

4.8.2 FTP Server

You can configure a FTP server on this page. Follow the instructions below to set up your FTP server:

- 1.Plug an external USB hard disk drive or USB flash drive into this Router.
- 2.Click the **Enable/Disable** radio box to enable/disable internet access to ftp from WAN port.
- 3.Change the **Service port** to specify a port for ftp server to use (default 21).
- 4.The **Internet Address** displays the WAN IP address of this router, so that others can access ftp through this address.
- 5.If WAN type is PPPOE/PPTP/L2TP, there would be two connections. Therefore, users can access the ftp server via two connections. Users in a private LAN can access ftp server via **Public Address** while internet users can access ftp server via **Internet Address**.
- 6.Click the **Start** button to start the ftp server.

On this page, when a share folder is added, you can view its display name, volume partition, folder path and you can delete the share folder by clicking the **delete** button.

FTP Server Configuration

Server Status: **Stopped**

Internet Access: Enable Disable

Service Port: **21** (The default is 21, do not change unless necessary)

Internet Address: **192.168.54.154**

Name	Partition	Folder	Modify
No folders set. Plug an external USB drive into this Router, and make sure it is connected to the Router.			

- **Name** - This folder's display name.
- **Partition** - The volume that the folder resides.
- **Folder** - The real full path of the specified folder.
- **Modify** - You can edit the share folder by clicking the **modify** button.
- **Delete** - You can delete the share folder by clicking the **delete** button.

Note:

The max share folders number is 10. If you want to share a new folder when the number has reached 10, you can delete a share folder and then add a new one.

If you want to change the FTP settings, you need to restart FTP Server to enable the Settings Change.

4.8.3 Media Server

You can configure media server on this page.

Follow the instructions below to set up your media server:

1. Plug an external USB hard disk drive or USB flash drive into this Router.
2. Click the **Start** button to initiate the media server.
3. Click the **Add share folder** button to specify a folder as the search path of media server.
4. Click the **Scan All** button to scan all the share folders immediately. You can also select **Auto-scan** and at same time choose the auto scan interval time from the pull-down list, and then click the **Save** button to save the new settings. In this case, the media server will auto scan the share folder.

On this page, when a share folder is added, you can view its display name, file system type, folder path and you can delete the share folder by clicking the **delete** button as shown in the corresponding dialog box.



- **Name** - This folder's display name.
- **File System** - The file system on the partition can be FAT32 or NTFS.
- **Folder** - The real full path of the specified folder.
- **Delete** - You can delete the share folder by clicking the delete button.

Note:

The max. share folders number is 3. If you want to share a new folder when the numbers have reached to be 3, you can delete a share folder and then add a new one.

Click the **Start** button to start the media server.

Click the **Stop** button to stop the media server.

Click the **Scan All** button to scan all the share folders immediately.

Click the **delete** button to delete the specified share folder.

4.8.4 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 stored in the USB drive. There are two Network Sharing users that can access the shares. They are Administrator and Guest. Administrator has read/write privileges 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.

User Accounts

Administrator (Read & Write)

User Name:

Password:

Confirm Password:

Guest (Read Only)

User Name:

Password:

Confirm Password:

Figure 4-32 User Accounts

- * **User Name** - Type the user name that you want to give access to the USB drive. The user name should consist of alphanumeric characters, not exceeding 15 in length.
- * **Password** - Enter the password in the Password field. The password should consist of alphanumeric characters, not exceeding 15 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 store 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. Next, **net use \\192.168.0.1/delete/yes** and press **Enter**. (192.168.0.1 is your Router's LAN IP address.)

4.9 Forwarding



Figure 4-33 The Forwarding menu

There are four submenus under **Forwarding** (shown in Figure 4-33): **Virtual Servers**, **Port Triggering**, **DMZ** and **UPnP**. Click on any of these items in order to configure the corresponding function.

4.9.1 Virtual Servers

Go to "**Forwarding → Virtual Servers**" in the menu, in order to visualize and add virtual servers, as shown in the following screen (Figure 4-34). 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.

ID	Service Port	Internal Port	IP Address	Protocol	Status	Modify
1	21	21	192.168.0.101	ALL	Enabled	Modify Delete

Figure 4-34 Virtual Servers

- * **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.
- * **Internal Port** - The Internal Service Port number of the PC running the service application. You can leave it blank if the **Internal Port** is the same as the **Service Port**, or enter a specific port number when **Service Port** is a single one.
- * **Protocol** - The protocol used for this application, either **TCP**, **UDP**, or **All** (all protocols supported by the router).
- * **Status** - This field displays either **Enabled** or **Disabled**, as the current status for the device.

To setup a virtual server entry:

1. Click the **"Add New..."** button (as in Figure 4-35).
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. Click on the check box to **Enable** the virtual server.
6. Click the **Save** button.

The screenshot shows a web form titled "Add or Modify a Virtual Server Entry". The form contains the following fields and controls:

- Service Port:** A text input field with a placeholder "(00-XX or XX)".
- Internal Port:** A text input field with a placeholder "(XX, Only valid for single Service Port or leave it blank)".
- IP Address:** A text input field.
- Protocol:** A dropdown menu with "ALL" selected.
- Status:** A dropdown menu with "Enabled" selected.
- Common Service Port:** A dropdown menu with "--Select One--" selected.
- At the bottom, there are two buttons: "Save" and "Back".

Figure 4-35 Add or Modify a Virtual Server Entry

Note:

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

To modify or delete an existing entry:

1. Click the **Modify** button next to in the entry you want to change. If you want to erase this entry, click on **Delete**.
2. Proceed with the changes you want to make.
3. Click the **Save** button.

Click the **Enable All** button to activate all entries
Click the **Disabled All** button to cancel all entries.
Click the **Delete All** button to erase all entries
Click the **Next** button to go to the following page
Click the **Previous** button to return to the last 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.

4.9.2 Port Triggering

Go to “**Forwarding** → **Port Triggering**” in the menu, in order to visualize and add port triggering, as shown in the next screen (Figure 4-36). 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 to let them work with a NAT router.

ID	Trigger Port	Trigger Protocol	Incoming Port	Incoming Protocol	Status	Modify
1	554	ALL	8970-8999	ALL	Enabled	Modify Delete

Figure 4-36 Port Triggering

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 - It displays the current status of this entry, either **Enabled** or **Disabled**.

To add a new rule, follow the steps below.

1. Click the **"Add New..."** button. The following screen will be displayed, as shown in Figure 4-37.
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 store the new rule.

The screenshot shows a web form titled "Add or Modify a Port Triggering Entry". The form contains the following fields and controls:

- Trigger Port:** A text input field.
- Trigger Protocol:** A dropdown menu with "ALL" selected.
- Incoming Ports:** A text input field.
- Incoming Protocol:** A dropdown menu with "ALL" selected.
- Status:** A dropdown menu with "Enabled" selected.
- Common Applications:** A dropdown menu with "--Select One--" selected.
- Buttons:** "Save" and "Back" buttons at the bottom.

Figure 4-37 Add or Modify a Triggering Entry

To modify or delete an existing entry:

1. Click the **Modify** button next to in the entry you want to change. If you want to erase this entry, click on **Delete**.
2. Proceed with the changes you want to make.
3. Click the **Save** button.

Click the **Enable All** button to activate all entries.
Click the **Disabled All** button to cancel all entries.
Click the **Delete All** button to erase all entries.

Note:

1. When the trigger connection is released, the corresponding opened ports will be closed.
2. Each rule allows only to be used by a single host on LAN synchronously. The trigger connection of other hosts on LAN will be refused.
3. Incoming Port Range cannot overlap each other.

