Status
--- Basic Settings ---
Quick Setup
WPS
Network
Wireless
--- Advanced Settings ---
DHCP
Forwarding
Security
Parental Control
Access Control
Static Routing
IP QoS
IP & MAC Binding
Dynamic DNS
--- Maintenance ---
System Tools

Firmware Version:	4.19.47 Build 120516 Rel.37372n
Hardware Version:	WR720N 1.0 00000000

LAN

MAC Address:	A0-F3-C1-C9-E4-1E
IP Address:	192.168.10.2
Subnet Mask:	255.255.255.0

Wireless

Wireless Radio:	Enable
Name (SSID):	TP-LINK_SS0024
Channel:	9
Mode:	11bgn mixed
Channel Width:	Automatic
MAC Address:	A0-F3-C1-C9-E4-1E
WDS Status:	Disable

WAN

MAC Address:	A0-F3-C1-C9-E4-1F
IP Address:	172.23.212.114
Subnet Mask:	255.255.255.252
Default Gateway:	172.23.212.113
DNS Server:	187.94.192.61 , 187.94.192.62

Traffic Statistics

	Received
Bytes:	**1305681798**
Packets:	**12488457**

System Up Time:	16 day(s) 15:12:33

Status Help

The **Status** page displays the Router's current status and configuration. All information is read-only.

LAN - The following parameters apply to the LAN port of the Router. You can configure them in the **Network -> LAN** page.

- **MAC Address** - The physical address of the Router, as seen from the LAN.
- **IP Address** - The LAN IP address of the Router.
- **Subnet Mask** - The subnet mask associated with LAN IP address.

Wireless - These are the current settings or information for Wireless.You can configure them in the **Wireless -> Wireless Settings** page.

- **Wireless Radio** - Indicates whether the wireless radio feature of the Router is enabled or disabled.
- **Name(SSID)** - The SSID of the Router.
- **Channel** - The current wireless channel in use.
- **Mode** - The current wireless mode which the Router works on.
- **MAC Address** - The physical address of the Router, as seen from the WLAN.
- **WDS Status** - The status of WDS' connection, Init: WDS connection is down; Scan: Try to find the AP; Auth: Try to authenticate; ASSOC: Try to associate; Run: Associated successfully.

WAN - The following parameters apply to the WAN ports of the Router. You can configure them in the **Network -> WAN** page.

- **MAC Address** - The physical address of the WAN port, as seen from the Internet.
- **IP Address** - The current WAN (Internet) IP Address. This field will be blank or 0.0.0.0 if the IP Address is assigned dynamically and there is no connection to Internet.
- **Subnet Mask** - The subnet mask associated with the WAN IP Address.
- **Default Gateway** - The Gateway currently used by the Router is shown here. When you use **Dynamic IP** as the connection Internet type, the **Renew** button will be displayed here. Click the **Renew** button to obtain new IP parameters dynamically from the ISP. And if you have got an IP address **Release** button will be displayed here. Click the **Release** button to release the IP address the Router has obtained from the ISP.
- **DNS Server** - The DNS (Domain Name System) Server IP addresses currently used by the Router. Multiple DNS IP settings are common. Usually, the first available DNS Server is used.

Status
--- Basic Settings ---
Quick Setup
WPS
Network
Wireless
--- Advanced Settings ---
DHCP
Forwarding
Security
Parental Control
Access Control
Static Routing
IP QoS
IP & MAC Binding
Dynamic DNS
--- Maintenance ---
System Tools

WPS (Wi-Fi Protected Setup)

Current SSID: TP-LINK_SS0024

WPS Status: Enabled Disable WPS

Current PIN: 76781957 Restore PIN Gen New PIN

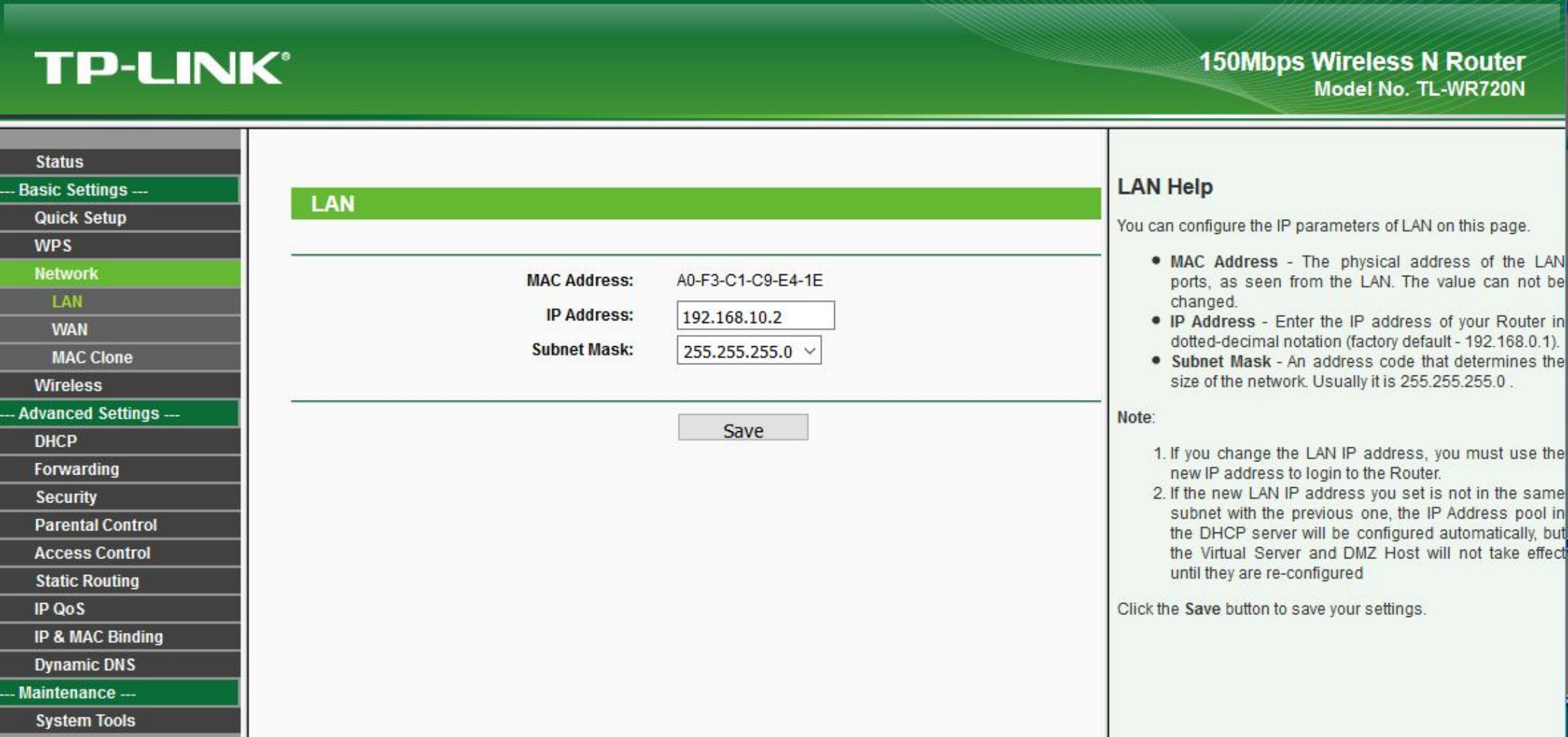
Add a new device: Add device

Wi-Fi Protected Setup Help

WPS function will help you add a new device to the network quickly. If the new device supports Wi-Fi Protected Setup and is equipped with a configuration button, you can add it to the network by pressing the configuration button on the device and then press the button on the Router within two minutes. The status LED on the Router will light green for five minutes if the device has been successfully added to the network. If the new device supports Wi-Fi Protected Setup and the connection way using PIN, you can add it to the network by entering the Router's PIN.

- **WPS Status** - Enable or disable the WPS function here.
- **Current PIN** - The current value of the Router's PIN displayed here. The default PIN of the Router can be found in the label or User Guide.
- **Restore PIN** - Restore the PIN of the Router to its default.
- **Gen New PIN** - Click this button, and then you can get a new random value for the Router's PIN. You can ensure the network security by generating a new PIN.
- **Add Device** - You can add the new device to the existing network manually by clicking this button.

