable E-mail Alert Notification'; 'Sender Address(Optional)' with a text input field containing 'test'; 'SMTP Server' with a text input field containing 'test.com'; 'E-mail Address 1' with a text input field containing 'test@test.com'; 'E-mail Address 2' with a text input field containing 'test1@test.com'; and a 'Mail Test' button. Below this is the 'Web Management (WAN Interface)' section with 'HTTP Port' set to '80'. The 'MTU Setting' section has 'MTU' set to '1500'.

Figure1-9 Enable E-mail Alert Notification

## 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.



The screenshot displays the 'Bandwidth Management Setting' interface. On the left is a vertical navigation menu with the following items: System, Admin, Setting, Date/Time, Language, Permitted IPs, Multiple NAT, Hacker Alert, Route Table, DHCP, DDNS, Logout, Software Updates, Interface, Address, Service, Schedule, QoS, Policy, Content Filtering, Virtual Server, Log, and Alarm. The 'Setting' menu item is highlighted. The main content area is titled 'Setting' and contains several sections:

- Reset Factory Settings:**  Reset Factory Settings
- E-mail Settings:**
  - Enable E-mail Alert Notification
  - Sender Address(Optional):
  - SMTP Server:
  - E-mail Address 1:
  - E-mail Address 2:
  - Mail Test:
- Web Management (WAN Interface):**
  - HTTP Port:
- MTU Setting:**
  - MTU:
- To Bandwidth Management Packets Log:**
  - Enable To Bandwidth Management Packets Log
- Bandwidth Management Rebooting!**
  - Reboot Bandwidth Management Appliance:

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

Figure1-10 Web Management

## MTU (set networking packet length)

The administrator can modify the networking packet length.

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



The screenshot shows the 'Bandwidth Management' configuration page. On the left is a navigation menu with options like System, Admin, Setting, Date/Time, Language, Permitted IPs, Multiple NAT, Hacker Alert, Route Table, DHCP, DDNS, Logout, Software Update, Interface, Address, Service, Schedule, QoS, Policy, Content Filtering, Virtual Server, Log, and Alarm. The 'Setting' menu item is selected. The main content area is titled 'Setting' and includes a link '(ex. bandwidth.com)'. It contains several sections: 'Reset Factory Settings' with a checkbox; 'E-mail Settings' with a checkbox and fields for 'Sender Address(Optional)', 'SMTP Server', 'E-mail Address 1', and 'E-mail Address 2', plus a 'Mail Test' button; 'Web Management (WAN Interface)' with an 'HTTP Port' field set to '80'; 'MTU Setting' with an 'MTU' field set to '1500'; 'To Bandwidth Management Packets Log' with a checkbox for 'Enable To Bandwidth Management Packets Log'; and 'Bandwidth Management Rebooting!' with a 'Reboot' button. 'Ok' and 'Cancel' buttons are at the bottom right.

Figure1-11 MTU

## To-Bandwidth Management Packets Log

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

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

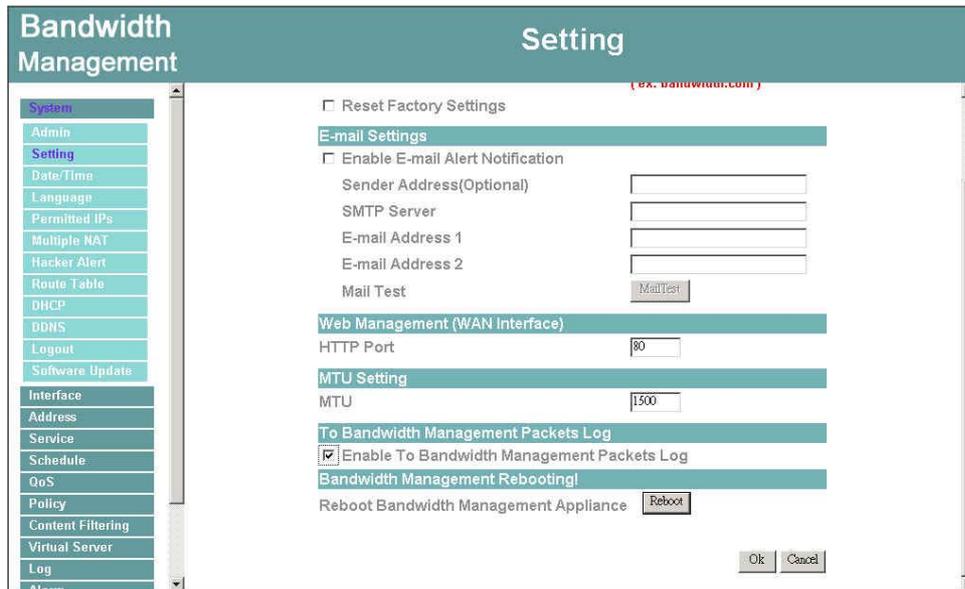


Figure1-12 Enable To Bandwidth Management Packets Log

## Bandwidth Management Reboot

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

Reboot Bandwidth Management: Click **Reboot**.

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

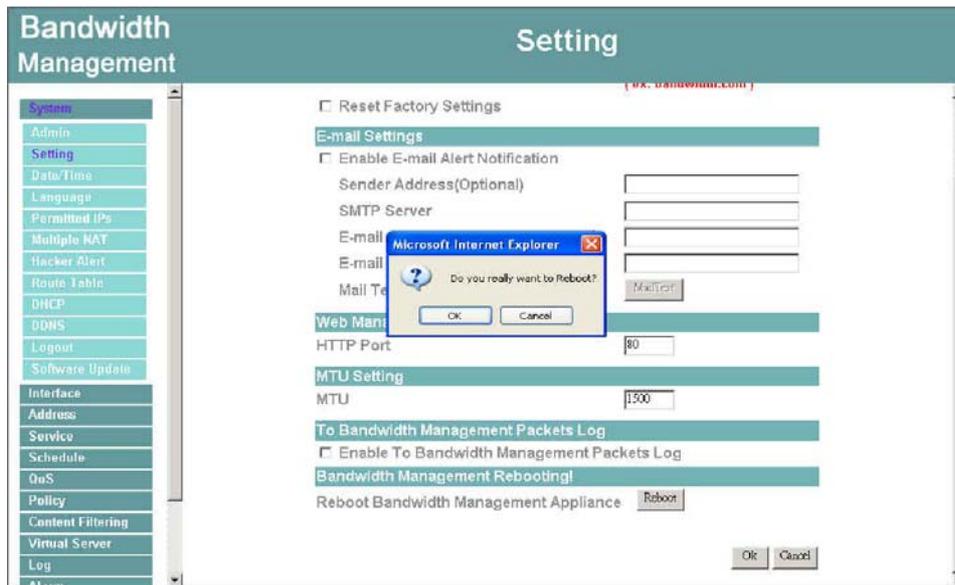


Figure1-13 Reboot Bandwidth Management

## Date/Time

### Synchronizing the Bandwidth Management with the System Clock

Admins can configure the Bandwidth Management'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 the **OK** button below to apply the setting or click **Cancel** to discard changes.

The screenshot shows the 'Date/Time' configuration page within the 'Bandwidth Management' section. The page has a teal header with 'Bandwidth Management' on the left and 'Date/Time' on the right. A sidebar on the left lists various system settings, with 'Date/Time' highlighted. The main content area displays the current system time as 'Mon Mar 10 14:19:17 2003'. Below this, there is a section titled 'Synchronize system clock' with a checked checkbox 'Enable synchronize with an Internet time Server'. The 'Set offset' is set to '0' hours from GMT, and the 'Server IP/Name' is '0.0.0.0'. The 'Update system clock every' is set to '0' minutes. At the bottom of this section, there is a 'Sync' button. At the very bottom of the page, there are 'OK' and 'Cancel' buttons.

**Figure1-14 System Time**

## Language

Admins can configure the Bandwidth Management 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.

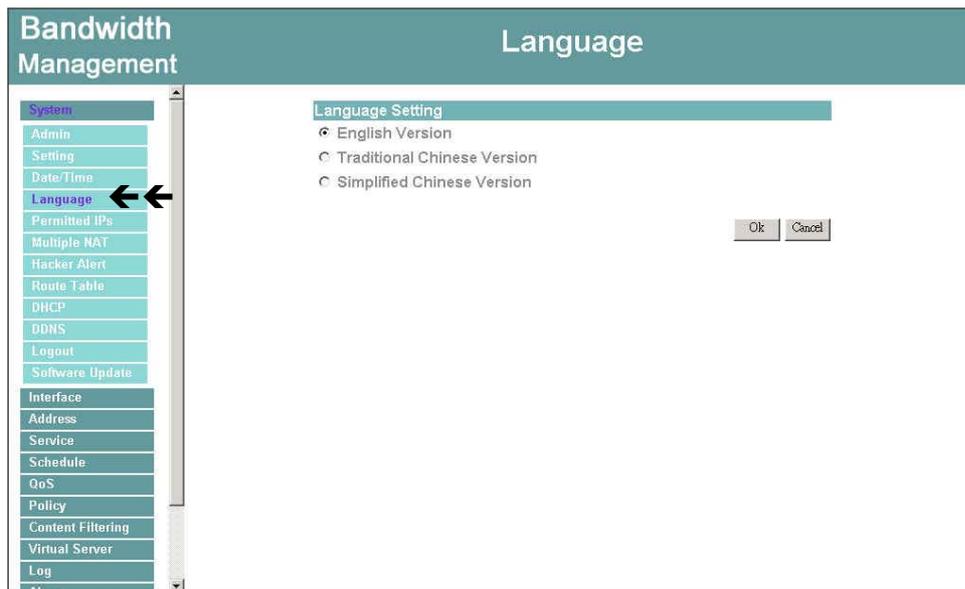


Figure1-15 Language Setting

## Permitted IPs

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

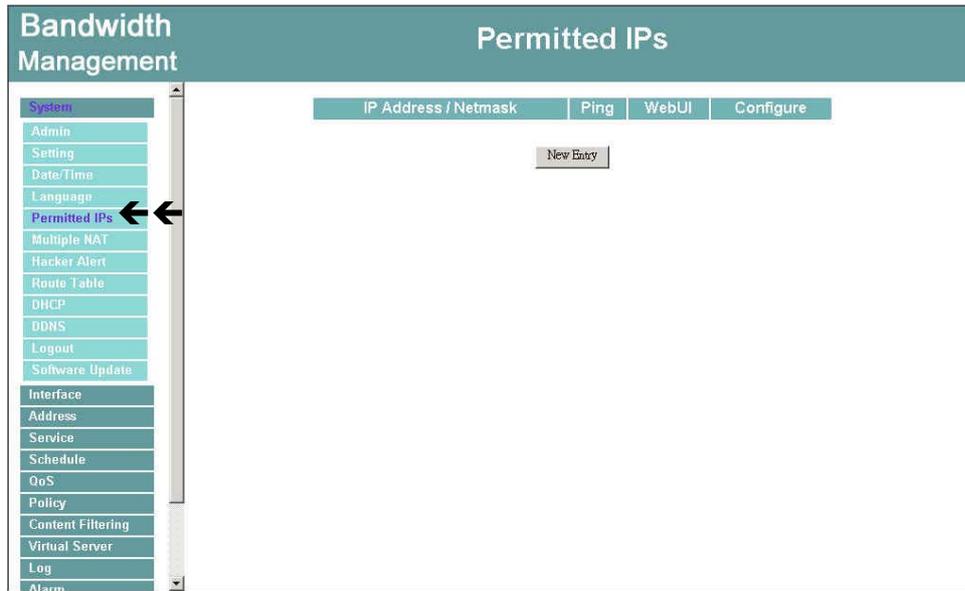


Figure1-16 Permitted IP Address

## 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.

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



The screenshot shows a web interface for "Bandwidth Management" with a sub-section for "Permitted IPs". On the left is a vertical menu with various system settings. The main area contains a form titled "Add New Permitted IPs" with the following fields:

Add New Permitted IPs	
IP Address	<input type="text" value="61.22.22.22"/>
Netmask	<input type="text" value="255.255.255.255"/>
Service:	<input checked="" type="checkbox"/> Ping <input checked="" type="checkbox"/> WebUI
<input type="button" value="Ok"/> <input type="button" value="Cancel"/>	

Figure1-17 Add New Permitted IPs

## 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.



The screenshot shows a web-based network management interface. On the left is a vertical sidebar menu with various system settings. The main area is titled 'Permitted IPs' and contains a 'Modify Permitted IPs' dialog box. The dialog box has three input fields: 'IP Address' with the value '51.22.22.22', 'Netmask' with the value '255.255.255.255', and 'Service:' with two checked checkboxes, 'Ping' and 'WebUI'. At the bottom right of the dialog box are 'Ok' and 'Cancel' buttons.

Bandwidth Management		Permitted IPs	
System	Admin	Modify Permitted IPs	
Setting	Date/Time	IP Address	51.22.22.22
Language	Permitted IPs	Netmask	255.255.255.255
Multiple NAT	Hacker Alert	Service:	<input checked="" type="checkbox"/> Ping <input checked="" type="checkbox"/> WebUI
Route Table	DHCP	<input type="button" value="Ok"/> <input type="button" value="Cancel"/>	
DDNS	Logout		
Software Update	Interface		
Address	Service		
Schedule	QoS		
Policy	Content Filtering		
Virtual Server	Log		
Alarm			

Figure1-18 Modify Permitted IPs

## 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.

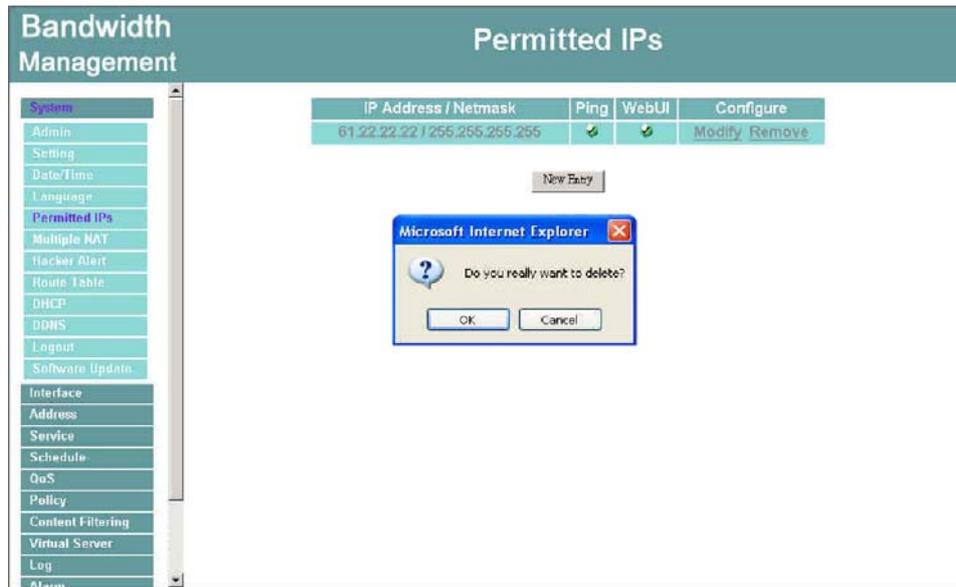


Figure1-19 Remove Permitted IPs

## Multiple NAT

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

For instance : The lease line of a company applies several real IP Addresses 168.85.88.0/24 , 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. The settings are as the following :

- 1.R&D department subnetwork : 192.168.1.11/24(Internal)  $\leftrightarrow$  168.85.88.253(WAN)
2. Service department subnetwork : 192.168.2.11/24(Internal)  $\leftrightarrow$  168.85.88.252(WAN)
- 3.Sales department subnetwork : 192.168.3.11/24(Internal)  $\leftrightarrow$  168.85.88.251(WAN)
- 4.Procurement department subnetwork 192.168.4.11/24(Internal)  $\leftrightarrow$  168.85.88.250(WAN)
- 5.Accounting department subnetwork 192.168.5.11/24(Internal)  $\leftrightarrow$  168.85.88.249(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	Alias IP of Int. Interface / Netmask	Configure
211.74.216.77	192.168.10.1 / 255.255.255.0	Modify_ Remove
211.74.216.77	192.168.20.1 / 255.255.255.0	Modify_ Remove
211.74.216.77	192.168.30.1 / 255.255.255.0	Modify_ Remove

New Entry

Figure1-20 Multiple NAT

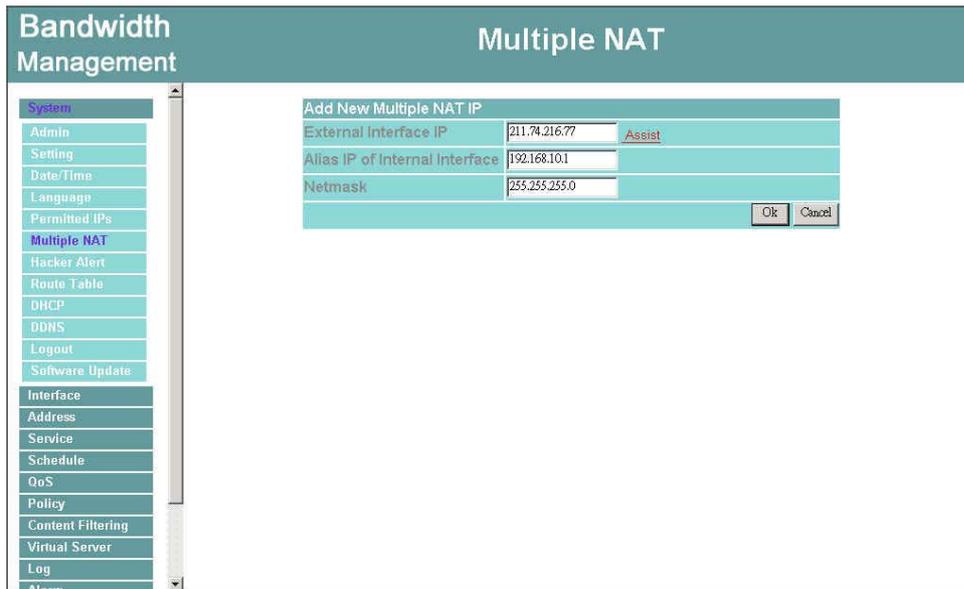
**Global port interface IP Address:**Global port IP Address.

**Local port interface IP Address:**Local port IP Address and subnet Mask.

**Modify:** 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.
- **Global port interface IP Address** : Select Global port IP Address.
  - **Local port interface IP Address** : Enter Local port IP Address.
  - **Subnet Mask** : Enter Local port subnet Mask.
- Step 3.** Click **OK** to add Multiple NAT or click **Cancel** to discard changes.



The screenshot shows a web-based configuration interface for 'Bandwidth Management' with a sub-section for 'Multiple NAT'. On the left is a vertical navigation menu with items like System, Admin, Setting, Date/Time, Language, Permitted IPs, Multiple NAT (highlighted), Hacker Alert, Route Table, DHCP, DDNS, Logout, Software Update, Interface, Address, Service, Schedule, QoS, Policy, Content Filtering, Virtual Server, Log, and Alarm. The main area displays a form titled 'Add New Multiple NAT IP' with three input fields: 'External Interface IP' (containing 211.74.216.77), 'Alias IP of Internal Interface' (containing 192.168.10.1), and 'Netmask' (containing 255.255.255.0). An 'Assist' link is next to the External Interface IP field. At the bottom right of the form are 'Ok' and 'Cancel' buttons.

Figure1-21 Add Multiple NAT

## 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.

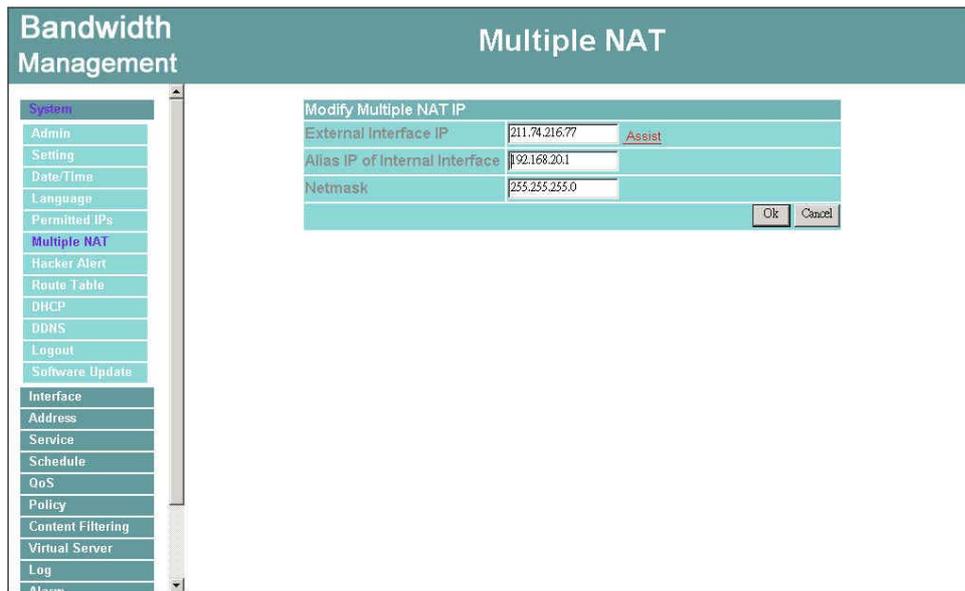


Figure1-22 Modify Multiple NAT

## Delete Multiple NAT

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

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

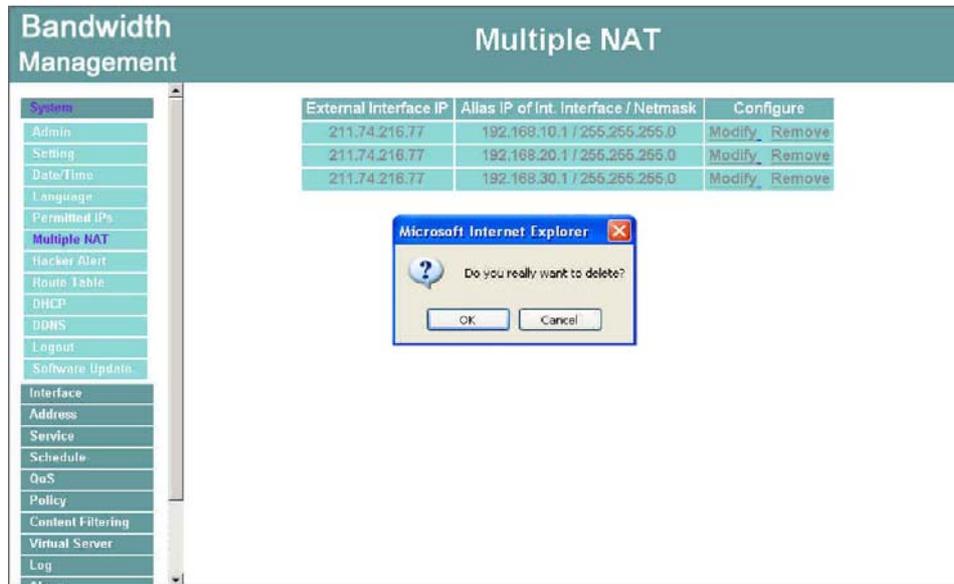


Figure1-23 Remove Multiple NAT

## Hacker Alarm

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

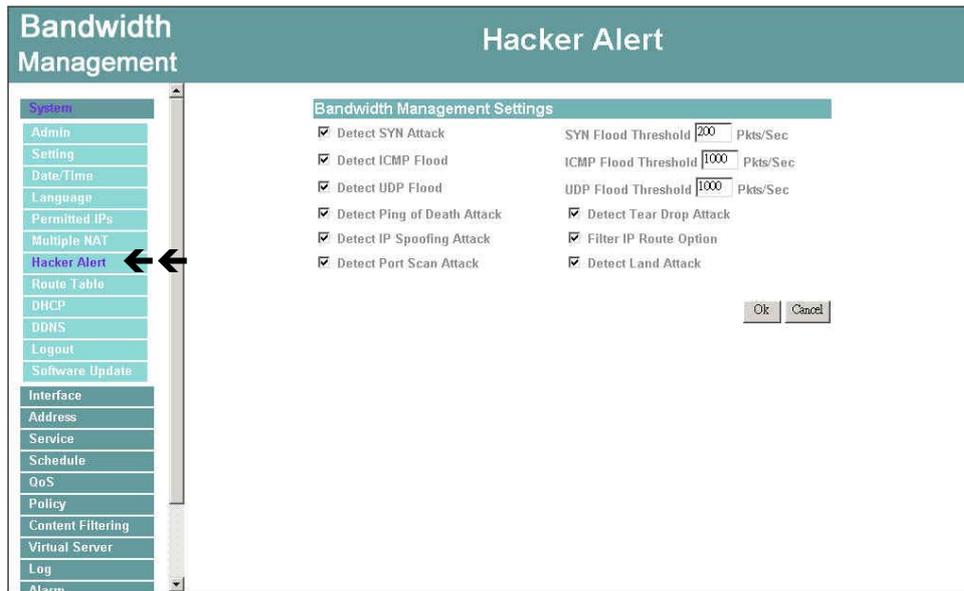


Figure1-24 Hacker Alert

## 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. 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, 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. 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. 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 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. 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.