4.9.3 DMZ (Demilitarized Zone)

Go to **“Forwarding → DMZ”**, in order to visualize and configure the DMZ host, as shown in the screen below (Figure 4-38). The DMZ host feature allows one local host to be exposed to the Internet so as to gain access to certain applications, 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 also have a new static IP Address assigned to it, because its IP Address may be changed when using the DHCP function.

DMZ

Current DMZ Status: Enable Disable

DMZ Host IP Address:

Save

Figure 4-38 DMZ

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:

Once you set the DMZ host, the firewall protection for that host will be disabled.

4.9.4 UPnP

Go to **“Forwarding → UPnP”** in the menu, in order to visualize the information related to the UPnP (Universal Plug and Play) feature, as shown in the screen below (Figure 4-39). The UPnP architecture allows any compatible device, such as Internet computers, to access the local host resources or other networking equipment, as needed. UPnP devices on the LAN can be automatically discovered using the UPnP application.

ID	App Description	External Port	Protocol	Internal Port	IP Address	Status
1	BtComet(192.168.0.100.23959)	23959	TCP	23959	192.168.0.100	Enabled
2	BtComet(192.168.0.100.23959)	23959	UDP	23959	192.168.0.100	Enabled

Figure 4-39 UPnP Setting

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

* **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 status is displayed in this field. "Enabled" means that the port is still active. Otherwise, the port is inactive.

Click **Refresh** to update the Current UPnP Settings List.

4.10 Security



Figure 4-40 Security menu

There are four submenus under the Security (shown in Figure 4-40): **Basic Security**, **Advanced Security**, **Local Management** and **Remote Management**. Click on any of these items in order to configure the corresponding function.

4.10.1 Basic Security

Go to “**Security** → **Basic Security**”, in order to configure the basic security settings, as shown in the screen below (Figure 4-37).

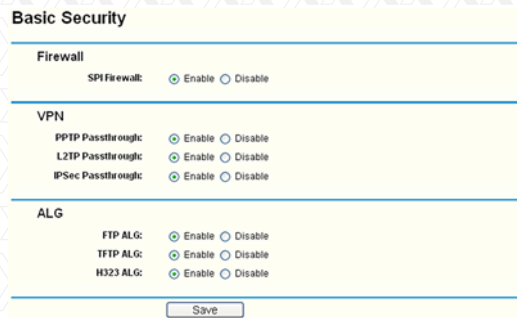


Figure 4-41 Basic Security

* **Firewall** - A firewall protects your network from the outside world. In this page, the user can enable or disable the router 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. enable or disable the router firewall.

* **VNP** - 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 its default configuration: **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 its default configuration: **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 its default configuration: **Enabled**.

* **ALG** - It is recommended to enable Application Layer Gateway (ALG) because it allows customized Network Address Translation (NAT) traversal filters to be plugged into the gateway, so as 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 its default configuration: **Enabled**.
- **TFTP ALG** - To allow TFTP clients and servers to transfer data across NAT, keep its default configuration: **Enabled**.
- **H323 ALG** - To allow Microsoft NetMeeting clients to communicate across NAT, keep its default configuration: **Enabled**.

Click the **Save** button to store your settings.

4.10.2 Advanced Security

Go to **“Security → Advanced Security”** in the menu, in order to protect the router from being attacked by TCP-SYN Flood, UDP Flood and ICMP-Flood, as shown in the following screen (Figure 4-42).

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

Save Blocked DoS Host List

Figure 4-42 Advanced Security

- * **Packets Statistics Interval (5~60)** - The default value is 10. Select the desired setting between 5 and 60 seconds from the drop-down list. This value determines the time interval between packets. 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 corresponding box to Enable or Disable this function. Only when DoS is enabled, flood filters will be effective.
Note:
You must first enable **Traffic Statistics** in "**System Tool** → **Traffic Statistics**" for the DoS Protection feature to work.
- * **Enable ICMP-FLOOD Attack Filtering** - Check this box to **Enable** or **Disable** the ICMP-FLOOD Attack Filtering.
- * **ICMP-FLOOD Packets Threshold (5~3600)** - The default value is 50. Select the desired setting 5 ~ 3600. When the current ICMP-FLOOD Packets number exceeds the set value, the router will immediately startup the blocking feature.
- * **Enable UDP-FLOOD Filtering** - Enable or Disable the UDP-FLOOD Filtering.
- * **UDP-FLOOD Packets Threshold (5~3600)** - The default value is 500. Select the desired setting between 5 ~ 3600. When the current UPD-FLOOD Packets number exceeds the set value, the router will immediately startup the blocking feature.
- * **Enable TCP-SYN-FLOOD Attack Filtering** - Check this box to Enable or Disable the TCP-SYN-FLOOD Attack Filtering.

- * **TCP-SYN-FLOOD Packets Threshold (5~3600)** - The default value is 50. Select the desired setting between 5 ~ 3600. When the current TCP-SYN-FLOOD Packets number exceeds the set value, the router will immediate startup the blocking feature.
- * **Ignore Ping Packet From WAN Port** - Check this box to Enable or Disable this option. The default setting is disabled. If enabled, the ping packet from the Internet cannot access the router.
- * **Forbid Ping Packet From LAN Port** - Check this box to **Enable** or **Disable** this option. The default setting is disabled. If enabled, the ping packet from LAN cannot access the router. This function can be used to defend the network against some viruses.

Click the **Save** button to store the settings.

Click the **DoS Host Block List** button to display the DoS host table with the items excluded.

4.10.3 Local Management

Go to "**Security → Local Management**" in the menu, in order to configure the management rule as shown in the screen below (Figure 4-43). The management feature allows you to deny computers in the LAN from accessing the Router.

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:

Figure 4-43 Local Management

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 (where X is any hexadecimal digit). Only the PCs with a 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 clicking the **Add** button, your PC’s MAC Address will be placed in the above list. Click the **Save** button to store 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 to its factory default values on the Web-Based Utility.

4.10.4 Remote Management

Go to “**Security → Remote Management**” in the menu, in order to configure the Remote Management feature, as shown in the screen below (Figure 4-44). This feature allows you to manage your router from a remote location via the Internet.

Remote Management

Web Management Port:

Remote Management IP Address: (Enter 255.255.255.255 for all)

Figure 4-44 Remote Management

- * **Web Management Port** - Web browser normally uses the standard HTTP port 80 for access. 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:

- 1) 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 to type the Router's password. After successfully entering the username and password, you will be able to access the router's web-based utility.
- 2) Be sure to change the router's default password to a more secure password.

4.11 Parental Control

Go to **"Parental Control"** in order to configure this monitoring feature, as shown in the screen below. (Figure 4-45). Parental Control can be used to monitor the internet activities of a child, limit his/her access to certain websites and to restrict the amount of time they spend surfing.

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:

ID	MAC address	Website Description	Schedule	Status	Modify
----	-------------	---------------------	----------	--------	--------

Page 1

Figure 4-45 Parental Control Settings

- * **Parental Control** - Check **Enable** if you want to activate this function; otherwise, check **Disable**.
- * **MAC Address of Parental PC** - In this field, enter the MAC address of the monitoring 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 enter this address into the **MAC Address of Parental PC** field above.
- * **Website Description** - Description of the allowed website for the monitored PC.
- * **Schedule** - The time period allowed for the monitored PC to have access to the Internet. For detailed information, please go to "**Access Control → Schedule**".
- * **Modify** - Use this link to edit or delete an existing entry.

