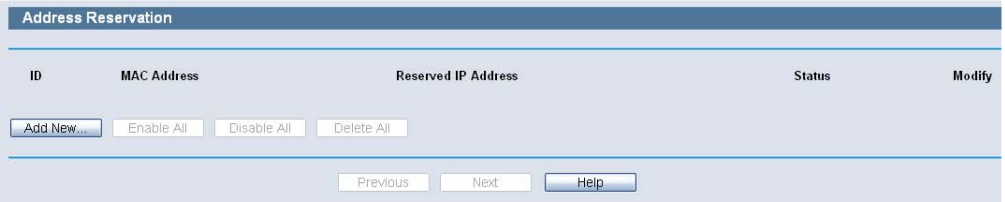
- **Lease Time** - The time of the DHCP client leased. After the dynamic IP address has expired, a new dynamic IP address will be automatically assigned to the user.

You cannot change any of the values on this page. To update this page and to show the current attached devices, click the Refresh button.

ADDRESS RESERVATION

Choose menu "DHCP->Address Reservation", you can view and add a reserved addresses for clients via the following figure.When you specify a reserved IP address for a PC on the LAN, that PC will always receive the same IP address each time when it accesses the DHCP server. Reserved IP addresses should be assigned to the servers that require permanent IP settings.

Figure 58: Address Reservation



Address Reservation

ID	MAC Address	Reserved IP Address	Status	Modify

- **MAC Address** - The MAC address of the PC for which you want to reserve IP address.

- **Assigned IP Address** - The IP address of the Router reserved.

- **Status** - The status of this entry either Enabled or Disabled.

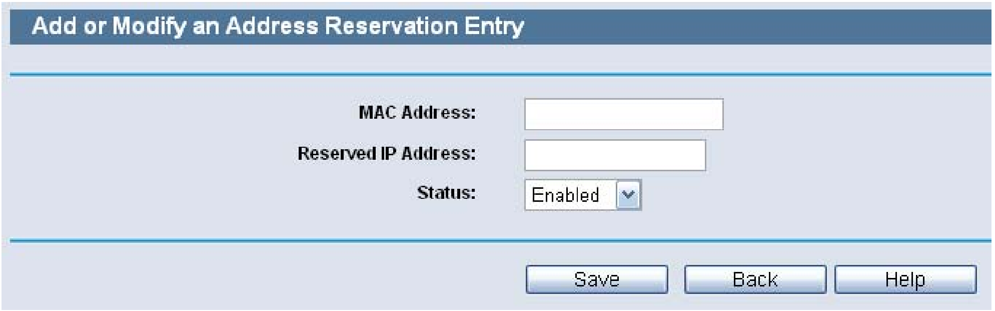
To Reserve IP addresses:

1. Click the Add New button.

2. Enter the MAC address (in XX-XX-XX-XX-XX-XX format.) and IP address in dotted-decimal notation of the computer you wish to add.

3. Click the Save button when finished.

Figure 59: Add or Modify an Address Reservation Entry



Add or Modify an Address Reservation Entry

MAC Address:

Reserved IP Address:

Status: Enabled

To modify or delete an existing entry:

1. Click the Modify in the entry you want to modify. If you want to delete the entry, click the Delete.
2. Modify the information.
3. Click the Save button.

Click the Enable/ Disabled All button to make all entries enabled/disabled

Click the Delete All button to delete all entries

Click the Next button to go to the next page and Click the Previous button to return the previous page.

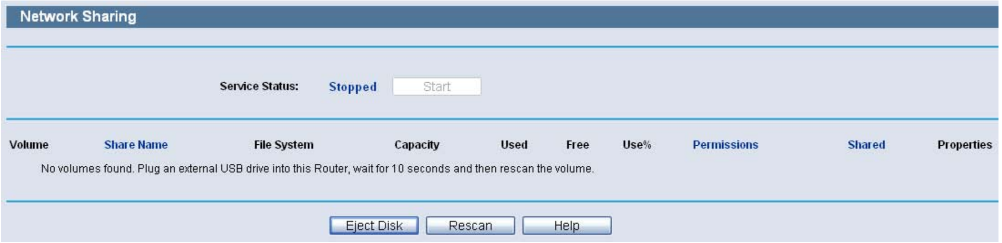
8 USB Storage Settings

There are two submenus under the Network Sharing menu: Sharing Service and User Accounts. Click any of them, and you will be able to configure the corresponding function.

Sharing Service

Choose menu "Network Sharing->Sharing Service", you can configure a USB disk drive attached to the Router on this page.

Figure 60: Network Sharing



Network Sharing

Service Status: Stopped

Volume	Share Name	File System	Capacity	Used	Free	Use%	Permissions	Shared	Properties

No volumes found. Plug an external USB drive into this Router, wait for 10 seconds and then rescan the volume.

- **Service Status** - Indicates the Network Sharing service's current status.
- **Volume** - The volume name of the USB drive the users have access to.
- **Share Name** - The specified share name of the volume.
- **File System** - The file system on the partition can be FAT32 or NTFS.
- **Capacity** - The storage capacity of the USB driver.
- **Used** - The used space of the USB driver.
- **Free** - The available space of the USB driver.
- **Use%** - The percentage of the used space.
- **Permissions** - Read-Only or Read/Write access to the volume designated as the share.
- **Shared** - Indicates the shared or non-shared status of the volume.

- **Properties** - Displays the Edit link to specify a volume that the Network Sharing users can access.

Click the Start button to start the Network Sharing service.

Click the Stop button to stop the Network Sharing service.

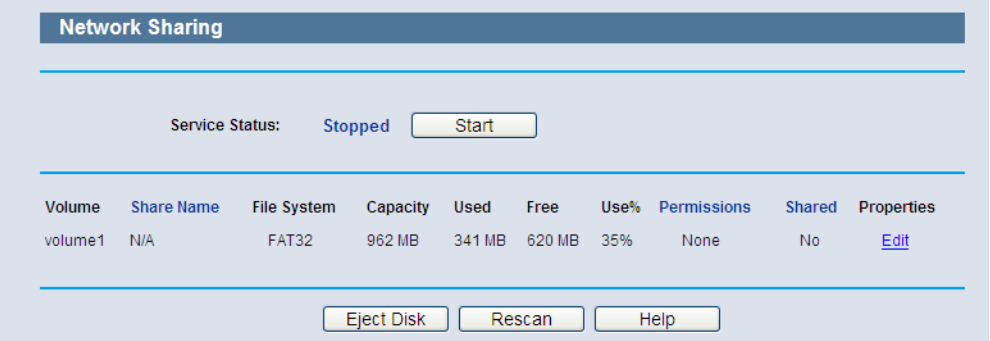
Click the Eject Disk button to safely remove the USB storage device that is connected to USB port. This takes the drive offline. A message will appear on your web browser when it is safe to detach the USB disk.

Click the Rescan button to start a new scan.

Follow the instructions below to set up your Router as a file server:

1. Plug an external USB hard disk drive or USB flash drive into this Router.
2. Click the Rescan button to find the USB drive that has been attached to the Router, and then the screen will appear as the following figure shown.

Figure 61: Sharing Settings - Rescan



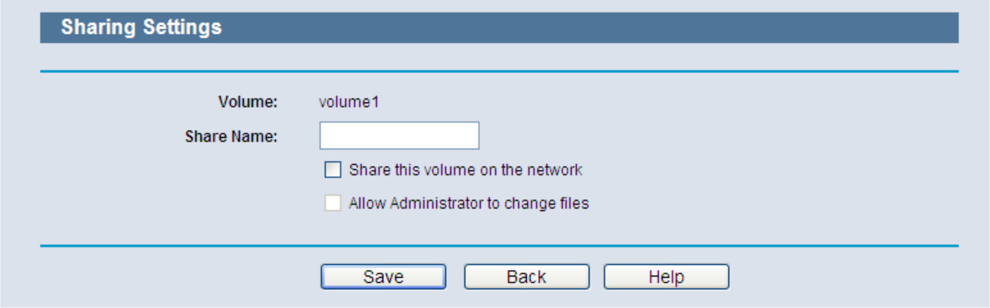
Network Sharing

Service Status: Stopped

Volume	Share Name	File System	Capacity	Used	Free	Use%	Permissions	Shared	Properties
volume1	N/A	FAT32	962 MB	341 MB	620 MB	35%	None	No	Edit

3. To specify a volume that the Network Sharing users can access, click the Edit link in the Properties column and configure the share settings.
4. Set the Network Sharing user's username and password on User Accounts page.
5. Click the Start button to start the Network Sharing service.
6. Now the Network Sharing users inside your local network can access files on the USB drive from Internet Explorer at its Share Name followed by the Router's LAN IP address, for example: \\192.168.2.1\MyShare.

Figure 62: Sharing Settings - Edit



Sharing Settings

Volume: volume1

Share Name:

□ Share this volume on the network

□ Allow Administrator to change files

NOTE: The Router cannot automatically locate new USB drive. You have to click the Rescan button manually to display a list of volumes and information about them.

NOTE: The new settings will not take effect until you restart the service.

NOTE: To unplug the USB drive, click Eject Disk button first. Simply pulling USB drive out of the USB port can cause damage to the device and loss of data.

NOTE: Mounted volumes are subject to the 8-volume limit. So you cannot access more than 8 volumes on the USB storage device.

NOTE: NTFS is the recommended file system for Network Sharing because it supports several features that the other file systems do not, such as large files and large volume support.

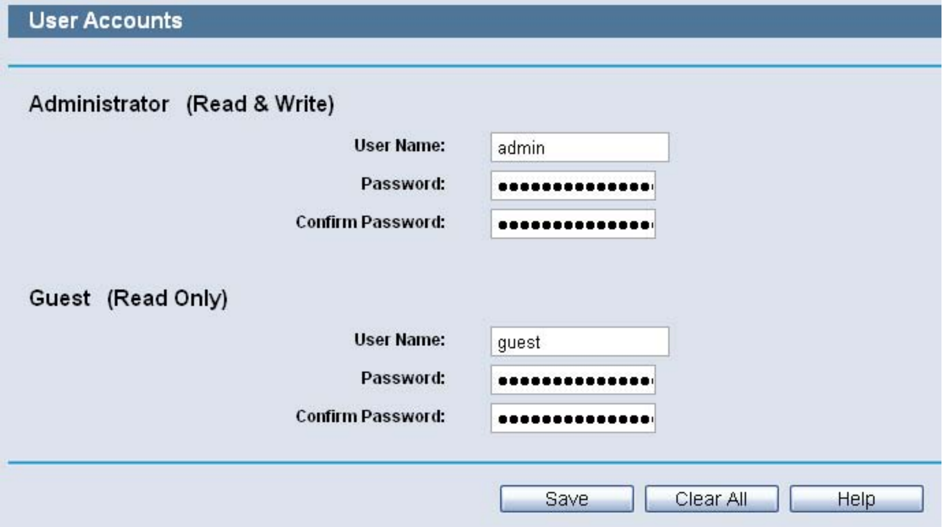
USER ACCOUNTS

You can specify the user name and password for Network Sharing users on the following User Accounts page. Network Sharing users can use Internet Explorer to access files on the USB drive.

There are two Network Sharing users that can access the shares. They are Administrator and Guest. Administrator has read/write access while Guest has read-only access.

Only Administrator can use a Web browser to transfer the files from a PC to the Writable shared volume on the USB drive.

Figure 63: User Accounts



User Accounts

Administrator (Read & Write)

User Name: admin
Password: ●●●●●●●●●●●●●●●
Confirm Password: ●●●●●●●●●●●●●●●

Guest (Read Only)

User Name: guest
Password: ●●●●●●●●●●●●●●●
Confirm Password: ●●●●●●●●●●●●●●●

- **User Name** - Type the user name that you want to give access to the USB drive. The user name must be composed of alphanumeric symbols not exceeding 15 characters in length.

- **Password** - Enter the password in the Password field. The password must be composed of alphanumeric symbols not exceeding 15 characters in length. For security purposes, the password for each user account is not displayed.

- **Confirm Password** - Re-enter the password here.

Click the Save button to save your settings.

Click the Clear All button to clear all the fields.

NOTE: 1. Please restart the service for the new settings to take effect.

2. If you cannot use the new user name and password to access the shares, press Windows logo + R to open the Run dialog box and type net use \\192.168.2.1 /delete /yes and press Enter. (192.168.2.1 is your Router's LAN IP address.)

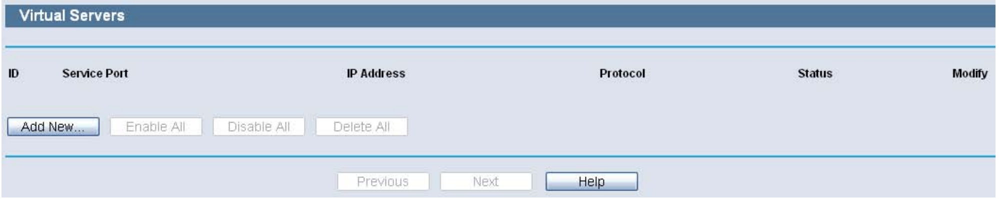
9 Special Application Settings

There are four submenus under the Special Application menu: Virtual Servers, Port Triggering, DMZ and UPnP. Click any of them, and you will be able to configure the corresponding function.

Virtual Servers

Choose menu “Special Application->Virtual Servers”, you can view and add virtual servers in the following screen. Virtual servers can be used for setting up public services on your LAN, such as DNS, Email and FTP. A virtual server is defined as a service port, and all requests from the Internet to this service port will be redirected to the computer specified by the server IP. Any PC that was used for a virtual server must have a static or reserved IP Address because its IP Address may be changed when using the DHCP function.

Figure 64: Virtual Servers Settings



Virtual Servers

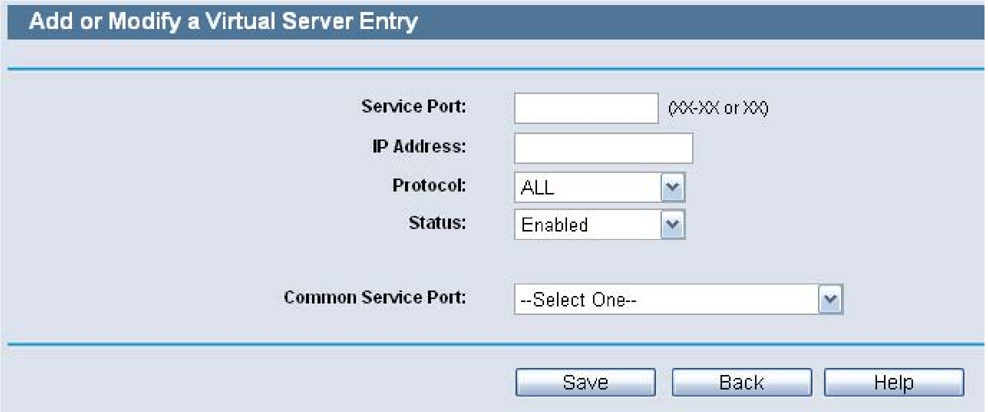
ID	Service Port	IP Address	Protocol	Status	Modify

- **Service Port** - The numbers of External Ports. You can type a service port or a range of service ports (in XXX – YYY format, XXX is the start port number, YYY is the end port number).
- **IP Address** - The IP Address of the PC providing the service application.
- **Protocol** - The protocol used for this application, either TCP, UDP, or All (all protocols supported by the Router).
- **Status** - The status of this entry either Enabled or Disabled.

To setup a virtual server entry:

1. Click the Add New button.
2. Select the service you want to use from the Common Service Port list. If the Common Service Port list does not have the service that you want to use, type the number of the service port or service port range in the Service Port box.
3. Type the IP Address of the computer in the IP Address box.
4. Select the protocol used for this application, either TCP or UDP, or All.
5. Select the Enable check box to enable the virtual server.
6. Click the Save button.

Figure 65: Add or Modify a Virtual Server Entry



Add or Modify a Virtual Server Entry

Service Port:	(XX-XX or XX)
IP Address:	
Protocol:	ALL
Status:	Enabled
Common Service Port:	--Select One--

NOTE: If your computer or server has more than one type of available service, please select another service, and enter the same IP Address for that computer or server.

To modify or delete an existing entry:

1. Click the Modify in the entry you want to modify. If you want to delete the entry, click the Delete.
2. Modify the information.
3. Click the Save button.

Click the Enable/ Disabled All button to make all entries enabled/ disabled.

Click the Delete All button to delete all entries.

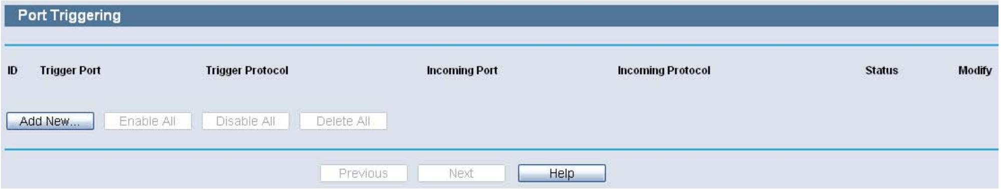
Click the Next button to go to the next page and click the Previous button to return the previous page.