## 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.

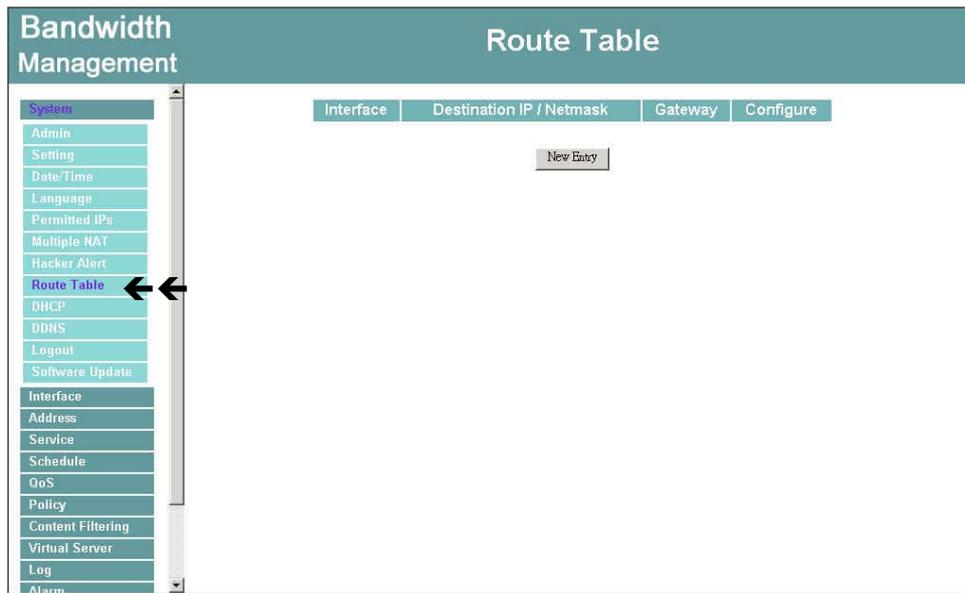


Figure1-25 Route Table

### 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.

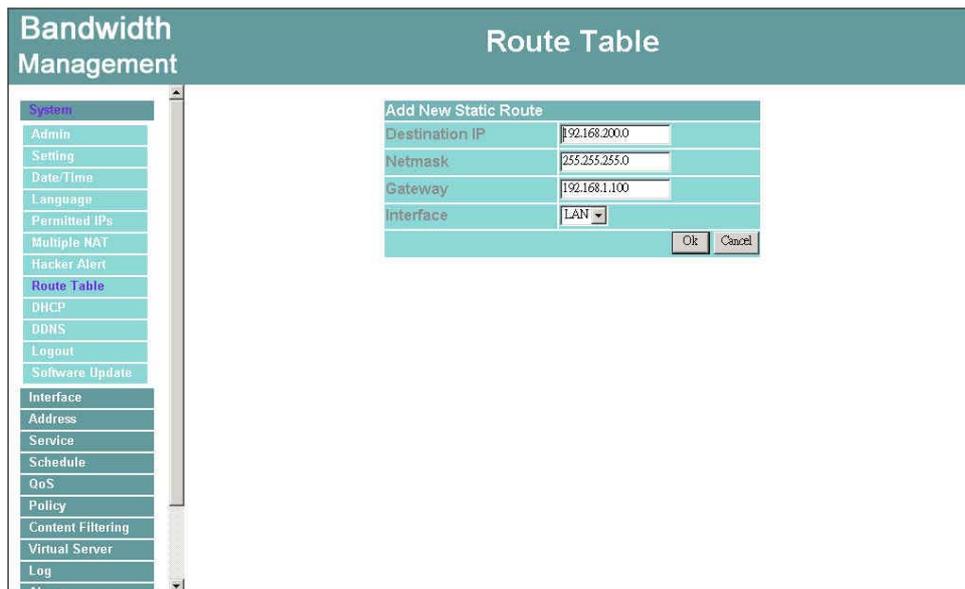


Figure1-26 Add New Static Route

## 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.



Figure1-27 Modify Static Route

## 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.

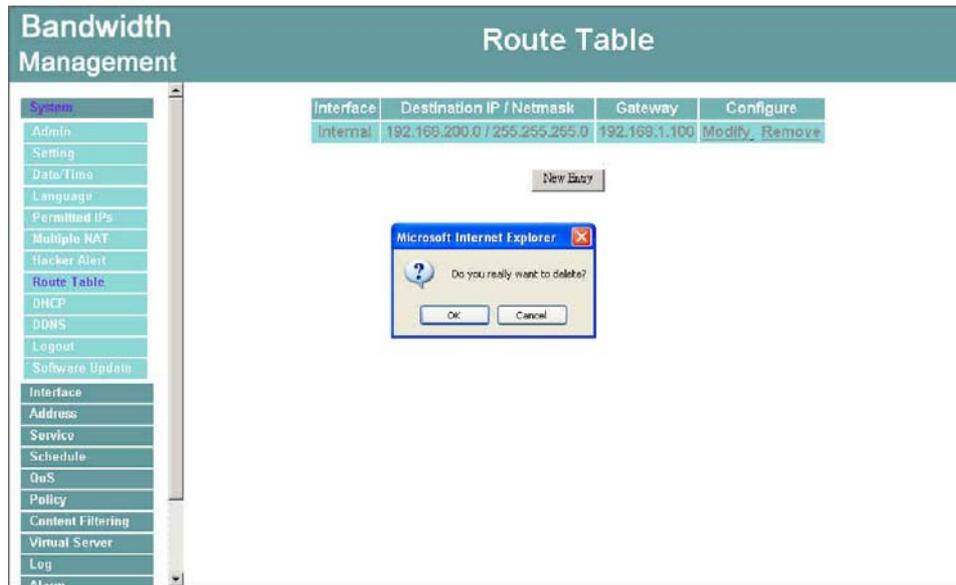


Figure1-28 Remove a Static Route

# 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	192.168.1.0	Netmask	255.255.255.0
Gateway	192.168.1.1	Broadcast	192.168.1.255

Enable DHCP Support

Domain Name

DNS Server 1

DNS Server 2

WINS Server 1

WINS Server 2

Client IP Range 1  To

Client IP Range 2  To

Leased Time  hours

Figure1-29 Dynamic IP address

## 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 Server1.

**DNS Server 2 :** Enter the distributed IP address of DNS Server2.

**WINS Server 1 :** Enter the distributed IP address of WINS Server1.

**WINS Server 2 :** Enter the distributed IP address of WINS Server2.

**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.

The screenshot shows a network management interface with a sidebar on the left and a main configuration area on the right. The sidebar contains a list of menu items: System, Admin, Setting, Date/Time, Language, Permitted IPs, Multiple NAT, Hacker Alert, Route Table, DHCP (highlighted), DDNS, Logout, Software Update, Interface, Address, Service, Schedule, QoS, Policy, Content Filtering, Virtual Server, Log, and Alarm. The main area is titled 'DHCP' and contains the following configuration options:

Dynamic IP Address			
Subnet	192.168.1.0	Netmask	255.255.255.0
Gateway	192.168.1.1	Broadcast	192.168.1.255

Enable DHCP Support

Domain Name:

DNS Server 1:

DNS Server 2:

WINS Server 1:

WINS Server 2:

Client IP Range 1:  To

Client IP Range 2:  To

Leased Time:  hours

Figure1-30 Enable DHCP Support

## 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.

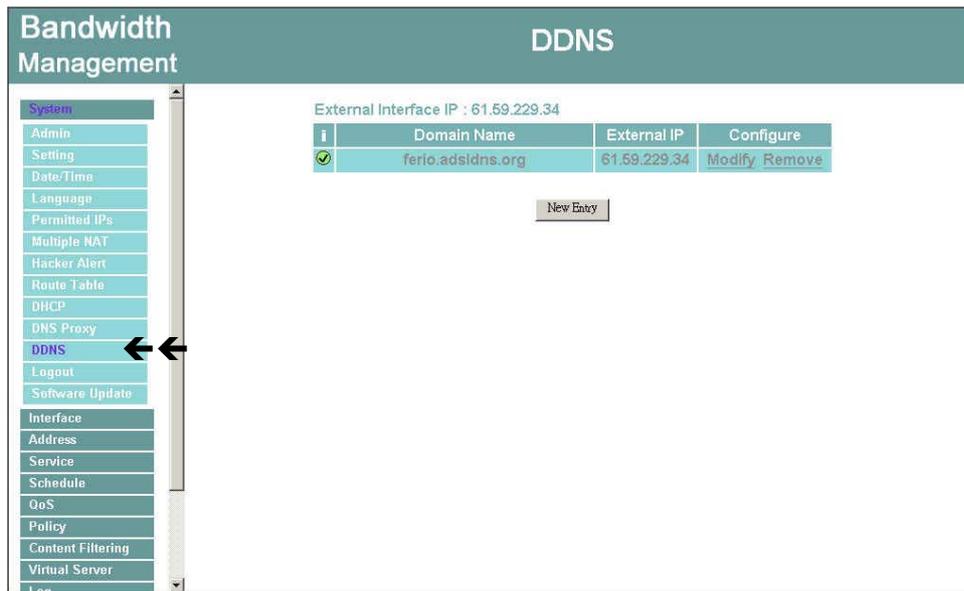


Figure1-31 Dynamic DNS

Click **Dynamic DNS** 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 provides 3 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.

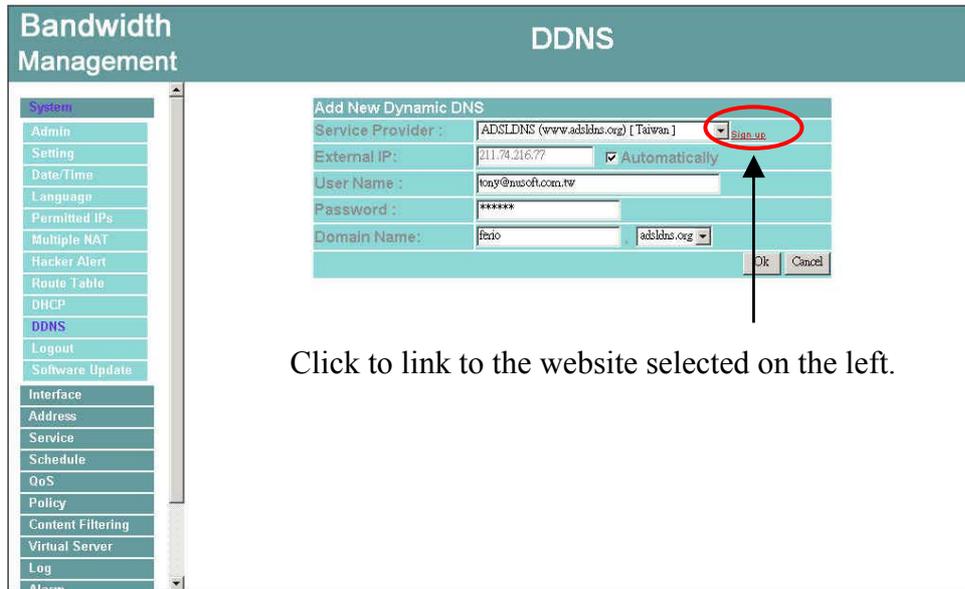


Figure1-32 Setting up DDNS

## 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.

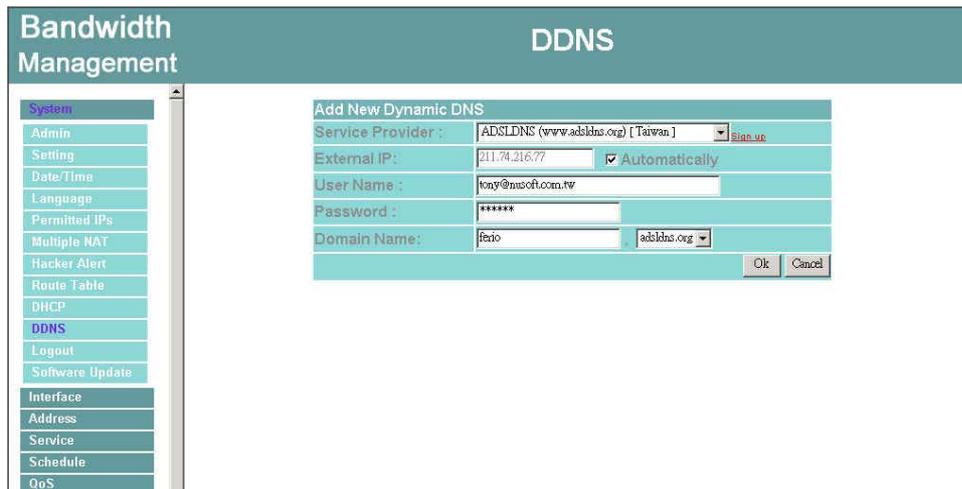
**automatically fill in the WAN IP** : Check to automatically fill in the WAN IP. ◦

**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.



The screenshot shows a web-based network management interface. On the left is a vertical menu with categories: System, Interface, and QoS. The 'System' category is expanded, showing sub-items: Admin, Setting, Date/Time, Language, Permitted IPs, Multiple NAT, Hacker Alert, Route Table, DHCP, DDNS (highlighted), Logout, and Software Updates. The main content area is titled 'DDNS' and contains a form titled 'Add New Dynamic DNS'. The form fields are: Service Provider (dropdown menu showing 'ADSLDNS (www.adslDNS.org) [Taiwan]'), External IP (text input '211.74.216.77' with a checked 'Automatically' checkbox), User Name (text input 'tony@mssoft.com.tw'), Password (text input with six asterisks), and Domain Name (text input 'ferio' with a dropdown menu showing 'adslDNS.org'). At the bottom right of the form are 'OK' and 'Cancel' buttons.

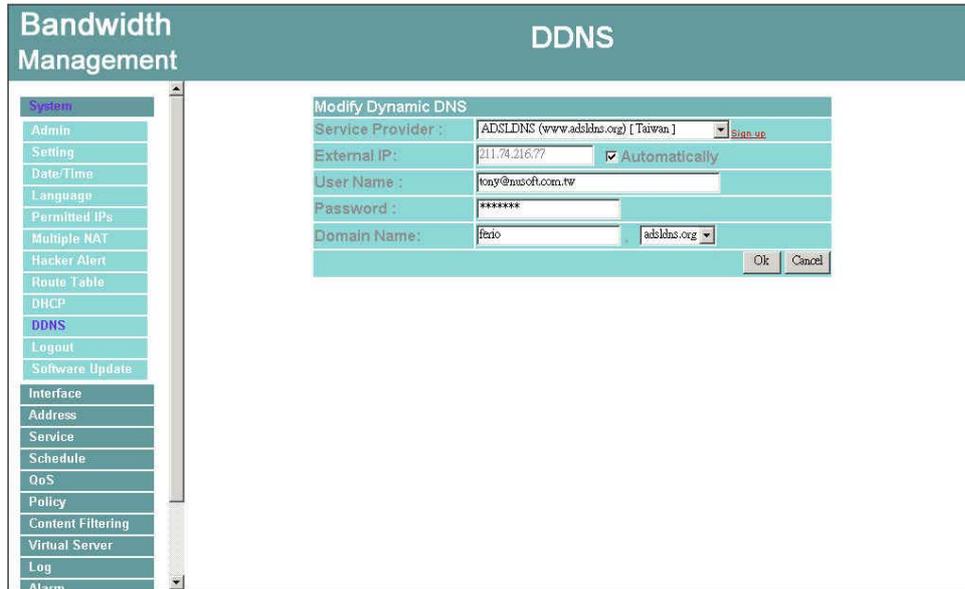
Figure1-33 Add New Dynamic DNS

## 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. ◦



The screenshot shows a web-based network management interface. On the left is a vertical menu titled "Bandwidth Management" with various system settings. The "DDNS" option is highlighted. The main content area is titled "DDNS" and contains a "Modify Dynamic DNS" form. The form fields are as follows:

Modify Dynamic DNS	
Service Provider :	ADSLDNS (www.adslDNS.org) [ Taiwan ] <a href="#">Sign up</a>
External IP:	211.74.216.77 <input checked="" type="checkbox"/> Automatically
User Name :	tony@mssoft.com.tw
Password :	*****
Domain Name:	fzrio adslDNS.org
<input type="button" value="Ok"/> <input type="button" value="Cancel"/>	

Figure1-34 Modify Dynamic DNS

## Delete Dynamic DNS

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

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



Figure1-35 Remove Dynamic DNS

## Logout

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

**Step 2.** Click Logout the Bandwidth Management.

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

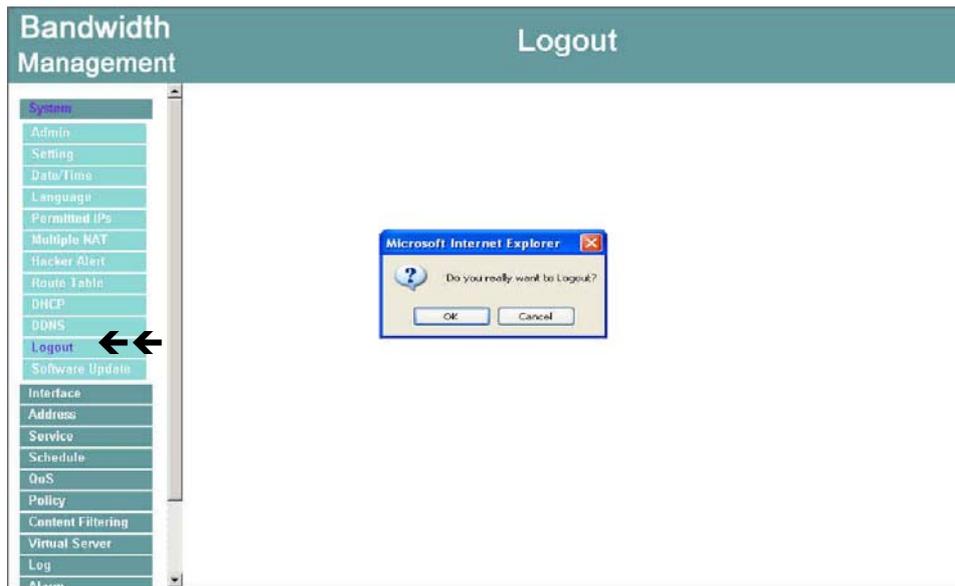


Figure1-36 Logout

## 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.

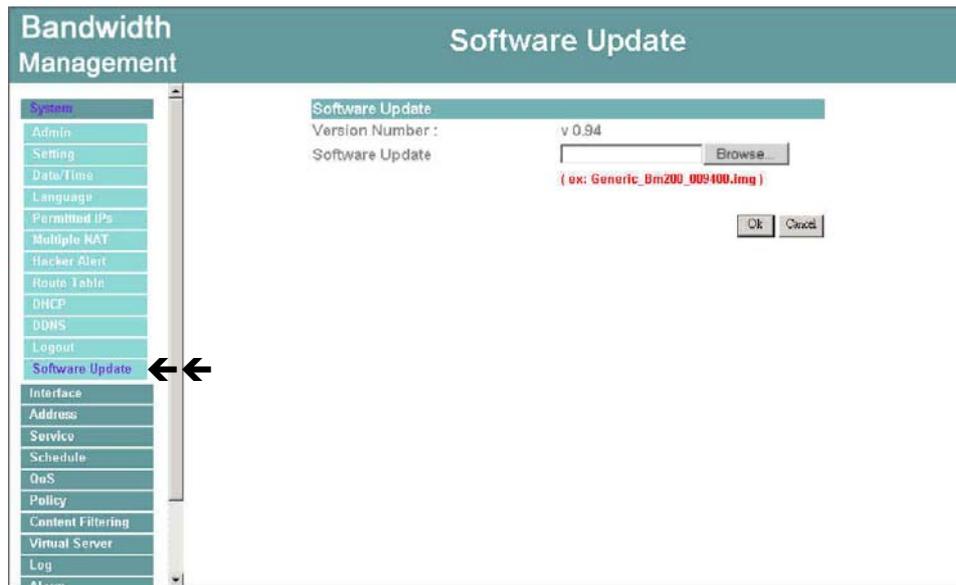


Figure1-37 Software Update



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

# 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. In **Interface** section, the **administrator** can configure IP address, Netmask, and Gateway of the LAN network/ WAN network inside the office network, depending on the ISP selected.

## 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.

### Internal 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. 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 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 will respond to ping packets from the internal network.

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

Bandwidth Management
Interface

- System
- Interface ← ←
- Address
- Service
- Schedule
- QoS
- Policy
- Content Filtering
- Virtual Server
- Log
- Alarm
- Accounting Report
- Statistics
- Status

#### LAN Interface

Transparent Mode

NAT Mode

IP Address:

Netmask:

Enable  Ping  WebUI

#### WAN Interface

PPPoE (ADSL User)

Dynamic IP Address (Cable Modem User)

Static IP Address

Current Status: Connected

IP Address:

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  minutes (0 : means not disconnect)

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.

The screenshot displays the 'Interface' configuration page in a network management system. The left sidebar contains a menu with options: System, Interface (selected), Address, Service, Schedule, QoS, Policy, Content Filtering, Virtual Server, Log, Alarm, Accounting Report, Statistics, and Status. The main content area is titled 'Interface' and is divided into two sections: 'LAN Interface' and 'WAN Interface'. The 'WAN Interface' section is highlighted with two black arrows pointing to the 'PPPoE (ADSL User)' option. Under 'WAN Interface', there are three radio button options: 'PPPoE (ADSL User)' (selected), 'Dynamic IP Address (Cable Modem User)', and 'Static IP Address'. Below these, the 'Current Status' is shown as 'Connected' with a 'Connected' button and a 'Disconnected' button. The 'IP Address' is 211.74.216.77. The 'User Name' is 'TU06928' and the 'Password' is masked with asterisks. The 'IP Address provided by ISP' is set to 'Dynamic'. There are input fields for 'IP Address', 'Netmask', and 'Default Gateway' under the 'Fixed' option. The 'Max. Downstream Bandwidth' is 12 Kbps and the 'Max. Upstream Bandwidth' is 64 Kbps. The 'Service-On-Demand' checkbox is checked. The 'Auto Disconnect if idle' is set to 0 minutes. The 'Enable' section has 'Ping' and 'WebUI' checkboxes checked. At the bottom right, there are 'Ok' and 'Cancel' buttons.