Note: The WPS function cannot be configured if the Wireless Function of the Router is disabled. Please make sure the Wireless Function is enabled before configuring the WPS.


TP-LINK
150Mbps Wireless N Router
Model No. TL-WR720N
Status
--- Basic Settings ---
Quick Setup
WPS
Network
LAN
WAN
MAC Clone
Wireless
--- Advanced Settings ---
DHCP
Forwarding
Security
Parental Control
Access Control
Static Routing
IP QoS
IP & MAC Binding
Dynamic DNS
--- Maintenance ---
System Tools
LAN
MAC Address: A0-F3-C1-C9-E4-1E
IP Address: 192.168.10.2
Subnet Mask: 255.255.255.0
Save
LAN Help
You can configure the IP parameters of LAN on this page.
MAC Address - The physical address of the LAN ports, as seen from the LAN. The value can not be changed.
IP Address - Enter the IP address of your Router in dotted-decimal notation (factory default - 192.168.0.1).
Subnet Mask - An address code that determines the size of the network. Usually it is 255.255.255.0 .
Note:
1. If you change the LAN IP address, you must use the new IP address to login to the Router.
2. If the new LAN IP address you set is not in the same subnet with the previous one, the IP Address pool in the DHCP server will be configured automatically, but the Virtual Server and DMZ Host will not take effect until they are re-configured
Click the Save button to save your settings.

Status
--- Basic Settings ---
Quick Setup
WPS
Network
LAN
WAN
MAC Clone
Wireless
--- Advanced Settings ---
DHCP
Forwarding
Security
Parental Control
Access Control
Static Routing
IP QoS
IP & MAC Binding
Dynamic DNS
--- Maintenance ---
System Tools

WAN

WAN Connection Type: Dynamic IP

IP Address: 172.23.212.114

Subnet Mask: 255.255.255.252

Default Gateway: 172.23.212.113

Renew | Release

MTU Size (in bytes): 1500 (The default is 1500, do not change unless nec

☐ Use These DNS Servers

Primary DNS: 187.94.192.61

Secondary DNS: 187.94.192.62 (Optional)

Host Name: WR720N

☐ Get IP with Unicast DHCP (It is usually not required.)

Save

WAN Help

WAN Connection Type:

If your ISP is running a DHCP server, select the **Dynamic IP** option.

If your ISP provides a static or fixed IP Address, Subnet Mask, Gateway and DNS setting, select the **Static IP** option.

If your ISP provides a PPPoE connection, select **PPPoE/Russia PPPoE** option.

If your ISP provides BigPond Cable (or Heart Beat Signal) connection, please select **BigPond Cable** option.

If your ISP provides L2TP connection, please select **L2TP/Russia L2TP** option.

If your ISP provides PPTP connection, please select **PPTP/Russia PPTP** option.

- **PPPoE/Russia PPPoE** - Connections which use PPPoE that requires a user name and password.
- **Dynamic IP** - Connections which use dynamic IP address assignment.
- **Static IP** - Connections which use static IP address assignment.

IP Address - The IP address assigned by your ISP dynamically.

Subnet Mask - The subnet mask assigned by your ISP dynamically.

Default Gateway - The default gateway assigned dynamically by your ISP.

Click the **Renew** button to renew the IP parameters from your ISP.

Click the **Release** button to release the IP parameters from your ISP.

Status
--- Basic Settings ---
Quick Setup
WPS
Network
Wireless
Wireless Settings
Wireless Security
Wireless MAC Filtering
Wireless Advanced
Wireless Statistics
--- Advanced Settings ---
DHCP
Forwarding
Security
Parental Control
Access Control
Static Routing
IP QoS
IP & MAC Binding
Dynamic DNS
--- Maintenance ---
System Tools

Wireless Settings

SSID1:	TP-LINK_SS0024
SSID2:	TP-LINK_C9E41E_2 ☐
SSID3:	TP-LINK_C9E41E_3 ☐
SSID4:	TP-LINK_C9E41E_4 ☐
Region:	United States
Warning:	Ensure you select a correct country to conform local law. Incorrect settings may cause interference.
Channel:	9
Mode:	11bgn mixed
Channel Width:	Auto

☑ Enable Wireless Router Radio
☑ Enable SSID Broadcast
☐ Enable WDS

Save

Wireless Settings Help

Note: The operating distance or range of your wireless connection varies significantly based on the physical placement of the Router. For best results, place your Router.

- Near the center of the area in which your wireless stations will operate.
- In an elevated location such as a high shelf.
- Away from the potential sources of interference, such as PCs, microwaves, and cordless phones.
- With the Antenna in the upright position.
- Away from large metal surfaces.

Note: Failure to follow these guidelines can result in significant performance degradation or inability to wirelessly connect to the Router.

SSID - Enter a value of up to 32 characters. The same Name (SSID) must be assigned to all wireless devices in your network.

Region - Select your region from the pull-down list. This field specifies the region where the wireless function of the Router can be used. It may be illegal to use the wireless function of the Router in a region other than one of those specified in this filed. If your country or region is not listed, please contact your local government agency for assistance.

Channel - This field determines which operating frequency will be used. It is not necessary to change the wireless channel unless you notice interference problems with another nearby access point. If you select auto, then AP will choose the best channel automatically.

Mode - If all of the wireless devices connected with this wireless router can connect in the same transmission mode(eg. 802.11b), you can choose "Only" mode(eg. 11b only). If you have some devices that use a different transmission mode, choose the appropriate "Mixed" mode.

Status
--- Basic Settings ---
Quick Setup
WPS
Network
Wireless
Wireless Settings
Wireless Security
Wireless MAC Filtering
Wireless Advanced
Wireless Statistics
--- Advanced Settings ---
DHCP
Forwarding
Security
Parental Control
Access Control
Static Routing
IP QoS
IP & MAC Binding
Dynamic DNS
--- Maintenance ---
System Tools

Wireless Security

Current SSID: TP-LINK_SS0024

○ **Disable Security**

○ **WEP**

Type: Automatic
WEP Key Format: ASCII

Key Selected	WEP Key	Key Type
Key 1: ◉	ABC3632320000	128bit
Key 2: ○		Disabled
Key 3: ○		Disabled
Key 4: ○		Disabled

○ **WPA/WPA2**

Version: Automatic
Encryption: Automatic
Radius Server IP:
Radius Port: 1812 (1-65535, 0 stands for default port 1812)
Radius password:
Group Key Update Period: 86400 (in second, minimum is 30, 0 means no upda

◉ **WPA-PSK/WPA2-PSK**

Version: WPA2-PSK
Encryption: AES
PSK Password: ABC3632320000
(You can enter ASCII characters between 8 and 63 or Hexade
Group Key Update Period: 86400 (in second, minimum is 30, 0 means no upda

Save

Wireless Security Help

You can select one of the following security options:

- **Disable Security** - The wireless security function can be enabled or disabled. If disabled, the wireless stations will be able to connect the Router without encryption. It is recommended strongly that you choose one of following options to enable security.
- **WEP** - Select 802.11 WEP security.
- **WPA-PSK** - Select WPA based on pre-shared passphrase.
- **WPA** - Select WPA based on Radius Server.

Each security option has its own settings as described follows,

WEP

Type - You can select one of following types,

- **Automatic** - Select **Shared Key** or **Open System** authentication type automatically based on the wireless station's capability and request.
- **Shared Key** - Select 802.11 Shared Key authentication.
- **Open System** - Select 802.11 Open System authentication.

WEP Key Format - You can select **ASCII** or **Hexadecimal** format. ASCII Format stands for any combination of keyboard characters in the specified length. Hexadecimal format stands for any combination of hexadecimal digits (0-9, a-f, A-F) in the specified length.

WEP Key settings - Select which of the four keys will be used and enter the matching WEP key information for your network in the selected key radio button. These values must be identical on all wireless stations in your network.