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

1. Click the **Add New** button. The screen shown in figure 4-46 below will appear.
2. In the **MAC Address of Child PC** field, enter the MAC address of the PC (e.g. 00-11-22-33-44-AA) you want to control. 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 open the **Advanced Schedule Settings** page, and create the schedule you need.
6. In the Status field, select the **Enabled** or **Disabled** condition for that entry.
7. Click the **Save** button.

Click the **Enable All** button to activate all entries.
Click the **Disabled All** button to cancel all entries.
Click the **Delete All** button to erase all entries.
Click the **Next** button to go to the following page
Click the **Previous** button to return to the last page.

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:

Website Description:

Allowed Domain Name:

Effective Time:
The time schedule can be set in "Access Control->[Schedule](#)"

Status:

Figure 4-46 Add or Modify Parental Control Entry

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

1. Click "**Parental Control**" menu on the left to enter the Parental Control Settings page. Check Enable and enter the MAC address OO-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. Click the **Add New** button to create a new schedule, being identified as Schedule_1. The day is Sat, and the Time is all day-24 hours.
3. Click the "**Parental Control**" menu on the left to go back to the Add or Modify Parental Control Entry page:
 - Click the **Add New** button.
 - Enter OO-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 the "Schedule_1" you just created from the **Effective Time** drop-down list.
 - In **Status** field, select **Enable**.
4. Click Save to complete your settings. Return to the **Parental Control Settings** page to open the following list, as shown in figure 4-47.

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

[Add New...](#) [Enable All](#) [Disable All](#) [Delete All](#)

Figure 4-47 Parental Control Settings

4.12 Access Control



Figure 4-48 Access Control

There are four submenus under **Access Control** (Figure 4 48): **Rule**, **Host**, **Target** and **Schedule**. Click on any of these items in order to configure the corresponding function.

4.12.1 Rule

Go to "**Access Control → Rule**", in order to visualize and set Access Control rules in the screen below, as shown in Figure 4-49.

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
1	1	Host_1	Target_1	Schedule_1	Deny	Enabled	Edit Delete

ID To ID

Page **1**

Figure 4-49 Access Control Rule Management

- * **Enable Internet Access Control** - Check this box to enable the Internet Access Control feature, so that the Default Filter Policy can take effect.
- * **Rule Name** - The name of the rule is displayed here, which is unique.
- * **Host** - The host selected with the corresponding rule is displayed in this field.
- * **Target** - The target selected with the corresponding rule is displayed in this field.
- * **Schedule** - The schedule selected with the corresponding rule is displayed in this field.
- * **Action** - The action taken by the router to deal with the packets is displayed here. It could be **Allow** or **Deny**. **Allow** means that the router permits the packets to pass through. **Deny** means that the router is configured to reject the packets.
- * **Status** - This field displays the current status of the rule. **Enabled** means the rule will be applied.

Disabled means the rule will not take effect.

* **Modify** – Use this link to edit or delete an existing rule.

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

1. Click the **Add New** button. The screen shown in figure 4-50 below will appear.
2. Assign a name (e.g. Rule_1) to 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-down 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 the **Enabled** or **Disabled** condition for that entry.
8. Click the **Save** button.

Click the **Enable All** button to activate all entries.
Click the **Disabled All** button to cancel all entries.
Click the **Delete All** button to erase all entries.

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 following page, or click the **Previous** button to return to the last page.

Add or Modify Internet Access Control Entry

Rule Name:	<input type="text"/>
Host:	<input type="text"/> Click Here To Add New Host List
Target:	<input type="text" value="Any Target"/> Click Here To Add New Target List
Schedule:	<input type="text" value="Anytime"/> Click Here To Add New Schedule
Action:	<input type="text" value="Deny"/>
Status:	<input type="text" value="Enabled"/>

Figure 4-50 Add or Modify Internet Access Control Entry

For example: If you wish 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 **Saturdays and Sundays**, and forbid other hosts in the LAN from accessing the Internet, you should follow the steps as described below:

1. Click "**Access Control → Host**" on the left to open the **Host Settings** page. Add a new entry identified as Host_1, using 00-11-22-33-44-AA as the MAC Address.
2. Click "**Access Control → Target**" on the left to enter the **Target Settings** page. Add a new identified as Target_1, using www.google.com as the Domain Name.
3. Click "**Access Control → Schedule**" on the left to open the **Schedule Settings** page. Add a new entry identified as Schedule_1. The days are Sat and Sun, Start Time is 1800 and Stop Time is 2000.
4. Click "**Access Control → Rule**" on 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 insert a new rule as follows:

- In the **Rule Name** field, create a name for the rule. Note that this name should be unique, for example Rule_1.
- In the **Host** field, select Host_1.
- In the **Target** field, select Target_1.
- In the **Schedule** field, select Schedule_1.
- In the **Action** field, select Allow.
- In the **Status** field, select Enable.
- Click **Save** to complete your settings.

Then you will go back to the Access Control Rule Management page where the list below will be displayed.

ID	Rule Name	Host	Target	Schedule	Action	Status	Modify
1	1	Host_1	Target_1	Schedule_1	Deny	Enabled	Edit Delete

4.12.1.1.1. Host

Go to menu **“Access Control → Host”**, in order to visualize and set a Host list in the screen, as shown in figure 4-51 below. The host list is necessary for the Access Control Rule.

Host Settings		
ID	Host Description	Information
1	Host	IP: 192.168.0.2 - 192.168.0.23

[Add New...](#) [Delete All](#)

Previous Next Page 1

Figure 4-51 Host Settings

- * **Host Description** - The description of the host, which is unique, is displayed here.
- * **Information** - The data about the host is displayed in this field. It can be IP or MAC.
- * **Modify** - Use this link edit 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 an IP Address, the screen shown in figure 4-52 will be opened.
 - 1) In the **Host Description** field, create a unique description for the host (e.g. Host_1).
 - 2) In the **LAN IP Address** field, enter the IP address.
 - If you select the MAC Address, the screen shown in figure 4-53 will be opened.
 - 1) In the **Host Description** field, create a unique description for the host (e.g. Host_1).
 - 2) In the **MAC Address** field, enter the corresponding address.
 3. Click the **Save** button to complete your settings.
- Click the **Delete All** button to erase all the entries in the table.
- Click the **Next** button to go to the following page, or click the **Previous** button to return to the last page.

Add or Modify a Host Entry

Mode: IP Address

Host Description: Host_1

LAN IP Address: 192.168.0.1 - 192.168.0.23

Save Back

Figure 4-52 Add or Modify a Host Entry

Add or Modify a Host Entry

Mode:

Host Description:

MAC Address:

Figure 4-53 Add or Modify a Host Entry

For example: If you wish to restrict the internet activities of the host with MAC address 00-11-22-33-44-AA, first you must complete the steps as described below:

1. Click the **Add New** button in figure 4-51 to open the **Add or Modify a Host Entry** page.
2. In the **Mode** field, select **MAC Address** from the drop-down list.
3. In the **Host Description** field, create a unique description for the host (e.g. **Host_1**).
4. In the **MAC Address** field, enter 00-11-22-33-44-AA.
5. Click **Save** to complete your settings.

When done, you will return to the Host Settings page, where the following list will be displayed.

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

4.12.2 Target

Go to menu **“Access Control → Target”**, in order to visualize and set a Target list, as shown in the screen below (figure 4-54). The target list is necessary for the Access Control Rule.