Figure2-2 PPPoE ADSL User Interface

**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 will respond to echo request packets from the external network.

**WebUI:** Select this to allow the BANDWIDTH MANAGEMENT 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 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.

**MAC Address:** This is the MAC Address of the BANDWIDTH MANAGEMENT.

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

**Hostname:** This will be the name assign to the Bandwidth Management. 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 will respond to echo request packets from the external network.*

**WebUI:** Select this to allow the Bandwidth Management 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 always requires a username and password to enter the WebUI.

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

**Bandwidth Management** **Interface**

**System**  
**Interface**  
**Address**  
**Service**  
**Schedule**  
**QoS**  
**Policy**  
**Content Filtering**  
**Virtual Server**  
**Log**  
**Alarm**  
**Accounting Report**  
**Statistics**  
**Status**

**LAN Interface**

Transparent Mode  
 NAT Mode

IP Address   
Netmask

Enable  Ping  WebUI

**WAN Interface**

PPPoE (ADSL User)  
 Dynamic IP Address (Cable Modem User)  
 Static IP Address

IP Address

MAC Address

Hostname   
Domain Name

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

Enable  Ping  WebUI

**Figure2-3 Dynamic IP Address (Cable Modem User)**

**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.

**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 will respond to echo request packets from the external network.*

**WebUI:** Select this to allow the BANDWIDTH MANAGEMENT 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 always requires a username and password to enter the WebUI.

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

The screenshot shows the 'Bandwidth Management Interface' configuration window. On the left is a navigation menu with options: System, Interface (selected), Address, Service, Schedule, QoS, Policy, Content Filtering, Virtual Server, Log, Alarm, Accounting Report, Statistics, and Status. The main area is titled 'Interface' and is divided into 'LAN Interface' and 'WAN Interface' sections. The 'LAN Interface' section is currently selected and shows: 'Transparent Mode' (radio button), 'NAT Mode' (radio button), 'IP Address' (192.168.1.1), 'Netmask' (255.255.255.0), and 'Enable' (checkbox) with 'Ping' and 'WebUI' (checkboxes) checked. The 'WAN Interface' section shows: 'PPPoE (ADSL User)' (radio button), 'Dynamic IP Address (Cable Modem User)' (radio button), 'Static IP Address' (radio button, selected), 'IP Address' (211.22.22.22), 'Netmask' (255.255.255.0), 'Default Gateway' (211.22.22.254), 'DNS Server 1' (168.95.1.1), 'DNS Server 2' (empty), 'Max. Downstream Bandwidth' (512 Kbps), 'Max. Upstream Bandwidth' (512 Kbps), and 'Enable' (checkbox) with 'Ping' and 'WebUI' (checkboxes) checked. At the bottom right are 'OK' and 'Cancel' buttons. Two black arrows point to the 'Static IP Address' radio button in the WAN section.

Figure2-4 WAN interface setup for Static IP Address

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.

# Address

The Bandwidth Management allows the Administrator to set Interface addresses of the LAN network, LAN network group, WAN network, WAN group.

## 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.

# 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.

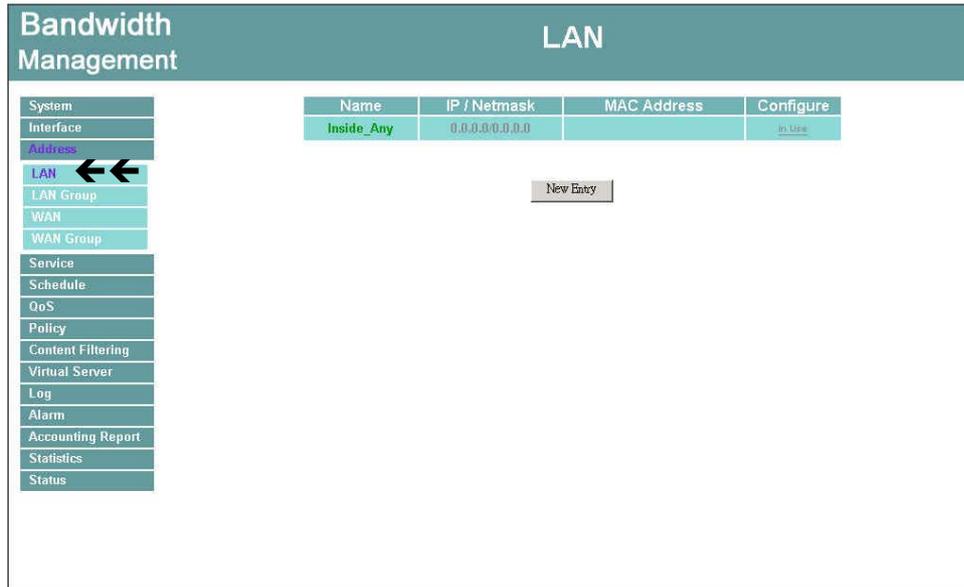


Figure3-1 LAN

### 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.

The screenshot shows a web-based configuration interface. On the left is a vertical menu titled 'Bandwidth Management' with options: System, Interface, Address (highlighted), LAN, LAN Group, WAN, WAN Group, Service, Schedule, QoS, Policy, Content Filtering, Virtual Server, Log, Alarm, Accounting Report, Statistics, and Status. The main area is titled 'LAN' and contains a dialog box titled 'Add New Address'. The dialog has the following fields: 'Name' with value '001', 'IP Address' with value '192.168.1.2', 'Netmask' with value '255.255.255.255', and 'MAC Address' with value '00:50:EF:16:EA:CE' and a 'Clone MAC Address' button. There is a checked checkbox for 'Add in Static DHCP'. At the bottom right of the dialog are 'Ok' and 'Cancel' buttons.

Figure3-2 Add New IP Address in LAN

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.

The screenshot shows a web-based configuration interface. On the left is a vertical sidebar menu with the following items: System, Interface, Address, LAN (highlighted in blue), LAN Group, WAN, WAN Group, Service, Schedule, QoS, Policy, Content Filtering, Virtual Server, Log, Alarm, Accounting Report, Statistics, and Status. The main content area is titled 'LAN' and contains a 'Modify Address' form. The form fields are: Name (001), IP Address (192.168.1.2), Netmask (255.255.255.255), and MAC Address (00:50:BF:16:EA:CE). There is a 'Clone MAC Address' button next to the MAC Address field. A checkbox labeled 'Add in Static DHCP' is checked. At the bottom right of the form are 'Ok' and 'Cancel' buttons.

Figure3-3 Modify LAN IP Address

## 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.



Figure3-4 Remove LAN IP Addresses

## 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.



Figure3-5 LAN Group

**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.

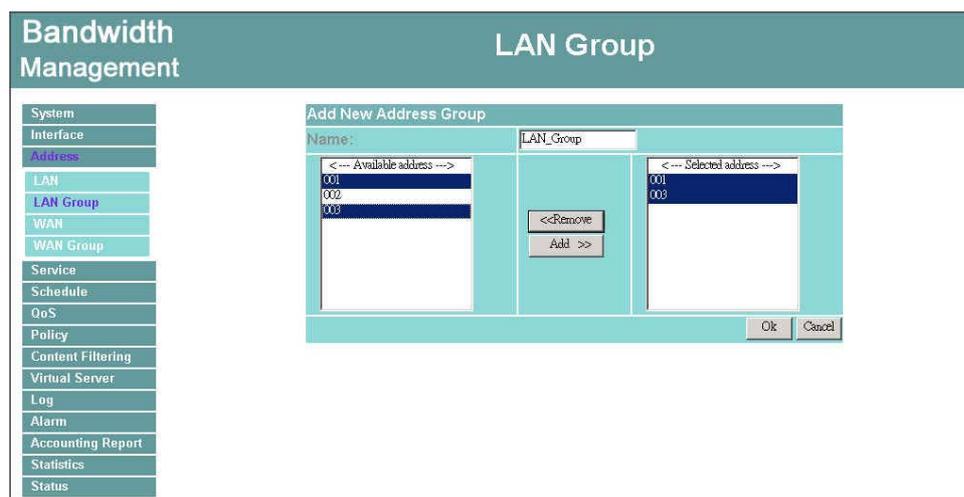


Figure3-6 Add New LAN Group

## 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.

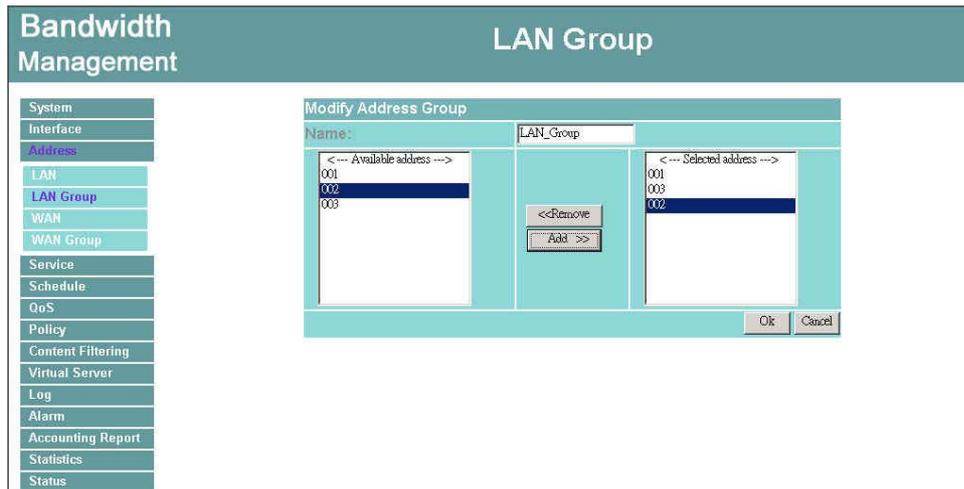


Figure3-7 Modify LAN Group

## 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.



Figure 3-8 Remove LAN Group

# 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

Figure3-9 WAN

### 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.



**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.



The screenshot shows a web-based configuration interface for WAN management. The main window is titled "WAN" and has a sidebar menu on the left with the following items: System, Interface, Address, LAN, LAN Group, WAN, WAN Group, Service, Schedule, QoS, Policy, Content Filtering, Virtual Server, Log, Alarm, Accounting Report, Statistics, and Status. The "Address" menu item is highlighted. The main content area displays the "Add New Address" dialog box with the following fields:

Add New Address	
Name	Test
IP Address	202.1.237.23
Netmask	255.255.255.255
<input type="button" value="Ok"/> <input type="button" value="Cancel"/>	

Figure3-10 Add WAN IP Address

## 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.



The screenshot shows a web-based network management interface. On the left is a vertical sidebar menu titled "Bandwidth Management" with various configuration options. The "WAN" option is highlighted. The main content area is titled "WAN" and displays a "Modify Address" dialog box. This dialog box has three input fields: "Name" with the value "Test", "IP Address" with the value "202.1.237.23", and "Netmask" with the value "255.255.255.255". At the bottom right of the dialog box are "Ok" and "Cancel" buttons.

Bandwidth Management		WAN	
System		Modify Address	
Interface		Name	Test
Address		IP Address	202.1.237.23
LAN		Netmask	255.255.255.255
LAN Group		Ok Cancel	
WAN			
WAN Group			
Service			
Schedule			
QoS			
Policy			
Content Filtering			
Virtual Server			
Log			
Alarm			
Accounting Report			
Statistics			
Status			

Figure3-11 Modify WAN IP Address

## 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.



Figure3-12 Remove a WAN IP address

## 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.

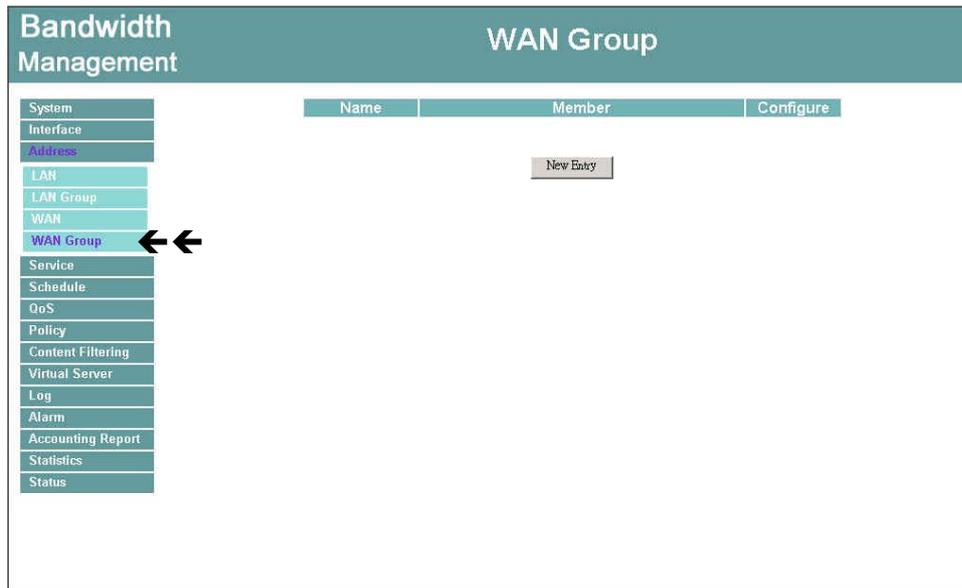


Figure3-13 WAN Group

#### 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.



*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.*

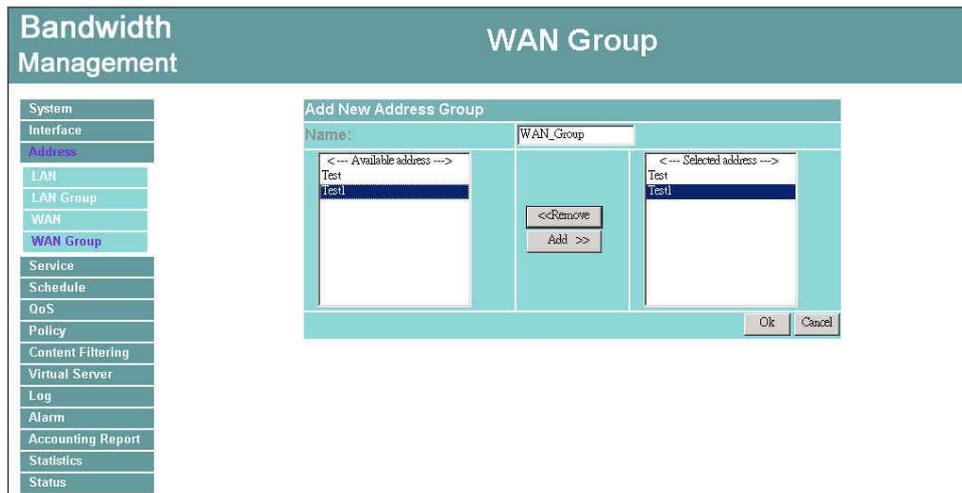
## Adding an WAN Group

**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:

- **Name:** enter the name of the new group.
- **Available Address:** List the names of all the members of the WAN network.
- **Selected Address:** List the names to assign to the new group.
- **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.
- **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.



3-14 Add a new WAN Group

## 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.

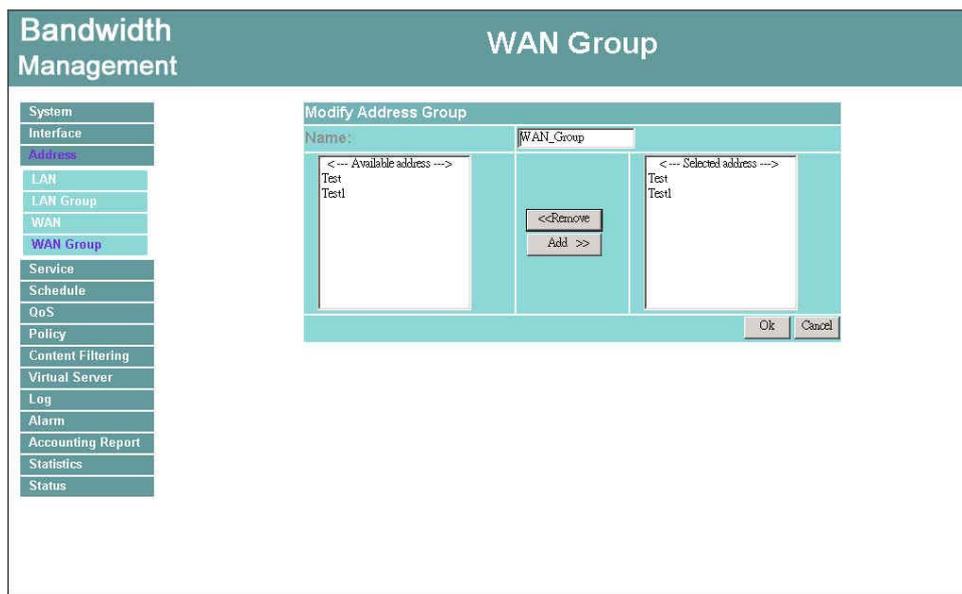
**Step 2.** A window displaying the information of the selected group appears:

- **Available Address:** list the names of all the members of the WAN network.
- **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.



3-15 Modify a WAN Group

## 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.



Figure 3-16 Remove WAN Group

# 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 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.

## 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.

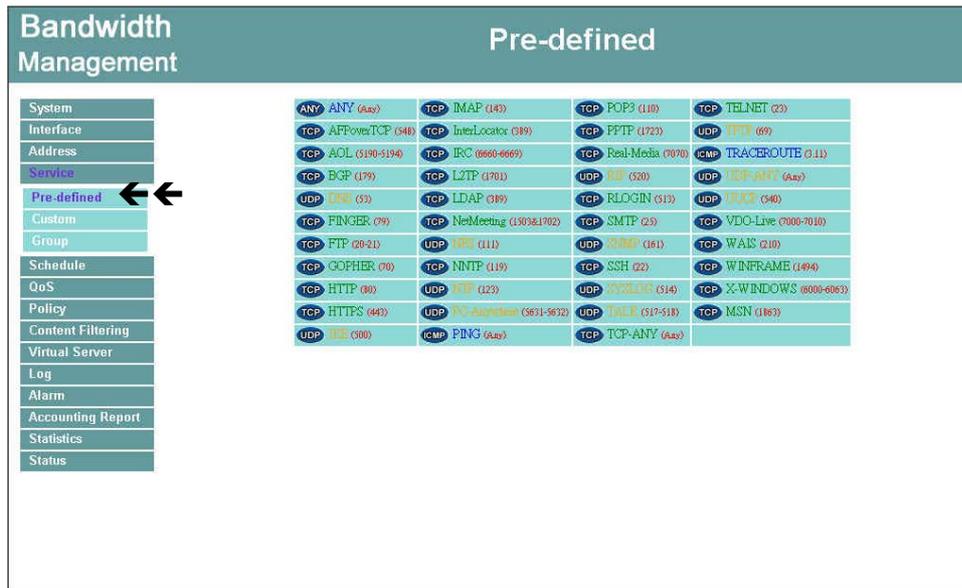


Figure4-1 Pre-defined Service

### Icons and Descriptions

Fig	Description
	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、
	UDP services, i.g. IKE、DNS、NTP、IRC、RIP、SNMP、SYSLOG、TALK、TFTP、UDP-ANY、UUC, etc.
	ICMP services, i.g. PING、TRACEROUTE, etc.

## 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.

The screenshot shows the 'Bandwidth Management' interface with the 'Custom' tab selected. On the left is a sidebar menu with options: System, Interface, Address, Service, Pre-defined, Custom (highlighted with two left-pointing arrows), Group, Schedule, QoS, Policy, Content Filtering, Virtual Server, Log, Alarm, Accounting Report, Statistics, and Status. The main area contains a table with the following data:

Service name	Protocol	Client Port	Server Port	Configure
eDonkey	TCP	1024:65535	4661:4665	Modify Remove
eDonkey-2	UDP	1024:65535	4665:4665	Modify Remove

Below the table is a 'New Entry' button.

Figure4-2 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**.

The screenshot shows the 'Bandwidth Management' interface with the 'Custom' tab selected. A dialog box titled 'Add User Define Service' is open. It contains a table with 8 rows for defining services. The first row is filled with 'TCP', '1024 : 65535', and '4661 : 4669'. The other rows are empty. The 'Service NAME' field contains 'eDonkey'. There are 'Ok' and 'Cancel' buttons at the bottom right of the dialog.

#	Protocol	Client Port	Server Port
1	<input checked="" type="radio"/> TCP <input type="radio"/> UDP <input type="radio"/> Other	1024 : 65535	4661 : 4669
2	<input checked="" type="radio"/> TCP <input type="radio"/> UDP <input type="radio"/> Other	1024 : 65535	0 : 0
3	<input checked="" type="radio"/> TCP <input type="radio"/> UDP <input type="radio"/> Other	1024 : 65535	0 : 0
4	<input checked="" type="radio"/> TCP <input type="radio"/> UDP <input type="radio"/> Other	1024 : 65535	0 : 0
5	<input checked="" type="radio"/> TCP <input type="radio"/> UDP <input type="radio"/> Other	1024 : 65535	0 : 0
6	<input checked="" type="radio"/> TCP <input type="radio"/> UDP <input type="radio"/> Other	1024 : 65535	0 : 0
7	<input checked="" type="radio"/> TCP <input type="radio"/> UDP <input type="radio"/> Other	1024 : 65535	0 : 0
8	<input checked="" type="radio"/> TCP <input type="radio"/> UDP <input type="radio"/> Other	1024 : 65535	0 : 0

Figure4-3 Add New Custom Service

## 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**.

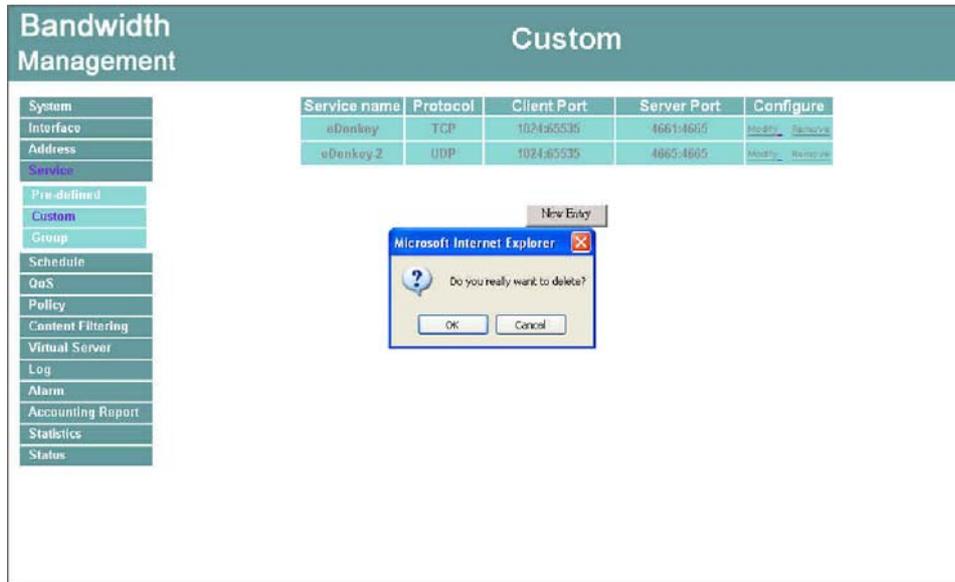
Bandwidth Management Custom									
Modify User Define Service									
System		Service NAME : eDonkey							
Address									
Service									
Pre-defined									
Custom									
Group									
Schedule									
QoS									
Policy									
Content Filtering									
Virtual Server									
Log									
Alarm									
Accounting Report									
Statistics									
Status									
#	Protocol	Client Port		Server Port					
1	<input checked="" type="radio"/> TCP <input type="radio"/> UDP <input type="radio"/> Other	6	1024	:	65535	4661	:	4665	
2	<input checked="" type="radio"/> TCP <input type="radio"/> UDP <input type="radio"/> Other	6	1024	:	65535	0	:	0	
3	<input checked="" type="radio"/> TCP <input type="radio"/> UDP <input type="radio"/> Other	6	1024	:	65535	0	:	0	
4	<input checked="" type="radio"/> TCP <input type="radio"/> UDP <input type="radio"/> Other	6	1024	:	65535	0	:	0	
5	<input checked="" type="radio"/> TCP <input type="radio"/> UDP <input type="radio"/> Other	6	1024	:	65535	0	:	0	
6	<input checked="" type="radio"/> TCP <input type="radio"/> UDP <input type="radio"/> Other	6	1024	:	65535	0	:	0	
7	<input checked="" type="radio"/> TCP <input type="radio"/> UDP <input type="radio"/> Other	6	1024	:	65535	0	:	0	
8	<input checked="" type="radio"/> TCP <input type="radio"/> UDP <input type="radio"/> Other	6	1024	:	65535	0	:	0	

Figure4-4 Modify Custom Service

## 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.



The screenshot displays the 'Bandwidth Management' interface with the 'Custom' tab selected. A table lists two services: 'eDonkey' (TCP, 1024:65535, 4661:4665) and 'eDonkey-2' (UDP, 1024:65535, 4665:4665). A 'New Entry' button is visible above the table. A 'Microsoft Internet Explorer' dialog box is overlaid on the screen, asking 'Do you really want to delete?' with 'OK' and 'Cancel' buttons.