Key Type - You can select the WEP key length (**64-bit**, or **128-bit**, or **152-bit**.) for encryption. "Disabled" means this WEP key entry is invalid.

- For **64-bit** encryption - You can enter 10 hexadecimal digits (any combination of 0-9, a-f, A-F, and null key is not permitted) or 5 ASCII characters.
- For **128-bit** encryption - You can enter 26 hexadecimal digits (any combination of 0-9, a-f, A-F, and null key is not permitted) or 13 ASCII characters.
- For **152-bit** encryption - You can enter 32 hexadecimal digits (any combination of 0-9, a-f, A-F, and null key is not permitted) or 16 ASCII characters.

Status
--- Basic Settings ---
Quick Setup
WPS
Network
Wireless
Wireless Settings
Wireless Security
Wireless MAC Filtering
Wireless Advanced
Wireless Statistics
--- Advanced Settings ---
DHCP
Forwarding
Security
Parental Control
Access Control
Static Routing
IP QoS
IP & MAC Binding
Dynamic DNS
--- Maintenance ---
System Tools

Wireless MAC Filtering

Current SSID: TP-LINK_SS0024

Wireless MAC Filtering: Disabled Enable

Filtering Rules

- (•) Allow the stations not specified by any enabled entries in the list to access.
- ( ) Deny the stations not specified by any enabled entries in the list to access.

ID	MAC Address	Status	Description

Add New... Enable All Disable All Delete All

Previous Next

Wireless MAC Filtering Help

The Wireless MAC Address Filtering feature allows you to control the wireless stations accessing the AP, which depend on the station's MAC addresses.

- **MAC Address** - The wireless station's MAC address that you want to access.
- **Description** - A simple description of the wireless station.
- **Status** - The status of this entry , either **Enabled** or **Disabled**.

To disable the Wireless MAC Address Filters feature, keep the default setting, **Disable**.

To set up an entry, click **Enable**, and follow these instructions:
First, you must decide whether the unspecified wireless stations can or cannot access the AP. If you desire that the unspecified wireless stations can access the AP, please select the radio button **Allow the stations not specified by any enabled entries in the list to access**, otherwise, select the radio button **Deny the stations not specified by any enabled entries in the list to access**.

To Add a Wireless MAC Address filtering entry, clicking the **Add New...** button, and following these instructions:

1. Enter the appropriate MAC Address into the **MAC Address** field. The format of the MAC Address is XX-XX-XX-XX-XX-XX (X is any hexadecimal digit). For example, 00-0A-EB-B0-00-0B.
2. Enter a simple description of the wireless station in the **Description** field. For example, Wireless station A.
3. **Status** - Select **Enabled** or **Disabled** for this entry on the **Status** pull-down list.
4. Click the **Save** button to save this entry.

To add another entries, repeat steps 1~4.

Status
--- Basic Settings ---
Quick Setup
WPS
Network
Wireless
Wireless Settings
Wireless Security
Wireless MAC Filtering
Wireless Advanced
Wireless Statistics
--- Advanced Settings ---
DHCP
Forwarding
Security
Parental Control
Access Control
Static Routing
IP QoS
IP & MAC Binding
Dynamic DNS
--- Maintenance ---
System Tools

Wireless Advanced

Transmit Power:	High
Beacon Interval:	100 (40-1000)
RTS Threshold:	2346 (1-2346)
Fragmentation Threshold:	2346 (256-2346)
DTIM Interval:	1 (1-255)

☑ Enable WMM
☑ Enable Short GI
☐ Enable AP Isolation

Save

Wireless Advanced Help

- **Transmit Power** - Here you can specify the transmit power of the Router. You can select High, Middle or Low which you would like. High is the default setting and is recommended.
- **Beacon Interval** - The beacons are the packets sent by the Router to synchronize a wireless network. Beacon Interval value determines the time interval of the beacons. You can specify a value between 40-1000 milliseconds. The default value is 100.
- **RTS Threshold** - Here you can specify the RTS (Request to Send) Threshold. If the packet is larger than the specified RTS Threshold size, the Router will send RTS frames to a particular receiving station and negotiate the sending of a data frame. The default value is 2346.
- **Fragmentation Threshold** - This value is the maximum size determining whether packets will be fragmented. Setting the Fragmentation Threshold too low may result in poor network performance since excessive packets. 2346 is the default setting and is recommended.
- **DTIM Interval** - This value determines the interval of the Delivery Traffic Indication Message (DTIM). You can specify the value between 1-255 Beacon Intervals. The default value is 1, which indicates the DTIM Interval is the same as Beacon Interval.
- **Enable WMM** - WMM function can guarantee the packets with high- priority messages being transmitted preferentially. It is strongly recommended enabled.
- **Enable Short GI** - This function is recommended for it will increase the data capacity by reducing the guard interval time.
- **Enable AP Isolation** - Isolate all connected wireless stations so that wireless stations cannot access each other through WLAN. This function will be disabled if WDS/Bridge is enabled.

Status
--- Basic Settings ---
Quick Setup
WPS
Network
Wireless
--- Advanced Settings ---
DHCP
DHCP Settings
DHCP Clients List
Address Reservation
Forwarding
Security
Parental Control
Access Control
Static Routing
IP QoS
IP & MAC Binding
Dynamic DNS
--- Maintenance ---
System Tools

DHCP Settings

DHCP Server:	○ Disable ◉ Enable
Start IP Address:	192.168.10.100
End IP Address:	192.168.10.199
Address Lease Time:	120 minutes (1~2880 minutes, the default value is 1
Default Gateway:	0.0.0.0 (optional)
Default Domain:	(optional)
Primary DNS:	187.94.192.61 (optional)
Secondary DNS:	187.94.192.62 (optional)

Save

DHCP Settings Help

The Router is set up by default as a DHCP (Dynamic Host Configuration Protocol) server, which provides the TCP/IP configuration for all the PCs that are connected to the Router in the LAN.

- **DHCP Server** - **Enable** or **Disable** the server. If you disable the Server, you must have another DHCP server within your network or else you must configure the IP address of the computer manually.
- **Start IP Address** - This field specifies the first address in the IP Address pool. 192.168.0.100 is the default start IP address.
- **End IP Address** - This field specifies the last address in the IP Address pool. 192.168.0.199 is the default end IP address.
- **Address Lease Time** - The **Address Lease Time** is the length of time a network user will be allowed to keep connecting to the Router with the current DHCP Address. Enter the amount of time, in minutes, that the DHCP address will be "leased". The time range is 1~2880 minutes. The default value is 120 minutes.
- **Default Gateway** - (Optional) Suggest to input the IP Address of the LAN port of the Router, default value is 0.0.0.0.
- **Default Domain** - (Optional) Input the domain name of your network.
- **Primary DNS** - (Optional) Input the DNS IP address provided by your ISP. Or consult your ISP.
- **Secondary DNS** - (Optional) You can input the IP Address of another DNS server if your ISP provides two DNS servers.

Status
--- Basic Settings ---
Quick Setup
WPS
Network
Wireless
--- Advanced Settings ---
DHCP
DHCP Settings
DHCP Clients List
Address Reservation
Forwarding
Security
Parental Control
Access Control
Static Routing
IP QoS
IP & MAC Binding
Dynamic DNS
--- Maintenance ---
System Tools

DHCP Clients List

ID	Client Name	MAC Address
1	none	54-C9-DF-F6-C7-2D
2	ImobiliariaPrad	00-E0-4C-80-01-4B
3	android-8fce24205d0f7a64	38-9A-F6-4E-E5-A9
4	android-9d119fe8014cd	E8-B4-C8-21-64-A6

Refresh

DHCP Clients List Help

This page shows **Client Name**, **MAC Address**, **Assigned IP** and **Lease Time** of each DHCP Client connected to the Router.

- **Client Name** - The name of the DHCP client.
- **MAC Address** - The MAC address of the DHCP client.
- **Assigned IP** - The IP address that the Router has allocated to the DHCP client.
- **Lease Time** - The time of the DHCP client leased.