Target Settings

ID	Target Description	Information	Modify
1	Target	191.168.0.2 - 192.168.0.2321 - 23TCP	Edit Delete

Current No. 1 Page

Figure 4-54 Target Settings

- * **Target Description** - The target name, which is unique, is displayed in this field.
- * **Information** - The target can be an IP address, port, or domain name.
- * **Modify** - Use this link to edit 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 Domain Name.
 - If you select IP Address, the screen shown in figure 4-55 will be displayed.
 - 1) In the **Target Description** field, create a unique description for the target (e.g. Target_1).
 - 2) In the **IP Address** field, enter the corresponding address for the target.
 - 3) Select a common service from the **Common Service Port** from the drop-down list, so that the **Target Port** will be automatically filled out. If the **Common Service Port** drop-down list does not have the service you want, specify the Target Port manually.
 - 4) In the **Protocol** field, select **TCP**, **UDP**, **ICMP** or **ALL**.
 - If you select Domain Name, the screen shown in figure 4-56 will be displayed.
 - 1) In the **Target Description** field, create a unique name for the target (e.g. Target_1).

- 2) Enter the domain name, either the full name or the keywords (for example google) in the **Domain Name** blank field. Any domain name with keywords in it (www.google.com, www.google.cn) will be blocked or allowed. You can enter up to 4 domain names.
 3. Click the **Save** button.
- Click the **Delete All** button to erase all the entries in the table.
- Click the **Next** button to go to the following page, or click the Previous button return to the last page.

Add or Modify an Access Target Entry

Mode: IP Address

Target Description: [text input]

IP Address: [text input] - [text input]

Target Port: [text input] - [text input]

Protocol: ALL

Common Service Port: --please select--

Save Back

Figure 4-55 Add or Modify an Access Target Entry

Add or Modify an Access Target Entry

Mode: Domain Name

Target Description: [text input]

Domain Name: [text input]
[text input]
[text input]
[text input]

Save Back

Figure 4-56 Add or Modify an Access Target Entry

For example: If you wish to restrict the internet activities of the host with MAC address 00-11-22-33-44-AA in the LAN, so that it is able to access **www.google.com** only, first you must complete the steps as described below.

1. Click the **Add New** button in figure 4-54 to open the **Add or Modify an Access Target Entry** page.
2. In the **Mode** field, select **Domain Name** from the drop-down list.
3. In the **Target Description** field, create a unique description to identify the target (e.g. Target_1).
4. In the **Domain Name** field, enter www.google.com.
5. Click **Save** to complete your settings.

When done, you will return to the Target Settings page, where following list will be displayed.

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

4.12.3 Schedule

Go to “**Access Control → Schedule**” in the menu, in order to visualize and set a Schedule list in the next screen, as shown in figure 4-57. The Schedule list is necessary to establish the Access Control Rule.

Schedule Settings				
ID	Schedule Description	Day	Time	Modify
1	Schedule	Sat	0000 - 2400	Edit Delete

Page 1

Figure 4-57 Schedule Settings

- * **Schedule Description** - The name assigned to the schedule, which is unique, is displayed in this field.
- * **Day** - The day(s) of the week is shown in this field.
- * **Time** - The 24-hour period of the day is displayed in this field.
- * **Modify** – Use this link to edit or delete an existing schedule.

To add a new schedule, follow the steps below.

1. Click the **Add New** button, as shown in figure 4-57. The screen displayed in figure 4-58 will open in this step.
2. In the **Schedule Description** field, create a unique name to identify the schedule (e.g. Schedule_1).
3. In the **Day** field, select the day or days you want to include.
4. In the **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 your settings.

Click the **Delete All** button to erase all the entries in the table.

Click the **Next** button to go to the following page, or click the **Previous** button return to the last page.

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: (H-MM)

Stop Time: (H-MM)

Figure 4-58 Advanced Schedule Settings

For example: If you wish to restrict the internet activities of the host with MAC address 00-11-22-33-44-AA, so that it is able to access www.google.com only from 18:00 to 20:00 on **Saturdays** and **Sundays**, you must first complete the steps as described below:

1. Click the **Add New** button shown in figure 4-57 to enter to the **Advanced Schedule Settings** page.
2. In the **Schedule Description** field, create a unique name to identify the schedule (e.g. Schedule_1).
3. In the **Day** field, check the **Select Days** radio button, and choose Sat and Sun next.
4. In the **Time** field, enter 1800 in the **Start Time** field, and 2000 in the **Stop Time** field.
5. Click **Save** to complete your settings.

When done, you will return to the Schedule Settings page, where following list will be displayed.

ID	Schedule Description	Day	Time	Modify
1	Schedule_1	Sat Sun	1800 - 2000	Edit Delete

4.13 Static Routing

Go to **Advanced Routing** → **Static Routing List**, in order to configure the static route as shown in the next screen (Figure 4-59). A static route is a pre-determined path that network information must travel to reach a specific host or network.

Static Routing					
ID	Destination IP Address	Subnet Mask	Default Gateway	Status	Modify
1	202.108.37.42	255.255.255.0	202.108.37.1	Disabled	Modify Delete

Figure 4-59 Static Routing

To add static routing entries:

1. Click the **Add New** button as shown in figure 4-59. The following screen will open.

Add or Modify a Static Route Entry

Destination IP Address:

Subnet Mask:

Default Gateway:

Status: Enabled

Figure 4-60 Add or Modify a Static Route Entry

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 a static route to.
- * **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 from the **Status** pull-down list.
4. Click the **Save** button to make the entry take effect.

Other configurations for the entries:

- Click the **Delete All** button to erase all entries.
- Click the **Enable All** button to activate all entries
- Click the **Disabled All** button to cancel all entries.

Click the **Previous** button to view the information in the last screen, click the **Next** button to view the information in the following screen.

4.14 Bandwidth Control

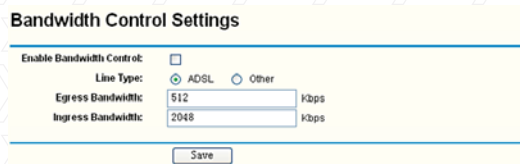


Figure 4-61

There are two submenus under the **Bandwidth Control** menu as shown in Figure 4-57. Click on any of these items in order to configure the corresponding function. Below you will find detailed descriptions for each of these items.

4.14.1 Control Settings

Go to "**Bandwidth Control → Control Settings**" in the menu, in order to configure the Egress and Ingress Bandwidth using the screen shown below. Enter the appropriate values in kbps, with settings below 100000. For optimal control of the bandwidth, please select the correct Line Type and ask your ISP what is the maximum egress and ingress bandwidth that can be set.

A screenshot of the "Bandwidth Control Settings" configuration page. It features a yellow background and a blue border. The settings include: "Enable Bandwidth Control" with an unchecked checkbox; "Line Type" with radio buttons for "ADSL" (selected) and "Other"; "Egress Bandwidth" with a text input field containing "512" and a "Kbps" label; and "Ingress Bandwidth" with a text input field containing "2048" and a "Kbps" label. A "Save" button is located at the bottom center of the form.

Bandwidth Control Settings	
Enable Bandwidth Control:	<input type="checkbox"/>
Line Type:	<input checked="" type="radio"/> ADSL <input type="radio"/> Other
Egress Bandwidth:	<input type="text" value="512"/> Kbps
Ingress Bandwidth:	<input type="text" value="2048"/> Kbps
<input type="button" value="Save"/>	

Figure 4-62 Bandwidth Control Settings

- * **Enable Bandwidth Control** - Check this box so that the Bandwidth Control settings can take effect.
- * **Line Type** - Select the right type for you network connection. If you are unsure about the type you should choose, please contact your ISP directly to find out.
- * **Egress Bandwidth** - The upload speed through the WAN port.
- * **Ingress Bandwidth** - The download speed through the WAN port.

4.14.2 Rules List

Go to “**Bandwidth Control → Rules List**” in the menu, in order to visualize and configure the Bandwidth Control rules in the screen below.