Service name	Protocol	Client Port	Server Port	Configure
eDonkey	TCP	1024:65535	4661:4665	Modify Remove
eDonkey-2	UDP	1024:65535	4665:4665	Modify Remove

Figure4-5 Remove Custom Service

## 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.

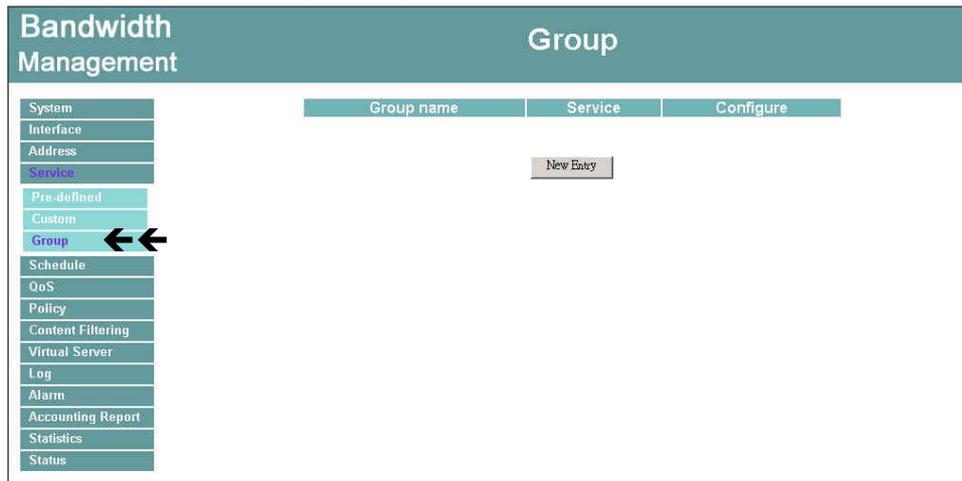


Figure4-6 Service Group

#### 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.



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:

- **Available Services:** list all the available services.
- **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.

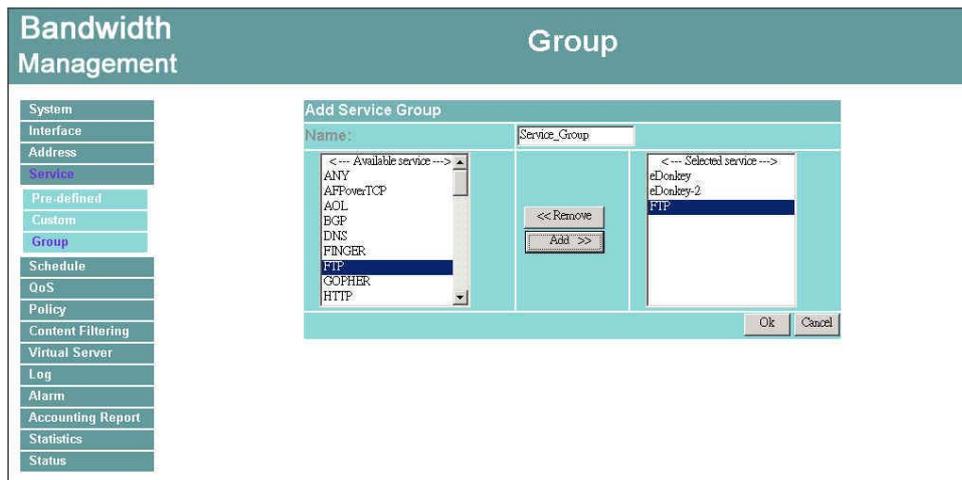


Figure4-7 Add New Group

## Modifying Service Groups

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

- **Available Services:** lists all the available services.
- **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 these services from the group.

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

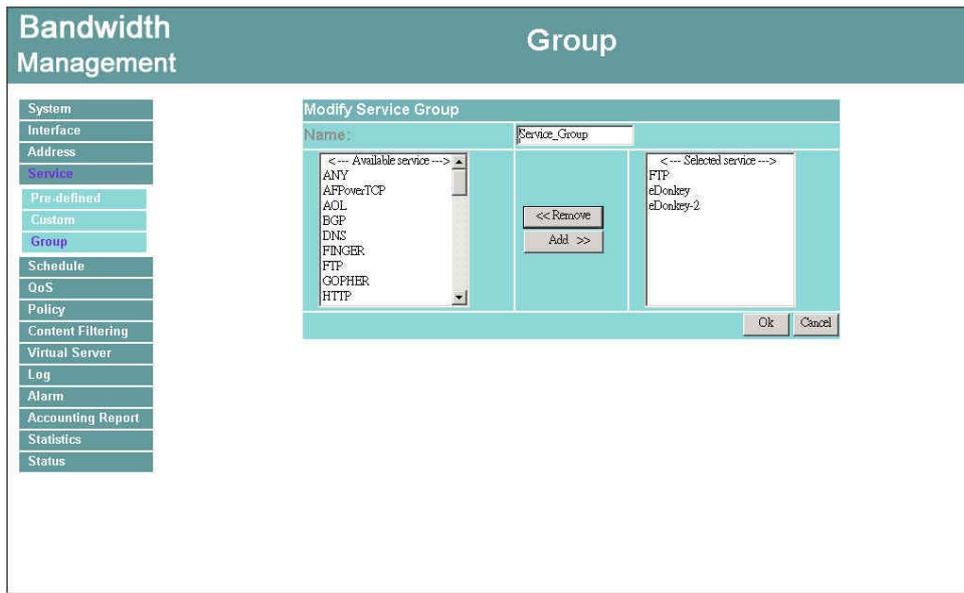


Figure4-8 Modify Group

## Removing Service Groups

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



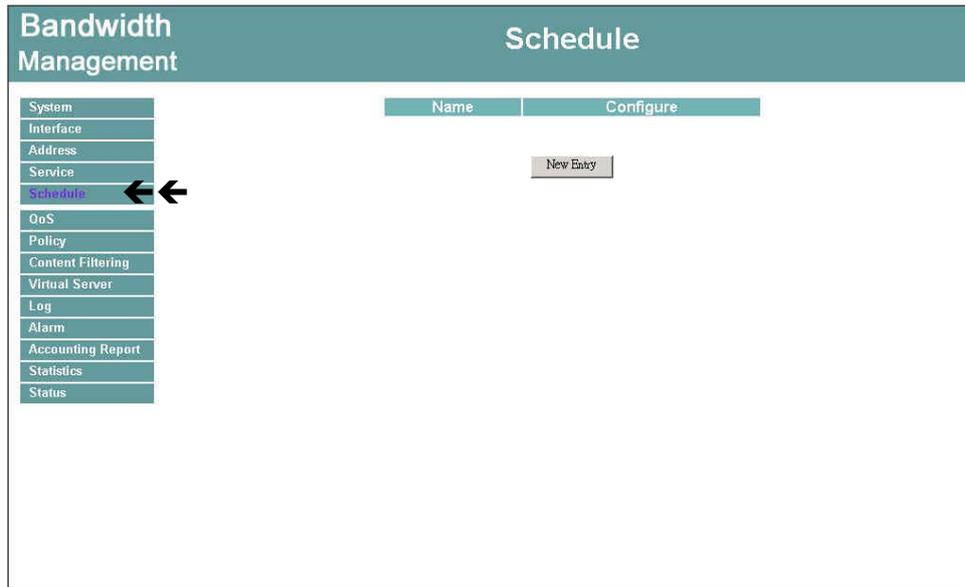
Figure4-9 Remove Group

# Schedule

The Bandwidth Management allows the Administrator to configure a schedule for policies to take affect. By creating a schedule, the Administrator is allowing the Bandwidth Management policies to be used at those designated times only. Any activities outside of the scheduled time slot will not follow the Bandwidth Management policies therefore will likely not be permitted to pass through the Bandwidth Management. 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 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 to work Monday-Friday, 8AM-5PM only. During the non-work hours, the Bandwidth Management 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.



**Figure5-1** Schedule

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.

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

Week Day	Period	
	Start Time	Stop Time
Monday	08:00	20:00
Tuesday	00:00	23:30
Wednesday	All day	All day
Thursday	00:00	18:00
Friday	Disable	Disable
Saturday	All day	All day
Sunday	Disable	Disable

Figure5-2 Add New Schedule



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.

The screenshot shows the 'Bandwidth Management Schedule' window. On the left is a navigation menu with options: System, Interface, Address, Service, Schedule (highlighted), QoS, Policy, Content Filtering, Virtual Server, Log, Alarm, Accounting Report, Statistics, and Status. The main area is titled 'Schedule' and contains a 'Modify Schedule' dialog. The dialog has a 'Schedule Name' field with the value 'Test'. Below this is a table with columns 'Week Day' and 'Period' (subdivided into 'Start Time' and 'Stop Time'). The table contains the following data:

Week Day	Period	
	Start Time	Stop Time
Monday	08:00	20:00
Tuesday	00:00	23:30
Wednesday	All day	All day
Thursday	00:00	18:00
Friday	Disable	Disable
Saturday	All day	All day
Sunday	Disable	Disable

At the bottom right of the dialog are 'Ok' and 'Cancel' buttons.

Figure5-3 Modify Schedule

## 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.

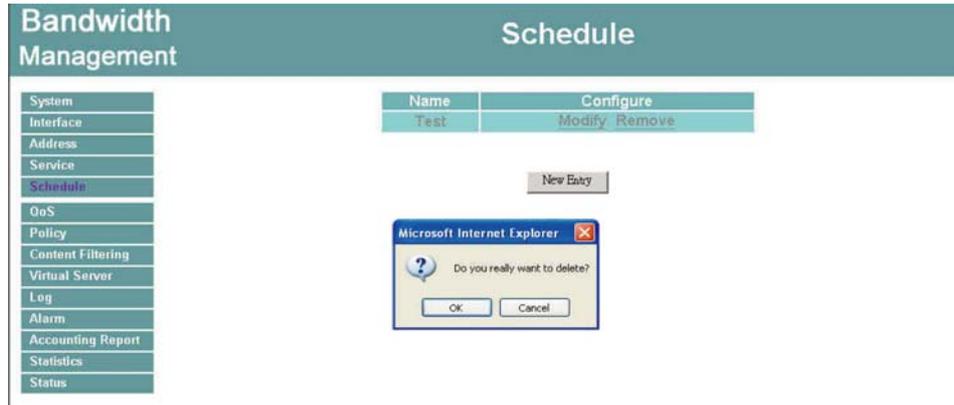


Figure5-4 Remove Schedule

# 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.

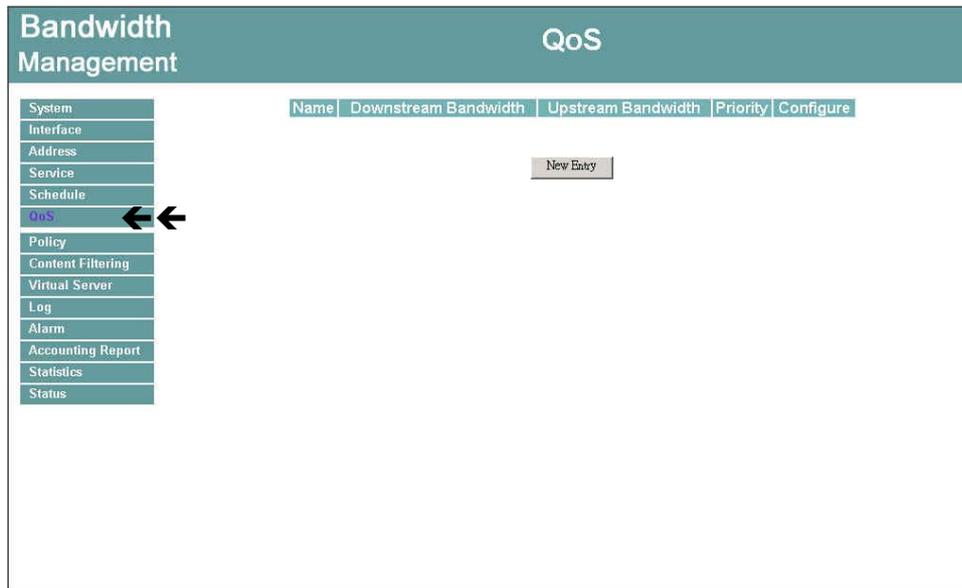
**Upstream Bandwidth** : To configure the Guaranteed Bandwidth and Maximum Bandwidth.

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

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

The screenshot shows a web interface for 'Bandwidth Management' with a 'QoS' menu item highlighted. A 'Add New QoS' dialog box is open, containing the following fields:

Add New QoS			
Name	<input type="text" value="Adsl"/>		
Downstream	Guaranteed Bandwidth	<input type="text" value="300"/>	kbps
	Maximum Bandwidth	<input type="text" value="350"/>	kbps
Upstream	Guaranteed Bandwidth	<input type="text" value="30"/>	kbps
	Maximum Bandwidth	<input type="text" value="40"/>	kbps
QoS Priority	<input type="text" value="Middle"/>		
			<input type="button" value="OK"/> <input type="button" value="Cancel"/>

**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 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.**

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

## Modify QoS

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

Bandwidth Management		QoS	
System		Modify QoS	
Interface		Name	Qos_1
Address		Downstream	Guaranteed Bandwidth 300 kbps
Service			Maximum Bandwidth 350 kbps
Schedule		Upstream	Guaranteed Bandwidth 60 kbps
QoS			Maximum Bandwidth 64 kbps
Policy		QoS Priority	Middle
Content Filtering			OK Cancel
Virtual Server			
Log			
Alarm			
Accounting Report			
Statistics			
Status			

Click the Modify button to modify QoS.

Definition:

**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**.

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.

The screenshot shows the 'Bandwidth Management' interface with the 'QoS' tab selected. A table lists the QoS configuration for 'Qos\_1'. A 'New Entry' button is visible above the table. A 'Microsoft Internet Explorer' dialog box is overlaid on the table, asking 'Do you really want to delete?' with 'OK' and 'Cancel' buttons.

Name	Downstream Bandwidth	Upstream Bandwidth	Priority	Configure
Qos_1	G.Bandwidth = 300 Kbps M.Bandwidth = 350 Kbps	G.Bandwidth = 60 Kbps M.Bandwidth = 64 Kbps	Medium	Modify Remove

# Policy

This section provides the Administrator with facilities to set 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.

## 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.

## 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.

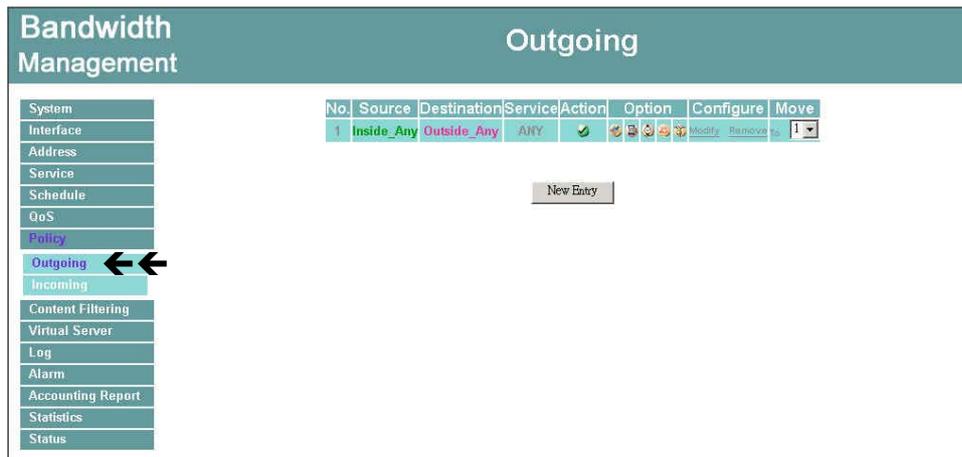


Figure7-1 Create an Outgoing Policy

The fields in the Outgoing window are:

- **Source:** source network addresses that are specified in the LAN section of Address menu, or all the LAN network addresses.
- **Destination:** destination network addresses that are specified in the WAN section of the Address menu, or all of the WAN network addresses.
- **Service:** specify services provided by WAN network servers.
- **Action:** control actions to permit or reject/deny packets from LAN networks to WANnetwork travelling through the Bandwidth Management.
- **Option:** specify the monitoring functions on packets from LAN networks to WANnetworks travelling through the Bandwidth Management.
- **Configure:** modify settings.
- **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.
<p>Remarks:</p> <p>To view the traffic and event log  of the system, click <b>Log</b> function in the menu bar on the left hand side.</p> <p>To view the alarm records  of the system, click <b>Alarm</b> function in the menu bar on the left hand side.</p> <p>To view the statistics  of the system, click <b>Statistics</b> function in the menu bar on the left hand side.</p> <p>Bandwidth Management can execute the schedule  function automatically in a certain time and range. To modify the schedule, click the <b>Schedule</b> function in the menu bar on the left hand side.</p> <p>Bandwidth Management can execute the QoS function  function automatically. To modify the QoS, click the <b>QoS</b> function in the menu bar on the left hand side.</p>		

## Adding a new Outgoing Policy

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

The screenshot shows a web interface for configuring an outgoing policy. On the left is a navigation menu with options: System, Interface, Address, Service, Schedule, QoS, Policy, Outgoing (highlighted), Incoming, Content Filtering, Virtual Server, Log, Alarm, Accounting Report, Statistics, and Status. The main area is titled 'Add New Policy' and contains the following fields:

Source Address	Inside_Any
Destination Address	Outside_Any
Service	ANY
Action	PERMIT
Logging	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
Schedule	None
Alarm Threshold	0.0 KBytes/Sec
QoS	None

At the bottom right of the form are 'Ok' and 'Cancel' buttons.

Figure7-2 Add a new Outgoing Policy

**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 WANnetworks 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 srvcies/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.

The screenshot shows the 'Bandwidth Management' window with the 'Outgoing' tab selected. The 'Modify Policy' section contains the following fields:

Modify Policy	
Source Address	Inside_Any
Destination Address	Outside_Any
Service	ANY
Action	PERMIT
Logging	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
Schedule	None
Alarm Threshold	0.0 KBytes/Sec
QoS	None

At the bottom right of the 'Modify Policy' section are 'Ok' and 'Cancel' buttons. On the left side of the window, a vertical menu lists various configuration options: System, Interface, Address, Service, Schedule, QoS, Policy, Outgoing (highlighted), Incoming, Content Filtering, Virtual Server, Log, Alarm, Accounting Report, Statistics, and Status.

**Figure7-3 Modify the Outgoing Policy**

**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.



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.

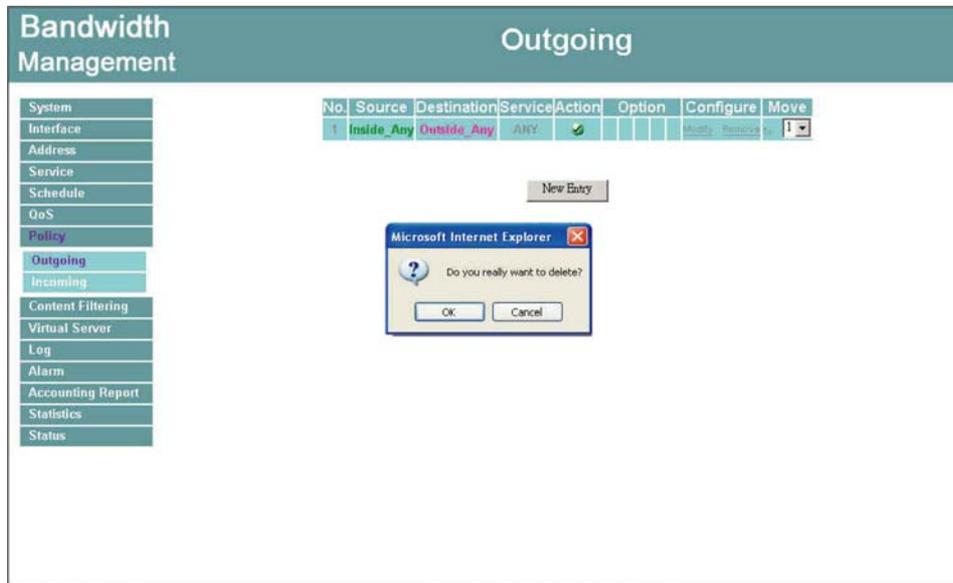


Figure7-4 Remove a Outgoing Policy

## 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.

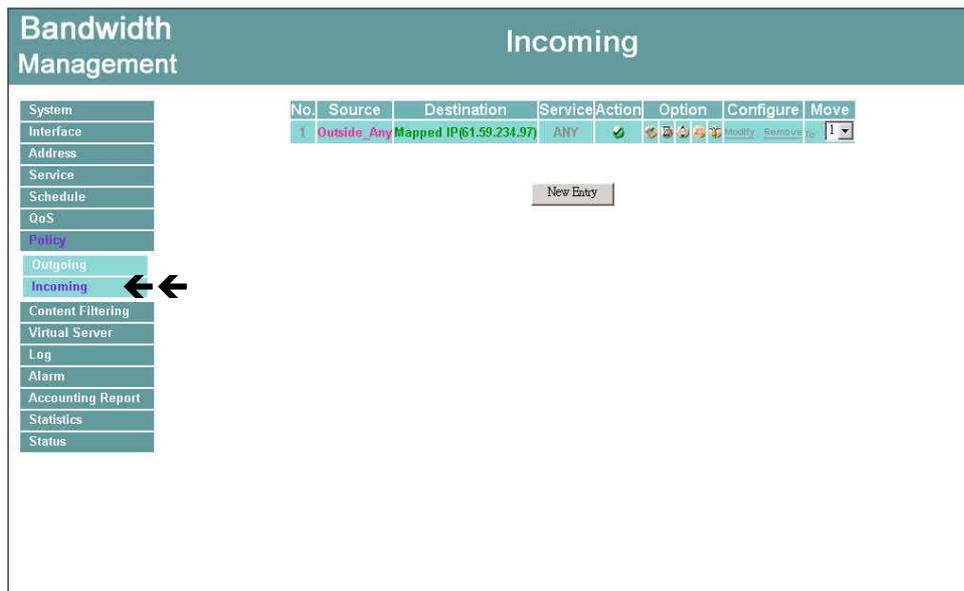


Figure7-5 Incoming Policy

**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.

**Option:** Control actions to monitor packets from WAN network or Virtual Server (Mapped IP)

traveling through the Bandwidth Management. 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.
- **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 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.