NOTE: If you set the service port of the virtual server as 80, you must set the Web management port on System Tools –> Remote Management page to be any other value except 80 such as 8080. Otherwise there will be a conflict to disable the virtual server.

PORT TRIGGERING

Choose menu "Special Application->Port Triggering", you can view and add port triggering in the following screen. Some applications require multiple connections, like Internet games, video conferencing, Internet calling and so on. These applications cannot work with a pure NAT Router. Port Triggering is used for some of these applications that can work with an NAT Router.

Figure 66: Port Triggering



Port Triggering

ID	Trigger Port	Trigger Protocol	Incoming Port	Incoming Protocol	Status	Modify

Once the Router is configured, the operation is as follows:

1. A local host makes an outgoing connection using a destination port number defined in the Trigger Port field.

2. The Router records this connection, opens the incoming port or ports associated with this entry in the Port Triggering table, and associates them with the local host.

3. When necessary the external host will be able to connect to the local host using one of the ports defined in the Incoming Ports field.

- **Trigger Port** - The port for outgoing traffic. An outgoing connection using this port will "Trigger" this rule.

- **Trigger Protocol** - The protocol used for Trigger Ports, either TCP, UDP, or All (all protocols supported by the Router).

- **Incoming Ports Range** - The port or port range used by the remote system when it responds to the outgoing request. A response using one of these ports will be forwarded to the PC that triggered this rule. You can input at most 5 groups of ports (or port section). Every group of ports must be set apart with ",". For example, 2000-2038, 2050-2051, 2085, 3010-3030.

- **Incoming Protocol** - The protocol used for Incoming Ports Range, either TCP or UDP, or ALL (all protocols supported by the Router).

- **Status** - The status of this entry either Enabled or Disabled.

To add a new rule, follow the steps below.

1. Click the Add New button.

2. Select a common application from the Common Applications drop-down list, then the Trigger Port field and the Incoming Ports field will be automatically filled. If the Common Applications do not have the application you need, enter the Trigger Port and the Incoming Ports manually.

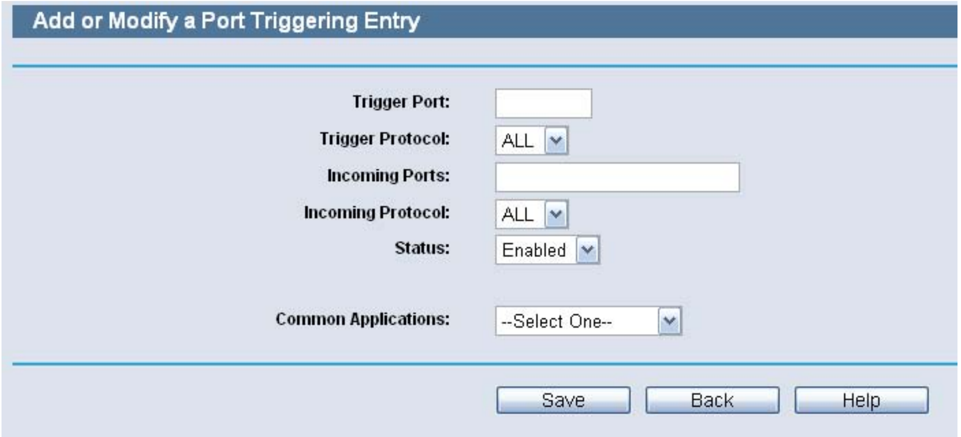
3. Select the protocol used for Trigger Port from the Trigger Protocol drop-down list, either TCP, UDP, or All.

4. Select the protocol used for Incoming Ports from the Incoming Protocol drop-down list, either TCP or UDP, or All.

5. Select Enable in Status field.

6. Click the Save button to save the new rule.

Figure 67: Add or Modify a Triggering Entry



Add or Modify a Port Triggering Entry

Trigger Port:

Trigger Protocol: ALL

Incoming Ports:

Incoming Protocol: ALL

Status: Enabled

Common Applications: --Select One--

To modify or delete an existing entry:

1. Click the Modify in the entry you want to modify. If you want to delete the entry, click the Delete.

2. Modify the information.

3. Click the Save button.

Click the Enable All button to make all entries enabled

Click the Disabled All button to make all entries disabled.

Click the Delete All button to delete all entries

NOTE: 1. When the trigger connection is released, the according opening ports will be closed.

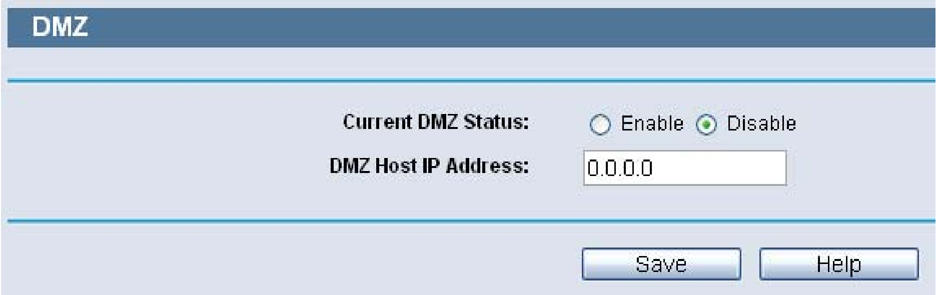
2. Each rule allowed to be used only by one host on LAN synchronously. The trigger connection of other hosts on LAN will be refused.

3. Incoming Port Range cannot overlap each other.

DMZ

Choose menu “Special Application->DMZ”, you can view and configure DMZ host in the screen. The DMZ host feature allows one local host to be exposed to the Internet for a special-purpose service such as Internet gaming or videoconferencing. DMZ host forwards all the ports at the same time. Any PC whose port is being forwarded must have its DHCP client function disabled and should have a new static IP Address assigned to it because its IP Address may be changed when using the DHCP function.

Figure 68: DMZ Settings



Current DMZ Status: ○ Enable ● Disable

DMZ Host IP Address: 0.0.0.0

To assign a computer or server to be a DMZ server:

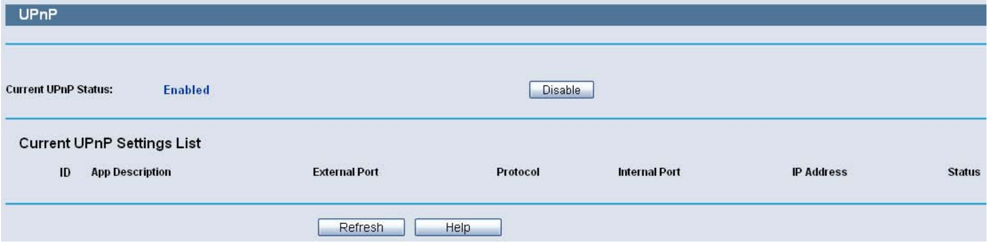
1. Click the Enable radio button
2. Enter the local host IP Address in the DMZ Host IP Address field
3. Click the Save button.

NOTE: After you set the DMZ host, the firewall related to the host will not work.

UPNP

Choose menu “Special Application->UPnP”, you can view the information about UPnP(Universal Plug and Play) in the screen. The UPnP feature allows the devices, such as Internet computers, to access the local host resources or devices as needed. UPnP devices can be automatically discovered by the UPnP service application on the LAN.

Figure 69: UPnP Settings



UPnP

Current UPnP Status: Enabled

Current UPnP Settings List

ID	App Description	External Port	Protocol	Internal Port	IP Address	Status

- **Current UPnP Status** - UPnP can be enabled or disabled by clicking the Enable or Disable button. As allowing this may present a risk to security, this feature is enabled by default.

- **Current UPnP Settings List** - This table displays the current UPnP information.

  - App Description -The description provided by the application in the UPnP request

  - External Port - External port, which the router opened for the application.

  - Protocol - Shows which type of protocol is opened.

  - Internal Port - Internal port, which the router opened for local host.

  - IP Address - The UPnP device that is currently accessing the router.

  - Status - The port’s status displayed here. “Enabled” means that port is still active. Otherwise, the port is inactive.

Click Refresh to update the Current UPnP Settings List.

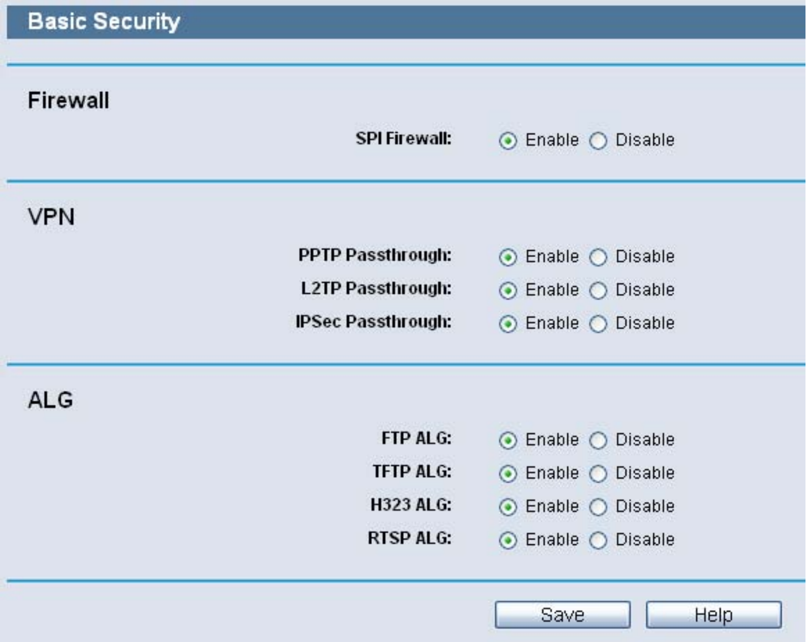
10 SECURITY SETTINGS

There are two submenus under the Security menu: Basic Security, and Advanced Security. Click any of them, and you will be able to configure the corresponding function.

BASIC SECURITY

Choose menu "Security->Basic Security", you can configure the basic security in the following screen.

Figure 70: Basic Security Settings



Basic Security

Firewall

SPI Firewall: ● Enable ○ Disable

VPN

PPTP Passthrough: ● Enable ○ Disable

L2TP Passthrough: ● Enable ○ Disable

IPSec Passthrough: ● Enable ○ Disable

ALG

FTP ALG: ● Enable ○ Disable

TFTP ALG: ● Enable ○ Disable

H323 ALG: ● Enable ○ Disable

RTSP ALG: ● Enable ○ Disable

- **Firewall** - A firewall protects your network from the outside world. Here you can enable or disable the Router's firewall.
  - SPI Firewall - SPI (Stateful Packet Inspection, also known as dynamic packet filtering) helps to prevent cyber attacks by tracking more state per session. It validates that the traffic passing through the session conforms to the protocol. SPI Firewall is enabled by factory default. If you want all the computers on the LAN exposed to the outside world, you can disable it.
- **VPN** - VPN Passthrough must be enabled if you want to allow VPN tunnels using IPSec, PPTP, or L2TP protocols to pass through the Router's firewall.

  - PPTP Passthrough - Point-to-Point Tunneling Protocol (PPTP) allows the Point-to-Point Protocol (PPP) to be tunneled through an IP network. To allow PPTP tunnels to pass through the Router, keep the default, Enabled.
  - L2TP Passthrough - Layer 2 Tunneling Protocol (L2TP) is the method used to enable Point-to-Point sessions via the Internet on the Layer 2 level. To allow L2TP tunnels to pass through the Router, keep the default, Enabled.
  - IPSec Passthrough - Internet Protocol Security (IPSec) is a suite of protocols for ensuring private, secure communications over Internet Protocol (IP) networks, through the use of cryptographic security services. To allow IPSec tunnels to pass through the Router, keep the default, Enabled.

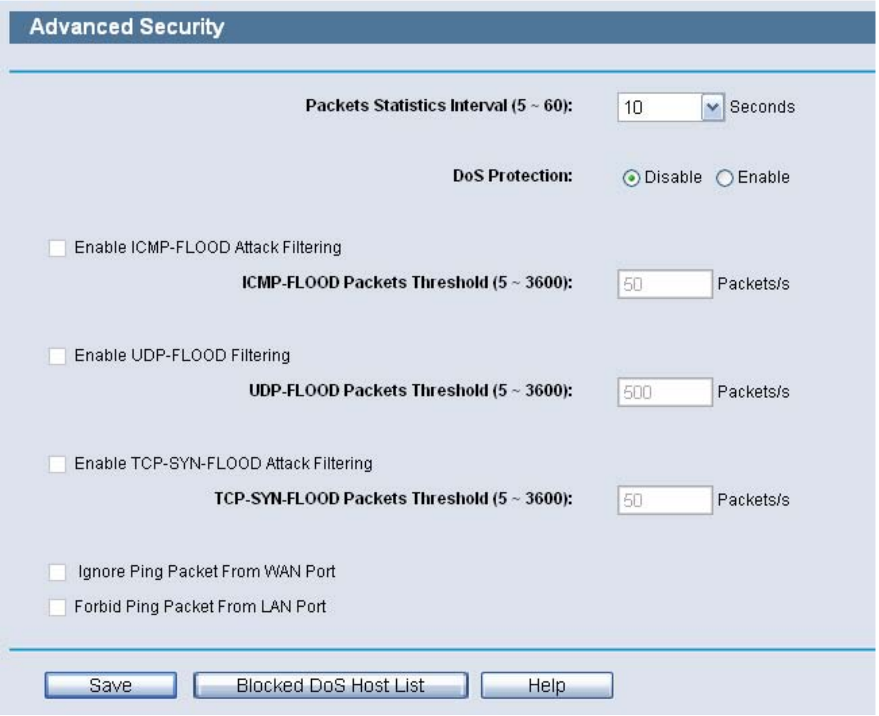
- **ALG** - It is recommended to enable Application Layer Gateway (ALG) because ALG allows customized Network Address Translation (NAT) traversal filters to be plugged into the gateway to support address and port translation for certain application layer "control/data" protocols such as FTP, TFTP, H323 etc.
  - FTP ALG - To allow FTP clients and servers to transfer data across NAT, keep the default Enable.
  - TFTP ALG - To allow TFTP clients and servers to transfer data across NAT, keep the default Enable.
  - H323 ALG - To allow Microsoft NetMeeting clients to communicate across NAT, keep the default Enable.

Click the Save button to save your settings.

ADVANCED SECURITY

Choose menu “Security->Advanced Security”, you can protect the Router from being attacked by TCP-SYN Flood, UDP Flood and ICMP-Flood in the following screen.

Figure 71: Advanced Security Settings



Advanced Security

Packets Statistics Interval (5 ~ 60): 10 Seconds

DoS Protection: ● Disable ○ Enable

□ Enable ICMP-FLOOD Attack Filtering

ICMP-FLOOD Packets Threshold (5 ~ 3600): 50 Packets/s

□ Enable UDP-FLOOD Filtering

UDP-FLOOD Packets Threshold (5 ~ 3600): 500 Packets/s

□ Enable TCP-SYN-FLOOD Attack Filtering

TCP-SYN-FLOOD Packets Threshold (5 ~ 3600): 50 Packets/s

□ Ignore Ping Packet From WAN Port

□ Forbid Ping Packet From LAN Port

- **Packets Statistics Interval (5~60)** - The default value is 10. Select a value between 5 and 60 seconds from the drop-down list. The Packets Statistics Interval value indicates the time section of the packets statistics. The result of the statistics is used for analysis by SYN Flood, UDP Flood and ICMP-Flood.

- **DoS Protection** - Denial of Service protection. Check the Enable or Disable button to enable or disable the DoS protection function. Only when it is enabled, will the flood filters be enabled.

NOTE: Dos Protection will take effect only when the Traffic Statistics in “System Tool->Traffic Statistics” is enabled.

- **Enable ICMP-FLOOD Attack Filtering** - Enable or Disable the ICMP-FLOOD Attack Filtering.

- **ICMP-FLOOD Packets Threshold (5~3600)** - The default value is 50. Enter a value between 5 ~ 3600. When the current ICMP-FLOOD Packets number is beyond the set value, the Router will startup the blocking function immediately.

- **Enable UDP-FLOOD Filtering** - Enable or Disable the UDP-FLOOD Filtering.

- **UDP-FLOOD Packets Threshold (5~3600)** - The default value is 500. Enter a value between 5 ~ 3600. When the current UPD-FLOOD Packets number is beyond the set value, the Router will startup the blocking function immediately.

- **Enable TCP-SYN-FLOOD Attack Filtering** - Enable or Disable the TCP-SYN-FLOOD Attack Filtering.

- **TCP-SYN-FLOOD Packets Threshold (5~3600)** - The default value is 50. Enter a value between 5 ~ 3600. When the current TCP-SYN-FLOOD Packets numbers is beyond the set value, the Router will startup the blocking function immediately.