ID	Description	Egress Bandwidth(kbps)		Ingress Bandwidth(kbps)		Enable	Modify
		Min	Max	Min	Max		
1	192.168.0.2 - 192.168.0.23/21	0	1000	0	4000	<input checked="" type="checkbox"/>	Modify Delete

Now is the 1 page

Figure 4-63 Bandwidth Control Rules List

- * **Description** - It displays information about the rule, such as address range.
- * **Egress bandwidth** - This field displays the max and min upload bandwidth through the WAN port, the default is 0.
- * **Ingress bandwidth** - This field displays the max and min download bandwidth through the WAN port, the default is 0.
- * **Enable** - This field displays the status of the rule.

- * **Modify** – Click the Modify link to edit the rule.
Click Delete link to erase the rule.

To add/modify a **Bandwidth Control** rule, follow the steps below.

Step 1: Click the **Add New** button as shown in figure 4-63. A new screen will open, just like the one included in figure 4-64.

Step 2: Enter the information in the corresponding fields.

Bandwidth Control Rule Settings

Enable:

IP Range: 192.168.0.2 - 192.168.0.23

Port Range: 21

Protocol: ALL

	Min Bandwidth(kbps)	Max Bandwidth(kbps)
Egress Bandwidth:	0	1000
Ingress Bandwidth:	0	4000

Save Back

Figure 4-64 Bandwidth Control Rule Settings

Step 3: Click the **Save** button.

4.15 IP & MAC Binding Setting



Figure 4-65 IP & MAC Binding menu

There are two submenus under **IP & MAC Binding** (shown in Figure 4-61): **Binding Setting** and **ARP List**. Click on any of these items in order to scan

or configure the corresponding function. Detailed descriptions of each of these items are provided below.

4.15.1 Binding Setting

This page displays the **IP & MAC Binding Setting** table; which you can set up based on your individual preferences (figure 4-66).

Binding Settings

ARP Binding: Disable Enable

ID	MAC Address	IP Address	Bind	Modify
The list is empty				

Page 1

Figure 4-66 Binding Setting

- * **MAC Address** - The MAC address of the monitored computer in the LAN.
- * **IP Address** - The assigned IP address of the monitored computer in the LAN.
- * **Bind** - Check this option to enable ARP binding for a specific device.
- * **Modify** – Use this link to edit or delete an existing entry.

When you want to add or edit an IP & MAC Binding entry, click the **Add New** button or **Modify** button, and then you will be directed to the next page. This page is used for adding or modifying an IP & MAC Binding entry (shown in Figure 4-66).

IP & MAC Binding Settings

Bind
 MAC Address:
 IP Address:

Figure 4-67 IP & MAC Binding Setting (Add & Modify)

To add IP & MAC Binding entries, follow the steps below.

1. Click the **Add New** button, as shown in figure 4-67.
2. Enter the **MAC Address** and **IP Address**.
3. Select the **Bind** checkbox.
4. Click the **Save** button to accept your changes.

To modify or delete an existing entry, follow the steps below.

1. Find the desired entry in the table.
2. Click Modify or Delete as desired on the Modify column.

To find an existing entry, follow the steps below.

1. Click the Find button, as shown in figure 4-68.
2. Enter the MAC Address or IP Address.
3. Click the Find button in the page.

Find IP & MAC Binding Entry

MAC Address:
 IP Address:

ID	MAC Address	IP Address	Bind	Link
2	00-14-5E-91-19-E3	192.168.0.56	<input checked="" type="checkbox"/>	To page

Figure 4-68 Find IP & MAC Binding Entry

Click the **Enable All** button to activate all entries.
 Click the **Delete All** button to erase all entries.

4.15.2 ARP List

You can see IP addresses on the LAN and their associated MAC addresses by viewing the ARP list. Also, you can use the Load and Delete buttons to manage the list. The user can use this list to visualize all the existing IP & MAC binding entries (shown in figure 4-69).

ARP List				
ID	MAC Address	IP Address	Status	Configure
1	00-0F-E2-80-30-90	172.31.70.1	Unbound	Load Delete
2	00-19-66-80-53-BD	192.168.0.101	Unbound	Load Delete

Figure 4-69 ARP List

- * **MAC Address** - The MAC address of the monitored computer in the LAN.
- * **IP Address** - The assigned IP address of the monitored computer in the LAN.
- * **Status** - Indicates whether or not the MAC and IP addresses are bound.
- * **Configure** - To load or delete an item.
 - **Load** - To load the item into the IP & MAC Binding list.
 - **Delete** - To erase the item.

Click the **Bind All** button to bind all the current items. This option is only available when the ARP binding is enabled.

Click the **Load All** button to include all items to the

IP & MAC Binding list.

Click the Refresh button to update all items.

Note:

An item cannot be entered to the IP & MAC Binding list if the IP address of the item has been loaded before. An error warning will be displayed as well. Likewise, the "Load All" command will only load the items without interfering with the IP & MAC Binding list.

4.16 Dynamic DNS

Go to "**Dynamic DNS**" in order to configure the Dynamic DNS feature.

The router offers the **DDNS** (Dynamic Domain Name System) feature, which allows the hosting of a website, FTP server, or e-mail server with a fixed domain name (defined by the user) and a dynamic IP address. Your friends can then connect to your server by entering the domain name you provide, no matter what your IP address is. Before using this feature, you need to sign up for DDNS service providers, such as www.comexe.cn, www.dyndns.org, or www.no-ip.com. The Dynamic DNS client service provider will give you a password or key.

4.16.1 Comexe.cn DDNS

If the dynamic DNS **Service Provider** you select is www.comexe.cn, the page will appear as shown in figure 4-70.

DDNS

Service Provider: Comexe (www.comexe.cn) [Go to register](#)

Domain Name:

Domain Name:

Domain Name:

Domain Name:

User Name:

Password:

Enable DDNS

Connection Status: DDNS not launching!

Figure 4-70 Comexe.cn DDNS Settings

To set up for DDNS, follow these instructions:

1. Type the **Domain Name** received from your dynamic DNS service provider.
2. Type the **User Name** for your DDNS account.
3. Type the **Password** for your DDNS account.
4. Click the **Login** button to log into the DDNS service.

Connection Status -The status of the DDNS service connection is displayed here.
Click **Logout** to exit the DDNS service.

4.16.2 Dyndns.org DDNS

If the dynamic DNS **Service Provider** you select is www.dyndns.org, the page will appear as shown in figure 4-71.

DDNS

Service Provider: DynDNS (www.dynDNS.org) [Go to register...](#)

User Name: username

Password: *****

Domain Name: _____

Enable DDNS

Connection Status: DDNS not launching!

Login Logout

Save

Figure 4-71 DynDNS.org DDNS Settings

To set up for DDNS, follow these instructions:

1. Type the **User Name** for your DDNS account.
2. Type the **Password** for your DDNS account.
3. Type the **Domain Name** you received from dynamic DNS service provider here.
4. Click the **Login** button to log into the DDNS service.

Connection Status -The status of the DDNS service connection is displayed here.
Click **Logout** to exit the DDNS service.

4.16.3 No-ip.com DDNS

If the dynamic DNS **Service Provider** you select is www.no-ip.com, the page will appear as shown in figure 4-72.

DDNS

Service Provider: No-IP (www.no-ip.com) [Go to register.](#)

User Name: username

Password: ●●●●●●

Domain Name:

Enable DDNS

Connection Status: DDNS not launching!

Figure 4-72 No-ip.com DDNS Settings

To set up for DDNS, follow these instructions:

1. Type the **User Name** for your DDNS account.
2. Type the **Password** for your DDNS account.
3. Type the **Domain Name** you received from dynamic DNS service provider.
4. Click the **Login** button to log into the DDNS service.