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

Status
--- Basic Settings ---
Quick Setup
WPS
Network
Wireless
--- Advanced Settings ---
DHCP
DHCP Settings
DHCP Clients List
Address Reservation
Forwarding
Security
Parental Control
Access Control
Static Routing
IP QoS
IP & MAC Binding
Dynamic DNS
--- Maintenance ---
System Tools

Address Reservation

ID	MAC Address	Reserved IP Address

Add New... | Enable All | Disable All | Delete All

Previous | Next

Address Reservation Help

When you specify a reserved IP address for a PC in the LAN, that PC will always receive the same IP address each time when it accesses the DHCP server. Reserved IP addresses could be assigned to servers that require permanent IP settings.

- **MAC Address** - The MAC Address of the PC that you want to reserve an IP address for.
- **Reserved IP Address** - The IP address that the Router reserved.
- **Status** - It shows whether the entry is enabled or not
- **Modify** - To modify or delete an existing entry.

To Reserve IP Addresses, you can follow these steps:

1. Enter the MAC Address (The format for the MAC Address is XX-XX-XX-XX-XX-XX) and the IP address in dotted-decimal notation of the computer you wish to add.
2. Click the **Save** button.

To modify a Reserved IP Address, you can follow these steps:

1. Select the reserved address entry as you desired, modify it. If you wish to delete the entry, click the **Delete** link of the entry.
2. Click the **Save** button.

Click the **Add New...** button to add a new Address Reservation entry.

Status
--- Basic Settings ---
Quick Setup
WPS
Network
Wireless
--- Advanced Settings ---
DHCP
Forwarding
Virtual Servers
Port Triggering
DMZ
UPnP
Security
Parental Control
Access Control
Static Routing
IP QoS
IP & MAC Binding
Dynamic DNS
--- Maintenance ---
System Tools

Virtual Servers

ID	Service Ports	IP Address	Protocol

Add New... | Enable All | Disable All | Delete All

Previous | Next

Virtual Servers Help

Virtual servers can be used for setting up public services on your LAN. A virtual server is defined as a service port, and all requests from 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 change when using the DHCP function.

- **Service Port** - The numbers of External Ports. You can enter a service port or a range of service ports (the format is XXX - YYY, XXX is Start port, YYY is End port).
- **IP Address** - The IP address of the PC running 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, "Enabled" means the virtual server entry is enabled.
- **Common Service Port** - Some common services already exist in the pull-down list.
- **Modify** - To modify or delete an existing entry.

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** menu does not list the service that you want to use, enter the number of the service port or service port range in the **Service Port** box.
3. Enter the IP address of the computer running the service application in the **IP Address** box.
4. Select the protocol used for this application in the Protocol box, either **TCP**, **UDP**, or **All**.
5. Select the **Enabled** option in the **Status** pull-down list.
6. Click the **Save** button.

Status
--- Basic Settings ---
Quick Setup
WPS
Network
Wireless
--- Advanced Settings ---
DHCP
Forwarding
Virtual Servers
Port Triggering
DMZ
UPnP
Security
Parental Control
Access Control
Static Routing
IP QoS
IP & MAC Binding
Dynamic DNS
--- Maintenance ---
System Tools

Add or Modify a Virtual Server Entry

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

Save Back

Virtual Servers Help

Virtual servers can be used for setting up public services on your LAN. A virtual server is defined as a service port, and all requests from 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 change when using the DHCP function.

- **Service Port** - The numbers of External Ports. You can enter a service port or a range of service ports (the format is XXX - YYY, XXX is Start port, YYY is End port).
- **IP Address** - The IP address of the PC running 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, "Enabled" means the virtual server entry is enabled.
- **Common Service Port** - Some common services already exist in the pull-down list.
- **Modify** - To modify or delete an existing entry.

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** menu does not list the service that you want to use, enter the number of the service port or service port range in the **Service Port** box.
3. Enter the IP address of the computer running the service application in the **IP Address** box.
4. Select the protocol used for this application in the Protocol box, either **TCP**, **UDP**, or **All**.
5. Select the **Enabled** option in the **Status** pull-down list.
6. Click the **Save** button.

Status
--- Basic Settings ---
Quick Setup
WPS
Network
Wireless
--- Advanced Settings ---
DHCP
Forwarding
Virtual Servers
Port Triggering
DMZ
UPnP
Security
Parental Control
Access Control
Static Routing
IP QoS
IP & MAC Binding
Dynamic DNS
--- Maintenance ---
System Tools

DMZ

Current DMZ Status: ○ Enable ◉ Disable

DMZ Host IP Address: 0.0.0.0

Save

DMZ Help

The DMZ host feature allows one local host to be exposed to the Internet for a special-purpose service such as Internet gaming or video conferencing. The Router forwards packets of all services to the DMZ host. Any PC that is set to be DMZ host must have its DHCP client function disabled and should have a new static IP address assigned to it because its IP Address may change when using the DHCP function.

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

1. Click the **Enable** button.
2. Enter the IP address of a local PC that is set to be DMZ host in the **DMZ Host IP Address** field.
3. Click the **Save** button.

Status
--- Basic Settings ---
Quick Setup
WPS
Network
Wireless
--- Advanced Settings ---
DHCP
Forwarding
Virtual Servers
Port Triggering
DMZ
UPnP
Security
Parental Control
Access Control
Static Routing
IP QoS
IP & MAC Binding
Dynamic DNS
--- Maintenance ---
System Tools

UPnP

Current UPnP Status: Enabled Disable

Current UPnP Settings List

ID	App Description	External Port	Protocol	Internal

Refresh

UPnP Help

The Universal Plug and Play (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.

Enable UPnP - UPnP can be enabled or disabled by clicking the **Enable** or **Disable** button. This feature is enabled by default.

Current UPnP Settings List:

This table displays the current UPnP information.

- **App Description** - The description about the application which initiates the UPnP request.
- **External Port** - External port, which the Router opened for the application.
- **Protocol** - Which type of protocol is opened.
- **Internal Port** - Internal port, which the Router opened for local host.
- **IP Address** - The IP address of the local host which initiates the UPnP request.
- **Status** - Either Enabled or Disabled, "Enabled" means that port is still active, otherwise, the port is inactive.

Click the **Enable** button to enable UPnP.

Click the **Disable** button to disable UPnP.

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

Status
--- Basic Settings ---
Quick Setup
WPS
Network
Wireless
--- Advanced Settings ---
DHCP
Forwarding
Security
Firewall
IP Address Filtering
Domain Filtering
MAC Address Filtering
Local Management
Remote Management
Advanced Security
Parental Control
Access Control
Static Routing
IP QoS
IP & MAC Binding
Dynamic DNS
--- Maintenance ---
System Tools

Firewall

☐ Enable Firewall (the general firewall switch)

☐ Enable IP Address Filtering

Default IP Address Filtering Rules:

○ Allow the packets not specified by any filtering rules to pass through the device

◉ Deny the packets not specified by any filtering rules to pass through the device

☐ Enable Domain Filtering

☐ Enable MAC Address Filtering

Default MAC Address Filtering Rules:

○ Allow these PCs with enabled rules to access the Internet

◉ Deny these PCs with enabled rules to access the Internet

Save

Firewall Help

Using the **Firewall** page, you can turn the general firewall switch on or off. The default setting for the switch is off. Turning the general firewall switch off will disable IP Address Filtering, Domain Filtering and MAC Address Filtering even if their individual settings are enabled.

- **Enable Firewall** - Enable or disable the function of Firewall.
- **Enable IP Address Filtering** - Enable or disable the function of IP Address Filtering. There are two default filtering rules for IP Address Filtering: Allow or Deny the packets not specified by any filtering rules to pass through the device.
- **Enable Domain Filtering** - Enable or disable the function of Domain Filtering.
- **Enable MAC Address Filtering** - Enable or disable the function of MAC Address Filtering. There are two default filtering rules for MAC Address Filtering: Allow or Deny these PCs with enabled rules to access the Internet.

When finished, click the **Save** button to save your settings.