- **Ignore Ping Packet From WAN Port** - Enable or Disable Ignore Ping Packet From WAN Port. The default setting is disabled. If enabled, the ping packet from the Internet cannot access the Router.

- **Forbid Ping Packet From LAN Port** - Enable or Disable Forbid Ping Packet From LAN Port. The default setting is disabled. If enabled, the ping packet from LAN cannot access the Router. This function can be used to defend against some viruses.

Click the Save button to save the settings.

Click the Blocked DoS Host List button to display the DoS host table by blocking.

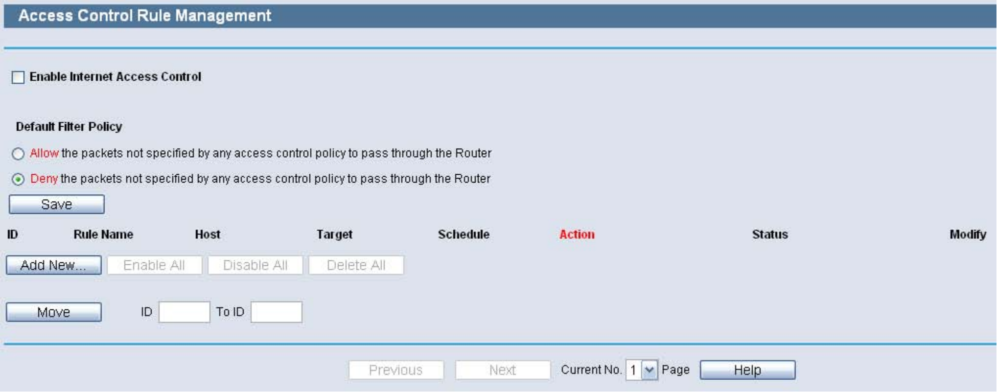
11 ACCESS CONTROL SETTINGS

There are five submenus under the Access Control menu: Rule, Host, Target, Schedule and Parental Control. Click any of them, and you will be able to configure the corresponding function.

RULE

Choose menu "Access Control->Rule", you can view and set Access Control rules in the screen as shown in the following.

Figure 72: Access Control Rule Management



Access Control Rule Management

□ Enable Internet Access Control

Default Filter Policy

○ Allow the packets not specified by any access control policy to pass through the Router

● Deny the packets not specified by any access control policy to pass through the Router

ID	Rule Name	Host	Target	Schedule	Action	Status	Modify

Current No. 1 Page

- **Enable Internet Access Control** - Select the check box to enable the Internet Access Control function, so the Default Filter Policy can take effect.
- **Rule Name** - Here displays the name of the rule and this name is unique.
- **Host** - Here displays the host selected in the corresponding rule.
- **Target** - Here displays the target selected in the corresponding rule.
- **Schedule** - Here displays the schedule selected in the corresponding rule.

- **Action** - Here displays the action the Router takes to deal with the packets. It could be Allow or Deny. Allow means that the Router permits the packets to go through the Router. Deny means that the Router rejects the packets to go through the Router.

- **Status** - This field displays the status of the rule. Enabled means the rule will take effect, Disabled means the rule will not take effect.

- **Modify** - Here you can edit or delete an existing rule.

To add a new rule, please follow the steps below.

1. Click the Add New button and the next screen will pop-up.

2. Give a name (e.g. Rule_1) for the rule in the Rule Name field.

3. Select a host from the Host drop-down list or choose "Click Here To Add New Host List".

4. Select a target from the Target drop-sown list or choose "Click Here To Add New Target List".

5. Select a schedule from the Schedule drop-down list or choose "Click Here To Add New Schedule".

6. In the Action field, select Deny or Allow.

7. In the Status field, select Enabled or Disabled to enable or disable your entry.

Click the Save button.

Click the Enable All button to enable all the rules in the list.

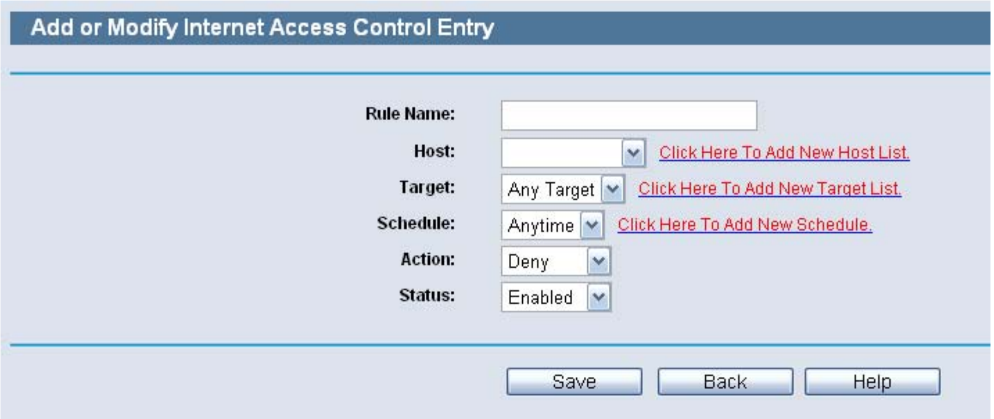
Click the Disable All button to disable all the rules in the list.

Click the Delete All button to delete all the entries in the table.

You can change the entry's order as desired. Fore entries are before hind entries. Enter the ID number in the first box you want to move and another ID number in second box you want to move to, and then click the Move button to change the entry's order.

Click the Next button to go to the next page, or click the Previous button return to the previous page.

Figure 73: Add or Modity Internet Access Control Entry



Add or Modify Internet Access Control Entry

Rule Name:

Host: Click Here To Add New Host List.

Target: Any Target Click Here To Add New Target List.

Schedule: Anytime Click Here To Add New Schedule.

Action: Deny

Status: Enabled

For example: If you desire to allow the host with MAC address 00-11-22-33-44-AA to access www.google.com only from 18:00 to 20:00 on Saturday and Sunday, and forbid other hosts in the LAN to access the Internet, you should follow the settings below:

1. Click “Access Control->Host” in the left to enter the Host Settings page. Add a new entry with the Host Description is Host_1 and MAC Address is 00-11-22-33-44-AA.

2. Click “Access Control->Target” in the left to enter the Target Settings page. Add a new entry with the Target Description is Target_1 and Domain Name is www.google.com.

3. Click “Access Control->Schedule” in the left to enter the Schedule Settings page. Add a new entry with the Schedule Description is Schedule_1, Day is Sat and Sun, Start Time is 1800 and Stop Time is 2000.

4. Click “Access Control->Rule” in the left to return to the Access Control Rule Management page. Select “Enable Internet Access Control” and choose "Deny the packets not specified by any access control policy to pass through the Router".

5. Click the Add New button to add a new rule as follows:

   - In Rule Name field, create a name for the rule. Note that this name should be unique, for example Rule_1.

   - In Host field, select Host_1.

   - In Target field, select Target_1.

   - In Schedule field, select Schedule_1.

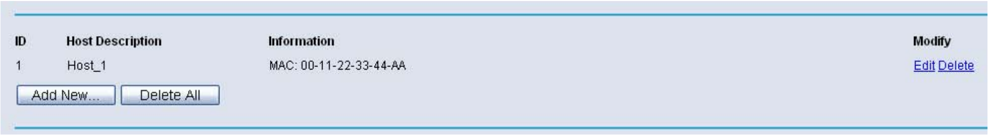
   - In Action field, select Allow.

   - In Status field, select Enable.

- Click Save to complete the settings.

Then you will go back to the Access Control Rule Management page and see the following list.

Figure 74: Display Access Control Entry

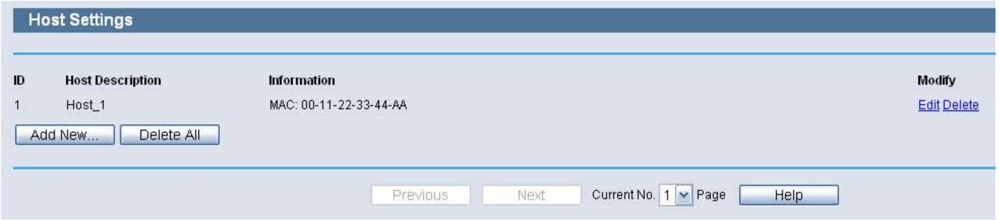


ID	Host Description	Information	Modify
1	Host_1	MAC: 00-11-22-33-44-AA	Edit Delete

HOST

Choose menu “Access Control->Host”, you can view and set a Host list in the following screen. The host list is necessary for the Access Control Rule.

Figure 75: Host Settings



Host Settings

ID	Host Description	Information	Modify
1	Host_1	MAC: 00-11-22-33-44-AA	Edit Delete

- **Host Description** - Here displays the description of the host and this description is unique.
- **Information** - Here displays the information about the host. It can be IP or MAC.
- **Modify** - To modify or delete an existing entry.

To add a new entry, please follow the steps below.

1. Click the Add New button.
2. In the Mode field, select IP Address or MAC Address.
   - If you select IP Address, the screen shown is Figure 75.

     1) In Host Description field, create a unique description for the host (e.g. Host_1).

     2) In LAN IP Address field, enter the IP address.
   - If you select MAC Address, the screen shown is Figure 76.

1) In Host Description field, create a unique description for the host (e.g. Host_1).

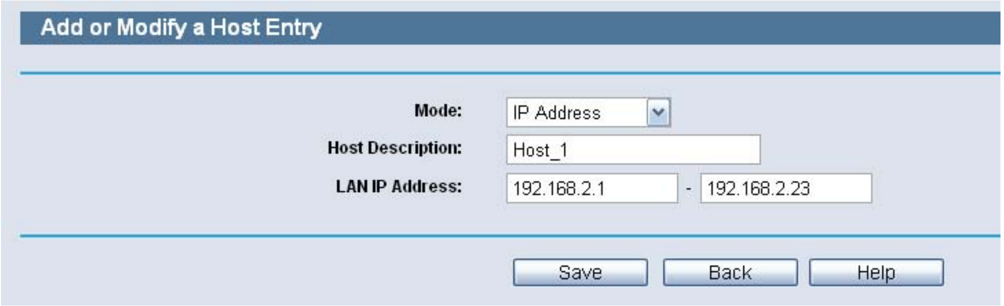
2) In MAC Address field, enter the MAC address.

3. Click the Save button to complete the settings.

Click the Delete All button to delete all the entries in the table.

Click the Next button to go to the next page, or click the Previous button return to the previous page.

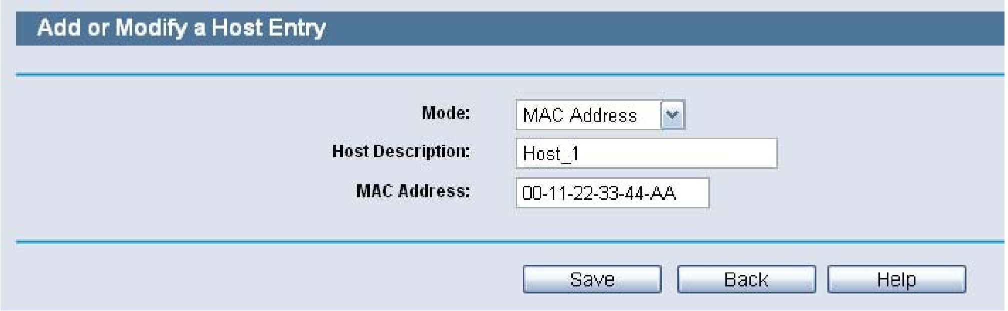
Figure 76: Host Entry IP address Mode



Add or Modify a Host Entry

Mode: IP Address
Host Description: Host_1
LAN IP Address: 192.168.2.1 - 192.168.2.23

Figure 77: Host Entry MAC address Mode



Add or Modify a Host Entry

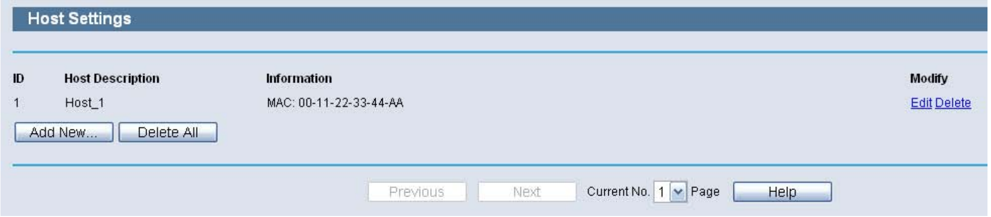
Mode: MAC Address
Host Description: Host_1
MAC Address: 00-11-22-33-44-AA

For example: If you desire to restrict the internet activities of host with MAC address 00-11-22-33-44-AA, you should first follow the settings below:

1. Click the Add New button.
2. In Mode field, select MAC Address from the drop-down list.
3. In Host Description field, create a unique description for the host (e.g. Host_1).
4. In MAC Address field, enter 00-11-22-33-44-AA.
5. Click Save to complete the settings.

Then you will go back to the Host Settings page and see the following list.

Figure 78: Host Settings



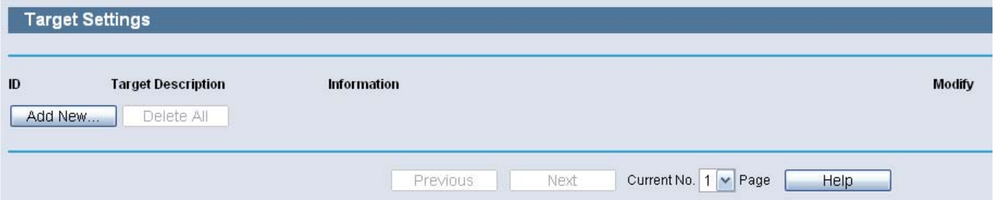
Host Settings

ID	Host Description	Information	Modify
1	Host_1	MAC: 00-11-22-33-44-AA	Edit Delete

TARGET

Choose menu “Access Control->Target”, you can view and set a Target list in the screen as shown in the following figure. The target list is necessary for the Access Control Rule.

Figure 79: Target Settings



Target Settings

ID	Target Description	Information	Modify

- **Target Description** - Here displays the description about the target and this description is unique.
- **Information** - The target can be IP address, port, or domain name.
- **Modify** - To modify or delete an existing entry.

To add a new entry, please follow the steps below.

1. Click the Add New button.
2. In Mode field, select IP Address or Domain Name.
   - If you select IP Address, the screen shown is Figure 79.

     1) In Target Description field, create a unique description for the target (e.g. Target_1).

     2) In IP Address field, enter the IP address of the target.

     3) Select a common service from Common Service Port drop-down list, so that the Target Port will be automatically filled. If the

Common Service Port drop-down list doesn’t have the service you want, specify the Target Port manually.

4) In Protocol field, select TCP, UDP, ICMP or ALL.

- If you select Domain Name, the screen shown is Figure 80.

  1) In Target Description field, create a unique description for the target (e.g. Target_1).

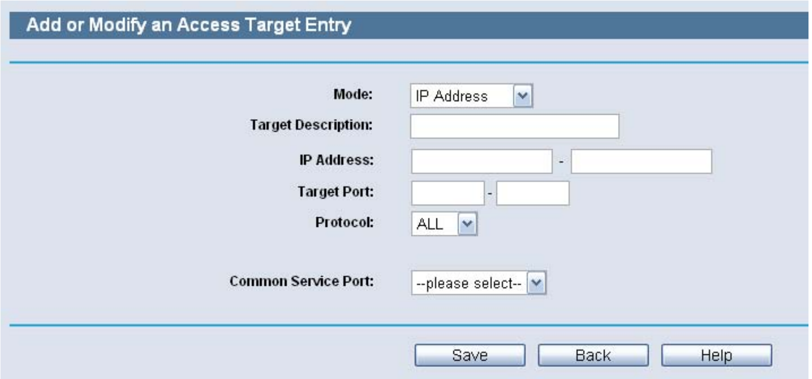
  2) In Domain Name field, enter the domain name, either the full name or the keywords (for example google) in the blank. Any domain name with keywords in it (www.google.com, www.google.cn) will be blocked or allowed. You can enter 4 domain names.

3. Click the Save button.

Click the Delete All button to delete all the entries in the table.

Click the Next button to go to the next page, or click the Previous button return to the previous page.