The screenshot shows the 'Bandwidth Management' interface with the 'Incoming' tab selected. A 'Add New Policy' dialog box is open, containing the following fields:

Add New Policy	
Source Address	Outside_Any
Destination Address	Mapped IP(61.59.234.97)
Service	ANY
Action	PERMIT
Logging	<input checked="" type="checkbox"/> Enable
Statistics	<input checked="" type="checkbox"/> Enable
Schedule	chen
Alarm Threshold	0.1 KBytes/Sec
QoS	Qos_1
<input type="button" value="Ok"/> <input type="button" value="Cancel"/>	

Figure7-6 Add a Incoming Policy

**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 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.

**Service** : Select the name of service from the pull-down menu.

The names of service 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.

**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 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.



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.

Bandwidth Management		Incoming	
<b>Modify Policy</b>			
Source Address	Outside_Any	Destination Address	Mapped IP(61.59.234.97)
Service	ANY	Action	PERMIT
Logging	<input checked="" type="checkbox"/> Enable	Statistics	<input checked="" type="checkbox"/> Enable
Schedule	chen	Alarm Threshold	0.1 KBytes/Sec
QoS	Qos_1		
		Ok Cancel	

**Figure7-7 Modify an Incoming Policy**

**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 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.



*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.

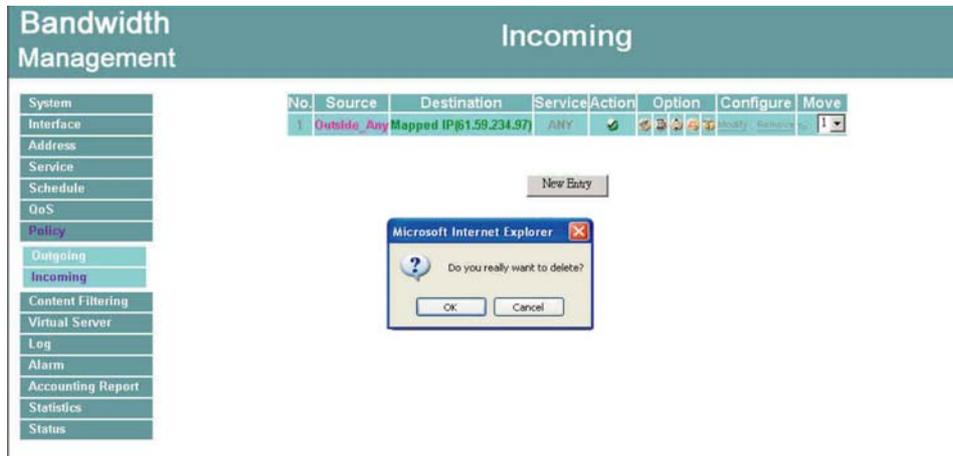


Figure7-8 Remove an Incoming Policy

# 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.

## Apply Policy

Administrator can use a complete domain name, key word, wild card (“~” or “\*”) to permit or block access to certain websites.

## 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**.

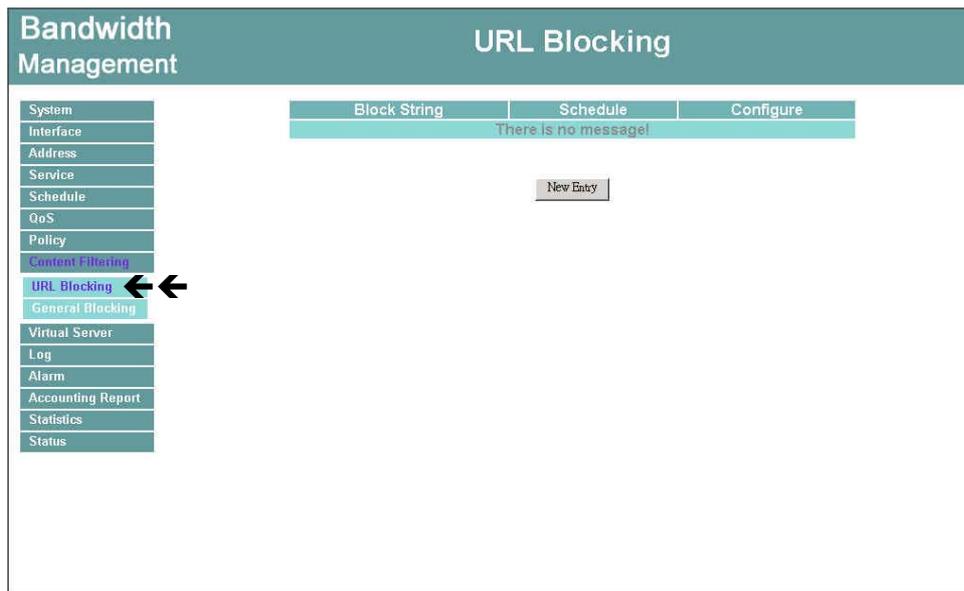


Figure8-1 Enter the URL Blocking

#### Definition:

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

**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](http://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
~www.hinet.net	None	<a href="#">Modify</a> <a href="#">Remove</a>
~www.kimo.com	None	<a href="#">Modify</a> <a href="#">Remove</a>
www.yahoo.com	None	<a href="#">Modify</a> <a href="#">Remove</a>
*	None	<a href="#">Modify</a> <a href="#">Remove</a>

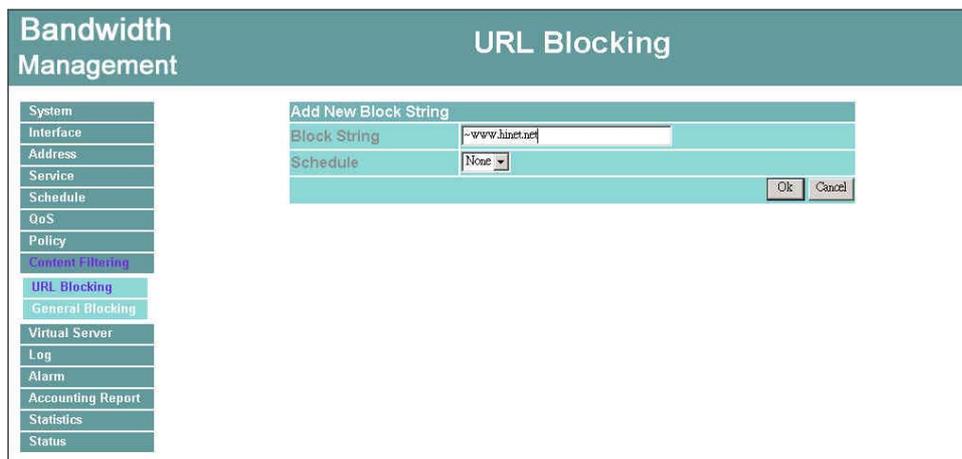
New Entry

## 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.



The screenshot shows a web-based configuration interface. On the left is a vertical menu titled 'Bandwidth Management' with various options: System, Interface, Address, Service, Schedule, QoS, Policy, Content Filtering, URL Blocking (highlighted in light blue), General Blocking, Virtual Server, Log, Alarm, Accounting Report, Statistics, and Status. The main area is titled 'URL Blocking' and contains a 'Add New Block String' dialog box. This dialog has two input fields: 'Block String' with the text '-www.linet.net' and 'Schedule' with a dropdown menu set to 'None'. At the bottom right of the dialog are 'Ok' and 'Cancel' buttons.

Figure8-2 Add a New URL Blocking

## 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.

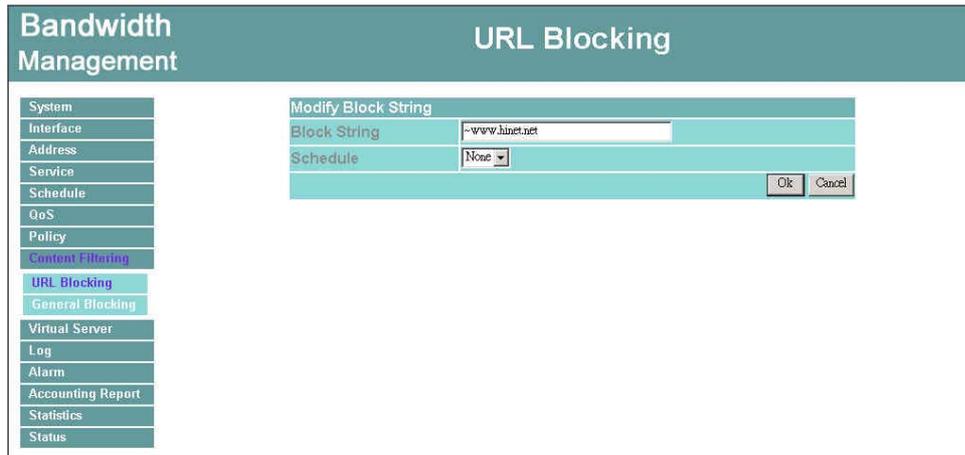


Figure8-3 Modify the URL Blocking

## 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.

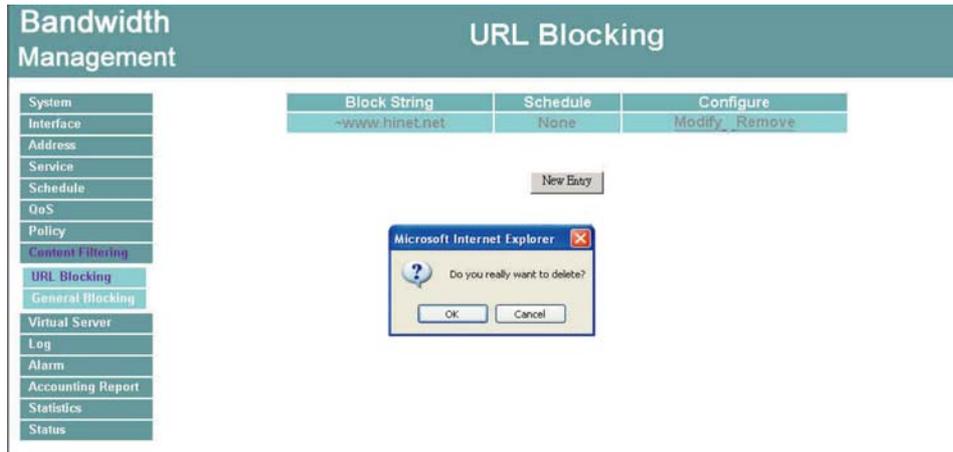
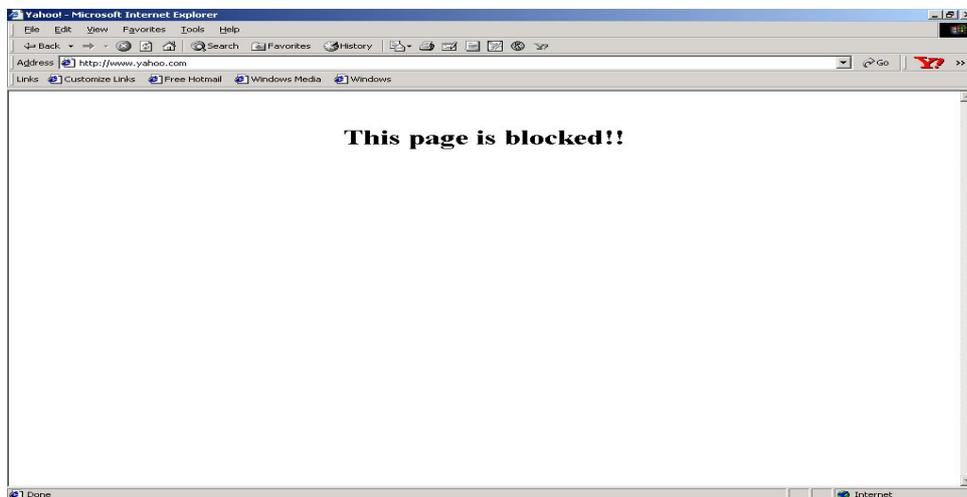


Figure8-4 Remove a URL Blocking

### Blocked URL site:

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



## General Blocking

To let Popups, 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.

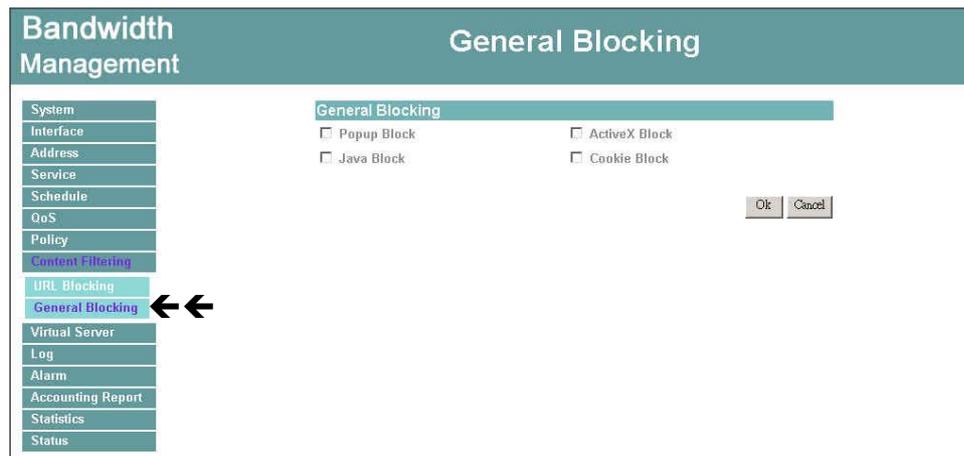


Figure8-5 General Blocking Policy

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

# Virtual Server

The Bandwidth Management 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'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's Virtual Server can solve this problem. A virtual server has set the real IP address of the Bandwidth Management's WAN network interface to be the Virtual Server IP. Through the virtual server feature, the Bandwidth Management 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 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.

## 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 WANIP 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.

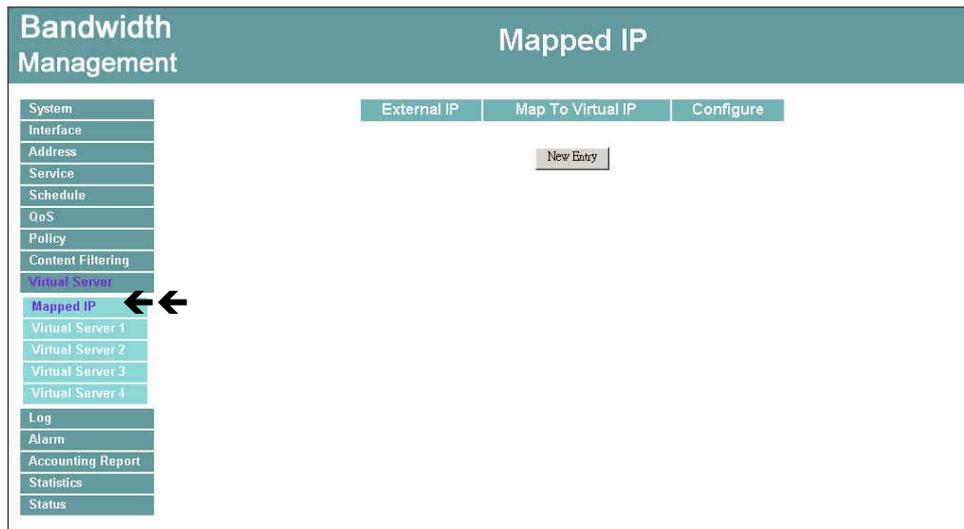


Figure9-1 Mapped IP

#### 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.

The screenshot shows the 'Mapped IP' configuration window. On the left is a sidebar menu with the following items: System, Interface, Address, Service, Schedule, QoS, Policy, Content Filtering, Virtual Server, Mapped IP (highlighted), Virtual Server 1, Virtual Server 2, Virtual Server 3, Virtual Server 4, Log, Alarm, Accounting Report, Statistics, and Status. The main content area displays the 'Add New Mapped IP' dialog box. This dialog has two input fields: 'External IP' with the value '61.59.234.97' and an 'Assist' button, and 'Map To Virtual IP' with the value '192.168.1.2'. At the bottom right of the dialog are 'OK' and 'Cancel' buttons.

**Figure9-2** Add New Mapped IP

## 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.

Bandwidth Management		Mapped IP	
System		Modify Mapped IP	
Interface		External IP	51.59.234.97 Assist
Address		Map To Virtual IP	192.168.1.2
Service			Ok Cancel
Schedule			
QoS			
Policy			
Content Filtering			
Virtual Server			
Mapped IP			
Virtual Server 1			
Virtual Server 2			
Virtual Server 3			
Virtual Server 4			
Log			
Alarm			
Accounting Report			
Statistics			
Status			

**Figure9-3 Modify Mapped IP**



**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.

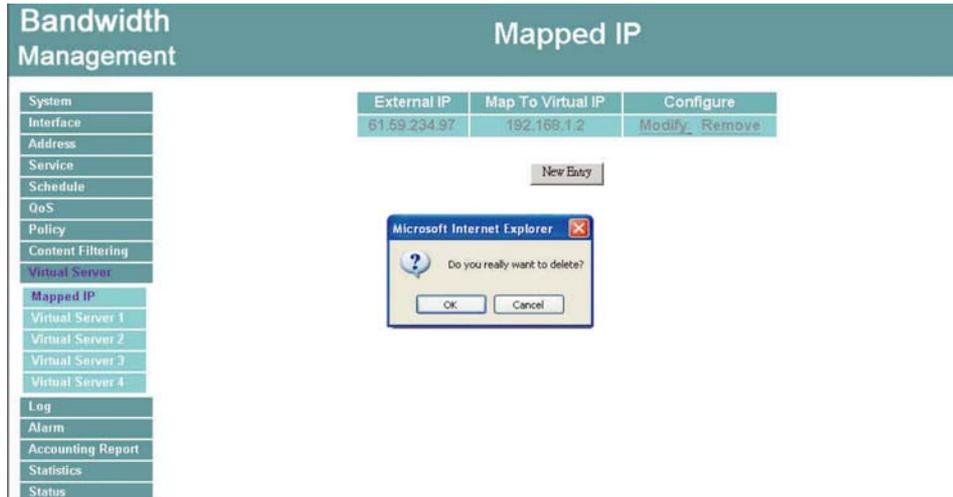


Figure9-4 Remove Mapped IP

## 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 an WANIP to an LAN IP, virtual server binds WAN IP ports to LAN IP ports.



Figure9-5 Virtual Server

### 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 Server1/2/3/4under 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.

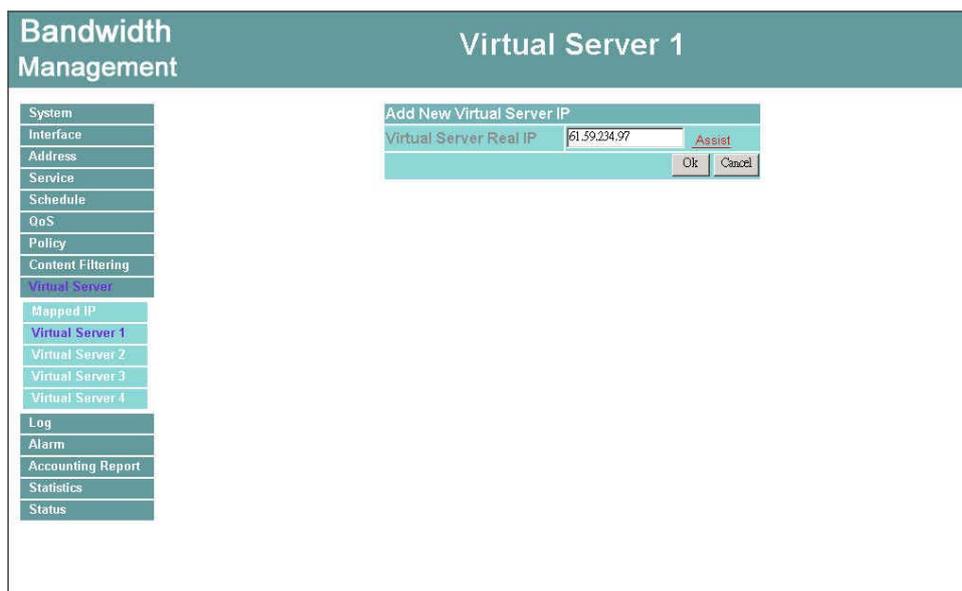


Figure 9-6 Add New Virtual Server

## 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.

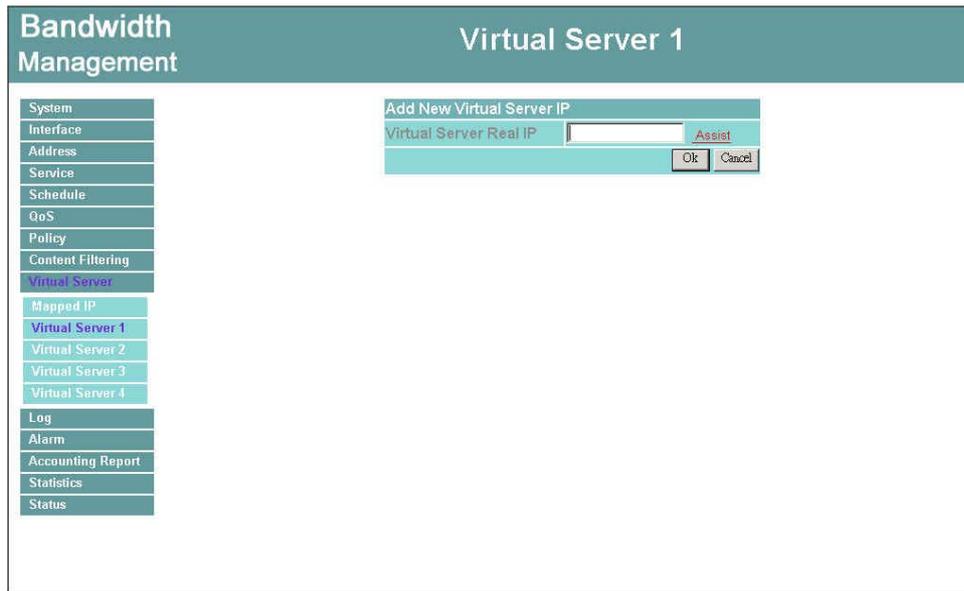


Figure9-7 Modify Virtual Server IP Address

## 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.** Select Disable in the drop-down list in.

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

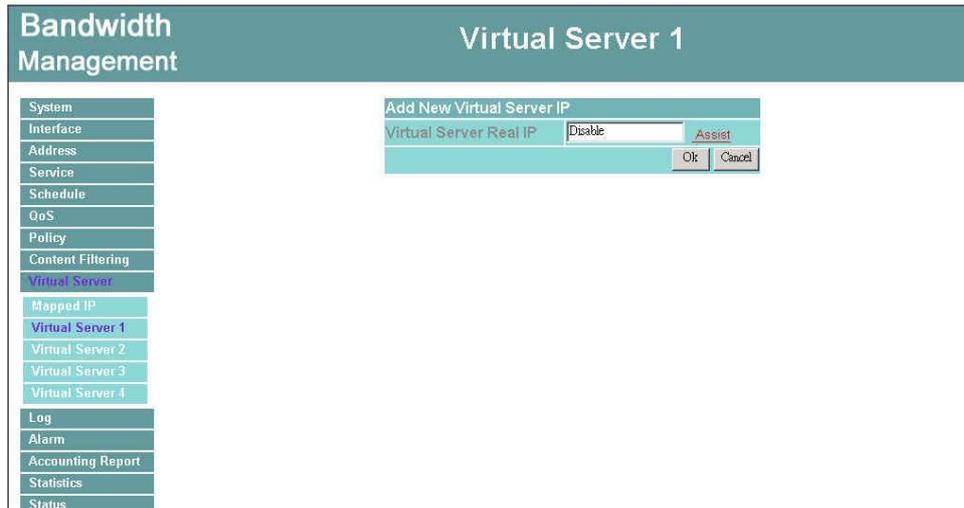


Figure9-8 Remove Virtual Server

## 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:

- **Server Virtual IP:** displays the WAN IP address assigned to the Virtual Server
- **External Service Port:** select the port number that the virtual server will use. Changing the Service will change the port number to match the service.
- **Service:** select the service from the pull down list that will be provided by the Virtual Server.
- **Internal Server IP :** 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.