Connection Status - The status of the DDNS service connection is displayed here.

Click **Logout** to exit the DDNS service.

4.17 System Tools

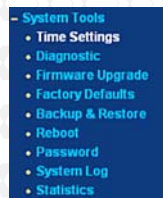


Figure 4-73 System Tools menu

Go to “**System Tools**” in order to display the submenus under the main menu: **Time Settings, Diagnostic, Firmware Upgrade, Factory Defaults, Backup & Restore, Reboot, Password, System Log** and **Statistics**. Click on any of these items in order to configure the corresponding function. You will find detailed descriptions for each of these items below.

4.17.1 Time Setting

Go to menu “**System Tools → Time Setting**”, in order to configure the time on the following screen.

The screenshot shows the 'Time Settings' interface. At the top, the title 'Time Settings' is displayed. Below it, there is a dropdown menu for 'Time zone' currently set to '(GMT+08:00) Beijing, Hong Kong, Perth, Singapore'. Underneath, there are three rows of input fields: 'Date' with fields for month (1), day (1), and year (2000); 'Time' with fields for hour (0), minute (29), and second (3); and 'NTP Server Prior' with two input fields, both containing '0.0.0.0'. A 'Get GMT' button is located below the NTP Server Prior fields, with a tooltip that says '(Get GMT when connected to Internet)'. At the bottom of the form is a 'Save' button.

Figure 4-74 Time settings

- ***Time Zone** - Select your local time zone from this pull down list.
- ***Date** - Enter your local date in MM/DD/YY into the corresponding blank fields.
- ***Time** - Enter your local time in HH/MM/SS into the corresponding blank fields.
- ***NTP Server Prior** - Enter the address for the NTP Server, then the router will preferentially obtain the time from the NTP Server. In addition, the router can automatically update the time from any enabled NTP server once it connects to the Internet.

To configure the system manually:

1. Select your local time zone.
2. Enter date and time in the corresponding blank fields.
3. Click Save to store your new settings.

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 obtain the system time from Internet if you are already connected.

Note:

1. 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, none of these functions will work.
2. The time will be lost if the router is turned off.
3. The router will obtain the GMT automatically from the Internet as long as it is connected to Internet.

4.17.2 Diagnostic

Go to "**System Tools → Diagnostic**" in the menu, in order to start the Ping or Traceroute functions, which are designed to check the connectivity status of your network, as shown in the screen below.

Diagnostic Tools

Diagnostic Parameters

Diagnostic Tool: Ping Traceroute

IP Address/Domain Name:

Ping Count: (1-50)

Ping Packet Size: (4-1472 Bytes)

Ping Timeout: (100-2000 Milliseconds)

Traceroute Max TTL: (1-30)

Diagnostic Results

The Router is ready.

Figure 4-75 Diagnostic Tools

Diagnostic Tool - Check the radio button to select one of the diagnostic tools.

- **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, make sure 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 of the PC whose connection you wish to diagnose.
- * **Pings Count** - Specifies the number of Echo Request messages sent. The default is 4.
- * **Ping Packet Size** - Specifies the number of data bytes to be sent. 64 is the default value.
- * **Ping Timeout** - Sets the maximum time that the application will wait for a reply, in milliseconds. When time exceeds the timeout limit, the session will expire. 800 is the default value.
- * **Traceroute Max TTL** - Sets the maximum number of hops (max TTL to be reached) in the path to search for the target (destination). The default is 20.

Click **Start** to check the connectivity of the Internet. The **Diagnostic Results** page displays the outcome of the diagnosis.

If the results you obtained are similar to the values that appear in the screen below, it means that the connectivity to the Internet is fine.

```
Diagnostic Results
: Pinging 202.108.22.5 with 64 bytes of data:
: Reply from 202.108.22.5: bytes=64 time=1 TTL=127 seq=1
: Reply from 202.108.22.5: bytes=64 time=1 TTL=127 seq=2
: Reply from 202.108.22.5: bytes=64 time=1 TTL=127 seq=3
: Reply from 202.108.22.5: bytes=64 time=1 TTL=127 seq=4
: Ping statistics for 202.108.22.5
: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
: Approximate round trip times in milliseconds:
: Minimum = 1, Maximum = 1, Average = 1
```

Figure 4-76 Diagnostic Results

Note:
Only one user can use this tool at a time. “**Number of Pings**”, “**Ping Size**” and “**Ping Timeout**” are Ping parameters. “**Tracert Hops**” is a Traceroute parameter.

4.17.3 Firmware Upgrade

Go to “**System Tools → Firmware Upgrade**” in the menu, in order to update the latest firmware version available for the router. The following screen will be displayed.

Firmware Upgrade

File:

Firmware Version: 3.13.4 Build 111121 Rel.36959n

Hardware Version: ARN033004U1 v1 00000000

Figure 4-77 Firmware Upgrade

- * **Firmware Version** - The current firmware version is displayed here.
- * **Hardware Version** - The current hardware version is displayed here. The hardware version of the upgrade file must match the router's current hardware version.

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

1. Download the latest firmware upgrade file from our website (<http://www.nexxtsolutions.com>).
2. Type or select 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:

- 1) New firmware versions are posted at <http://www.nexxtsolutions.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.

- 2) When you upgrade the router's firmware, you may lose its current configuration. Therefore, before upgrading the firmware, please write down your customized parameters to avoid losing important settings.
- 3) Do not turn off power or press the reset button while the firmware is being upgraded; doing so might cause serious damage to the router.
- 4) The router will reboot after the upgrading has been finished.

4.17.4 Factory Defaults

Go to "**System Tools → Factory Defaults**" in the menu, in order to restore the router configuration to its factory default values, as seen on the following screen.

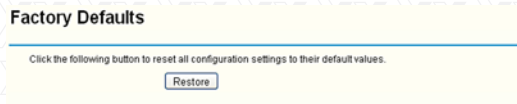


Figure 4-78 Restore Factory Default

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

- Default **User Name**: admin
- Default **Password**: admin
- Default **IP Address**: 192.168.0.1
- Default **Subnet Mask**: 255.255.255.0

Note:

Any settings you have saved will be lost after the default settings are restored.

4.17.5 Backup & Restore

Go to “**System Tools** → **Backup & Restore**” in the menu, in order to save the current configuration of the router as a backup file and restore the original settings using a backup file as shown in Figure 4-75.



Figure 4-79 Backup & Restore Configuration

- * Click the **Backup** button to save all configuration settings as a backup file in your local computer.
- * To upgrade the Router's configuration, follow the instructions below.
 - 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 overwritten by the uploaded configuration file. The upgrade process lasts around 20 seconds, after which the router will restart automatically. Keep the router on during the entire upgrading process to prevent any potential damage to the unit.

4.17.6 Reboot

Go to “**System Tools → Reboot**”, and press the **Reboot** button in order to reset the device, as shown in the screen below.

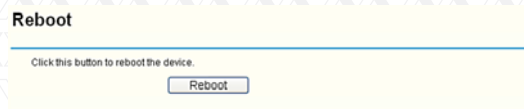


Figure 4-80 Reboot the Router

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

- LAN IP Address change (system will reboot automatically).
- DHCP Settings change.
- Wireless configuration change.
- Web Management Port change.
- 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).

4.17.7 Password

Go to **"System Tools → Password"**, in order to change the router's factory default user name and password, using the screen shown in figure 4-81.