Figure 80: Target Settings-IP Address Mode



Add or Modify an Access Target Entry

Mode: IP Address

Target Description:

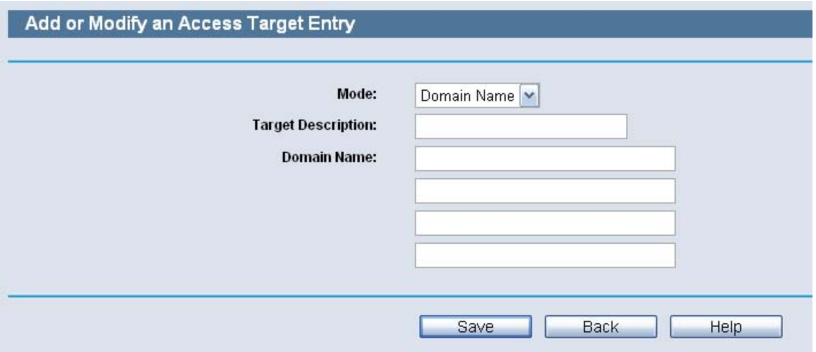
IP Address: -

Target Port: -

Protocol: ALL

Common Service Port: --please select--

Figure 81: Target Settings-Domain Name Mode



Add or Modify an Access Target Entry

Mode: Domain Name

Target Description:

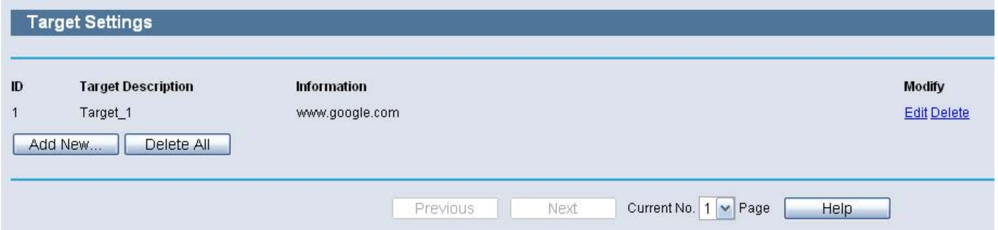
Domain Name:

For example: If you desire to restrict the internet activities of host with MAC address 00-11-22-33-44-AA in the LAN to access www.google.com only, you should first follow the settings below:

1. Click the Add New button.
2. In Mode field, select Domain Name from the drop-down list.
3. In Target Description field, create a unique description for the target (e.g. Target_1).
4. In Domain Name field, enter www.google.com.
5. Click Save to complete the settings.

Then you will go back to the Target Settings page and see the following list.

Figure 82: Target Settings-Domain Name Mode



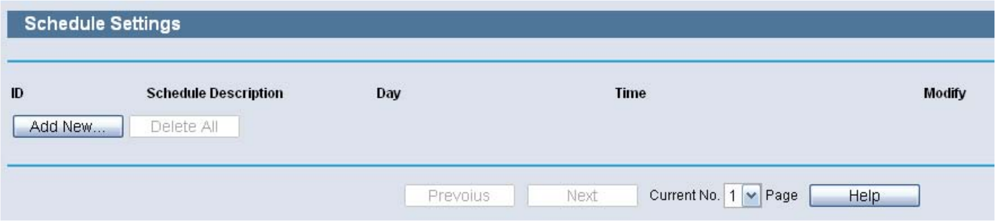
Target Settings

ID	Target Description	Information	Modify
1	Target_1	www.google.com	Edit Delete

SCHEDULE

Choose menu “Access Control->Schedule”, you can view and set a Schedule list in the next screen as shown in the following figure. The Schedule list is necessary for the Access Control Rule.

Figure 83: Schedule Settings



Schedule Settings

ID	Schedule Description	Day	Time	Modify

- **Schedule Description** - Here displays the description of the schedule and this description is unique.
- **Day** - Here displays the day(s) in a week.

- **Time** - Here displays the time period in a day.
- **Modify** - Here you can edit or delete an existing schedule.

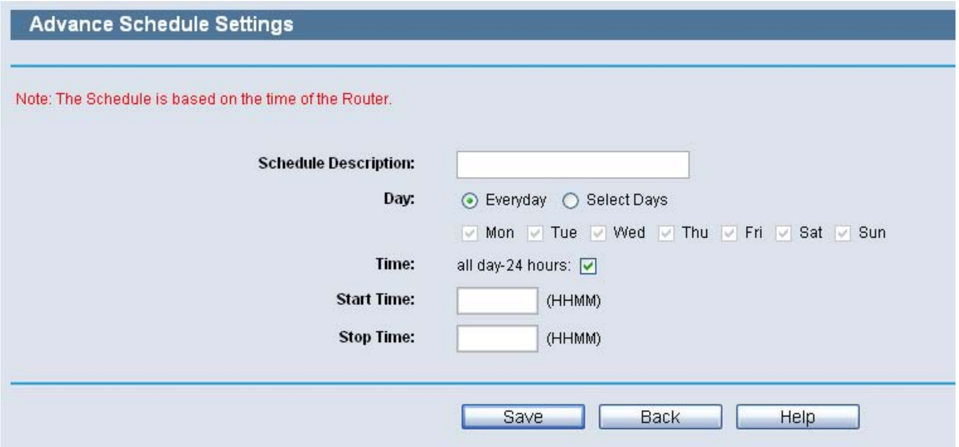
To add a new schedule, follow the steps below.

1. Click the Add New button shown in Figure 82 and the next screen will pop-up.
2. In Schedule Description field, create a unique description for the schedule (e.g. Schedule_1).
3. In Day field, select the day or days you need.
4. In Time field, you can select all day-24 hours or you may enter the Start Time and Stop Time in the corresponding field.
5. Click Save to complete the settings.

Click the Delete All button to delete all the entries in the table.

Click the Next button to go to the next page, or click the Previous button return to the previous page.

Figure 84: Advanced Schedule Settings



Advance Schedule Settings

Note: The Schedule is based on the time of the Router.

Schedule Description:	
Day:	● Everyday ○ Select Days
	☑ Mon ☑ Tue ☑ Wed ☑ Thu ☑ Fri ☑ Sat ☑ Sun
Time:	all day-24 hours: ☑
Start Time:	(HHMM)
Stop Time:	(HHMM)

For example: If you desire to restrict the internet activities of host with MAC address 00-11-22-33-44-AA to access www.google.com only from 18:00 to 20:00 on Saturday and Sunday, you should first follow the settings below:

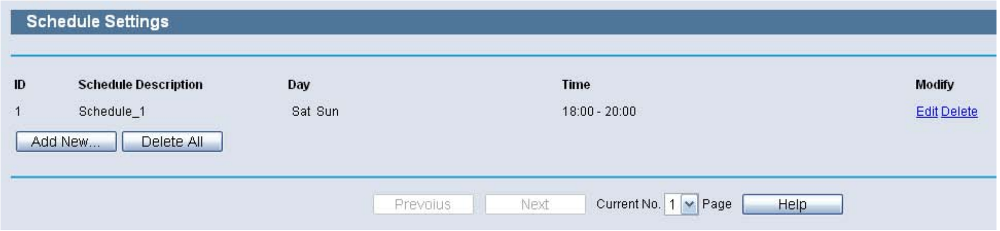
1. Click the Add New button.
2. In Schedule Description field, create a unique description for the schedule (e.g. Schedule_1).
3. In Day field, check the Select Days radio button and then select Sat and Sun.

4. In Time field, enter 1800 in Start Time field and 2000 in Stop Time field.

5. Click Save to complete the settings.

Then you will go back to the Schedule Settings page and see the following list.

Figure 85: Schedule Settings



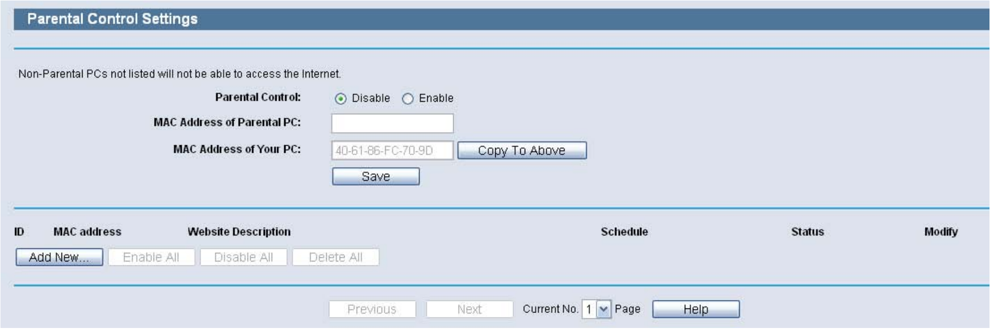
Schedule Settings

ID	Schedule Description	Day	Time	Modify
1	Schedule_1	Sat Sun	18:00 - 20:00	Edit Delete

PARENTAL CONTROL

Choose menu “Parental Control”, and you can configure the parental control in the screen as shown in the following figure. The Parental Control function can be used to control the internet activities of the child, limit the child to access certain websites and restrict the time of surfing.

Figure 86: Parental Control Settings



Parental Control Settings

Non-Parental PCs not listed will not be able to access the Internet.

Parental Control: ● Disable ○ Enable

MAC Address of Parental PC:

MAC Address of Your PC: 40-61-86-FC-70-9D

ID	MAC address	Website Description	Schedule	Status	Modify

- **Parental Control** - Check Enable if you want this function to take effect, otherwise check Disable.

- **MAC Address of Parental PC** - In this field, enter the MAC address of the controlling PC, or you can make use of the Copy To Above button below.

- **MAC Address of Your PC** - This field displays the MAC address of the PC that is managing this Router. If the MAC Address of your adapter is registered, you can click the Copy To Above button to fill this address to the MAC Address of Parental PC field above.
- **Website Description** - Description of the allowed website for the PC controlled.
- **Schedule** - The time period allowed for the PC controlled to access the Internet. For detailed information, please go to “Access Control ? Schedule”.
- **Modify** - Here you can edit or delete an existing entry.

To add a new entry, please follow the steps below.

1. Click the Add New button.
2. Enter the MAC address of the PC (e.g. 00-11-22-33-44-AA) you’d like to control in the MAC Address of Child PC field. Or you can choose the MAC address from the All Address in Current LAN drop-down list.
3. Give a description (e.g. Allow Google) for the website allowed to be accessed in the Website Description field.
4. Enter the allowed domain name of the website, either the full name or the keywords (e.g. google) in the Allowed Domain Name field. Any domain name with keywords in it (www.google.com.cn) will be allowed.
5. Select from the Effective Time drop-down list the schedule (e.g. Schedule_1) you want the entry to take effect. If there are not suitable schedules for you, click the Schedule in red below to go to the Advance Schedule Settings page and create the schedule you need.
6. In the Status field, you can select Enabled or Disabled to enable or disable your entry.
7. Click the Save button.

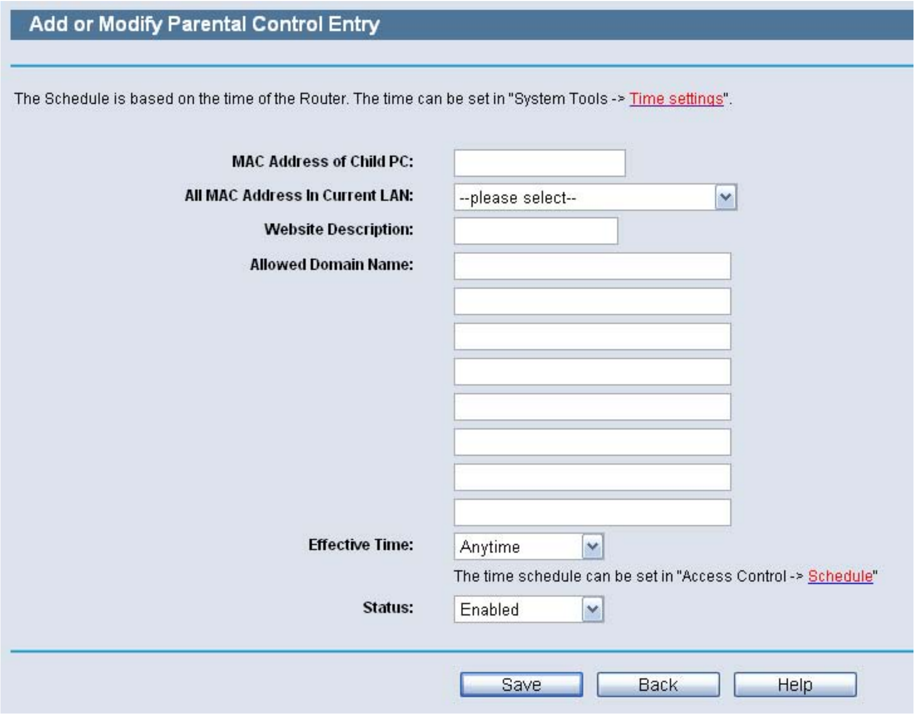
Click the Enable All button to enable all the rules in the list.

Click the Disable All button to disable all the rules in the list.

Click the Delete All button to delete all the entries in the table.

Click the Next button to go to the next page, or click the Previous button return to the previous page.

Figure 87: Add or Modify Parental Control Entry



Add or Modify Parental Control Entry

The Schedule is based on the time of the Router. The time can be set in "System Tools -> Time settings".

MAC Address of Child PC:

All MAC Address In Current LAN: --please select--

Website Description:

Allowed Domain Name:

Effective Time: Anytime

The time schedule can be set in "Access Control -> Schedule"

Status: Enabled

For example: If you desire that the child PC with MAC address 00-11-22-33-44-AA can access www.google.com on Saturday only while the parent PC with MAC address 00-11-22-33-44-BB is without any restriction, you should follow the settings below.

1. Click "Parental Control" menu on the left to enter the Parental Control Settings page. Check Enable and enter the MAC address 00-11-22-33-44-BB in the MAC Address of Parental PC field.

2. Click "Access Control->Schedule" on the left to enter the Schedule Settings page. Clickthe Add New button to create a new schedule with Schedule Description is Schedule_1, Day is Sat and Time is all day-24 hours.

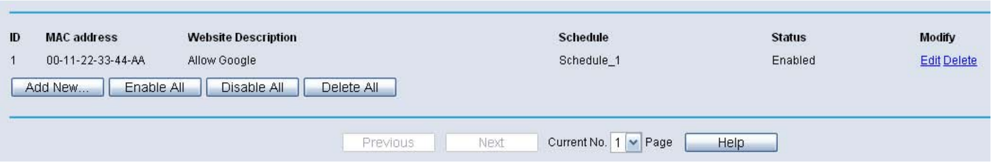
3. Click "Parental Control" menu on the left to go back to the Add or Modify Parental Control Entry page:

   - Click the Add New button.
   - Enter 00-11-22-33-44-AA in the MAC Address of Child PC field.
   - Enter "Allow Google" in the Website Description field.
   - Enter "www.google.com" in the Allowed Domain Name field.
   - Select "Schedule_1" you create just now from the Effective Time drop-down list.
   - In Status field, select Enable.

4. Click Save to complete the settings.

Then you will go back to the Parental Control Settings page and see the following list, as shown in the following figure.

Figure 88: Parental Control Settings



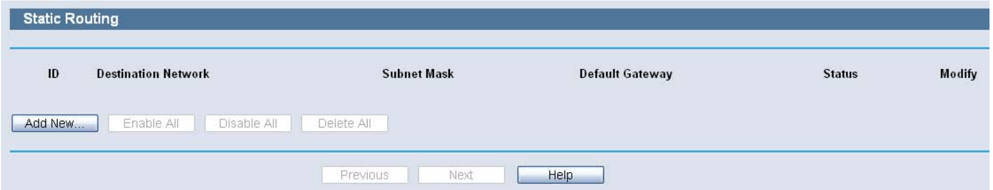
ID	MAC address	Website Description	Schedule	Status	Modify
1	00-11-22-33-44-AA	Allow Google	Schedule_1	Enabled	Edit Delete

12 ADVANCED ROUTING

STATIC ROUTING LIST

Choose menu “Advanced Routing”, you can configure the static route in the next screen. A static route is a pre-determined path that network information must travel to reach a specific host or network.

Figure 89: Static Routing



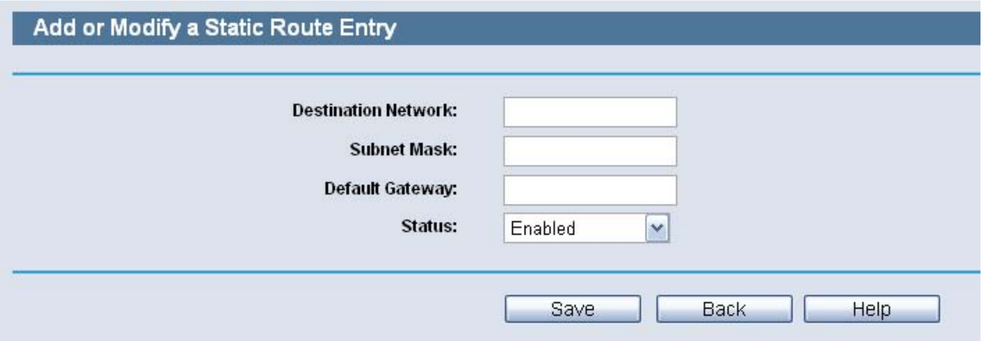
Static Routing

ID	Destination Network	Subnet Mask	Default Gateway	Status	Modify

To add static routing entries:

1. Click the Add New button.

Figure 90: Add or Modify a Static Route Entry



Add or Modify a Static Route Entry

Destination Network:

Subnet Mask:

Default Gateway:

Status: Enabled

2. Enter the following data:

- **Destination IP Address** - The Destination IP Address is the address of the network or host that you want to assign to a static route.
- **Subnet Mask** - The Subnet Mask determines which portion of an IP Address is the network portion, and which portion is the host portion.
- **Gateway** - This is the IP Address of the gateway device that allows for contact between the Router and the network or host.