**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	51.59.234.97
Service Name (Port)	HTTP (80)
External Service Port	80
Load Balance Server	Server Virtual IP
1	192.168.1.2
2	192.168.1.3
3	192.168.1.4
4	192.168.1.5
OK Cancel	

Figure9-9 Add New Virtual Server

## 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 “Click here to configure” button.

**Step 3.** Enter the parameters in the Server Virtual IP column.

Virtual Server Configuration	
Virtual Server Real IP	61.59.234.97
Service Name (Port)	HTTP (80)
External Service Port	80
Load Balance Server	Server Virtual IP
1	192.168.1.2
2	192.168.1.3
3	192.168.1.4
4	192.168.1.5

**Figure9-10 Add Virtual Server**

**Server Virtual IP** : Enter the WAN IP address configured by the virtual server.

**Service Name (Port)** : Click the pull-down menu the system will display you the service item port.

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

**Internal Server IP** : 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.

Click **OK** to execute adding new virtual server service, or click **Cancel** to discard adding.

The administrator can click the “Click here to configure” button in the Virtual Server window to add the service items of virtual server. 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.

The screenshot shows a window titled "Bandwidth Management" with a sub-header "Virtual Server 1". On the left is a navigation menu with options: System, Interface, Address, Service, Schedule, QoS, Policy, Content Filtering, Virtual Server (highlighted), Mapped IP, Virtual Server 1, Virtual Server 2, Virtual Server 3, Virtual Server 4, Log, Alarm, Accounting Report, Statistics, and Status. The main area displays the "Virtual Server Configuration" form. It includes fields for "Virtual Server Real IP" (51.59.234.97), "Service Name (Port)" (HTTP (80)), and "External Service Port" (80). Below these is a table for "Load Balance Server" with columns "Load Balance Server" and "Server Virtual IP". The table contains four rows with values 1, 2, 3, and 4, and IP addresses 192.168.1.2, 192.168.1.3, 192.168.1.4, and 192.168.1.5 respectively. At the bottom right of the form are "Ok" and "Cancel" buttons.

Figure9-11 Modify Virtual Server

**WAN** : Enter the WAN IP address that configured by the virtual server.

**Port** : Click the pull-down menu and the system will display you the service item port

**Service Name** : The service names provided by the virtual server.

**Server Virtual IP** : Enter the internal IP address mapped by the virtual server. Four computer IP addresses can be set at most.

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



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.

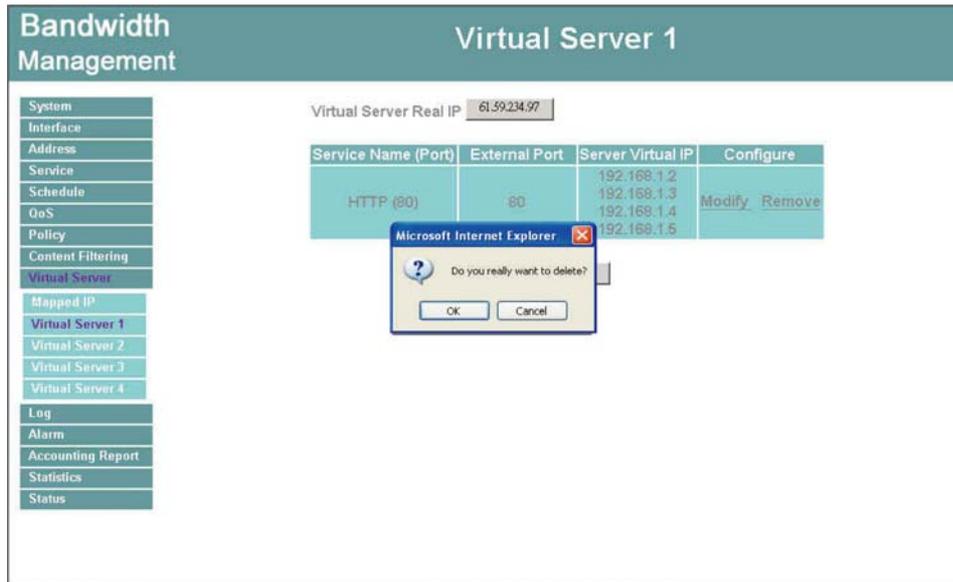


Figure9-12 Remove Virtual Server



*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.*

# Log

The Bandwidth Management 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.

## What is Log?

Log records all connections that pass through the Bandwidth Management'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.

## Traffic Log

The Administrator queries the Bandwidth Management 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 1 01:10:32	192.168.1.3	192.168.1.1	TCP : 80	ACCEPT
May 1 01:10:10	192.168.1.3	192.168.1.1	TCP : 80	ACCEPT
May 1 00:59:27	192.168.1.3	192.168.1.1	TCP : 80	ACCEPT
May 1 00:58:57	192.168.1.3	192.168.1.1	TCP : 80	ACCEPT
May 1 00:56:18	192.168.1.3	192.168.1.1	TCP : 80	ACCEPT
May 1 00:54:43	192.168.1.3	192.168.1.1	TCP : 80	ACCEPT
May 1 00:53:36	192.168.1.3	192.168.1.1	TCP : 80	ACCEPT
May 1 00:52:39	192.168.1.3	192.168.1.1	TCP : 80	ACCEPT
May 1 00:52:35	192.168.1.3	192.168.1.1	TCP : 80	ACCEPT
May 1 00:51:43	192.168.1.3	192.168.1.1	TCP : 80	ACCEPT
May 1 00:51:42	61.154.246.190	192.168.1.2	UDP : 137	DROP
May 1 00:51:01	192.168.1.3	192.168.1.1	TCP : 80	ACCEPT
May 1 00:50:14	192.168.1.3	192.168.1.1	TCP : 80	ACCEPT
May 1 00:49:30	192.168.1.3	192.168.1.1	TCP : 80	ACCEPT
May 1 00:49:29	192.168.1.3	192.168.1.1	TCP : 80	ACCEPT
May 1 00:48:41	192.168.1.3	192.168.1.1	TCP : 80	ACCEPT
May 1 00:48:40	192.168.1.3	192.168.1.1	TCP : 80	ACCEPT
May 1 00:48:39	192.168.1.3	192.168.1.1	TCP : 80	ACCEPT
May 1 00:48:11	192.168.1.3	192.168.1.1	TCP : 80	ACCEPT
May 1 00:47:47	192.168.1.3	192.168.1.1	TCP : 80	ACCEPT

Figure10-1 Traffic Log

### Traffic Log Table

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

#### Definition:

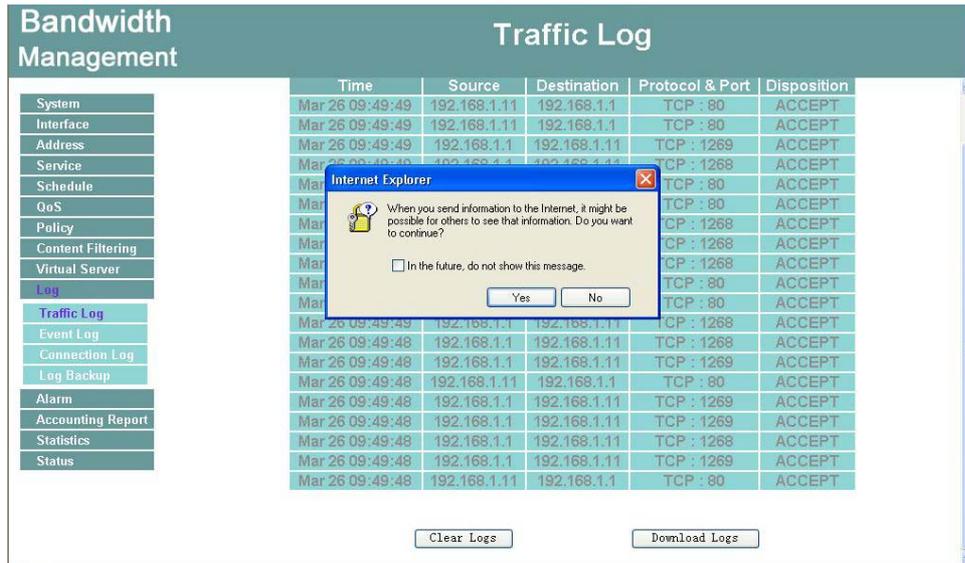
- **Time:** The start time of the connection.
- **Source:** IP address of the source network of the specific connection.
- **Destination:** IP address of the destination network of the specific connection.
- **Protocol & Port:** Protocol type and Port number of the specific connection.
- **Disposition:**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



The screenshot displays the 'Bandwidth Management' interface with a 'Traffic Log' window. On the left is a navigation menu with options like System, Interface, Address, Service, Schedule, QoS, Policy, Content Filtering, Virtual Server, Log, Traffic Log, Event Log, Connection Log, Log Backup, Alarm, Accounting Report, Statistics, and Status. The 'Traffic Log' window shows a table with columns: Time, Source, Destination, Protocol & Port, and Disposition. The table contains 15 rows of log entries. An 'Internet Explorer' dialog box is overlaid on the table, asking for permission to download the file. At the bottom of the Traffic Log window are 'Clear Logs' and 'Download Logs' buttons.

Time	Source	Destination	Protocol & Port	Disposition
Mar 26 09:49:49	192.168.1.11	192.168.1.1	TCP : 80	ACCEPT
Mar 26 09:49:49	192.168.1.11	192.168.1.1	TCP : 80	ACCEPT
Mar 26 09:49:49	192.168.1.1	192.168.1.11	TCP : 1269	ACCEPT
Mar 26 09:49:48	192.168.1.1	192.168.1.11	TCP : 1268	ACCEPT
Mar 26 09:49:48	192.168.1.1	192.168.1.11	TCP : 80	ACCEPT
Mar 26 09:49:48	192.168.1.1	192.168.1.11	TCP : 80	ACCEPT
Mar 26 09:49:48	192.168.1.1	192.168.1.11	TCP : 1268	ACCEPT
Mar 26 09:49:48	192.168.1.1	192.168.1.11	TCP : 1268	ACCEPT
Mar 26 09:49:48	192.168.1.1	192.168.1.11	TCP : 1268	ACCEPT
Mar 26 09:49:48	192.168.1.1	192.168.1.11	TCP : 80	ACCEPT
Mar 26 09:49:48	192.168.1.1	192.168.1.11	TCP : 80	ACCEPT
Mar 26 09:49:48	192.168.1.1	192.168.1.11	TCP : 1268	ACCEPT
Mar 26 09:49:48	192.168.1.1	192.168.1.11	TCP : 1269	ACCEPT
Mar 26 09:49:48	192.168.1.1	192.168.1.11	TCP : 1269	ACCEPT
Mar 26 09:49:48	192.168.1.1	192.168.1.1	TCP : 80	ACCEPT

Figure10-2 Traffic Log

## 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.

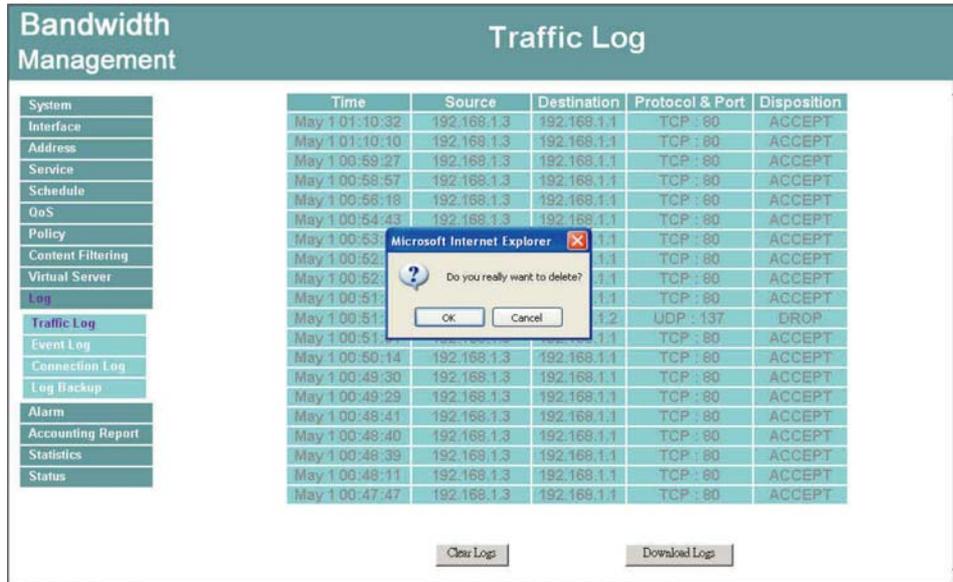


Figure10-3 Clear Traffic Logs

## Event Log

When the Bandwidth Management 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.



The screenshot shows the 'Event Log' window within the 'Bandwidth Management' interface. The window title is 'Event Log' and it features a dropdown menu set to 'May 1 01:10:29' and a 'Next' link. On the left, a sidebar menu lists various system components, with 'Event Log' highlighted and two arrows pointing to it. The main area contains a table with the following data:

Time	Event
May 1 01:10:29	admin Remove [Virtual Server 1] from 192.168.1.3
May 1 01:10:10	admin Remove [HTTP] (Virtual Server 1) from 192.168.1.3
May 1 00:58:58	admin Add [HTTP] (Virtual Server 1) from 192.168.1.3
May 1 00:56:21	admin Modify [Virtual Server 1] from 192.168.1.3
May 1 00:54:43	admin Add [Virtual Server 1] from 192.168.1.3
May 1 00:52:35	admin Remove [Mapped IP] (External IP : 61.59.234.97 Internal IP : 192.168.1.2) from 192.168.1.3
May 1 00:51:01	admin Add [Mapped IP] (External IP : 61.59.234.97 Internal IP : 192.168.1.2) from 192.168.1.3
May 1 00:49:36	admin Remove [Mapped IP] (External IP : 61.59.234.97 Internal IP : 192.168.1.2) from 192.168.1.3
May 1 00:48:39	admin Delete [URL Blocking](~www.hinet.net,None) from 192.168.1.3
May 1 00:47:46	admin Add [URL Blocking](~www.hinet.net,None) from 192.168.1.3

At the bottom of the window, there are 'Clear Logs' and 'Download Logs' buttons.

Figure10-4 Event Log

**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.

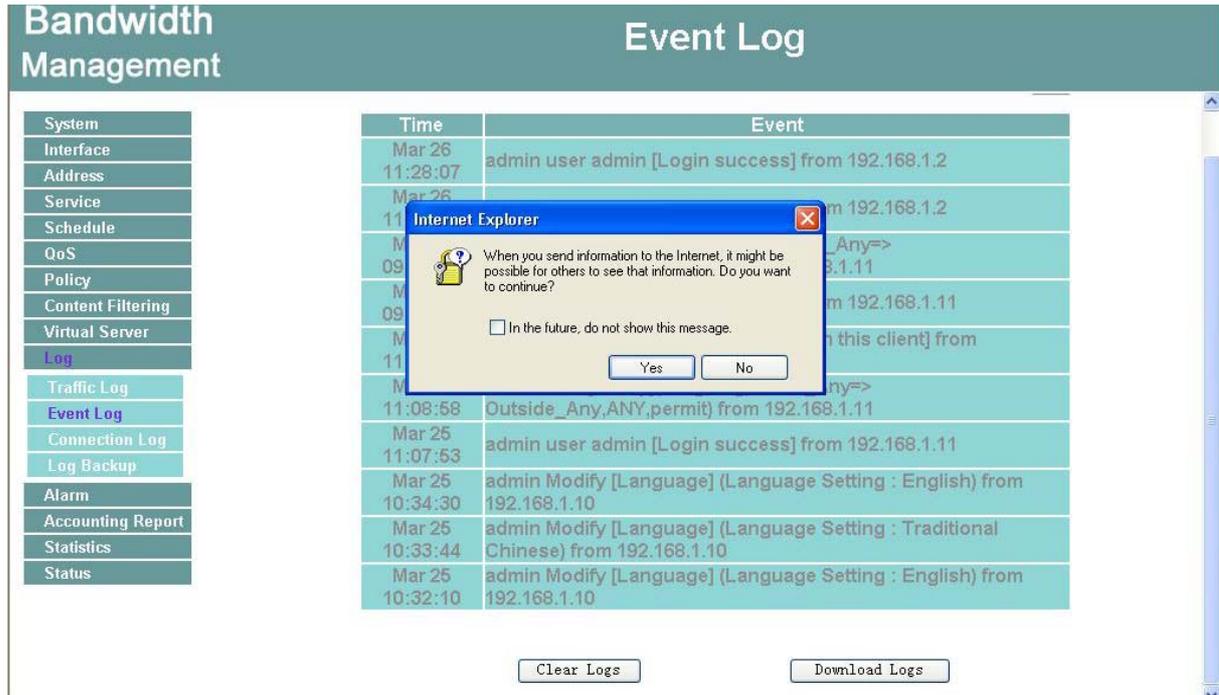


Figure10-5 Download the Event Logs

## 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.

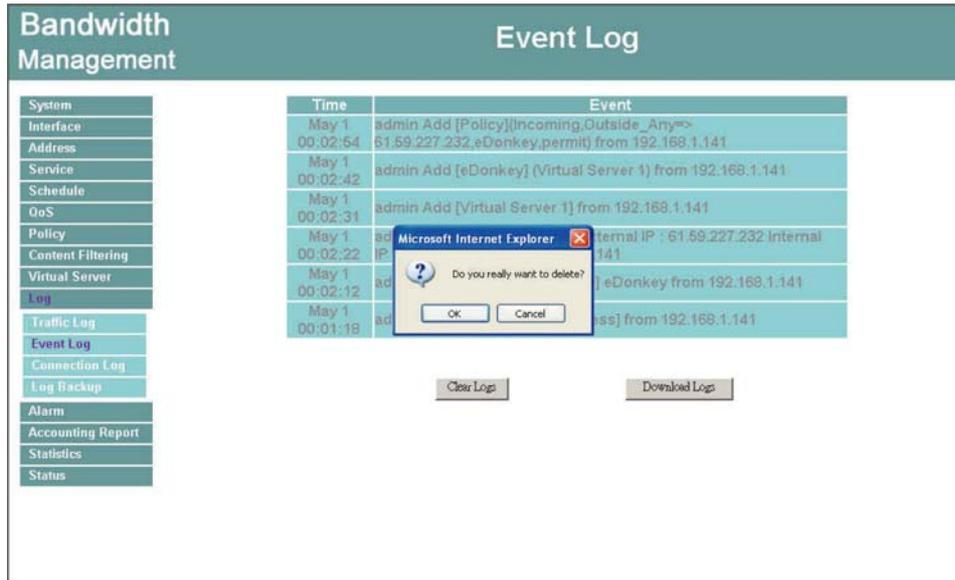
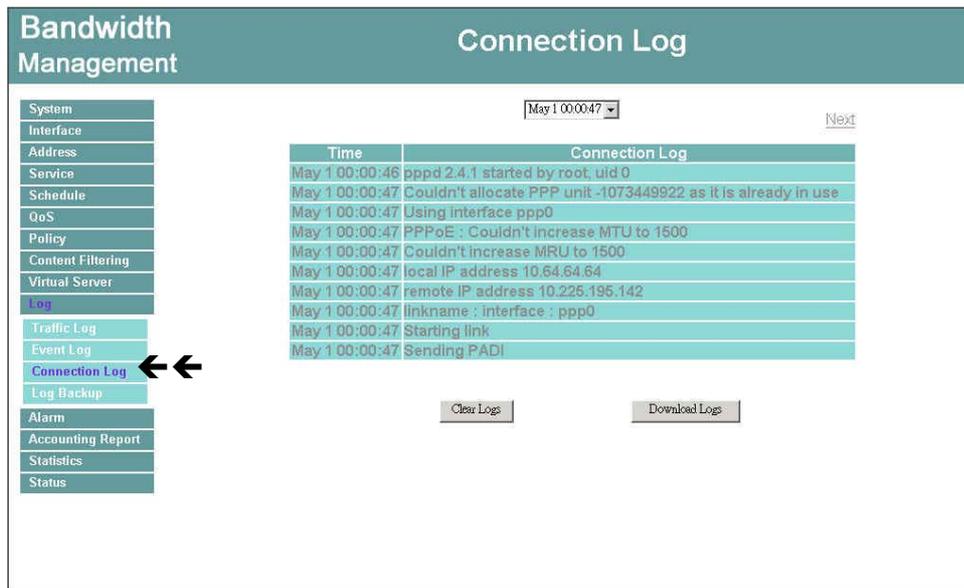


Figure10-6 Clear the Event Logs

## Connection Log

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



The screenshot shows a web interface for 'Bandwidth Management' with a 'Connection Log' section. On the left is a vertical menu with options: System, Interface, Address, Service, Schedule, QoS, Policy, Content Filtering, Virtual Server, Log, Traffic Log, Event Log, Connection Log (highlighted with two arrows), Log Backup, Alarm, Accounting Report, Statistics, and Status. The main area displays a table of connection logs for 'May 1 00:00:47'. The table has two columns: 'Time' and 'Connection Log'. Below the table are 'Clear Logs' and 'Download Logs' buttons. A 'Next' link is visible in the top right corner of the log area.