The screenshot shows a web form titled "Password" with a yellow background. It contains the following fields and buttons:

- Old User Name:
- Old Password:
- New User Name:
- New Password:
- Confirm New Password:
- Save button
- Clear All button

Figure 4-81 Password

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

Note:

The new user name and password must not exceed 14 characters in length and must not include any spaces. Enter the new Password twice to confirm. Click the **Save** button when finished. Click the **Clear All** button to erase all entries.

4.17.8 System Log

Go to **"System Tools → System Log"**, in order to view the logs of the router.

System Log

Auto Mail Feature: **Disabled**

Log Type: All

Index	Time	Type	Level	Log Content
3	Jan 30 09:55:31	SECURITY	INFO	SPI Firewall enabled
2	Jan 30 09:55:20	SECURITY	INFO	SPI Firewall disabled
1	Jan 30 09:54:23	OTHER	INFO	User clear system log

Time = 2012-01-30 9:55:39 3021s
 H-Ver = ARN033004U1 v1 00000000 : S-Ver = 3.13.4 Build 111121 Rel.36959n
 L = 192.168.0.1 : M = 255.255.255.0
 W1 = DHCP : W = 192.168.54.164 : M = 255.255.255.0 : G = 192.168.54.254

Current No. 1 Page

Figure 4-82 System Log

- * **Auto Mail Feature** - Indicates whether the automatic 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 4-83.

Mail Account Settings

From:

To:

SMTP Server:

Authentication

Enable Auto Mail Feature

Everyday, mail the log at :

Mail the log every hours

Figure 4-83 Mail Account Settings

- **From** - Your mail box address. The email account the router will use to send logging messages.
 - **To** - The recipient's address. The destination mailbox where the logs would be received.
 - **SMTP Server** - Your SMTP server. The mail server which will be used for sending emails using the address you entered in the From field. You can log into the applicable website for Help if you are unsure about the address.
 - **Authentication** - Most SMTP servers require authentication. It is required by most mailboxes that need User Name and Password to log in.
- Note:**
Only when you select **Authentication**, you have to enter the User Name and Password in the following fields.
- **User Name** - Your mail account name entered in the From field. The part following the @ is excluded.
 - **Password** - Your email 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 every day or at intervals, but only one rule can be effective at a time. Enter the desired time or intervals in the corresponding field, as shown in figure 4-83.

Click **Save** to keep your settings.

Click **Back** to return to the previous page.

- * **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.

Click the **Next** button to go to the following page, or click the **Previous** button return to the last page.

4.17.9 Statistics

Go to “**System Tools** → **Statistics**” in the menu, in order to visualize the router statistics, including the total traffic and current traffic of the last Packets Statistic Interval.

Statistics

Current Statistics Status: Disabled

Packets Statistics Interval(5-60): 10 Seconds

Auto-refresh

Sorted Rules: Sorted by IP Address

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

Per page 5 entries Current No. 1 page

Figure 4-84 Statistics

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

* **Packets Statistics Interval (5-60)** - The default value is 10. Select a value between 5 and 60 seconds from the pull-down list. This statistics interval defines the time between each transmission of data packets.

Select the **Auto-refresh** checkbox to update data automatically.

Click the **Refresh** button to update data immediately.

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

Click **Reset All** to restore the values of all the entries to zero.

Click **Delete All** to erase all entries in the table.

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 expressed in seconds.
	Bytes	The total amount of bytes received and transmitted in the last Packets Statistic interval expressed in seconds.
	ICMP Tx	The total amount of the ICMP packets transmitted to WAN in the last Packets Statistic interval expressed in seconds
	UDP Tx	The total amount of the UDP packets transmitted to WAN in the last Packets Statistic interval expressed in seconds
	TCP SYN Tx	The total amount of the TCP SYN packets transmitted to WAN in the last Packets Statistic interval expressed in seconds

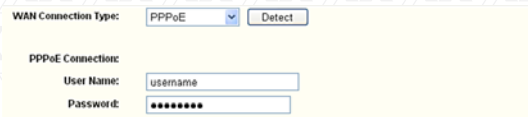
There would be 5 entries on each page.

Click **Previous** to return to the last page and **Next** to go to the following page.

Appendix A: FAQ

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

- 1) First, configure the ADSL modem in the RFC1483 bridge mode.
- 2) Connect the Ethernet cable from your ADSL modem to the WAN port on the router. The telephone cord must be plugged into the "Line" port of the ADSL modem.
- 3) Login to the router. Go to the "Network" in the menu located on the left of your browser, and select "WAN" in the submenu. Once the WAN page opens, select "PPPoE" as the WAN Connection Type. Type the "User Name" and "Password" in the corresponding fields, and finish by clicking on the "Connect" button.



The screenshot shows the WAN configuration interface. At the top, there is a dropdown menu for "WAN Connection Type" set to "PPPoE" and a "Detect" button. Below this, the "PPPoE Connection" section contains two input fields: "User Name" with the text "username" and "Password" with a masked field of seven asterisks.

Figure A-1 PPPoE Connection Type

- 4) If your ADSL access rates are "based on connection time", select "Connect on Demand" or "Connect Manually" as your Internet connection mode. Type an appropriate number for "Max Idle Time" to avoid wasting paid time. Otherwise, you can select "Auto-connecting" as your Internet connection mode.



Figure A-2 PPPoE Connection Mode

Note:

- i. Sometimes the connection cannot be terminated despite your setting of the "Max Idle Time" interval. This is due to some applications are continually linked to the internet in the background.
- ii. If you are a cable user, you must configure the router following the above steps.

2. How do I configure the router for Ethernet users to access the Internet?

- 1) Login to the router. Go to the "Network" in the menu located on the left of your browser, and select "WAN" in the submenu. Once the WAN page opens, select "Dynamic IP" as the **WAN Connection Type**, and finish by clicking on the "Save" button.
- 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 on the "Network" menu link on the left of your browser, before selecting "MAC Clone" in the submenu. On the "MAC Clone" page, if your PC's MAC address is a proper MAC address, click the "Clone MAC Address" button and your PC's

MAC address will be copied into the "WAN MAC Address" field. Or you may type the MAC Address directly into the "WAN MAC Address" field. The MAC Address format is XX-XX-XX-XX-XX-XX. Click the "Save" button when you are done. This setting will be effective only after the router has rebooted.

MAC Clone

WAN MAC Address:	<input type="text" value="00-1D-0F-88-88-8F"/>	<input type="button" value="Restore Factory MAC"/>
Your PC's MAC Address:	<input type="text" value="00-19-66-80-53-B0"/>	<input type="button" value="Clone MAC Address"/>
<input type="button" value="Save"/>		

Figure A-3 MAC Clone

3. 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 the Virtual Server or DMZ Host and make sure the H323 ALG is enabled.
- 3) How to configure the Virtual Server: Log in to the router, go to the "Forwarding" menu located on the left of your browser, and then select "Virtual Servers" submenu. On the "Virtual Servers" page, click **Add New**.... Once the "Add or Modify a Virtual Server Entry" page opens, enter "1720" in the "Service Port" blank field, and your IP address in the corresponding field, using 192.168.0.169 as an example. Remember to **Enable** and **Save** your settings at the end.

Virtual Servers

ID	Service Port	Internal Port	IP Address	Protocol	Status	Modify
1	1720	1720	192.168.0.169	ALL	Enabled	Modify Delete

Figure A-4 Virtual Servers

Add or Modify a Virtual Server Entry

Service Port: (XX-XX or XX)
Internal Port: (XX, Only valid for single Service Port or leave it blank)
IP Address:
Protocol:
Status:
Common Service Port:

Figure A-5 Add or Modify a Virtual server Entry

Note:

The caller on the other end should call your WAN IP, which is displayed on the "Status" page.