3. Select Enabled or Disabled for this entry on the Status pull-down list.

4. Click the Save button to make the entry take effect.

Other configurations for the entries:

Click the Delete button to delete the entry.

Click the Enable All button to enable all the entries.

Click the Disable All button to disable all the entries.

Click the Delete All button to delete all the entries.

Click the Previous button to view the information in the previous screen, click the Next button to view the information in the next screen.

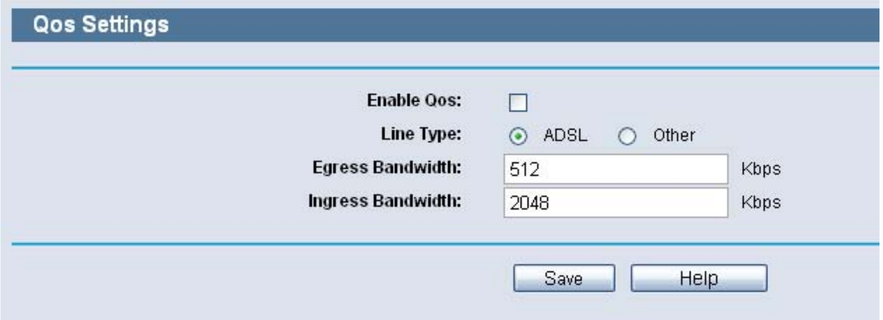
13 QoS Settings

There are two submenus under the QoS menu: QoS Settings and Rules List. Click any of them, and you will be able to configure the corresponding function. The detailed explanations for each submenu are provided below.

QoS Settings

Choose menu “QoS->QoS Settings”, you can configure the Egress Bandwidth and Ingress Bandwidth in the next screen. Their values you configure should be less than 100000Kbps. For optimal control of the bandwidth, please select the right Line Type and ask your ISP for the total bandwidth of the egress and ingress.

Figure 91: QoS Settings



Qos Settings

Enable Qos: □

Line Type: ● ADSL ○ Other

Egress Bandwidth: 512 Kbps

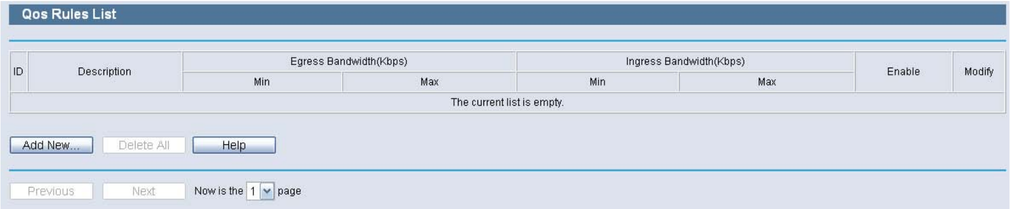
Ingress Bandwidth: 2048 Kbps

- **Enable QoS** - Check this box so that the QoS settings can take effect.
- **Line Type** - Select the right type for you network connection. If you don’t know how to choose, please ask your ISP for the information.
- **Egress Bandwidth** - The upload speed through the WAN port.
- **Ingress Bandwidth** - The download speed through the WAN port.

RULES LIST

Choose menu “QoS->Rules List”, you can view and configure the QoS rules in the screen below.

Figure 92: QoS Rules List



Qos Rules List

ID	Description	Egress Bandwidth(Kbps)		Ingress Bandwidth(Kbps)		Enable	Modify
		Min	Max	Min	Max		
The current list is empty.							

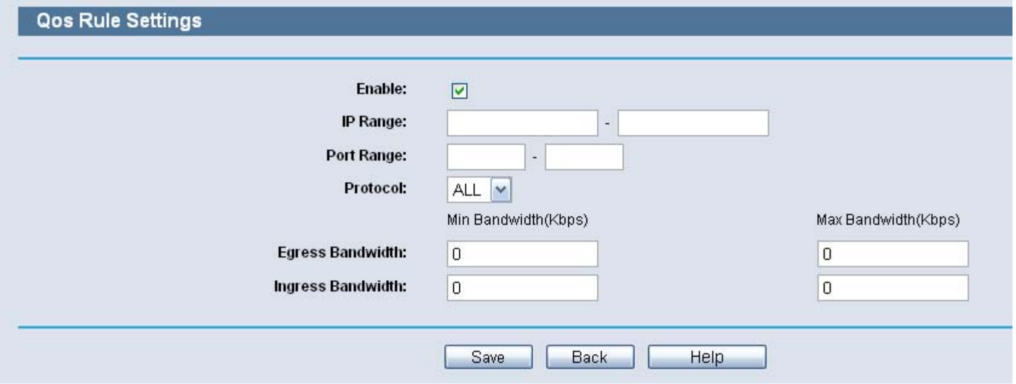
Now is the 1 page

- **Description** - This is the information about the rules such as address range.
- **Egress bandwidth** - This field displays the max and mix upload bandwidth through the WAN port, the default is 0.
- **Ingress bandwidth** - This field displays the max and mix download bandwidth through the WAN port, the default is 0.
- **Enable** - This displays the status of the rule.
- **Modify** - Click Modify to edit the rule. Click Delete to delete the rule.

To add/modify a QoS rule, follow the steps below.

1. Click the Add New buttonshown in Figure 91, you will see a new screen shown in Figure 92.
2. Enter the information like the screen shown below.
3. Click the Save button.

Figure 93: QoS Rule Settings



Qos Rule Settings

Enable: ☑

IP Range: ______ - ______

Port Range: ______ - ______

Protocol: ALL

	Min Bandwidth(Kbps)	Max Bandwidth(Kbps)
Egress Bandwidth:	0	0
Ingress Bandwidth:	0	0

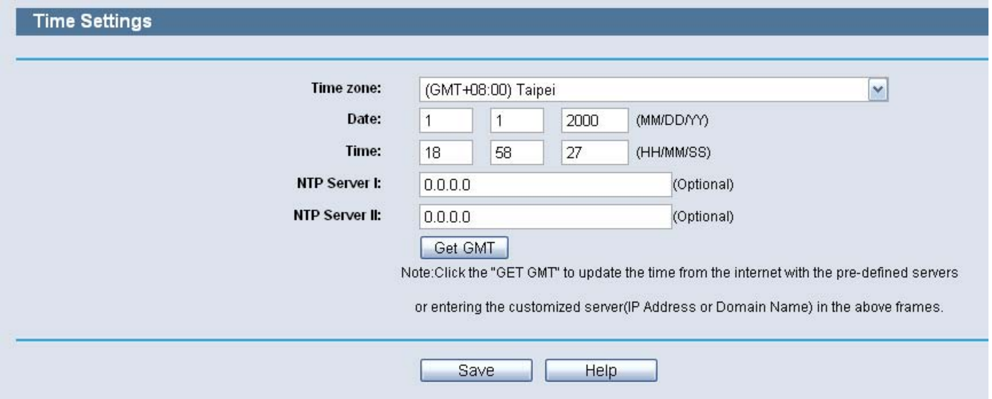
14 SYSTEM TOOLS

Choose menu “System Tools”, and you can see the submenus under the main menu: Time Settings, Diagnostic, Setting Management, Password, System Log, Statistics, Local Management and Remote Management. Click any of them, and you will be able to configure the corresponding function. The detailed explanations for each submenu are provided below.

TIME SETTING

Choose menu “System Tools->Time Setting”, you can configure the time on the following screen.

Figure 94: Time Settings



Time Settings

Time zone: (GMT+08:00) Taipei

Date: 1 1 2000 (MM/DD/YY)

Time: 18 58 27 (HH/MM/SS)

NTP Server I: 0.0.0.0 (Optional)

NTP Server II: 0.0.0.0 (Optional)

Note:Click the "GET GMT" to update the time from the internet with the pre-defined servers or entering the customized server(IP Address or Domain Name) in the above frames.

- **Time Zone** - Select your local time zone from this pull down list.
- **Date** - Enter your local date in MM/DD/YY into the right blanks.
- **Time** - Enter your local time in HH/MM/SS into the right blanks.
- **NTP Server Prior** - Enter the address for the NTP Server, then the Router will get the time from the NTP Server preferentially. In addition, the Router built-in some common NTP Servers, so it can get time automatically once it connects the Internet.

To configure the system manually:

1. Select your local time zone.
2. Enter date and time in the right blanks.

3. Click Save to save the configuration.

To configure the system automatically:

1. Select your local time zone.

2. Enter the IP address for NTP Server Prior.

3. Click the Get GMT button to get system time from Internet if you have connected to the Internet.

NOTE: This setting will be used for some time-based functions such as firewall. You must specify your time zone once you login to the router successfully, otherwise, these functions will not take effect.

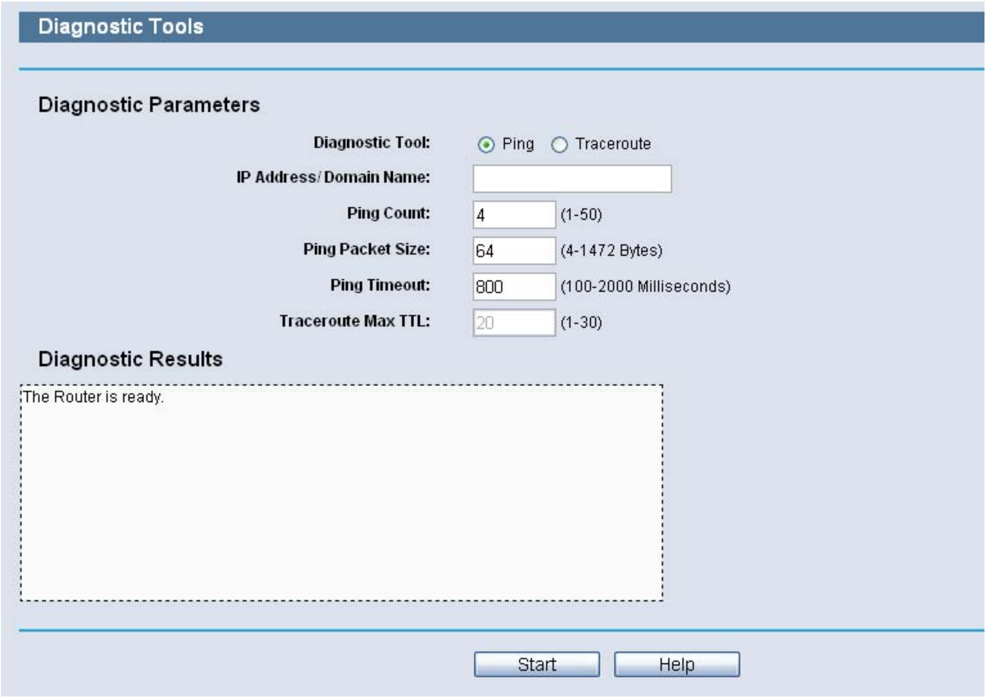
NOTE: The time will be lost if the router is turned off.

NOTE: The router will obtain GMT automatically from Internet if it has already connected to Internet.

DIAGNOSTIC

Choose menu "System Tools->Diagnostic", you can transact Ping or Traceroute function to check connectivity of your network in the following screen.

Figure 95: Diagnostic Tools



Diagnostic Tools

Diagnostic Parameters

Diagnostic Tool:	● Ping ○ Traceroute
IP Address/ Domain Name:	
Ping Count:	4 (1-50)
Ping Packet Size:	64 (4-1472 Bytes)
Ping Timeout:	800 (100-2000 Milliseconds)
Traceroute Max TTL:	20 (1-30)

Diagnostic Results

The Router is ready.

- **Diagnostic Tool** - Check the radio button to select one diagnostic too.
  - **Ping** - This diagnostic tool troubleshoots connectivity, reachability, and name resolution to a given host or gateway.
  - **Traceroute** - This diagnostic tool tests the performance of a connection.

NOTE: You can use ping/traceroute to test both numeric IP address or domain name. If pinging/tracerouting the IP address is successful, but pinging/tracerouting the domain name is not, you might have a name resolution problem. In this case, ensure that the domain name you are specifying can be resolved by using Domain Name System (DNS) queries.

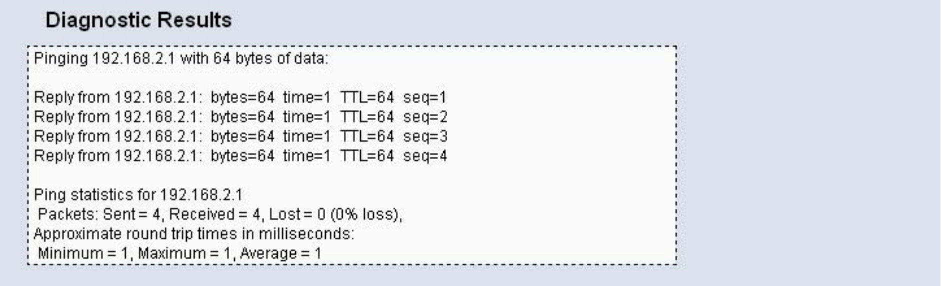
- **IP Address/Domain Name** - Type the destination IP address (such as 202.108.22.5) or Domain name (such as http://www.smc.com)
- **Pings Count** - The number of Ping packets for a Ping connection.
- **Ping Packet Size** - The size of Ping packet.
- **Ping Timeout** - Set the waiting time for the reply of each Ping packet. If there is no reply in the specified time, the connection is overtime.
- **Traceroute Max TTL** - The max number of hops for a Traceroute connection.

Click Start to check the connectivity of the Internet.

The Diagnostic Results page displays the result of diagnosis.

If the result is similar to the following screen, the connectivity of the Internet is fine.

Figure 96: Diagnostic Results



Diagnostic Results

```
Pinging 192.168.2.1 with 64 bytes of data:

Reply from 192.168.2.1:  bytes=64  time=1  TTL=64  seq=1
Reply from 192.168.2.1:  bytes=64  time=1  TTL=64  seq=2
Reply from 192.168.2.1:  bytes=64  time=1  TTL=64  seq=3
Reply from 192.168.2.1:  bytes=64  time=1  TTL=64  seq=4

Ping statistics for 192.168.2.1
 Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milliseconds:
 Minimum = 1, Maximum = 1, Average = 1
```

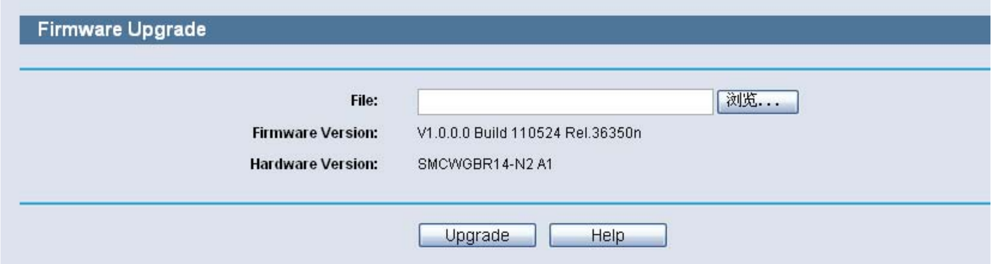
NOTE: Only one user can use this tool at one time. Options “Number of Pings”, “Ping Size” and “Ping Timeout” are used for Ping function. Option “Tracert Hops” are used for Tracert function.

SETTINGS MANAGEMENT

FIRMWARE UPGRADE

Choose menu "System Tools->Firmware Upgrade", you can update the latest version of firmware for the Router on the following screen.

Figure 97: Firmware Upgrade



Firmware Upgrade

File:

Firmware Version: V1.0.0.0 Build 110524 Rel.36350n

Hardware Version: SMCWGBR14-N2 A1

- **Firmware Version** - This displays the current firmware version.
- **Hardware Version** - This displays the current hardware version. The hardware version of the upgrade file must accord with the Router's current hardware version.

To upgrade the Router's firmware, follow these instructions below:

1. Download a more recent firmware upgrade file from the SMC website (http://www.smc.com).
2. Type the path and file name of the update file into the File field. Or click the Browse button to locate the update file.
3. Click the Upgrade button.

NOTE: New firmware versions are posted at http://www.smc.com and can be downloaded for free. There is no need to upgrade the firmware unless the new firmware has a new feature you want to use. However, when experiencing problems caused by the Router rather than the configuration, you can try to upgrade the firmware.

NOTE: When you upgrade the Router's firmware, you may lose its current configurations, so before upgrading the firmware please write down some of your customized settings to avoid losing important settings.