Time	Connection Log
May 1 00:00:46	pppd 2.4.1 started by root, uid 0
May 1 00:00:47	Couldn't allocate PPP unit -1073449922 as it is already in use
May 1 00:00:47	Using interface ppp0
May 1 00:00:47	PPPoE : Couldn't increase MTU to 1500
May 1 00:00:47	Couldn't increase MRU to 1500
May 1 00:00:47	local IP address 10.64.64.64
May 1 00:00:47	remote IP address 10.225.195.142
May 1 00:00:47	linkname : interface : ppp0
May 1 00:00:47	Starting link
May 1 00:00:47	Sending PADI

Figure10-7 Connection Log

### 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.

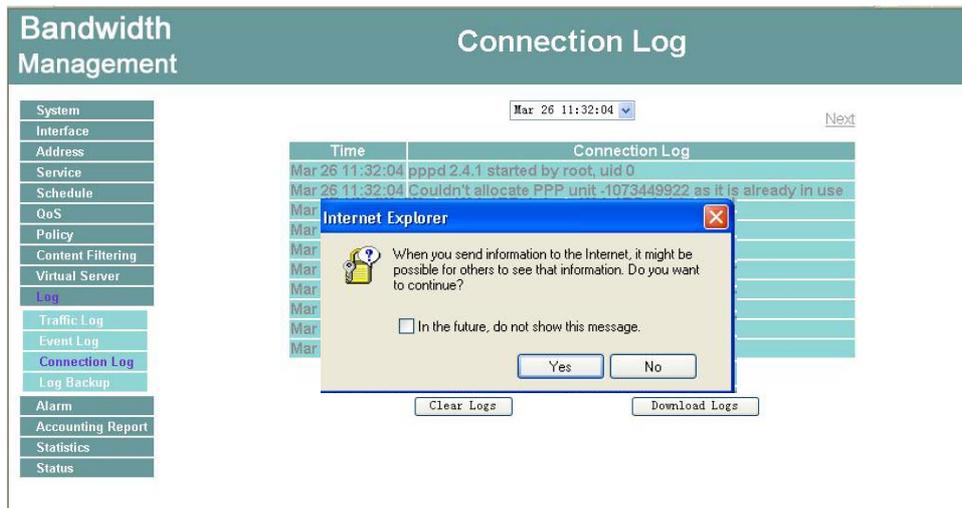


Figure10-8 Connection Log

## 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.

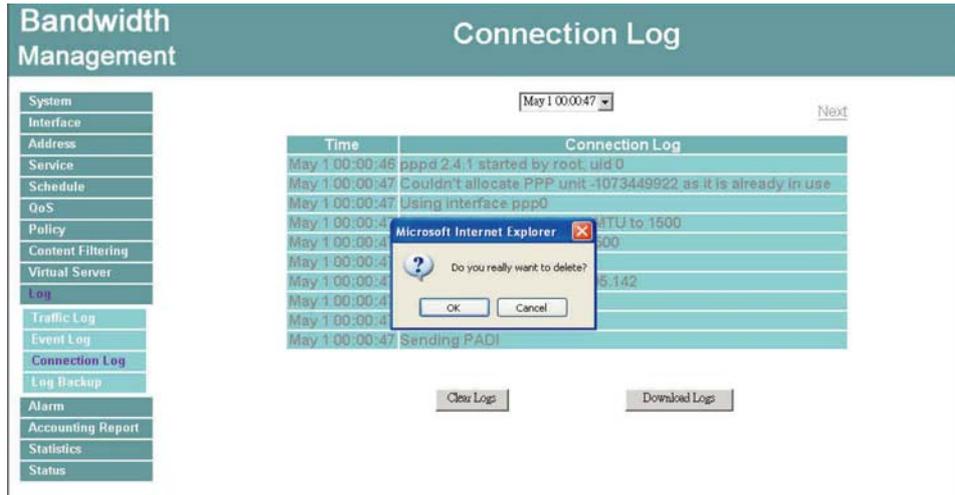
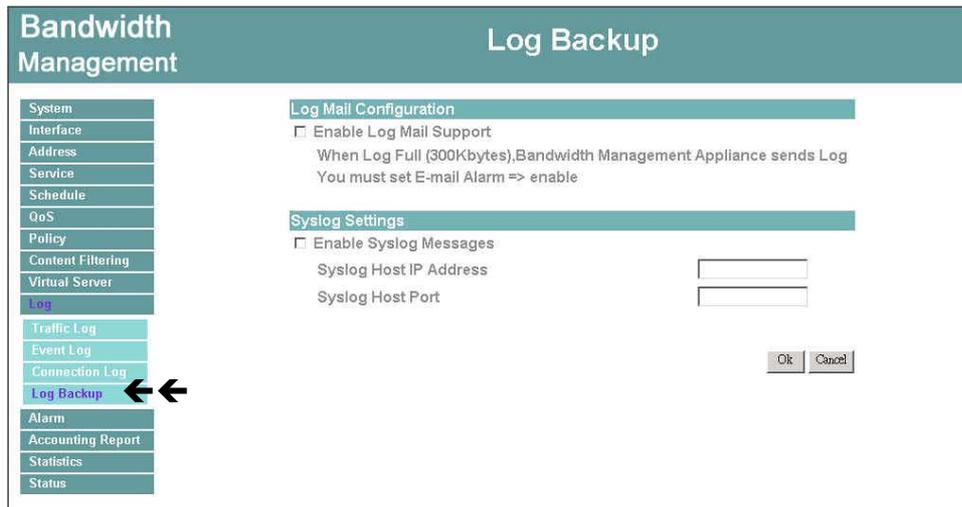


Figure10-9 Clear the Connection Logs

# Log Backup

**Step 1.** Click **Log** → **Log Backup**.



**Figure10-10** Log Backup

**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 enable E-mail Alarm in Administrator.

**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.



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** →**Log 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**.

**Bandwidth Management** **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

Figure10-11 Log Backup

## Disable Log Mail Support & Syslog Message

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

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

**Bandwidth Management** **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

OK Cancel

Figure10-12 Disable Log Backup

# Alarm

In this chapter, the Administrator can view traffic alarms and event alarms that occur and the Bandwidth Management has logged.

Bandwidth Management 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 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.



## **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.

## 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.

### Entering the Traffic Alarm window

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

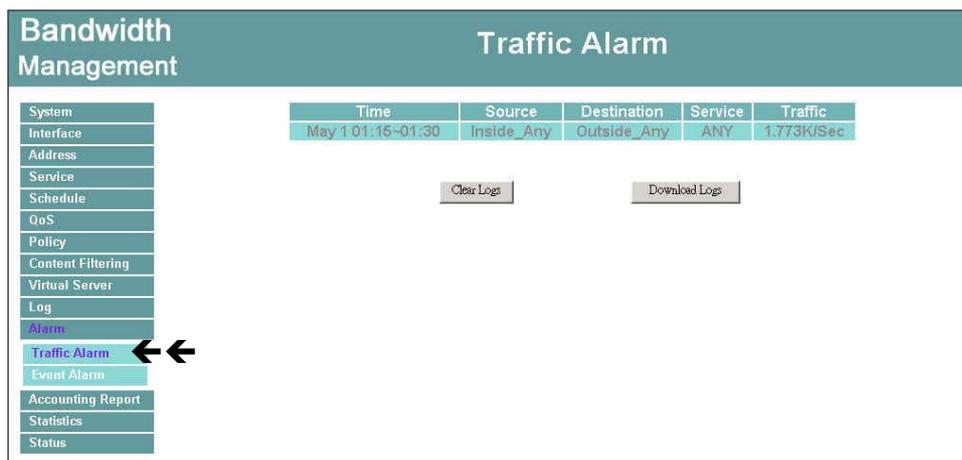


Figure11-1 Traffic Alarm

**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.

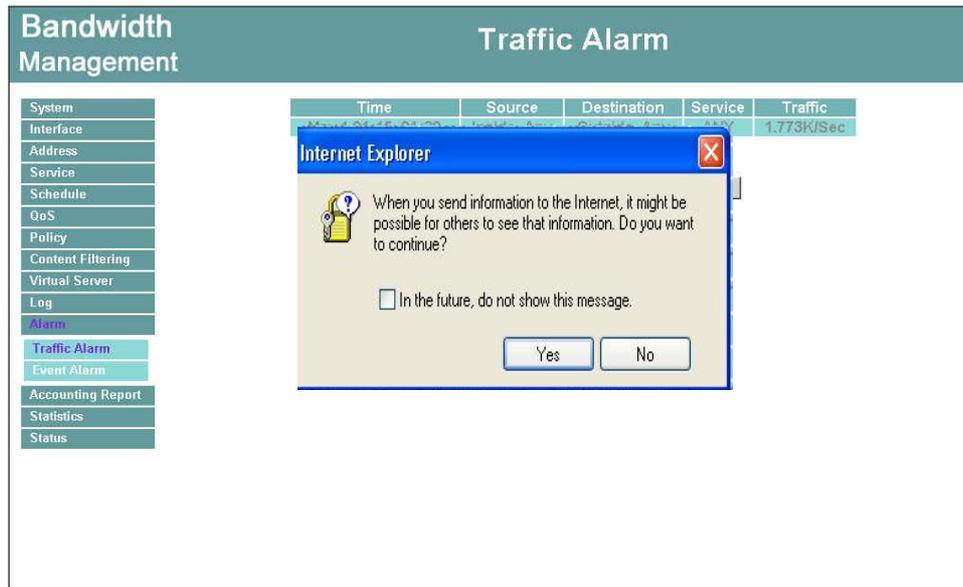


Figure11-2 Traffic Alarm

## 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.



Figure11-3 Clear Traffic Alarm

## Event Alarm

When Bandwidth Management 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
May 1 02:26:19	Possible ICMP FLOOD from 211.22.93.138 (00:02:3b:00:86:1c) against 61.69.234.97, recieved 2 packets
May 1 02:26:56	Possible ICMP FLOOD from 211.22.93.138 (00:02:3b:00:86:1c) against 61.69.234.97, recieved 2 packets
May 1 02:26:43	Possible ICMP FLOOD from 211.22.93.138 (00:02:3b:00:86:1c) against 61.69.234.97, recieved 2 packets

Figure11-4 Event Alarm

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.

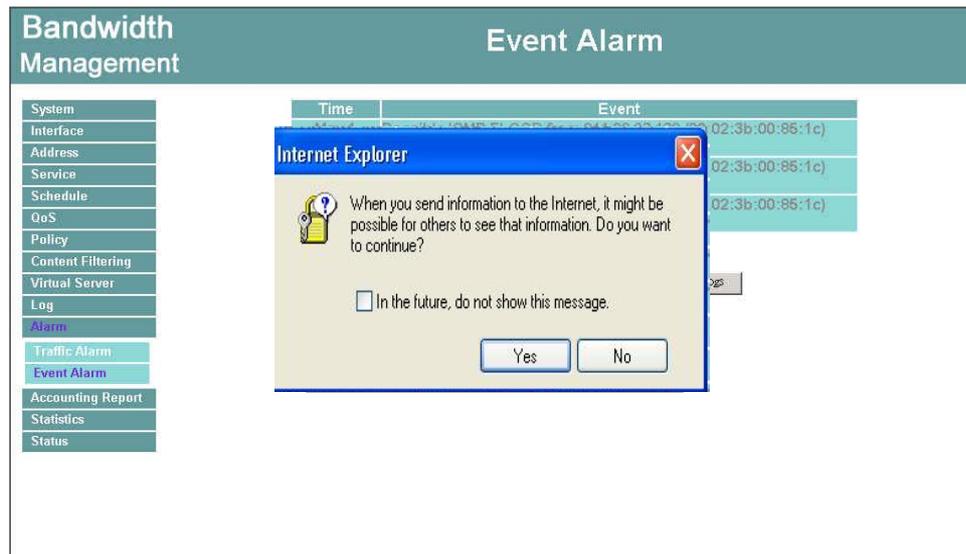


Figure11-5 Event Alarm

## 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**.

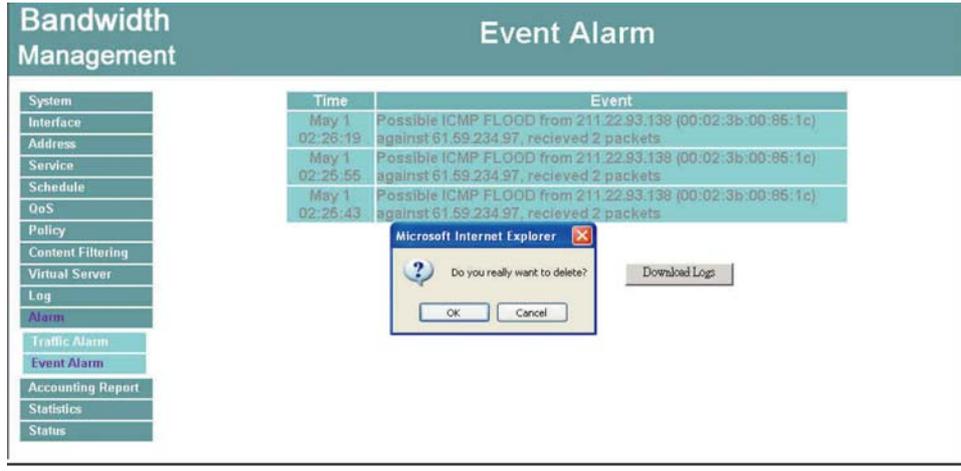


Figure11-6 Clear the Event Alarm

# 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



It 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

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

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

## Inbound Accounting Report



It 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 to connect to LAN Service Server.

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

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

**Service** : The communication service which listed in the pull-down menu when WAN users use bandwidth management 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.

# Outbound Accounting Report

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

## Bandwidth Management

### Outbound

System Top: [1-1]  
Interface Reset Time : Wed May 1 00:44:49 2002  
Address  
Service  
Schedule  
QoS  
Policy  
Content Filtering  
Virtual Server  
Log  
Alarm  
Accounting Report  
Outbound ←←  
Inbound  
Statistics  
Status

No.	Source IP	Downstream	Upstream	First Packet	Last Packet	Duration
1	192.168.1.3	2.4 MB 100.0%	432.9 KB 100.0%	05/01 00:51:30	05/01 02:28:02	01:36:32
<b>Total Traffic</b>		<b>2.4 MBytes</b>	<b>432.9 KBytes</b>	Reporting time: Wed May 1 02:29:11 2002		

## Outbound source IP Accounting Report

**Source IP** : When LAN users use Bandwidth Management to connect to WAN 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 results in one page.

Pull-down menu selection

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

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

**Upstream** : The percentage of upstream and the value of each LAN user who uses Bandwidth Management 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.

**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.

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

**Total Traffic** : The Bandwidth Management 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.

Bandwidth Management		Outbound					
System	Top: 1-1						
Interface	Reset Time : Wed May 1 00:44:49 2002						
Address							
Service							
Schedule							
QoS							
Policy							
Content Filtering							
Virtual Server							
Log							
Alarm							
Accounting Report							
Outbound							
Inbound							
Statistics							
Status							
Reporting time: Wed May 1 02:29:11 2002							
<a href="#">Reset Counter</a>							

No.	Source IP	Downstream	Upstream	First Packet	Last Packet	Duration
1	192.168.1.3	2.4 MB 100.0%	432.9 KB 100.0%	05/01 00:51:30	05/01 02:28:02	01:36:32
<b>Total Traffic</b>		<b>2.4 MBytes</b>	<b>432.9 KBytes</b>			

## **Outbound Destination IP Accounting Report**

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

### **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.

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

**Upstream** : The percentage of upstream and the value of each LAN user who uses Bandwidth Management 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.

**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.

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

**Total Traffic** : The Bandwidth management 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.

# Bandwidth Management

## Outbound

- System
- Interface
- Address
- Service
- Schedule
- QoS
- Policy
- Content Filtering
- Virtual Server
- Log
- Alarm
- Accounting Report
- Outbound
- Inbound
- Statistics
- Status

Top: 1-10

Reset Time : Wed May 1 00:44:49 2002

No.	Destination IP	Downstream	Upstream	First Packet	Last Packet	Duration
1	202.1.237.22	421.4 KB 17.5%	71.8 KB 16.6%	05/01 00:51:48	05/01 02:21:43	01:29:56
2	66.160.0.176	346.9 KB 14.4%	88.5 KB 20.4%	05/01 00:56:56	05/01 00:58:01	00:02:05
3	210.189.92.161	277.5 KB 11.5%	26.7 KB 6.2%	05/01 01:25:13	05/01 01:26:59	00:01:46
4	61.219.199.158	239.0 KB 9.9%	33.6 KB 7.8%	05/01 02:21:46	05/01 02:22:26	00:00:40
5	202.43.85.160	214.1 KB 8.9%	41.8 KB 9.6%	05/01 01:23:45	05/01 01:27:03	00:03:18
6	203.86.87.18	199.3 KB 8.3%	7.7 KB 1.8%	05/01 00:57:25	05/01 00:57:47	00:00:22
7	202.43.85.161	192.6 KB 8.0%	100.4 KB 23.2%	05/01 01:23:40	05/01 01:27:21	00:03:41
8	143.166.83.83	75.8 KB 3.1%	5.7 KB 1.3%	05/01 01:25:15	05/01 01:26:59	00:01:44
9	61.64.127.25	57.2 KB 2.4%	2.8 KB 0.7%	05/01 01:24:30	05/01 01:24:50	00:00:20
10	204.176.88.4	50.6 KB 2.1%	1.9 KB 0.4%	05/01 01:24:30	05/01 01:24:50	00:00:20
<b>Total Traffic</b>		<b>2.4 MBytes</b>	<b>432.9 KBytes</b>	Reporting Time Wed May 1 02:30:25 2002		

Reset Counter

## Outbound Service Accounting Report

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

### 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.

### Pull-down menu selection

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

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

**Upstream** : The percentage of upstream and the value of each LAN user who uses Bandwidth Management 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.

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

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

**Total Traffic** : The Bandwidth Management 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.

## Bandwidth Management Outbound

- System
- Interface
- Address
- Service
- Schedule
- QoS
- Policy
- Content Filtering
- Virtual Server
- Log
- Alarm
- Accounting Report
- Outbound
- Inbound
- Statistics
- Status

Top: 1-3  
 Reset Time : Wed May 1 00:44:49 2002

No.	Service	Downstream	Upstream	First Packet	Last Packet	Duration
1	HTTP [80]	2.3 MB 98.9%	428.5 KB 99.0%	05/01 00:51:30	05/01 02:22:26	01:30:56
2	POP3 [110]	18.1 KB 0.8%	1.9 KB 0.4%	05/01 01:22:35	05/01 02:28:02	01:05:27
3	DNS [53]	8.0 KB 0.3%	2.4 KB 0.6%	05/01 00:51:30	05/01 02:21:46	01:30:16
<b>Total Traffic</b>		<b>2.4 MBytes</b>	<b>432.9 KBytes</b>	Reporting Time: Wed May 1 02:30:53 2002		

## Bandwidth Management Outbound

### Protocol Distribution

- System
- Interface
- Address
- Service
- Schedule
- QoS
- Policy
- Content Filtering
- Virtual Server
- Log
- Alarm
- Accounting Report
- Outbound
- Inbound
- Statistics
- Status

Downstream	
No.	Service
1	HTTP [80]
2	POP3 [110]
3	DNS [53]
4	OTHER

Upstream	
No.	Service
1	HTTP [80]
2	DNS [53]
3	POP3 [110]
4	OTHER

Press to return to **Accounting Report** window.

# Inbound

**Step 1.** Click **Service** in the menu bar on the left hand side of the window. Click **Group** under it.

**Bandwidth Management** **Inbound**

System  
Interface  
Address  
Service  
Schedule  
QoS  
Policy  
Content Filtering  
Virtual Server  
Log  
Alarm  
Accounting Report  
Outbound  
**Inbound** ←←  
Statistics  
Status

Top: 1-2  
Reset Time : Wed May 1 00:44:49 2002

No.	Source IP	Downstream	Upstream	First Packet	Last Packet	Duration
1	211.20.188.142	40.0 B 50.0%	48.0 B 50.0%	05/01 02:35:16	05/01 02:35:16	00:00:00
2	211.20.188.140	40.0 B 50.0%	48.0 B 50.0%	05/01 02:33:48	05/01 02:33:48	00:00:00
<b>Total Traffic</b>		<b>80.0 Bytes</b>	<b>96.0 Bytes</b>	Reporting Time: Wed May 1 02:35:24 2002		

Reset Counter

## Inbound Source IP Accounting Report

**Source IP** : When WAN users use Bandwidth Management 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.

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

**Upstream** : The percentage of Upstream and the value of each LAN service server who uses Bandwidth Management 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.

**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..

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

**Total Traffic** : The Bandwidth Management 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.

Bandwidth Management		Inbound						
System		Top: 1-2						
Interface		Reset Time : Wed May 1 00:44:49 2002						
Address		No.	Source IP	Downstream	Upstream	First Packet	Last Packet	Duration
Service		1	211.20.188.142	40.0 B 50.0%	48.0 B 50.0%	05/01 02:35:16	05/01 02:35:16	00:00:00
Schedule		2	211.20.188.140	40.0 B 50.0%	48.0 B 50.0%	05/01 02:33:48	05/01 02:33:48	00:00:00
QoS		<b>Total Traffic</b>		<b>80.0 Bytes</b>	<b>96.0 Bytes</b>	Reporting Time: Wed May 1 02:35:24 2002		
Policy		Reset Counter						
Content Filtering								
Virtual Server								
Log								
Alarm								
Accounting Report								
Outbound								
Inbound								
Statistics								
Status								

## Inbound Destination IP Accounting Report

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

### 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.

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

**Upstream** : The percentage of Upstream and the value of each LAN service server who uses Bandwidth Management 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.

**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..

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

**Total Traffic** : The Bandwidth management 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.

# Bandwidth Management

## Inbound

- System
- Interface
- Address
- Service
- Schedule
- QoS
- Policy
- Content Filtering
- Virtual Server
- Log
- Alarm
- Accounting Report
- Outbound
- Inbound**
- Statistics
- Status

Top:

Reset Time : Wed May 1 00:44:49 2002

No.	Destination IP	Downstream	Upstream	First Packet	Last Packet	Duration
1	192.168.1.3	469.0 B 100.0%	478.0 B 100.0%	05/01 02:33:48	05/01 02:42:37	00:08:49
<b>Total Traffic</b>		<b>469.0 Bytes</b>	<b>478.0 Bytes</b>	Reporting Time: Wed May 1 02:46:29 2002		

## Inbound Service Accounting Report

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

### 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.

Pull-down menu selection

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

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

**Upstream** : The percentage of upstream and the value of each LAN service server who uses Bandwidth Management 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.

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

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

**Total Traffic** : The Bandwidth Management 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.

# Bandwidth Management

## Inbound

- System
- Interface
- Address
- Service
- Schedule
- QoS
- Policy
- Content Filtering
- Virtual Server
- Log
- Alarm
- Accounting Report
- Outbound
- Inbound**
- Statistics
- Status

Top: 1-3

Reset Time : Wed May 1 00:44:49 2002



No.	Service	Downstream	Upstream	First Packet	Last Packet	Duration
1	NETBIOS-SSN [139]	132.0 B 28.1%	304.0 B 63.6%	05/01 02:42:37	05/01 02:42:37	00:00:00
2	AUTH [113]	80.0 B 17.1%	96.0 B 20.1%	05/01 02:33:48	05/01 02:36:16	00:01:28
3	NETBIOS-NS [137]	257.0 B 54.8%	78.0 B 16.3%	05/01 02:42:37	05/01 02:42:37	00:00:00
<b>Total Traffic</b>		<b>469.0 Bytes</b>	<b>478.0 Bytes</b>	Reporting Time Wed May 1 02:47:49 2002		

Reset Counter

# Bandwidth Management

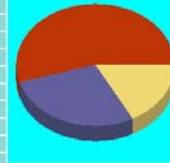
## Inbound

- System
- Interface
- Address
- Service
- Schedule
- QoS
- Policy
- Content Filtering
- Virtual Server
- Log
- Alarm
- Accounting Report
- Outbound
- Inbound**
- Statistics
- Status

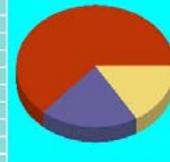
### Protocol Distribution



No.	Service	Downstream
1	NETBIOS-NS [137]	257.0 Bytes (54.8%)
2	NETBIOS-SSN [139]	132.0 Bytes (28.1%)
3	AUTH [113]	80.0 Bytes (17.1%)
	OTHER	0.0 Bytes (0.0%)



No.	Service	Upstream
1	NETBIOS-SSN [139]	304.0 Bytes (63.6%)
2	AUTH [113]	96.0 Bytes (20.1%)
3	NETBIOS-NS [137]	78.0 Bytes (16.3%)
	OTHER	0.0 Bytes (0.0%)



Press



and return to **Accounting Report** window.