- 1) How to enable DMZ Host: Log in to the Router, go to the **"Forwarding"** menu located on the left of your browser, and then select the **"DMZ"** submenu. On the **"DMZ"** page, click **Enable** radio button and type your IP address into the "DMZ Host IP Address" field, using 192.168.0.169 as an example. Remember to **Save** your settings when you are done.

DMZ

Current DMZ Status: Enable Disable

DMZ Host IP Address:

Figure A-6 DMZ

2) How to enable H323 ALG: Log in to the Router, go to the **"Security"** menu located on the left of your browser, and then select the **"Basic Security"** submenu. On the **"Basic Security"** page, check the **Enable** radio button next to **H323 ALG**. Remember to click the **Save** button at the end.

Basic Security

Firewall

SPI Firewall: Enable Disable

VPN

PPTP Passthrough: Enable Disable

LZTP Passthrough: Enable Disable

IPSEC Passthrough: Enable Disable

ALG

FTP ALG: Enable Disable

TFTP ALG: Enable Disable

H323 ALG: Enable Disable


Figure A-7 Basic Security

4. 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)2)To change the WEB management port number:

Log in to the router, go to the **"Security"** menu located on the left of your browser, and select the **"Remote Management"** submenu. On the **"Remote Management"** page, type any port number other than 80, such as 88, into the **"Web Management Port"** field. Click **Save** and reboot the Router.



Remote Management

Web Management Port:	<input type="text" value="88"/>
Remote Management IP Address:	<input type="text" value="0.0.0.0"/> (Enter 255.255.255.255 for all)

Figure A-8 Remote Management

Note:

If the above settings take effect, type `http://192.168.0.1:88` (the router's LAN IP address: Web Management Port) in the address field of the Web browser in order to configure to the router.

1)Log in to the Router, go to the **"Forwarding"** menu located on the left of your browser, and select the **"Virtual Servers"** submenu. On the **"Virtual Servers"** page, click **Add New...**, then on the **"Add or Modify a Virtual Server"** page, enter **"80"** into the blank field next to the **"Service Port"**, and your IP address next to the **"IP Address"**, taking 192.168.0.188 as an example. Remember to **Enable** and **Save** your settings at the end.

Virtual Servers

ID	Service Port	Internal Port	IP Address	Protocol	Status	Modify
1	1720	1720	192.168.0.169	ALL	Enabled	Modify Delete

Figure A-9 Virtual Servers

Add or Modify a Virtual Server Entry

Service Port: (XX-XX or XX)
Internal Port: (XX, Only valid for single Service Port or leave it blank)
IP Address:
Protocol:
Status:
Common Service Port:

Figure A-10 Add or Modify a Virtual server Entry

5. 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 matches the Router's SSID.
- 3) Make sure the wireless stations have chosen the right encryption KEY when the router is encrypted.
- 4) If the wireless connection is available, but you are unable to access the router, check the IP Address of your wireless stations.

Appendix B: Configuring the PCs

In this section, we will explain 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 for further information, if needed.

1. Install TCP/IP component

- 1) On the Windows taskbar, click the **Start** button, point to **Settings**, and then select **Control Panel**.
- 2) After clicking the **Network and Internet Connections** icon, select the **Network Connections** tab in the new window.
- 3) Right click the icon displayed below, and select **Properties** on the pop up menu.

LAN or High-Speed Internet



Figure B-1

- 4) In the page displayed below, double click on **Internet Protocol (TCP/IP)**.

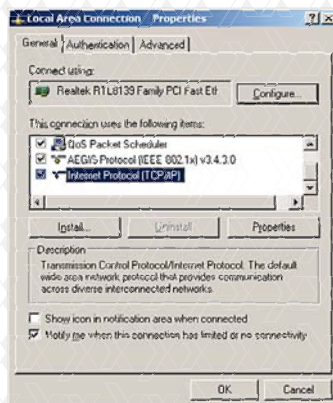


Figure B-2

5) The following **TCP/IP Properties** window will be displayed, with **IP Address** tab open by default.

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

* **Setting IP address automatically**

Select **Obtain an IP address automatically**, and then choose **Obtain DNS server automatically**, as shown in the figure below:

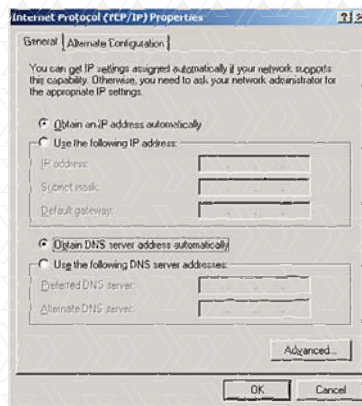


Figure B-3

*** Setting IP address manually**

1. Select **Use the following IP address** radio button.
The following items will be available:
2. If the Router's LAN IP address is 192.168.0.1, type IP address 192.168. 0.x (whereby x is any value 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. 0.1) 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 B-4

Appendix C: Specifications

General	
Standards	IEEE 802.3, 802.3u, 802.3ab, 802.11b, 802.11g and 802.11n
Protocols	TCP/IP, PPPoE, DHCP, ICMP, NAT, SNTP
Ports	One 10/100/1000M Auto-Negotiation WAN RJ45 port. Four 10/100/1000M Auto-Negotiation LAN RJ45 ports supporting Auto MDI/MDIX. One USB2.0 port
Cabling Type	10BASE-T: UTP category 3, 4, 5 cable (maximum 100m) EIA/TIA-568 100Ω STP (maximum 100m)
	100BASE-TX: UTP category 5, 5e cable (maximum 100m) EIA/TIA-568 100Ω STP (maximum 100m)
	1000BASE-TX: UTP category 5, 5e cable (maximum 100m) EIA/TIA-568 100Ω STP (maximum 100m)
LEDs	Power, System, WLAN, WAN, LAN (1-4), USB, WPS
Safety & Emissions	FCC
Wireless	
Frequency Band	2.4~2.4835GHz
Radio Data Rate	11n: up to 300Mbps (Automatic) 11g: 54/48/36/24/18/12/9/6Mbps (Automatic) 11b: 11/5.5/2/1Mbps (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	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)
Antenna Gain	3dBi per antenna (3)
Environmental and Physical	
Temperature	Operating: 0°C~40°C (32°F~104°F) Storage: -40°C~70°C(-40°F~158°F)
Humidity	Operating: 10% - 90% RH, Non-condensing Storage: 5% - 90% RH, Non-condensing

Appendix D: Glossary

- * **802.11n** - 802.11n builds upon previous 802.11 standards by adding MIMO (multiple-input multiple-output). MIMO uses multiple transmitter and receiver antennas to allow for increased data throughput via spatial multiplexing and increased range by exploiting the spatial diversity, perhaps through coding schemes like Alamouti coding. The Enhanced Wireless Consortium (EWC) [3] was formed to help accelerate the IEEE 802.11n development process and promote a technology specification for interoperability of next-generation wireless local area networking (WLAN) products.
- * **802.11b** - The 802.11b standard specifies a wireless networking at 11 Mbps using direct-sequence spread-spectrum (DSSS) technology and operating in the unlicensed radio spectrum at 2.4GHz, and WEP encryption for security. 802.11b networks are also referred to as Wi-Fi networks.
- * **802.11g** - Specification for wireless networking at 54 Mbps using direct-sequence spread-spectrum (DSSS) technology, using OFDM modulation and operating in the unlicensed radio spectrum at 2.4GHz, and backward compatibility with IEEE 802.11b devices, and WEP encryption for security.
- * **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)** - A protocol that automatically configure the TCP/IP parameters for the all the PC(s) that are connected to a DHCP server.

- * **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, in which network serving users are limited in a local area.