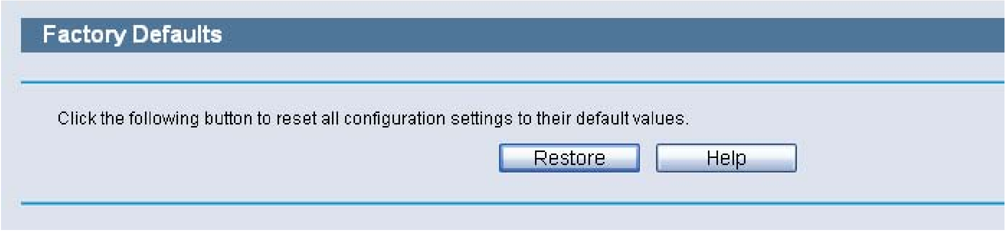
NOTE: Do not turn off the Router or press the Reset button while the firmware is being upgraded, otherwise, the Router may be damaged.

NOTE: The Router will reboot after the upgrading has been finished.

FACTORY DEFAULTS

Choose menu “System Tools-> Factory Defaults”, and you can restore the configurations of the Router to factory defaults on the following screen.

Figure 98: Restore Factory Default



Factory Defaults

Click the following button to reset all configuration settings to their default values.

Click the Restore button to reset all configuration settings to their default values.

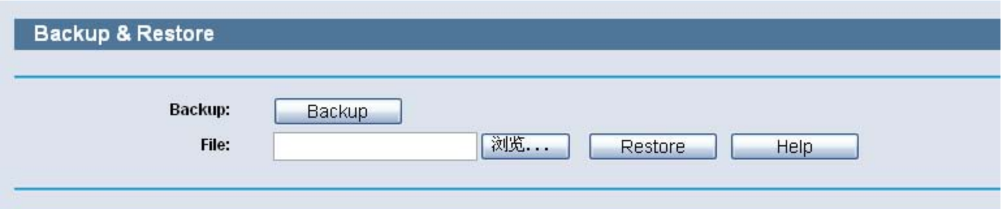
- The default User Name: admin
- The default Password: smcadmin
- The default IP Address: 192.168.2.1
- The default Subnet Mask: 255.255.255.0

NOTE: Any settings you have saved will be lost when the default settings are restored.

BACKUP & RESTORE

Choose menu “System Tools-> Backup & Restore”, you can save the current configuration of the Router as a backup file and restore the configuration via a backup file as shown in the following figure.

Figure 99: Backup & Restore Configuration



Backup & Restore

- Click the Backup button to save all configuration settings as a backup file in your local computer.
- To upgrade the Router's configuration, follow these instructions.
  - Click the Browse… button to locate the update file for the Router, or enter the exact path to the Setting file in the text box.

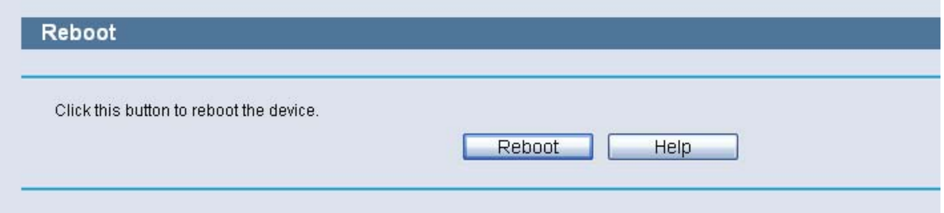
- Click the Restore button.

NOTE: The current configuration will be covered by the uploading configuration file. The upgrade process lasts for 20 seconds and the Router will restart automatically. Keep the Router on during the upgrading process to prevent any damage.

REBOOT

Choose menu “System Tools->Reboot”, you can click the Reboot button to reboot the Router via the next screen.

Figure 100: Reboot



Reboot

Click this button to reboot the device.

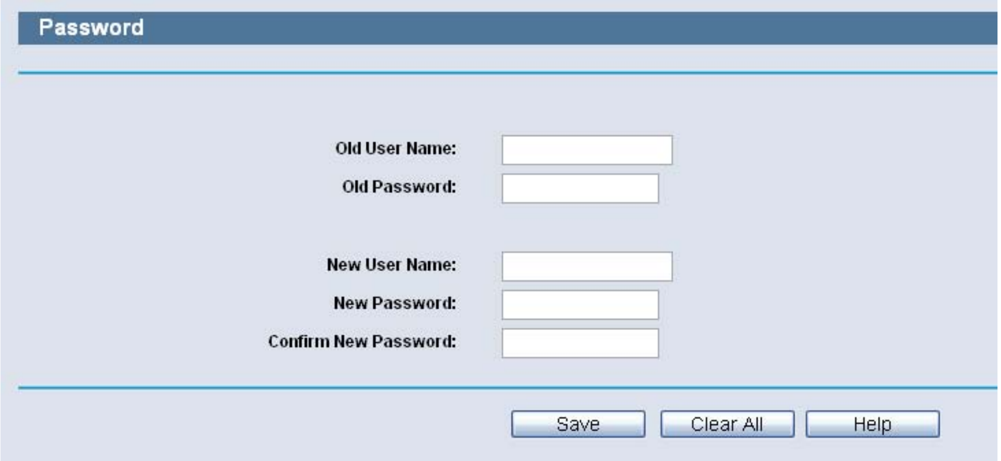
Some settings of the Router will take effect only after rebooting, which include

- Change the LAN IP Address (system will reboot automatically).
- Change the DHCP Settings.
- Change the Wireless configurations.
- Change the Web Management Port.
- Upgrade the firmware of the Router (system will reboot automatically).
- Restore the Router's settings to factory defaults (system will reboot automatically).
- Update the configuration with the file (system will reboot automatically.

PASSWORD

Choose menu “System Tools->Password”, you can change the factory default user name and password of the Router in the next screen as shown in the following figure.

Figure 101: Password



Old User Name:	
Old Password:	
New User Name:	
New Password:	
Confirm New Password:	

It is strongly recommended that you should change the factory default user name and password of the Router, because all users who try to access the Router's Web-based utility or Quick Setup will be prompted for the Router's default user name and password.

NOTE: The new user name and password must not exceed 14 characters in length and not include any spaces. Enter the new Password twice to confirm.

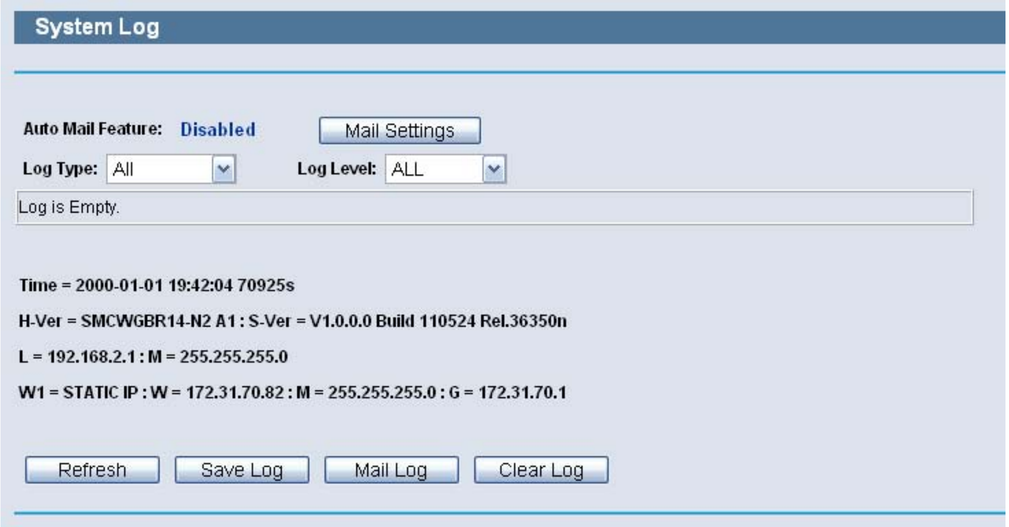
Click the Save button when finished.

Click the Clear All button to clear all.

SYSTEM LOG

Choose menu “System Tools->System Log”, you can view the logs of the Router.

Figure 102: System Log



Auto Mail Feature: Disabled

Log Type: All

Log Level: ALL

Log is Empty.

```
Time = 2000-01-01 19:42:04 70925s
H-Ver = SMCWGBR14-N2 A1 : S-Ver = V1.0.0.0 Build 110524 Rel.36350n
L = 192.168.2.1 : M = 255.255.255.0
W1 = STATIC IP : W = 172.31.70.82 : M = 255.255.255.0 : G = 172.31.70.1
```

- **Auto Mail Feature** - Indicates whether auto mail feature is enabled or not.

- **Mail Settings** - Set the receiving and sending mailbox address, server address, validation information as well as the timetable for Auto Mail Feature, as shown in Figure 101.

- **Log Type** - By selecting the log type, only logs of this type will be shown.

- **Log Level** - By selecting the log level, only logs of this level will be shown.

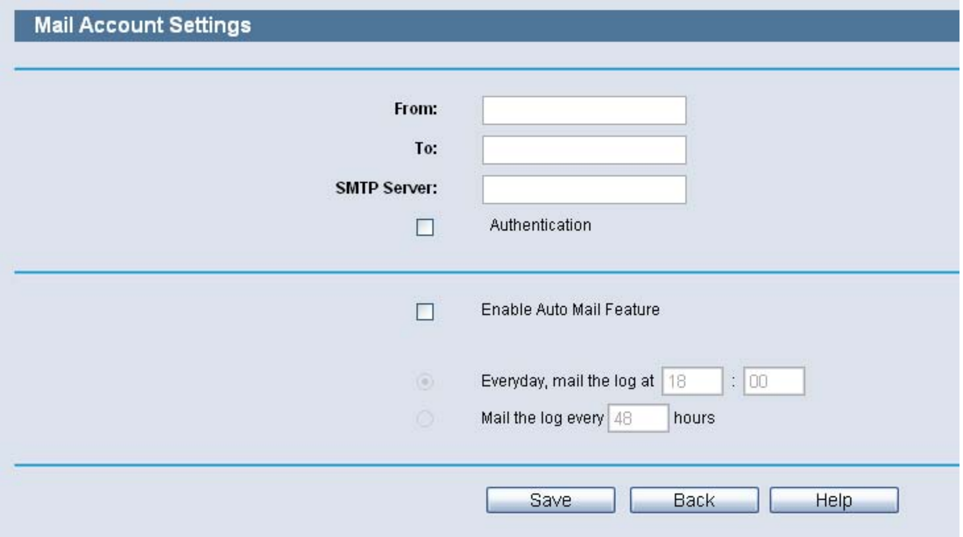
- **Refresh** - Refresh the page to show the latest log list.

- **Save Log** - Click to save all the logs in a txt file.

- **Mail Log** - Click to send an email of current logs manually according to the address and validation information set in Mail Settings.

- **Clear Log -** All the logs will be deleted from the Router permanently, not just from the page.

Figure 103: Mail Account Settings



Mail Account Settings

From:

To:

SMTP Server:

□ Authentication

□ Enable Auto Mail Feature

○ Everyday, mail the log at 18 : 00

○ Mail the log every 48 hours

- **From** - Your mail box address. The Router would connect it to send logs.

- **To** - Recipient’s address. The destination mailbox where the logs would be received.

- **SMTP Server** - Your smtp server. It corresponds with the mailbox filled in the From field. You can log on the relevant website for Help if you are not clear with the address.

- **Authentication** - Most SMTP Server requires Authentication. It is required by most mailboxes that need User Name and Password to log in.

NOTE: Only when you select Authentication, do you have to enter the User Name and Password in the following fields.

- **User Name** - Your mail account name filled in the From field. The part behind @ is excluded.

- **Password** - Your mail account password.

- **Confirm The Password** - Enter the password again to confirm.

- **Enable Auto Mail Feature** - Select it to mail logs automatically. You could mail the current logs either at a specified time everyday or by intervals, but only one could be the current effective rule. Enter the desired time or intervals in the corresponding field.

Click Save to keep your settings.

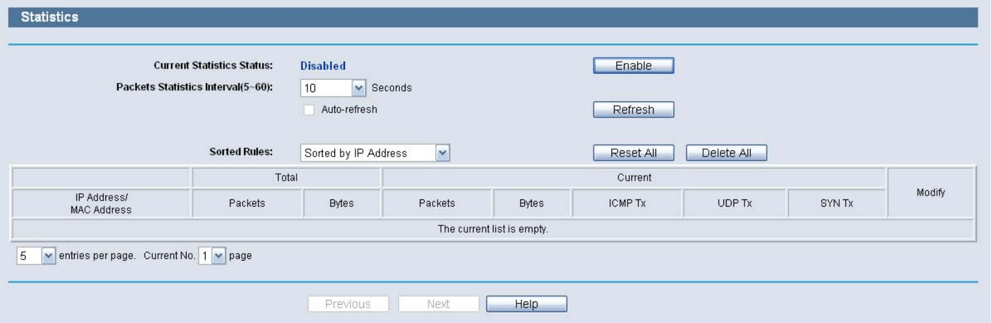
Click Back to return to the previous page.

Click the Next button to go to the next page, or click the Previous button return to the previous page.

STATISTICS

Choose menu “System Tools->Statistics”, you can view the statistics of the Router, including total traffic and current traffic of the last Packets Statistic Interval.

Figure 104: Statistics



Statistics

Current Statistics Status: Disabled

Packets Statistics Interval(5~60): 10 Seconds

□ Auto-refresh

Sorted Rules: Sorted by IP Address

	Total		Current					Modify
IP Address/ MAC Address	Packets	Bytes	Packets	Bytes	ICMP Tx	UDP Tx	SYN Tx	
The current list is empty.								

5 entries per page. Current No. 1 page

- **Current Statistics Status** - Enable or Disable. The default value is disabled. To enable, click the Enable button.

- **Packets Statistics Interval (5-60)** - The default value is 10. Select a value between 5 and 60 seconds in the pull-down list. The Packets Statistic interval indicates the time section of the packets statistic.

Select the Auto-refresh checkbox to refresh automatically.

Click the Refresh button to refresh immediately.

- **Sorted Rules** - Select a rule from the pull-down list to display the corresponding statistics..

Click Reset All to reset the values of all the entries to zero.

Click Delete All to delete all entries in the table.

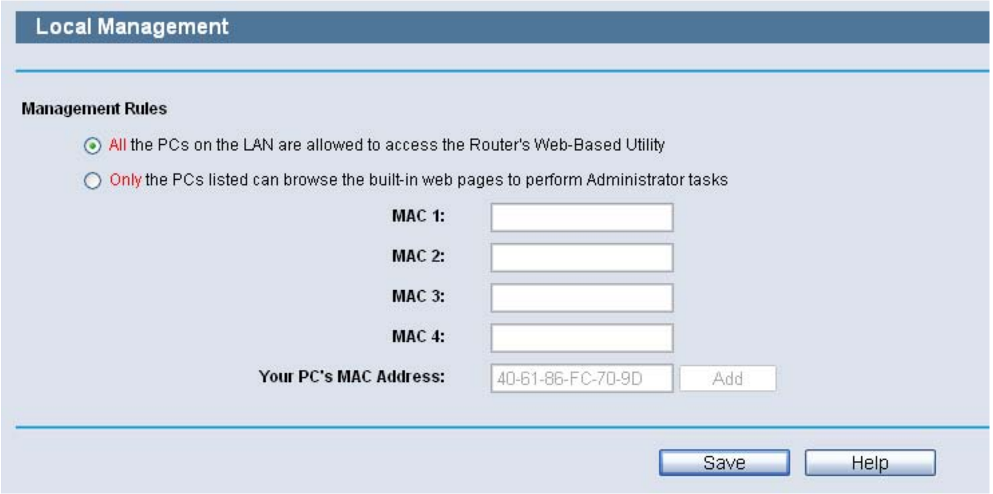
Table 3: Statistics Table

IP/MAC Address		The IP/MAC Address displayed with statistics
Total	Packets	The total amount of packets received and transmitted by the Router.
	Bytes	The total amount of bytes received and transmitted by the Router
Current	Packets	The total amount of packets received and transmitted in the last Packets Statistic interval seconds.
	Bytes	The total amount of bytes received and transmitted in the last Packets Statistic interval seconds.
	ICMP Tx	The total amount of the ICMP packets transmitted to WAN in the last Packets Statistic interval seconds.
	UDP Tx	The total amount of the UDP packets transmitted to WAN in the last Packets Statistic interval seconds.
	TCP SYN Tx	The total amount of the TCP SYN packets transmitted to WAN in the last Packets Statistic interval seconds.

LOCAL MANAGEMENT

Choose menu “Security->Local Management”, you can configure the management rule in the screen as shown in the following figure. The management feature allows you to deny computers in LAN from accessing the Router.