# Statistics

In this chapter, the Administrator queries the Bandwidth Management for statistics of packets and data which passes across the Bandwidth Management. 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 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 manage 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.**

# 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.

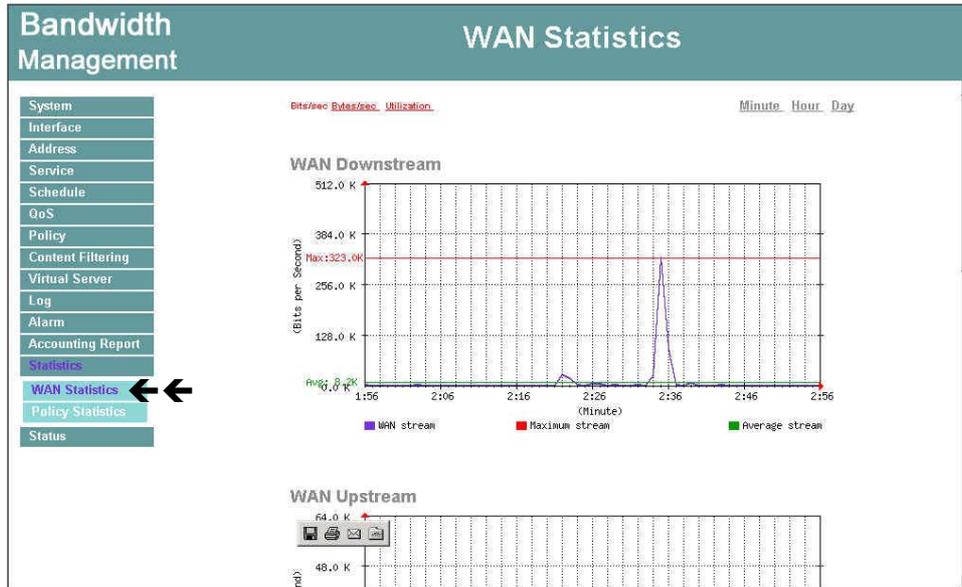


Figure13-1 WAN Statistics

**Time :** The statistics based on the units of minute, hour and day.

WAN Downstream Figure

WAN Upstream Figure

WAN Downstream Packet Figure

WAN upstream Packet Figure

## 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 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 ) .

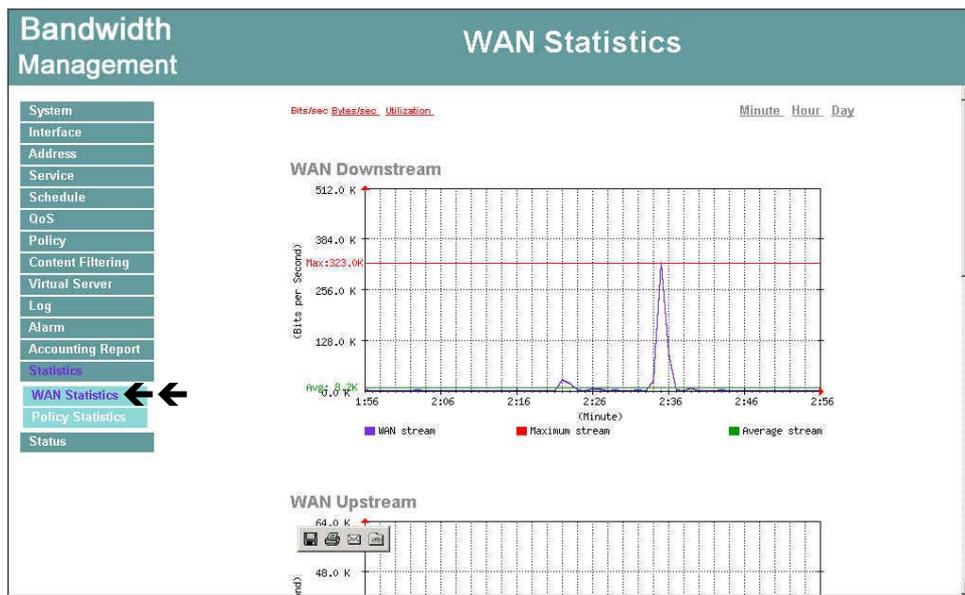


Figure13-2 WAN Statistics

# Policy Statistics

## Entering the Statistics window

**Step 1.** The Statistics window displays the statistics of current network connections.

- **Source:** the name of source address.
- **Destination:** the name of destination address.
- **Service:** the service requested.
- **Action:** permit or deny
- **Time:** viewable by minutes, hours, or days

The screenshot shows a web-based interface for network management. On the left is a vertical navigation menu with the following items: System, Interface, Address, Service, Schedule, QoS, Policy, Content Filtering, Virtual Server, Log, Alarm, Accounting Report, Statistics, WAN Statistics, Policy Status, and Status. The 'Policy Status' item is highlighted in blue and has two black arrows pointing to it from the right. The main content area is titled 'Policy Statistics' and contains a table with the following structure:

Source	Destination	Service	Action	Time		
Inside_Any	Outside_Any	ANY	PERMIT	Minute	Hour	Day

Figure13-3 Policy Statistics



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 ) ◦



Figure13-4 Checking Policy Statistics

# Status

In this section, the device displays the status information about the Bandwidth Management. 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.

# Interface Status

## Entering the Interface Status window

**Bandwidth Management** **Interface Status**

System Uptime  
0 Day 3 Hour 2 Min 46 Sec

	LAN Interface	WAN Interface
Forwarding Mode	NAT	PPPoE
Connection Status	---	Connected
PPPoE Connection Time	---	3:02:29
MAC Address	44:44:44:44:44:47	44:44:44:44:44:40
IP Address	192.168.1.1	61.59.234.97
Netmask	255.255.255.0	255.255.255.255
Default Gateway	---	61.59.234.1
DNS Server1	---	139.175.55.244
DNS Server2	---	139.175.252.16
Rx Pkts, Error Pkts	272712, 0	7473, 0
Tx Pkts, Error Pkts	273709, 0	6299, 0
Ping	Enable	Enable
WebUI	Enable	Enable

System  
Interface  
Address  
Service  
Schedule  
QoS  
Policy  
Content Filtering  
Virtual Server  
Log  
Alarm  
Accounting Report  
Statistics  
Status  
**Interface Status** ←←  
ARP Table  
DHCP Clients

Figure14-1 Interface Status

## Internal Interface

**In Internet Interface window:** The interface IP will be displayed.

**System Uptime :** The time of booting the Bandwidth Management.

**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.

## 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.

System	IP Address	MAC Address	Interface
Interface	192.168.1.3	00:48:54:4A:FB:66	LAN

Figure14-3 ARP Table

**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)

## 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's DHCP server function.

System Interface Address Service Schedule QoS Policy Content Filtering Virtual Server Log Alarm Accounting Report Statistics Status Interface Status ARP Table DHCP Clients	IP Address	MAC Address	Leased Time	
	Start	End		
	192.168.1.2	00:50:BF:16:EA:CE	---	---

Figure14-4 DHCP Clients

**IP Address:** the IP address of the LAN host computer

**MAC Address:** MAC address of the LAN host computer

**Leased Time:** The Start and End time of the DHCP lease for the LAN host computer.

# Setup Examples

**Example 1:** Allow the LAN network to be able to access the Internet

**Example 2:** The LAN network can only access Yahoo.com website

**Example 3:** Outside users can access the LAN FTP server through Virtual Servers

**Example 4:** I Install a server inside the LAN network and have the Internet (WAN) users access the server through IP Mapping

**Example 5:** Use QoS to setup LAN to WAN network to attain the maximum downstream/upstream bandwidth. The setup orders should be QoS and then Policy

## Example 1: Allow the LAN network to be able to access the Internet

Step 1. Enter the Outgoing window under the Policy menu.

Step 2. Click the **New Entry** button on the bottom of the screen.

Step 3. In the Add New Policy window, enter each parameter, then click OK.

The screenshot displays the 'Bandwidth Management' interface. On the left is a navigation menu with the following items: System, Interface, Address, Service, Schedule, QoS, Policy, Outgoing (highlighted), Incoming, Content Filtering, Virtual Server, Log, Alarm, Accounting Report, Statistics, and Status. The main area is titled 'Outgoing' and contains an 'Add New Policy' window. The configuration fields in this window are: Source Address (Inside\_Any), Destination Address (Outside\_Any), Service (ANY), Action (PERMIT), Logging (unchecked Enable), Statistics (unchecked Enable), Schedule (None), Alarm Threshold (0.0 KBytes/Sec), and QoS (None). 'Ok' and 'Cancel' buttons are located at the bottom right of the 'Add New Policy' window.

Step 4. When the following screen appears, the setup is completed.

Bandwidth Management		Outgoing							
System	No.	Source	Destination	Service	Action	Option	Configure	Move	
Interface	1	Inside_Any	Outside_Any	ANY	✓		Modify	Remove	Go
Address									1
Service									
Schedule									

New Entry

**Example 2:** The LAN network can only access Yahoo.com website.

- Step 1. Enter the WAN window under the Address menu.
- Step 2. Click the **New Entry** button.
- Step 3. In the Add New Address window, enter relating parameters.

Bandwidth Management		WAN	
System		Add New Address	
Interface		Name	yahoo
Address		IP Address	62.111.11.11
LAN		Netmask	255.255.255.255
LAN Group			
WAN			

Ok Cancel

- Step 4. Click **OK** to end the address table setup.
- Step 5. Go to the **Outgoing** window under the Policy menu.
- Step 6. Click the **New Entry** button.
- Step 7. In the **Add New Policy** window, enter corresponding parameters. Click **OK**.

Add New Policy	
Source Address	Inside_Any
Destination Address	yahoo
Service	ANY
Action	PERMIT
Logging	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
Schedule	None
Alarm Threshold	0.0 KBytes/Sec
QoS	None

Ok Cancel

Step 8. When the following screen appears, the setup is completed.

No.	Source	Destination	Service	Action	Option	Configure	Move
1	Inside_Any	Outside_Any	ANY			Modify Remove To	1 ▼
2	Inside_Any	yahoo	ANY			Modify Remove To	2 ▼

New Entry

### Example 3: Outside users can access the LAN FTP server through Virtual Servers

Step 1. Enter Virtual Server under the Virtual Server menu.

Step 2. Click the 'click here to configure' button.

Step 3. Select an WANIP address, then click OK.

Step 4. Click the New Service button on the bottom of the screen.

Step 5. Add the FTP service pointing to the LAN server IP address.

Step 6. Click OK.

The screenshot shows the 'Virtual Server 1' configuration window. On the left is a navigation menu with 'Virtual Server' selected. The main area is titled 'Virtual Server Configuration' and contains the following fields and table:

Virtual Server Real IP	61.59.234.97
Service Name (Port)	FTP (21)
External Service Port	21
<b>Load Balance Server</b>	
1	192.168.1.2
2	192.168.1.3
3	192.168.1.4
4	192.168.1.5
<input type="button" value="Ok"/> <input type="button" value="Cancel"/>	

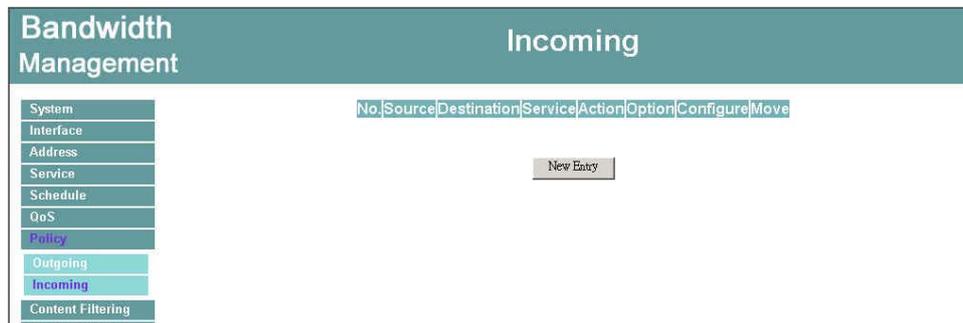
Step 7. A new Virtual Service should appear.

The screenshot shows the 'Virtual Server 1' configuration window after the service has been added. The 'Virtual Server Real IP' is 61.59.234.97. The 'Service Name (Port)' is FTP (21) and the 'External Port' is 21. Below this is a table of load balance servers:

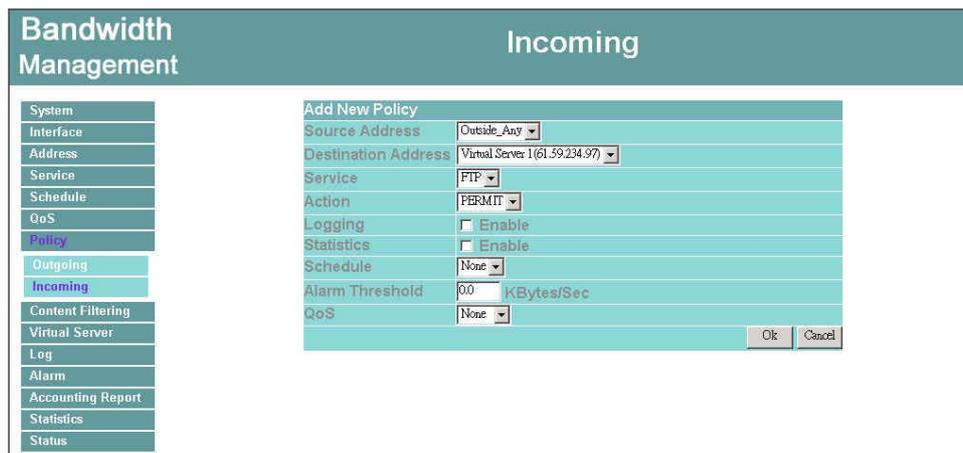
Service Name (Port)	External Port	Server Virtual IP	Configure
FTP (21)	21	192.168.1.2	Modify Remove
		192.168.1.3	
		192.168.1.4	
		192.168.1.5	

At the bottom of the window, there is a 'New Service' button.

Step 8. Go to the Incoming window under the Policy menu, then click on the **New Entry** button.



Step 9. In the **Add New Policy** window, set each parameter, then click OK.



Step 10. An Incoming FTP policy should now be created.

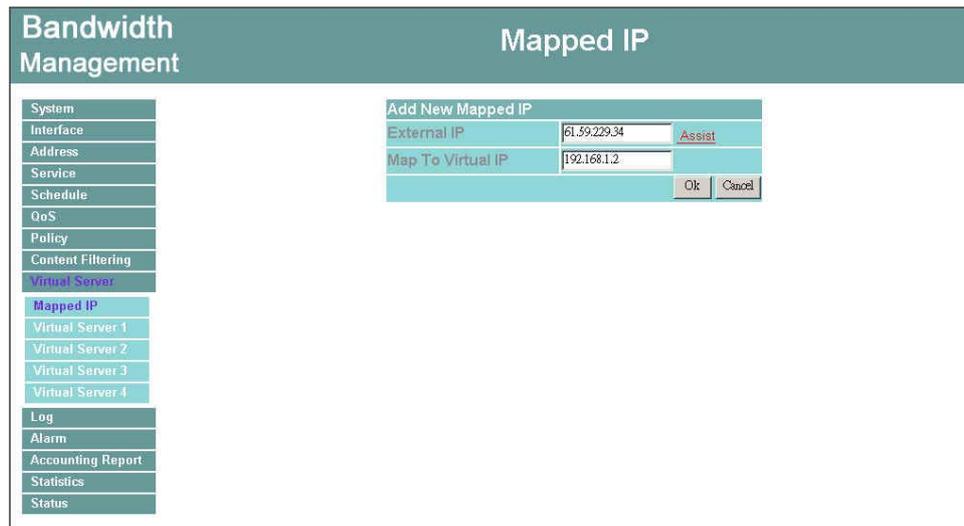
**Example 4: Install a server inside the LAN network and have the Internet (WAN) users access the server through IP Mapping**

**Step 1.** Enter the Mapped IP window under the Virtual Server menu.

**Step 2.** Click the **New Entry** button.

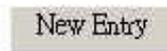
**Step 3.** In the Add New IP Mapping window, enter each parameter.

**Step 4.** Click **OK**.



**Step 3.** When the following screen appears, the IP Mapping setup is completed.

External IP	Map To Virtual IP	Configure
61.59.229.34	192.168.1.2	<a href="#">Modify</a> <a href="#">Remove</a>



**Step 4.** Go to the Incoming window under the Policy menu.

**Step 5.** Click the **New Entry** button.

Add New Policy	
Source Address	Outside_Any ▾
Destination Address	Mapped IP(61.59.229.34) ▾
Service	ANY ▾
Action	PERMIT ▾
Logging	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
Schedule	None ▾
Alarm Threshold	0.0 KBytes/Sec
QoS	None ▾
<input type="button" value="Ok"/> <input type="button" value="Cancel"/>	

**Step 6.** In the **Add New Policy** window, set each parameter, then click **OK**.

**Step 7.** Open all the services. (ANY)

**Step 8.** The setup is completed.

**Example 5:** Use QoS to setup LAN to WAN network to attain the maximum downstream/upstream bandwidth. The setup orders should be QoS and then Policy

**Step 1.** Enter the **QoS** window in the menu bar on the left hand side of the window.

**Step 2.** Click the **New Entry** button.

**Step 3.** In the **Add New QoS** window, enter each parameter.

**Step 4.** Click **OK**.

The screenshot shows the 'QoS' management interface. On the left is a menu bar with 'QoS' selected. The main area displays the 'Add New QoS' dialog box with the following fields:

Name		Qos_1	
Downstream	Guaranteed Bandwidth	300	kbps
	Maximum Bandwidth	350	kbps
Upstream	Guaranteed Bandwidth	60	kbps
	Maximum Bandwidth	64	kbps
QoS Priority		Middle	

Buttons for 'OK' and 'Cancel' are visible at the bottom right of the dialog box.

**Step 5.** When the following screen appears, the **QoS** setup is completed.

The screenshot shows the 'Bandwidth Management' interface with the 'QoS' configuration table. The table lists the configured QoS entry 'Qos\_1' with its bandwidth and priority settings.

Name	Downstream Bandwidth	Upstream Bandwidth	Priority	Configure
Qos_1	G Bandwidth = 200 Kbps M Bandwidth = 300 Kbps	G Bandwidth = 60 Kbps M Bandwidth = 64 Kbps	Middle	Modify Remove

A 'New Entry' button is located below the table.

**Step 6.** Go to the **Outgoing** window under the **Policy** menu.

**Step 7.** Click the **New Entry** button.

**Bandwidth Management** **Outgoing**

No.	Source	Destination	Service	Action	Option	Configure	Move
-----	--------	-------------	---------	--------	--------	-----------	------

- System
- Interface
- Address
- Service
- Schedule
- QoS
- Policy
- Outgoing**
- Incoming
- Content Filtering
- Virtual Server
- Log
- Alarm
- Accounting Report
- Statistics
- Status

**Step 8.** In **Add New Policy** window, set each parameter, then click **OK**.

**Bandwidth Management** **Outgoing**

**Add New Policy**

Source Address:

Destination Address:

Service:

Action:

Logging:  Enable

Statistics:  Enable

Schedule:

Alarm Threshold:  KBytes/Sec

QoS:

- System
- Interface
- Address
- Service
- Schedule
- QoS
- Policy
- Outgoing**
- Incoming
- Content Filtering
- Virtual Server
- Log
- Alarm
- Accounting Report
- Statistics

**Step 9.** Open all the services (ANY). The setup is completed.

## Bandwidth Management

### Outgoing

No.	Source	Destination	Service	Action	Option	Configure	Move
1	Inside Any	Outside Any	ANY			<a href="#">Modify</a> <a href="#">Remove</a>	1

Install a server inside the LAN network, open to all the IP addresses including LAN and WAN IPs to use QoS to attain the maximum downstream and upstream bandwidth. The setup orders should be QoS, Virtual Server and then Policy.

**Step 1.** Enter the **QoS** window in the menu bar on the left hand side of the window.

**Step 2.** Click the **New Entry** button.

**Step 3.** In the **Add New QoS** window, enter each parameter.

**Step 4.** Click **OK**.

**Step 5.** When the following screen appears, the **QoS** setup is completed.

Name	Downstream Bandwidth	Upstream Bandwidth	Priority	Configure
Qos_1	G.Bandwidth = 200 Kbps M.Bandwidth = 300 Kbps	G.Bandwidth = 60 Kbps M.Bandwidth = 64 Kbps	Middle	Modify Remove

**Step 6.** Go to the **Virtual server 1** window under the **Virtual server** menu.

**Step 7.** Click the **Click here to configure** button.

**Bandwidth Management** **Virtual Server 1**

System  
Interface  
Address  
Service  
Schedule  
QoS  
Policy  
Content Filtering  
Virtual Server  
Mapped IP  
Virtual Server 1  
Virtual Server 2  
Virtual Server 3  
Virtual Server 4  
Log  
Alarm  
Accounting Report  
Statistics  
Status

Virtual Server Real IP [click here to configure](#)

Service Name (Port)	External Port	Server Virtual IP	Configure
---------------------	---------------	-------------------	-----------

**Step 8.** In Virtual Server 1 window, enter the Virtual Server Real IP, and then click OK.

**Bandwidth Management** **Virtual Server 1**

System  
Interface  
Address  
Service  
Schedule  
QoS  
Policy  
Content Filtering  
Virtual Server  
Mapped IP  
Virtual Server 1  
Virtual Server 2  
Virtual Server 3  
Virtual Server 4  
Log  
Alarm  
Accounting Report  
Statistics  
Status

Add New Virtual Server IP

Virtual Server Real IP  [Assist](#)

**Step 9.** After adding new server IP, click the **New Service** button.

**Bandwidth Management** **Virtual Server 1**

Virtual Server Real IP

Service Name (Port)	External Port	Server Virtual IP	Configure
---------------------	---------------	-------------------	-----------

**Step 10.** In the **Virtual Server Configuration** window, set each parameter, then click **OK**.

**Bandwidth Management** **Virtual Server 1**

**Virtual Server Configuration**

Virtual Server Real IP

Service Name (Port)

External Service Port

Load Balance Server	Server Virtual IP
1	<input type="text" value="192.168.1.2"/>
2	<input type="text" value="192.168.1.3"/>
3	<input type="text" value="192.168.1.4"/>
4	<input type="text" value="192.168.1.5"/>

**Step 11.** When the following screen appears, the virtual server setup is complete.

**Bandwidth Management Virtual Server 1**

Virtual Server Real IP

Service Name (Port)	External Port	Server Virtual IP	Configure
FTP (21)	21	192.168.1.2	<a href="#">Modify</a> <a href="#">Remove</a>
		192.168.1.3	
		192.168.1.4	
		192.168.1.5	

**Step 12.** Enter the Incoming window under the Policy menu.

**Step 13.** Click the New Entry button.

**Bandwidth Management Incoming**

No.	Source	Destination	Service	Action	Option	Configure	Move
-----	--------	-------------	---------	--------	--------	-----------	------

**Step 14.** In the **Add New Policy** window, set each parameter, then click **OK**.

The screenshot shows the 'Bandwidth Management Incoming' configuration window. On the left is a navigation menu with the following items: System, Interface, Address, Service, Schedule, QoS, Policy, Outgoing, Incoming, Content Filtering, Virtual Server, Log, Alarm, Accounting Report, Statistics, and Status. The 'Incoming' item is selected. The main area is titled 'Add New Policy' and contains the following fields:

Source Address	Outside_Any
Destination Address	Virtual Server: 1 (61.59.234.97)
Service	FTP
Action	PERMIT
Logging	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
Schedule	None
Alarm Threshold	0.0 KBytes/Sec
QoS	None

At the bottom right of the 'Add New Policy' window are 'Ok' and 'Cancel' buttons.