Status
--- Basic Settings ---
Quick Setup
WPS
Network
Wireless
--- Advanced Settings ---
DHCP
Forwarding
Security
Firewall
IP Address Filtering
Domain Filtering
MAC Address Filtering
Local Management
Remote Management
Advanced Security
Parental Control
Access Control
Static Routing
IP QoS
IP & MAC Binding
Dynamic DNS
--- Maintenance ---
System Tools

IP Address Filtering

Firewall Settings (You can change them on Firewall page)

Enable Firewall: Disabled

Enable IP Address Filtering: Disabled

Default Filtering Rules: Deny the packets not specified by any filtering rule

ID	Effective time	LAN IP Address	LAN Port	WAN IP Address	WAN F

Add New... | Enable All | Disable All | Delete All

Move ID to ID

Previous | Next

IP Address Filtering Help

The **IP Address Filtering** feature allows you to control Internet Access by specific users in your LAN based on their IP addresses. To disable the **IP Address Filtering** feature, keep the IP Address Filtering setting **Disabled**.

To set up an **IP Address Filtering** entry, both **Enable Firewall** and **Enable IP Filtering** should be firstly selected on the **Firewall** page, and click the **Add New...** button, and then follow these instructions:

1. **Effective Time** - Enter the range of time in HHMM format, which points to the range time for the entry to take effect. For example, 0803 - 1705, the entry will take effect from 08:03 to 17:05.
2. **LAN IP Address** - Enter a LAN IP address or the range of LAN IP addresses in the field, in dotted-decimal notation format. For example, 192.168.0.20 - 192.168.0.30. Keep the field blank, which means all LAN IP addresses have been put into the field.
3. **LAN Port** - Enter a LAN Port or the range of LAN ports in the field. For example, 1030 - 2000. Keep the field blank, which means all LAN ports have been put into the field.
4. **WAN IP Address** - Enter a WAN IP address or the range of WAN IP addresses in the field, in dotted-decimal notation format. For example, 61.145.238.6 - 61.145.238.47. Keep the field blank, which means all WAN IP addresses have been put into the field.
5. **WAN Port** - Enter a WAN port or the range of WAN ports in the field. For example, 25 - 110. Keep the field blank, which means all WAN ports have been put into the field.
6. **Protocol** - Select which protocol is to be used, either **TCP**, **UDP**, or **All** (all protocols supported by the Router).
7. **Action** - Select either **Allow** or **Deny** the packets specified by the filtering rule pass through the Router.

Status
--- Basic Settings ---
Quick Setup
WPS
Network
Wireless
--- Advanced Settings ---
DHCP
Forwarding
Security
Firewall
IP Address Filtering
Domain Filtering
MAC Address Filtering
Local Management
Remote Management
Advanced Security
Parental Control
Access Control
Static Routing
IP QoS
IP & MAC Binding
Dynamic DNS
--- Maintenance ---
System Tools

MAC Address Filtering

Firewall Settings (You can change them on Firewall page)

Enable Firewall: Disabled

Enable MAC Address Filtering: Disabled

Default Filtering Rules: Deny these PCs with the enabled rules to access

ID	MAC Address	Description	Status	Modif

Add New... | Enable All | Disable All | Delete All

Previous | Next

MAC Address Filtering Help

Similar to **IP Address Filtering** page, the **MAC Address Filtering** page allows you to control to access Internet by users on your local network based on their MAC Addresses. Before setting up MAC Filtering entries, you must ensure that **Enable Firewall** and **Enable MAC Address Filtering** have been selected on the **Firewall** page.

To Add a MAC Address filtering entry, click the **Add New...** button, and follow these instructions:

1. Enter an appropriate MAC address into the **MAC Address** field. The format of the MAC address is XX-XX-XX-XX-XX-XX (X is any hexadecimal digit). For example: 00-0A-EB-B0-00-0B.
2. Enter a simple description of the station in the **Description** field. For example: John's PC.
3. **Status** - Select **Enabled** or **Disabled** for this entry from the **Status** pull-down list.
4. Click the **Save** button to save this entry.

To add another entry, repeat steps 1-4.

To modify or delete an existing entry:

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

Click the **Enable All** button to make all entries enabled.

Click the **Disable All** button to make all entries disabled.

Click the **Delete All** button to delete all entries.

Status
--- Basic Settings ---
Quick Setup
WPS
Network
Wireless
--- Advanced Settings ---
DHCP
Forwarding
Security
Firewall
IP Address Filtering
Domain Filtering
MAC Address Filtering
Local Management
Remote Management
Advanced Security
Parental Control
Access Control
Static Routing
IP QoS
IP & MAC Binding
Dynamic DNS
--- Maintenance ---
System Tools

Remote Management

Web Management Port: 58080

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

Save

Remote Management Help

This feature allows you to manage your Router from a remote location via the Internet.

- **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.

To access the Router, you should enter your Router's WAN IP address into your browser's address (in IE) or location (in Netscape) box, followed by a colon and the custom port number you set in the Web Management Port box. For example, if your Router's WAN address is 202.96.12.8 and you use port number 8080, enter http://202.96.12.8:8080 in your browser. You will be asked for the Router's password. After successfully entering the password, you will be able to access the Router's web-based utility.

Note:

1. Be sure to change the Router's default password to a secure password.
2. If the web management port conflicts with the one used for a **Virtual Server** entry, the entry will be automatically **disabled** after the setting is saved.

Status
--- Basic Settings ---
Quick Setup
WPS
Network
Wireless
--- Advanced Settings ---
DHCP
Forwarding
Security
Firewall
IP Address Filtering
Domain Filtering
MAC Address Filtering
Local Management
Remote Management
Advanced Security
Parental Control
Access Control
Static Routing
IP QoS
IP & MAC Binding
Dynamic DNS
--- Maintenance ---
System Tools

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

Advanced Security Help

Using the **Advanced Settings** page, you can protect the Router from being attacked by TCP-SYN Flood, UDP Flood and ICMP-Flood.

Note: FLOOD Filtering will take effect only when the **Statistics** in **System Tools** is enabled.

- **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 value indicates the time section of the packets statistic. The result of the statistic used for analysis by SYN Flood, UDP Flood and ICMP-Flood.
- **DoS Protection** - Enable or Disable the DoS protection function. Only when it is enabled, will the flood filters be 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.

Status
--- Basic Settings ---
Quick Setup
WPS
Network
Wireless
--- Advanced Settings ---
DHCP
Forwarding
Security
Parental Control
Access Control
Rule
Host
Target
Schedule
Static Routing
IP QoS
IP & MAC Binding
Dynamic DNS
--- Maintenance ---
System Tools

Access Control Rule Management

☐ Enable Internet Access Control

Default Filter Policy

○ Allow the packets specified by any enabled access control policy to pass through the Router

◉ Deny the packets specified by any enabled access control policy to pass through the Router

Save

ID	Rule Name	Host	Target	Schedule	Enable

Setup Wizard

Add New... Enable All Disable All Delete All

Move ID To ID

Previous Next Current No. 1

Internet Access Control Rule Management Help

The Router, providing convenient and strong **internet access control** function, can control the internet activities of hosts in the LAN. Moreover, you can flexibly combine the **Host List**, **Target List** and **Schedule** to restrict the Internet surfing of these hosts.

- **Enable Internet Access Control** - Select the check box to enable the Internet Access Control function, so the Default Filter Rule 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.
- **Enable** - Check this option to enable a specific entry.
- **Modify** - Here you can edit or delete an existing rule.

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 the submenu **Rule** of **Access Control** in the left to return to the Rule List page. Select Enable Internet Access Control and choose "Allow the packets specified by any enabled access control policy to pass through the Router".
2. We recommend that you click **Setup Wizard** button to finish all the following settings.
3. Click the submenu **Host** of **Access Control** in the left to enter the Host List page. Add a new entry with the Host Description is Host_1 and MAC Address is 00-11-22-33-44-AA.

Status
--- Basic Settings ---
Quick Setup
WPS
Network
Wireless
--- Advanced Settings ---
DHCP
Forwarding
Security
Parental Control
Access Control
Static Routing
Static Routing List
IP QoS
IP & MAC Binding
Dynamic DNS
--- Maintenance ---
System Tools

Static Routing List

ID	Destination IP Address	Subnet Mask	Default Ga

Add New... | Enable All | Disable All | Delete All

Previous | Next

Static Routing Help

A static route is a pre-determined path that network information must follow to reach a specific host or network. Use the Static Routing page to add or delete a route.