Figure 105: Local Management



Local Management

Management Rules

● All the PCs on the LAN are allowed to access the Router's Web-Based Utility

○ Only the PCs listed can browse the built-in web pages to perform Administrator tasks

MAC 1:

MAC 2:

MAC 3:

MAC 4:

Your PC's MAC Address: 40-61-86-FC-70-9D

By default, the radio button “All the PCs on the LAN are allowed to access the Router's Web-Based Utility” is checked. If you want to allow PCs with specific MAC Addresses to access the Setup page of the Router's Web-Based Utility locally from inside the network, check the radio button “Only the PCs listed can browse the built-in web pages to perform Administrator tasks”, and then enter each MAC Address in a separate field. The format for the MAC Address is XX-XX-XX-XX-XX-XX (X is any hexadecimal digit). Only the PCs with MAC address listed can use the password to browse the built-in web pages to perform Administrator tasks while all the others will be blocked.

After click the Add button, your PC's MAC Address will be placed in the list above.

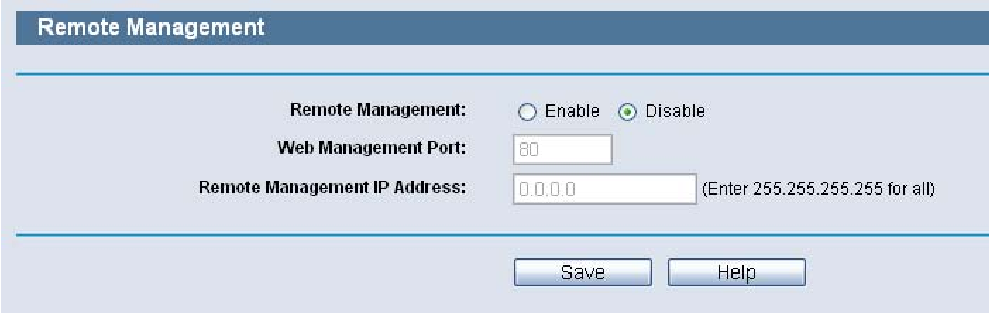
Click the Save button to save your settings.

NOTE: If your PC is blocked but you want to access the Router again, use a pin to press and hold the Reset Button (hole) on the back panel for about 5 seconds to reset the Router’s factory defaults on the Router’s Web-Based Utility.

REMOTE MANAGEMENT

Choose menu “Security->Remote Management”, you can configure the Remote Management function in the screen as shown in the following figure. This feature allows you to manage your Router from a remote location via the Internet.

Figure 106: Remote Management


Remote Management

Remote Management: ○ Enable ● Disable
Web Management Port: 80
Remote Management IP Address: 0.0.0.0 (Enter 255.255.255.255 for all)

- **Web Management Port** - Web browser access normally uses the standard HTTP service port 80. This Router's default remote management web port number is 80. For greater security, you can change the remote management web port to a custom port by entering that number in the box provided. Choose a number between 1 and 65534 but do not use the number of any common service port.

- **Remote Management IP Address** - This is the current address you will use when accessing your Router from the Internet. This function is disabled when the IP address is set to the default value of 0.0.0.0. To enable this function change 0.0.0.0 to a valid IP address. If set to 255.255.255.255, then all the hosts can access the Router from internet.

NOTE: To access the Router, you should type your Router's WAN IP address into your browser's address (in IE) or Location (in Navigator) box, followed by a colon and the custom port number. For example, if your Router's WAN address is 202.96.12.8, and the port number used is 8080, please enter http://202.96.12.8:8080 in your browser. Later, you may be asked for the Router's password. After successfully entering the username and password, you will be able to access the Router's web-based utility.

NOTE: Be sure to change the Router's default password to a very secure password.

A FAQ

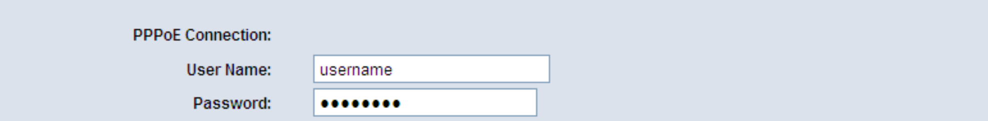
How do I configure the Router to access Internet by ADSL users?

1. First, configure the ADSL Modem configured in RFC1483 bridge model.

2. Connect the Ethernet cable from your ADSL Modem to the WAN port on the Router. The telephone cord plugs into the Line port of the ADSL Modem.

3. Login to the Router, click the "Network" menu on the left of your browser, and click "WAN" submenu. On the WAN page, select "PPPoE" for WAN Connection Type. Type user name in the "User Name" field and password in the "Password" field, finish by clicking "Connect".

Figure 107: PPPoE Connection Type



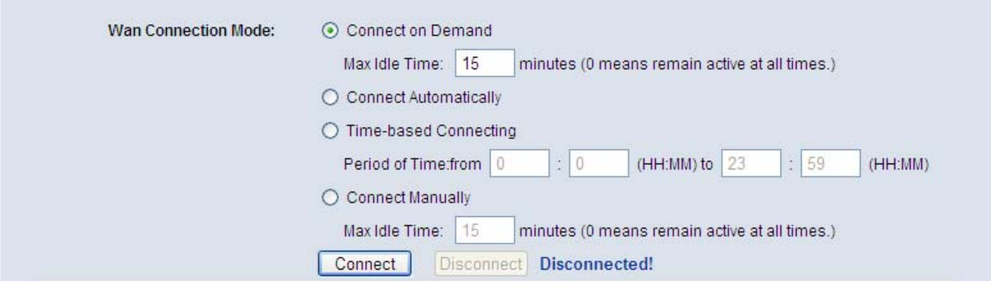
PPPoE Connection:

User Name: username

Password: ••••••••

4. If your ADSL lease is in "pay-according-time" mode, select "Connect on Demand" or "Connect Manually" for Internet connection mode. Type an appropriate number for "Max Idle Time" to avoid wasting paid time. Otherwise, you can select "Auto-connecting" for Internet connection mode.

Figure 108: PPPoE Connection Mode



Wan Connection Mode:
● Connect on Demand
Max Idle Time: 15 minutes (0 means remain active at all times.)
○ Connect Automatically
○ Time-based Connecting
Period of Time:from 0 : 0 (HH:MM) to 23 : 59 (HH:MM)
○ Connect Manually
Max Idle Time: 15 minutes (0 means remain active at all times.)

Disconnected!

NOTE: Sometimes the connection cannot be disconnected although you specify a time to Max Idle Time, since some applications is visiting the Internet continually in the background.

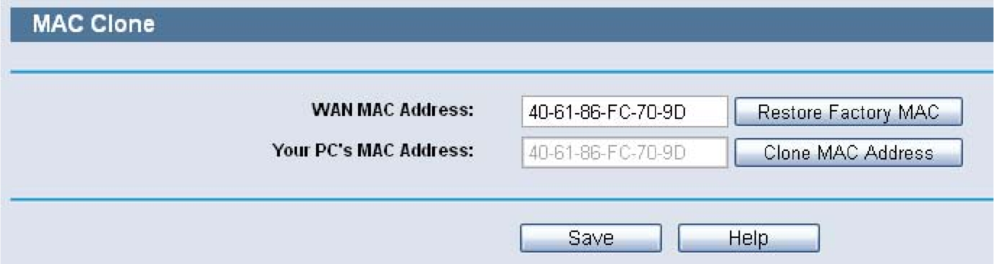
NOTE: If you are a Cable user, please configure the Router following the above steps.

How do I configure the Router to access Internet by Ethernet users?

1. Login to the Router, click the “Network” menu on the left of your browser, and click "WAN" submenu. On the WAN page, select “Dynamic IP” for "WAN Connection Type", finish by clicking “Save”.

2. Some ISPs require that you register the MAC Address of your adapter, which is connected to your cable/DSL Modem during installation. If your ISP requires MAC register, login to the Router and click the "Network" menu link on the left of your browser, and then click "MAC Clone" submenu link. On the "MAC Clone" page, if your PC’s MAC address is proper MAC address, click the "Clone MAC Address" button and your PC’s MAC address will fill in the "WAN MAC Address" field. Or else, type the MAC Address into the "WAN MAC Address" field. The format for the MAC Address is XX-XX-XX-XX-XX-XX. Then click the "Save" button. It will take effect after rebooting.

Figure 109: MAC Clone



MAC Clone

WAN MAC Address: 40-61-86-FC-70-9D

Your PC's MAC Address: 40-61-86-FC-70-9D

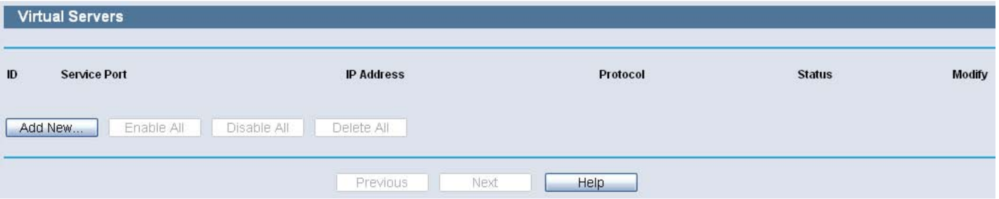
I want to use Netmeeting, what do I need to do?

1. If you start Netmeeting as a host, you don’t need to do anything with the Router.

2. If you start as a response, you need to configure Virtual Server or DMZ Host and make sure the H323 ALG is enabled.

3. How to configure Virtual Server: Log in to the Router, click the “Special Application” menu on the left of your browser, and click "Virtual Servers" submenu. On the "Virtual Servers" page, Click the Add New button. Then on the “Add or Modify a Virtual Server Entry” page, enter “1720” for the “Service Port” blank, and your IP address for the “IP Address” blank, taking 192.168.2.169 for an example, remember to Enable and Save.

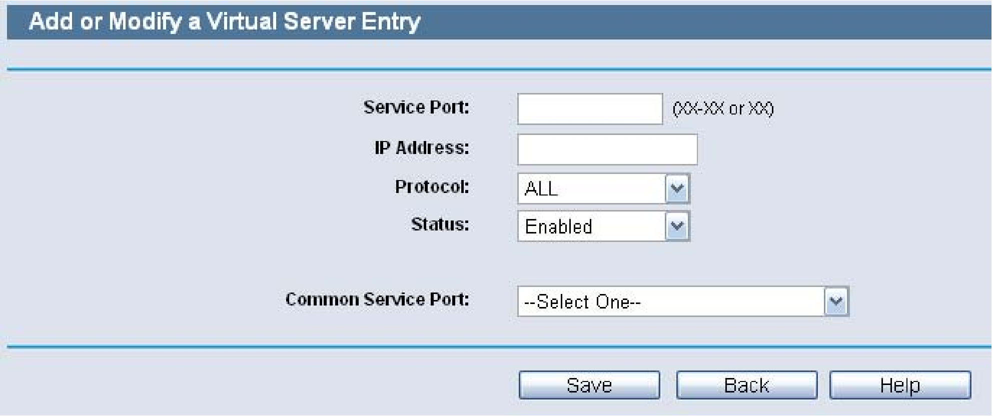
Figure 110: Virtual Servers



Virtual Servers

ID	Service Port	IP Address	Protocol	Status	Modify

Figure 111: Virtual Servers



Add or Modify a Virtual Server Entry

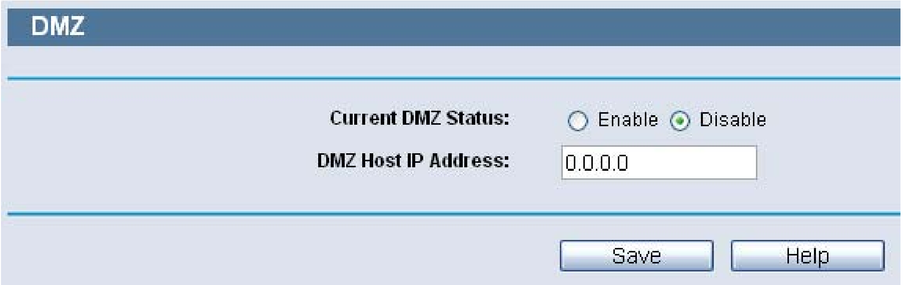
Service Port: (XX-XX or XX)
IP Address:
Protocol: ALL
Status: Enabled

Common Service Port: --Select One--

NOTE: Your opposite side should call your WAN IP, which is displayed on the "Status" page.

4. How to enable DMZ Host: Log in to the Router, click the "Special Application" menu on the left of your browser, and click "DMZ" submenu. On the "DMZ" page, click Enable radio button and type your IP address into the "DMZ Host IP Address" field, using 192.168.2.169 as an example, remember to click the Save button.

Figure 112: DMZ

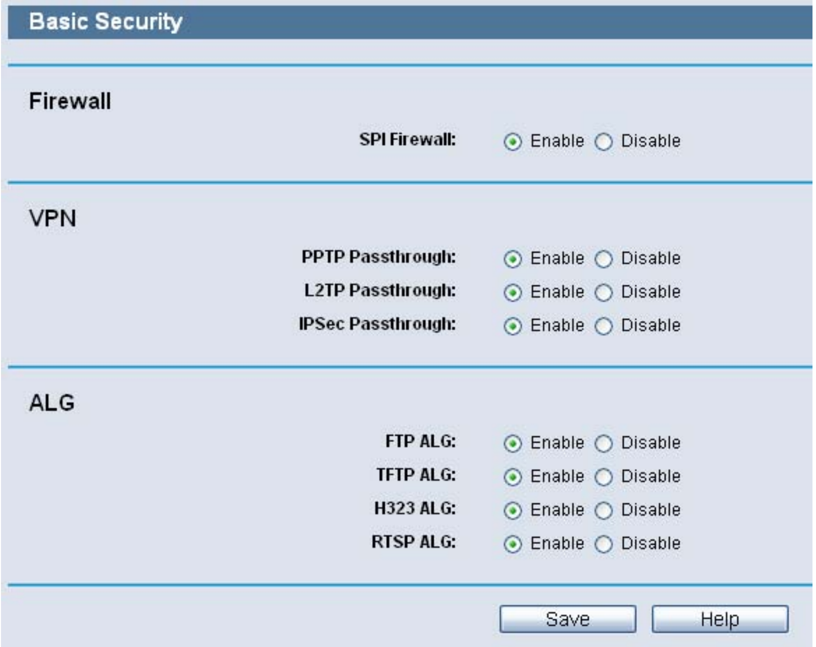


DMZ

Current DMZ Status: ○ Enable ● Disable
DMZ Host IP Address: 0.0.0.0

5. How to enable H323 ALG: Log in to the Router, click the "Security" menu on the left of your browser, and click "Basic Security" submenu. On the "Basic Security" page, check the Enable radio button next to H323 ALG. Remember to click the Save button.

Figure 113: Basic Security



Basic Security

Firewall

SPI Firewall: ● Enable ○ Disable

VPN

PPTP Passthrough: ● Enable ○ Disable

L2TP Passthrough: ● Enable ○ Disable

IPSec Passthrough: ● Enable ○ Disable

ALG

FTP ALG: ● Enable ○ Disable

TFTP ALG: ● Enable ○ Disable

H323 ALG: ● Enable ○ Disable

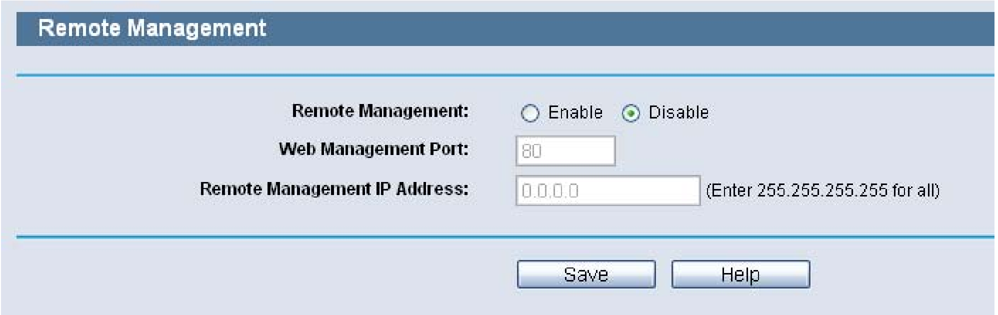
RTSP ALG: ● Enable ○ Disable

I want to build a WEB Server on the LAN, what should I do?

1. Because the WEB Server port 80 will interfere with the WEB management port 80 on the Router, you must change the WEB management port number to avoid interference.

2. To change the WEB management port number: Log in to the Router, click the “Security” menu on the left of your browser, and click "Remote Management" submenu. On the "Remote Management" page, type a port number except 80, such as 88, into the "Web Management Port" field. Click Save and reboot the Router.

Figure 114: Remote Management



Remote Management

Remote Management: ○ Enable ● Disable

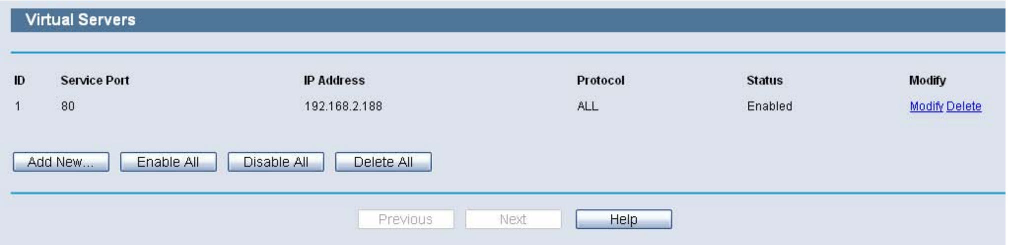
Web Management Port: 80

Remote Management IP Address: 0.0.0.0 (Enter 255.255.255.255 for all)

NOTE: If the above configuration takes effect, to configure to the Router by typing http://192.168.2.1:88 (the Router’s LAN IP address: Web Management Port) in the address field of the Web browser.

3. Log in to the Router, click the “Special Application” menu on the left of your browser, and click the "Virtual Servers" submenu. On the "Virtual Servers" page, Click the Add New button, then on the “Add or Modify a Virtual Server” page, enter “80” into the blank next to the “Service Port”, and your IP address next to the “IP Address”, assuming 192.168.2.188 for an example, remember to Enable and Save.

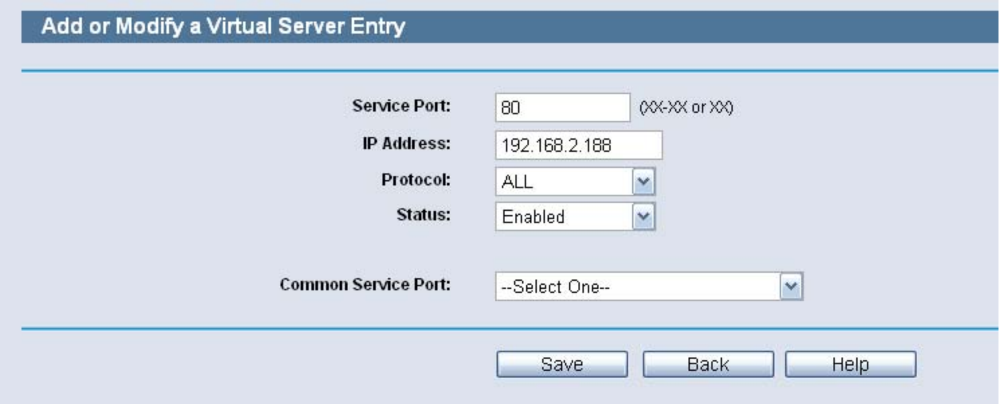
Figure 115: Virtual Servers



Virtual Servers

ID	Service Port	IP Address	Protocol	Status	Modify
1	80	192.168.2.188	ALL	Enabled	Modify Delete

Figure 116: Add or Modify a Virtual Server Entry



Add or Modify a Virtual Server Entry

Service Port: 80 (XX-XX or XX)
IP Address: 192.168.2.188
Protocol: ALL
Status: Enabled

Common Service Port: --Select One--

The wireless stations cannot connect to the Router.

1. Make sure the "Wireless Router Radio" is enabled.

2. Make sure that the wireless stations' SSID accord with the Router's SSID.

3. Make sure the wireless stations have right KEY for encryption when the Router is encrypted.

4. If the wireless connection is ready, but you can’t access the Router, check the IP Address of your wireless stations.

B CONFIGURING THE PCS

In this section, we'll introduce how to install and configure the TCP/IP correctly in Windows XP. First make sure your Ethernet Adapter is working, refer to the adapter's manual if needed.

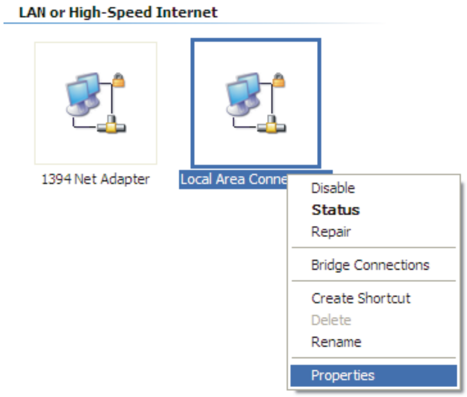
1. Install TCP/IP component

   a. On the Windows taskbar, click the Start button, point to Settings, and then click Control Panel.

   b. Click the Network and Internet Connections icon, and then click on the Network Connections tab in the appearing window.

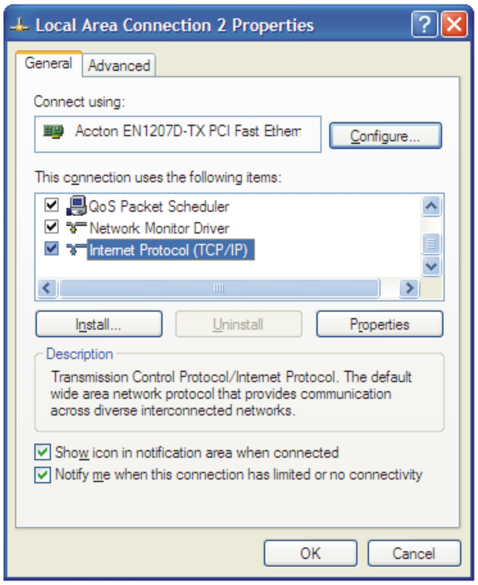
   c. Right click the icon that showed below, select Properties on the prompt page.

Figure 117: Internet Connection



   d. In the prompt page that showed below, double click on the Internet Protocol (TCP/IP).

Figure 118: Select TCP/IP



Local Area Connection 2 Properties

Connect using:

Accton EN1207D-TX PCI Fast Etherr

This connection uses the following items:

☑ QoS Packet Scheduler
☑ Network Monitor Driver
☑ Internet Protocol (TCP/IP)

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

☑ Show icon in notification area when connected
☑ Notify me when this connection has limited or no connectivity

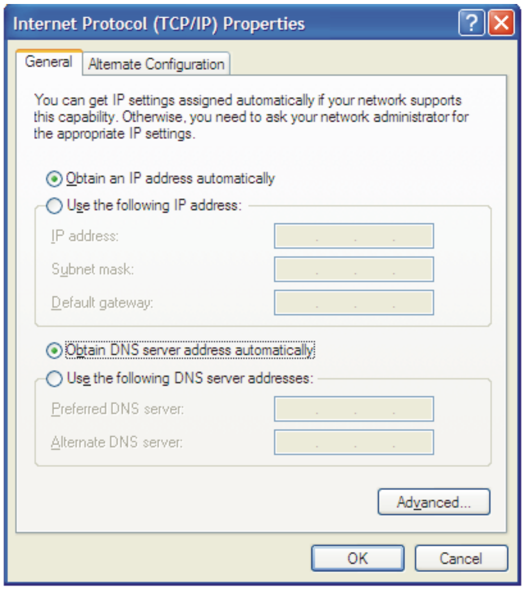
1.5 The following TCP/IP Properties window will display and the IP Address tab is open on this window by default.

Now you have two ways to configure the TCP/IP protocol below:

Setting IP address automatically

Select Obtain an IP address automatically, Choose Obtain DNS server automatically, as shown in the Figure below:

Figure 119: Obtain an IP address automatically



Internet Protocol (TCP/IP) Properties

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically
○ Use the following IP address:

IP address: . . .
Subnet mask: . . .
Default gateway: . . .

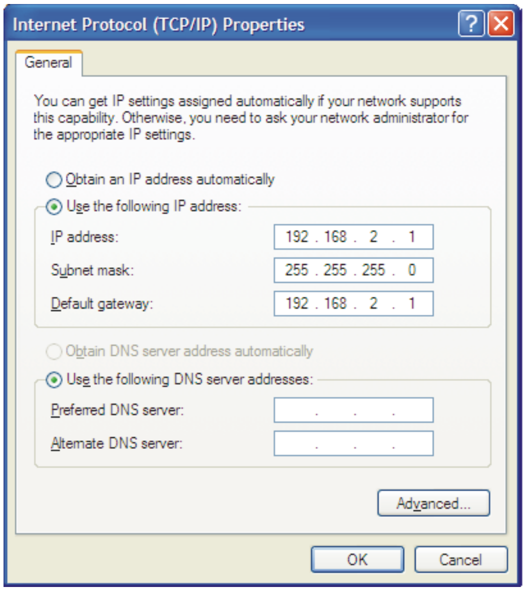
● Obtain DNS server address automatically
○ Use the following DNS server addresses:

Preferred DNS server: . . .
Alternate DNS server: . . .

Setting IP address manually

1. Select Use the following IP address radio button. And the following items available
2. If the Router's LAN IP address is 192.168.2.1, type IP address is 192.168.2.x (x is from 2 to 254), and Subnet mask is 255.255.255.0.
3. Type the Router’s LAN IP address (the default IP is 192.168.2.1) into the Default gateway field.
4. Select Use the following DNS server addresses radio button. In the Preferred DNS Server field you can type the DNS server IP address, which has been provided by your ISP.

Figure 120: Use the Following IP



Internet Protocol (TCP/IP) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 2 . 1

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 192 . 168 . 2 . 1

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

C Hardware Specifications

Standards	IEEE 802.3 10BASE-T IEEE 802.3u 100BASE-TX IEEE 802.3ab 1000BASE-T 802.11b 802.11g 802.11n
Protocol	TCP/IP, PPPoE, DHCP, ICMP, NAT, SNTP
Number of Ports	1 10/100/1000 Mbps Auto-Negotiation WAN RJ-45 port 4 10/100/1000 Mbps Auto-Negotiation LAN RJ-45 ports supporting Auto MDI/MDIX 1 USB 2.0 port
Cabling Type	10BASE-T: UTP Category 3, 4, 5 cable (maximum 100 m) EIA/TIA-568 100 STP (maximum 100 m) 100BASE-TX: UTP Category 5, 5e cable (maximum 100 m) EIA/TIA-568 100 STP (maximum 100 m) 1000BASE-TX: UTP Category 5e, 6 cable (maximum 100 m) EIA/TIA-568 100 STP (maximum 100 m)
LED Indicators	Power, System, WLAN, WAN, LAN (1-4), USB, WPS
Frequency Band	2.4 ~ 2.4835 GHz
Radio Data Rate	11b: 11/5.5/2/1M (Automatic) 11g: 54/48/36/24/18/12/9/6M (Automatic) 11n: up to 300 Mbps (Automatic)
Channels	13
Frequency Expansion	DSSS (Direct Sequence Spread Spectrum)

MODULATION	DBPSK, DQPSK, CCK, OFDM, 16-QAM, 64-QAM
SECURITY	WEP/WPA/WPA2/WPA2-PSK/WPA-PSK
SENSITIVITY @PER	270M: -68dBm@10% PER; 130M: -68dBm@10% PER 108M: -68dBm@10% PER; 54M: -68dBm@10% PER 11M: -85dBm@8% PER; 6M: -88dBm@10% PER 1M: -90dBm@8% PER
RF POWER	20dBm (max EIRP)
ANTENNA GAIN	3dBi*3
TEMPERATURE	Operating: 0 °C to 40 °C (32 to 104 °F) Storage: -40 °C to 70 °C (-40 to 158 °F)
HUMIDITY	Operating: 10% to 90% (non-condensing) Storge: 5%-90% (non-condensing)

GLOSSARY

IEEE 802.11B A wireless standard that supports wireless communications in the 2.4 GHz band using Direct Sequence Spread Spectrum (DSSS). The standard provides for data rates of 1, 2, 5.5, and 11 Mbps.

IEEE 802.11G A wireless standard that supports wireless communications in the 2.4 GHz band using Orthogonal Frequency Division Multiplexing (OFDM). The standard provides for data rates of 6, 9, 12, 18, 24, 36, 48, 54 Mbps. IEEE 802.11g is also backward compatible with IEEE 802.11b.

IEEE 802.11N A wireless standard that supports wireless communications in the 2.4 GHz band using Orthogonal Frequency Division Multiplexing (OFDM). The standard provides for data rates of 27, 54, 81, 108, 162, 216, 243, 270, 300 Mbps. IEEE 802.11n is also backward compatible with IEEE 802.11b/g.

DDNS (DYNAMIC DOMAIN NAME SYSTEM) The capability of assigning a fixed host and domain name to a dynamic Internet IP Address.

DHCP Dynamic Host Configuration Protocol: Provides a framework for passing configuration information to hosts on a TCP/IP network. DHCP is based on the Bootstrap Protocol (BOOTP), adding the capability of automatic allocation of reusable network addresses and additional configuration options.

DMZ (DEMILITARIZED ZONE) A Demilitarized Zone allows one local host to be exposed to the Internet for a special-purpose service such as Internet gaming or videoconferencing.

DNS (DOMAIN NAME SYSTEM) An Internet Service that translates the names of websites into IP addresses.

DOMAIN NAME A descriptive name for an address or group of addresses on the Internet.

DSL (DIGITAL SUBSCRIBER LINE) A technology that allows data to be sent or received over existing traditional phone lines.

ISP (Internet Service Provider) A company that provides access to the Internet.

MTU (Maximum Transmission Unit) The size in bytes of the largest packet that can be transmitted.

NAT (Network Address Translation) NAT technology translates IP addresses of a local area network to a different IP address for the Internet.

PPPoE (Point to Point Protocol over Ethernet) PPPoE is a protocol for connecting remote hosts to the Internet over an always-on connection by simulating a dial-up connection.

SSID A Service Set Identification is a thirty-two character (maximum) alphanumeric key identifying a wireless local area network. For the wireless devices in a network to communicate with each other, all devices must be configured with the same SSID. This is typically the configuration parameter for a wireless PC card. It corresponds to the ESSID in the wireless Access Point and to the wireless network name.

WEP (Wired Equivalent Privacy) A data privacy mechanism based on a 64-bit or 128-bit or 152-bit shared key algorithm, as described in the IEEE 802.11 standard.

Wi-Fi A trade name for the 802.11b wireless networking standard, given by the Wireless Ethernet Compatibility Alliance (WECA, see http://www.wi-fi.net), an industry standards group promoting interoperability among 802.11b devices.

WLAN (Wireless Local Area Network) A group of computers and associated devices communicate with each other wirelessly, which network serving users are limited in a local area.

Edge-corE® NETWORKS

SMC® Networks

Headquarters & Sub-Sahara Africa Office

No. 1, Creation Rd. III
Hsinchu Science Park
Taiwan 30077
Tel: +886 3 5770270
Fax: +886 3 5780764

Asia-Pacific Office

1 Coleman Street
#07-09, The Adelphi
Singapore 179803
Tel: +65-63387667
Fax: +65-63387767

Europe & N. Africa Office

C/Fructuós Gelabert 6-8, 2°, 2ª
Edificio Conata II
08970 Sant Joan Despí
Barcelona, Spain
Tel: +34 93 477 4920

Middle East Office

Office No. 416, Le Solarium Bldg
Dubai Silicon Oasis
Dubai, U.A.E.
Tel: +971-4-3564800
Fax:+971-4-3564801

North America Office

20 Mason
Irvine CA 92618 U.S.A.
Tel: +1 (949) 679-8000

SMC NETWORKS TECHNICAL SUPPORT

From Singapore in English and 中文 (Mon.-Fri. 9 AM to 5 PM)
Tel: +65-63387667, Ext. 4

From the United Arab Emirates in English (Sun.-Thu. 9 AM to 6 PM)
Tel: +971 800 222866/+971 4 3564810

From U.S.A. and Canada (24 hours a day, 7 days a week)
Tel: +1 (800) SMC-4-YOU/+1 (949) 679-8000 Fax: +1 (949) 679-1481

English: Technical Support information available at www.smc.com

English: (for Asia-Pacific): Technical Support information at www.smc-asia.com

English: (for Middle East): Technical Support information at muneer@smc-asia.com

Deutsch: Technischer Support und weitere Information unter www.smc.com

Español: En www.smc.com Ud. podrá encontrar la información relativa a servicios de soporte técnico

Français: Informations Support Technique sur www˙smc˙com

Português: Informações sobre Suporte Técnico em www.smc.com

Italiano: Le informazioni di supporto tecnico sono disponibili su www.smc.com

Svenska: Information om Teknisk Support finns tillgängligt på www.smc.com

Nederlands: Technische ondersteuningsinformatie beschikbaar op www·smc·com

Polski: Informacje o wsparciu technicznym sa dostepne na www·smc·com

Čeština: Technicka podpora je dostupna na www·smc·com

Magyar: Műszaki tamogat informacio elerhető -on www.smc.com

简体中文：技术支持讯息可通过www.smc-prc.com查询

繁體中文：產品技術支援與服務請上 www.smcnetworks.com.tw

ไทย: สามารถหาข้อมัลทางด้านเทคนิคได้ที่ www.smc-asia.com

한국어: 기술지원관련 정보는 www.smcnetworks.co.kr 을 참고하시기 바랍니다

INTERNET
E-mail address: www.smc.com→ Support→ By email
Driver updates: www smc com→ Support→ Downloads

SMCWGBR14-N2