To add static routing entries:

1. Click the **Add New...** button.
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.
   - **Default Gateway** - This is the IP address of the default gateway device that allows for the contact between the Router and the network or host.
3. Select the **Enabled** in the **Status** pull-down list.
4. Click the **Save** button to save the changes.

To modify or delete an existing entry:

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

Click the **Enable All** button to enable all entries.

Click the **Disable All** button to disable all entries.

Click the **Delete All** button to delete all entries.

Status
--- Basic Settings ---
Quick Setup
WPS
Network
Wireless
--- Advanced Settings ---
DHCP
Forwarding
Security
Parental Control
Access Control
Static Routing
IP QoS
IP & MAC Binding
Dynamic DNS
--- Maintenance ---
System Tools

IP QoS

☐ Enable IP QoS

Choose BandWidth Type: ADSL

Bandwidth Apply: 2000 Kbps

ID	IP Range	Mode	Bandwi
1	192.168.10. - 192.168.10.	Minimum Bandwidth Guarantee	
2	192.168.10. - 192.168.10.	Minimum Bandwidth Guarantee	
3	192.168.10. - 192.168.10.	Minimum Bandwidth Guarantee	
4	192.168.10. - 192.168.10.	Minimum Bandwidth Guarantee	
5	192.168.10. - 192.168.10.	Minimum Bandwidth Guarantee	
6	192.168.10. - 192.168.10.	Minimum Bandwidth Guarantee	
7	192.168.10. - 192.168.10.	Minimum Bandwidth Guarantee	
8	192.168.10. - 192.168.10.	Minimum Bandwidth Guarantee	

Clear All

Save

IP QoS Help

You can configure the IP QoS function on this page.

- **Enable IP QoS** - Enable or disable the function of IP QoS.
- **Choose BandWidth Type** - Network connection type.
- **Bandwidth Apply** - Bandwidth you get. If you are not clear about that, please contact with your ISP for help.
- **IP Range** - IP range of this entry.
- **Mode** - There are 2 types of mode: Minimum Bandwidth Guarantee and Maximum Bandwidth Limit.
- **Bandwidth** - Bandwidth you supply to this entry.
- **Description** - Description of this entry.
- **Enable** - Enable this entry.

Click the **Clear** button to clear single entry.

Click the **Clear All** button to clear all entries.

Click the **Save** button to save all configurations.

Note:

- The conversion relation of bandwidth: 1Mbps = 1000Kbps.
- Please choose the Network Connection Type and set the bandwidth according to your Network. If you are not clear about that, please contact with your ISP for help.
- If no IP QoS item is enabled, the Bandwidth Apply won't be effective.
- IP address range for different entries could not have intersection with each other.
- After the configurations, click the **Save** button for the change to take effect.

Status
--- Basic Settings ---
Quick Setup
WPS
Network
Wireless
--- Advanced Settings ---
DHCP
Forwarding
Security
Parental Control
Access Control
Static Routing
IP QoS
IP & MAC Binding
Binding Settings
ARP List
Dynamic DNS
--- Maintenance ---
System Tools

ARP List

ID	MAC Address	IP Address	Status	Configur
1	54-C9-DF-F6-C7-2D	192.168.10.101	Unbound	Load Dele
2	38-9A-F6-4E-E5-A9	192.168.10.104	Unbound	Load Dele

Bind All | Load All | Refresh

ARP List Help

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.

- **MAC Address** - The MAC address of a controlled computer in the LAN.
- **IP Address** - The assigned IP address of a controlled computer in the LAN.
- **Status** - Indicates whether or not the MAC and IP addresses are bound.
- **Configure** - These buttons are for loading or deleting an item.
  - **Load** - Load the item to the IP & MAC Binding list.
  - **Delete** - Delete the item from the list.
- **Bind All** - Bind all current items. This option is only available when ARP Binding is enabled and saved in the Binding Setting page.
- **Load All** - Load all items into the IP & MAC Binding list.

Note: An item can not be loaded to the IP & MAC Binding list if the IP address of the item has been loaded before. Error warning will prompt as well. Likewise, "Load All" only loads the items have no interference with the IP & MAC Binding list.

Status
--- Basic Settings ---
Quick Setup
WPS
Network
Wireless
--- Advanced Settings ---
DHCP
Forwarding
Security
Parental Control
Access Control
Static Routing
IP QoS
IP & MAC Binding
Dynamic DNS
--- Maintenance ---
System Tools
Time Settings
Diagnostic
Firmware Upgrade
Factory Defaults
Backup & Restore
Reboot
Password
System Log
Statistics

Time Settings

Time zone: (GMT+08:00) Beijing, Hong Kong, Perth, Singapore

Date: 7 5 2018 (MM/DD/YY)

Time: 19 28 31 (HH/MM/SS)

Primary NTP Server: 187.94.192.61 (Optional)

Secondary NTP Server: pool.ntp.br (Optional)

Get GMT

☐ Enable Daylight Saving

Note:Click the "GET GMT" to update the time from the internet with the

or entering the customized server(IP Address or Domain Name) in

Save

Time Settings Help

This page allows you to set the time manually or to configure automatic time synchronization. The Router can automatically update the time from an NTP server via the Internet.

Time Zone - Select your local time zone from this pull-down list.

To set time manually:

1. Select your local time zone.
2. Enter the **Date** in Month/Day/Year format.
3. Enter the **Time** in Hour/Minute/Second format.
4. Click **Save**.

For automatic time synchronization:

1. Enter the address of the **NTP Server I**.
2. Click the **Get GMT** button to get GMT from the Internet.

To enable daylight saving:

1. Select the **Enable Daylight Saving** checkbox to enable daylight saving function.
2. Select the correct **Start** time and **End** time for daylight saving range.
3. Click **Save**.

Note:

1. This setting will be used for some time-based functions such as firewall functions. These time dependant functions will not work if time is not set. So, it is important to specify time settings as soon as you successfully login to the Router.
2. The time will be lost if the Router is turned off.
3. The Router will automatically obtain GMT from the Internet if it is configured accordingly.
4. In daylight saving configuration, start time shall be earlier than end time.

Status
--- Basic Settings ---
Quick Setup
WPS
Network
Wireless
--- Advanced Settings ---
DHCP
Forwarding
Security
Parental Control
Access Control
Static Routing
IP QoS
IP & MAC Binding
Dynamic DNS
--- Maintenance ---
System Tools
Time Settings
Diagnostic
Firmware Upgrade
Factory Defaults
Backup & Restore
Reboot
Password
System Log
Statistics

Diagnostic Tools

Diagnostic Parameters

Diagnostic Tool:	(•) Ping ( ) Traceroute
IP Address/ Domain Name:	ix.br
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

```
Pinging ix.br [200.160.6.220] with 64 bytes of data:

Reply from 200.160.6.220:  bytes=64  time=16  TTL=56  seq=1
Reply from 200.160.6.220:  bytes=64  time=16  TTL=56  seq=2
Reply from 200.160.6.220:  bytes=64  time=16  TTL=56  seq=3
Reply from 200.160.6.220:  bytes=64  time=16  TTL=56  seq=4

Ping statistics for ix.br
 Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milliseconds:
 Minimum = 16, Maximum = 16, Average = 16
```

Start

Diagnostic Tools Help

The diagnostic tools (Ping and Traceroute) allow you to check the connections of your network components.

Diagnostic Tool - Click the radio button to select one diagnostic tool:

- **Ping** - This diagnostic tool troubleshoots connectivity, reachability, and name resolution to a given host or gateway by using the Internet Control Message Protocol (ICMP) protocol's mandatory Echo Request datagram to elicit an ICMP Echo Response from a host or gateway. You can use ping to test both numeric IP address or domain name. If pinging the IP address is successful, but pinging 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.
- **Traceroute** - This diagnostic tool determines the path taken to a given host by sending Internet Control Message Protocol (ICMP) Echo Request messages with varying Time to Live (TTL) values to the destination. Each gateway along the path is required to decrement the TTL in an IP packet by at least 1 before forwarding it. Effectively, the TTL is a maximum link counter. When the TTL on a packet reaches 0, the gateway is expected to return an ICMP Time Exceeded response to your Router. Traceroute determines the path by sending the first Echo Request message with a TTL of 1 and incrementing the TTL by 1 on each subsequent transmission until the target responds or the maximum number of hops is reached. The maximum number of hops is 20 by default and can be specified in the field "Traceroute Max TTL". The path is determined by examining the ICMP Time Exceeded messages returned by intermediate gateways and the Echo Reply message returned by the destination. However, some gateways do not

Status
--- Basic Settings ---
Quick Setup
WPS
Network
Wireless
--- Advanced Settings ---
DHCP
Forwarding
Security
Parental Control
Access Control
Static Routing
IP QoS
IP & MAC Binding
Dynamic DNS
--- Maintenance ---
System Tools
Time Settings
Diagnostic
Firmware Upgrade
Factory Defaults
Backup & Restore
Reboot
Password
System Log
Statistics

Diagnostic Tools

Diagnostic Parameters

Diagnostic Tool:	○ Ping ◉ Traceroute
IP Address/ Domain Name:	ix.br
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

Tracing route to ix.br [200.160.6.220] over a maximum of 20 hops

```
1   1ms   1ms   1ms   172.23.212.113
2   1ms   1ms   1ms   10.12.1.1
3   1ms   1ms   1ms   10.99.99.69
4   1ms   1ms   1ms   10.5.7.4
5 16ms 16ms 16ms   187.16.217.2
6 16ms 16ms 16ms   200.160.0.158
7 16ms 16ms 16ms   200.160.0.250
8 16ms 16ms 16ms   200.160.6.220
```

Trace complete.

Start

Diagnostic Tools Help

The diagnostic tools (Ping and Traceroute) allow you to check the connections of your network components.

Diagnostic Tool - Click the radio button to select one diagnostic tool:

- **Ping** - This diagnostic tool troubleshoots connectivity, reachability, and name resolution to a given host or gateway by using the Internet Control Message Protocol (ICMP) protocol's mandatory Echo Request datagram to elicit an ICMP Echo Response from a host or gateway. You can use ping to test both numeric IP address or domain name. If pinging the IP address is successful, but pinging 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.
- **Traceroute** - This diagnostic tool determines the path taken to a given host by sending Internet Control Message Protocol (ICMP) Echo Request messages with varying Time to Live (TTL) values to the destination. Each gateway along the path is required to decrement the TTL in an IP packet by at least 1 before forwarding it. Effectively, the TTL is a maximum link counter. When the TTL on a packet reaches 0, the gateway is expected to return an ICMP Time Exceeded response to your Router. Traceroute determines the path by sending the first Echo Request message with a TTL of 1 and incrementing the TTL by 1 on each subsequent transmission until the target responds or the maximum number of hops is reached. The maximum number of hops is 20 by default and can be specified in the field "Traceroute Max TTL". The path is determined by examining the ICMP Time Exceeded messages returned by intermediate gateways and the Echo Reply message returned

Status
--- Basic Settings ---
Quick Setup
WPS
Network
Wireless
--- Advanced Settings ---
DHCP
Forwarding
Security
Parental Control
Access Control
Static Routing
IP QoS
IP & MAC Binding
Dynamic DNS
--- Maintenance ---
System Tools
Time Settings
Diagnostic
Firmware Upgrade
Factory Defaults
Backup & Restore
Reboot
Password
System Log
Statistics

Firmware Upgrade

File: Selecionar arquivo... Nenhum arquivo selecionado.

Firmware Version: 4.19.47 Build 120516 Rel.37372n

Hardware Version: WR720N 1.0 00000000

Upgrade

Firmware Upgrade Help

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

1. Download a most recent firmware upgrade file from our website (www.tp-link.com).
2. Enter or select the path name where you save the downloaded file on the computer into the **File Name** blank.
3. Click the **Upgrade** button.
4. The Router will reboot while the upgrading has been finished.

Firmware Version - Displays the current firmware version.

Hardware Version - Displays the current hardware version. The hardware version of the upgrade file must accord with the current hardware version.

Note: The firmware version must correspond to the hardware. The upgrade process takes a few moments and the Router restarts automatically when the upgrade is complete. It is important to keep power applied during the entire process. Loss of power during the upgrade could damage the Router.

Status
--- Basic Settings ---
Quick Setup
WPS
Network
Wireless
--- Advanced Settings ---
DHCP
Forwarding
Security
Parental Control
Access Control
Static Routing
IP QoS
IP & MAC Binding
Dynamic DNS
--- Maintenance ---
System Tools
Time Settings
Diagnostic
Firmware Upgrade
Factory Defaults
Backup & Restore
Reboot
Password
System Log
Statistics

Backup & Restore

Backup: Backup

File: Selecionar arquivo... Nenhum arquivo selecionado. Restore

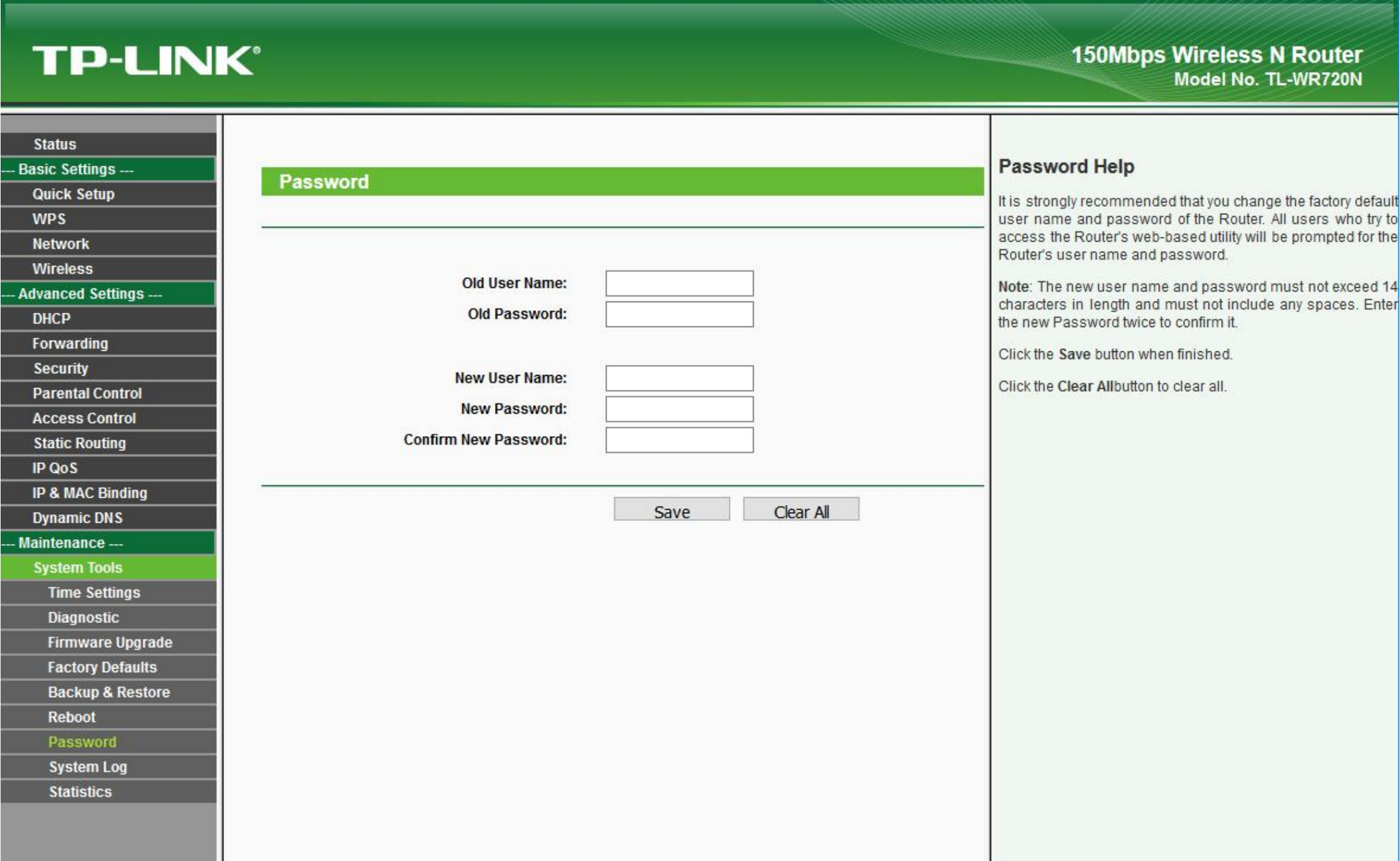
Backup & Restore Help

Click the **Backup** button to save all configuration settings to your local computer as a file.

To restore the Router's configuration, follow these instructions:

- Click the **Browse** button to find the configuration file which you want to restore.
- Click the **Restore** button to update the configuration with the file whose path is the one you have input or selected in the blank.

Note: The current configuration will be covered with the uploading configuration file. Wrong process will lead the device unmanaged. The restoring process lasts for 20 seconds and the Router will restart automatically then. Keep the power of the Router on during the process, in case of any damage.


TP-LINK
150Mbps Wireless N Router
Model No. TL-WR720N
Status
--- Basic Settings ---
Quick Setup
WPS
Network
Wireless
--- Advanced Settings ---
DHCP
Forwarding
Security
Parental Control
Access Control
Static Routing
IP QoS
IP & MAC Binding
Dynamic DNS
--- Maintenance ---
System Tools
Time Settings
Diagnostic
Firmware Upgrade
Factory Defaults
Backup & Restore
Reboot
Password
System Log
Statistics
Password
Old User Name:
Old Password:
New User Name:
New Password:
Confirm New Password:
Save
Clear All
Password Help
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 will be prompted for the Router's 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 it.
Click the Save button when finished.
Click the Clear Allbutton to clear all.

Status
--- Basic Settings ---
Quick Setup
WPS
Network
Wireless
--- Advanced Settings ---
DHCP
Forwarding
Security
Parental Control
Access Control
Static Routing
IP QoS
IP & MAC Binding
Dynamic DNS
--- Maintenance ---
System Tools
Time Settings
Diagnostic
Firmware Upgrade
Factory Defaults
Backup & Restore
Reboot
Password
System Log
Statistics

System Log

Auto Mail Feature: Disabled Mail Settings Mail Log

Index	Level	Log Content
400	INFO	INFO 2018-07-05 19:00:35|DHCPS: 1:0x54c9dff6c72d, 192.168.10.101, ACK in request.
399	INFO	INFO 2018-07-05 18:42:15|DHCPS: 1:0x00e04c80014b, 192.168.10.100, ACK in request
398	INFO	INFO 2018-07-05 18:41:25|DHCPS: 1:0x389af64ee5a9, 192.168.10.104, ACK in request.
397	INFO	INFO 2018-07-05 18:00:35|DHCPS: 1:0x54c9dff6c72d, 192.168.10.101, ACK in request.
396	INFO	INFO 2018-07-05 17:57:46|DHCPS: 1:0xe8b4c82164a6, 192.168.10.105, ACK in request
395	INFO	INFO 2018-07-05 17:00:34|DHCPS: 1:0x54c9dff6c72d, 192.168.10.101, ACK in request.
394	INFO	INFO 2018-07-05 16:06:56|DHCP client read, totlen = 368(1048).
393	INFO	INFO 2018-07-05 16:00:34|DHCPS: 1:0x54c9dff6c72d, 192.168.10.101, ACK in request.
392	INFO	INFO 2018-07-05 15:00:33|DHCPS: 1:0x54c9dff6c72d, 192.168.10.101, ACK in request.
391	INFO	INFO 2018-07-05 14:00:33|DHCPS: 1:0x54c9dff6c72d, 192.168.10.101, ACK in request.
390	INFO	INFO 2018-07-05 13:00:32|DHCPS: 1:0x54c9dff6c72d, 192.168.10.101, ACK in request.
389	INFO	INFO 2018-07-05 12:00:32|DHCPS: 1:0x54c9dff6c72d, 192.168.10.101, ACK in request.
388	INFO	INFO 2018-07-05 11:00:32|DHCPS: 1:0x54c9dff6c72d, 192.168.10.101, ACK in request.
387	INFO	INFO 2018-07-05 10:00:31|DHCPS: 1:0x54c9dff6c72d, 192.168.10.101, ACK in request.
386	INFO	INFO 2018-07-05 09:00:31|DHCPS: 1:0x54c9dff6c72d, 192.168.10.101, ACK in request.
385	INFO	INFO 2018-07-05 08:00:30|DHCPS: 1:0x54c9dff6c72d, 192.168.10.101, ACK in request.
384	INFO	INFO 2018-07-05 07:00:30|DHCPS: 1:0x54c9dff6c72d, 192.168.10.101, ACK in request.
383	INFO	INFO 2018-07-05 06:06:23|DHCPS: 1:0x9cb70dd52439, 192.168.10.106, ACK in request
382	INFO	INFO 2018-07-05 06:06:07|DHCPS: 1:0x88797e30f077, 192.168.10.110, ACK in request.
381	INFO	INFO 2018-07-05 06:01:06|DHCPS: 1:0x30cbf879ee1d, 192.168.10.107, ACK in request.
380	INFO	INFO 2018-07-05 06:00:30|DHCPS: 1:0x54c9dff6c72d, 192.168.10.101, ACK in request.
379	INFO	INFO 2018-07-05 06:00:16|DHCPS: 1:0x389af64ee5a9, 192.168.10.104, ACK in request.
378	INFO	INFO 2018-07-05 05:06:22|DHCPS: 1:0x9cb70dd52439, 192.168.10.106, ACK in request
377	INFO	INFO 2018-07-05 05:06:07|DHCPS: 1:0x88797e30f077, 192.168.10.110, ACK in request.
376	INFO	INFO 2018-07-05 05:03:29|DHCPS: 1:0x30cbf879ee1d, 192.168.10.107, ACK in request.
375	INFO	INFO 2018-07-05 05:00:29|DHCPS: 1:0x54c9dff6c72d, 192.168.10.101, ACK in request.
374	INFO	INFO 2018-07-05 04:26:40|DHCPS: 1:0x4849c708c1a4, 192.168.10.108, ACK in request
373	INFO	INFO 2018-07-05 04:06:56|DHCP client read, totlen = 368(1048).

System Log Help

- **Refresh** - Refresh the page to show the latest log list.
- **Clear All** - All the logs will be deleted from the Router permanently, not just from the page.

Status
--- Basic Settings ---
Quick Setup
WPS
Network
Wireless
--- Advanced Settings ---
DHCP
Forwarding
Security
Parental Control
Access Control
Static Routing
IP QoS
IP & MAC Binding
Dynamic DNS
--- Maintenance ---
System Tools
Time Settings
Diagnostic
Firmware Upgrade
Factory Defaults
Backup & Restore
Reboot
Password
System Log
Statistics

Mail Account Settings

From:	michell@mgconecta.com
To:	michell@michellti.com.br
SMTP Server:	smtp.mgconecta.com.br
SMTP Port:	587 (The default value is 25,do no
☑	Authentication
User Name:	user@mgconecta.com.br
Password:	••••••••••
Confirm The Password:	••••••••••

☑ Enable Auto Mail Feature

◉ Everyday, mail the log at 18 : 00

○ Mail the log every 48 hours

Save Back

Mail Account Settings Help

- **From** - Your mail box address.
- **To** - Recipient's address.
- **SMTP Server** - Your smtp server.
- **Authentication** - Most SMTP Server requires Authentication.
- **User Name** - Your mail account name.
- **Password** - Your mail account password.

Auto Mail Feature will help you monitor how your Router is running.

- Everyday, at specified time, the Router will automatically send the log to specifid mailbox.
- Every few hours, such as 2 hours, the Router will automatically send the log to specifid mailbox.