

# **DWR-923**

4G Integrated Access Device

User Manual

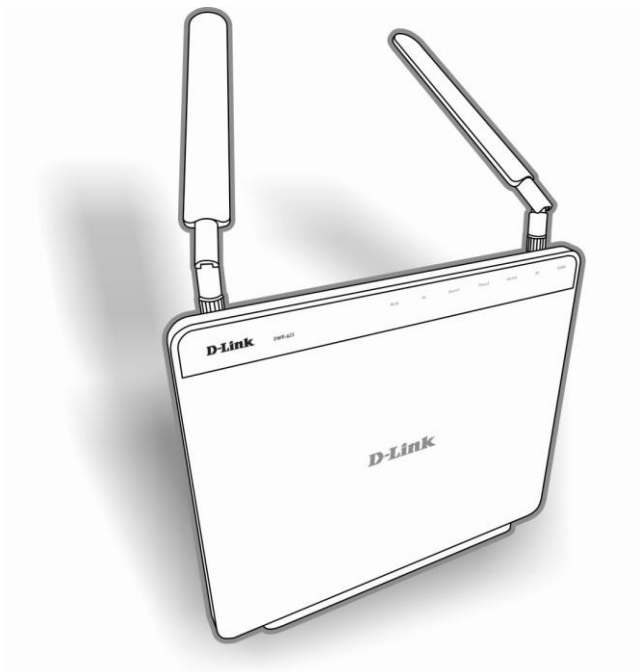
# **TABLE OF CONTENTS**

<b>1. GETTING TO KNOW THE DWR-923 .....</b>	<b>2</b>
1.1 Introduction .....	2
1.2 Package Contents .....	3
1.3 System Requirements .....	3
1.4 Hardware Overview - Front Panel & LEDs.....	4
1.5 Hardware Overview - Rear Panel .....	5
1.6 Hardware Overview - Side Panel.....	5
<b>2. INSTALLATION .....</b>	<b>6</b>
<b>3. USER CONFIGURATION INTERFACE .....</b>	<b>7</b>
3.1 Accessing the User Configuration Interface.....	7
3.2 Interface Layout .....	8
3.3 Using the User Configuration Interface .....	9
3.3.1 Home .....	9
3.3.2 Internet .....	11
3.3.3 Wi-Fi .....	17
3.3.4 LAN .....	26
3.3.5 Advanced.....	30
3.3.6 System .....	53
<b>4. APPENDIX .....</b>	<b>62</b>
4.1 Connected PC IP Address Configuration .....	62

# 1. Getting to know the DWR-923

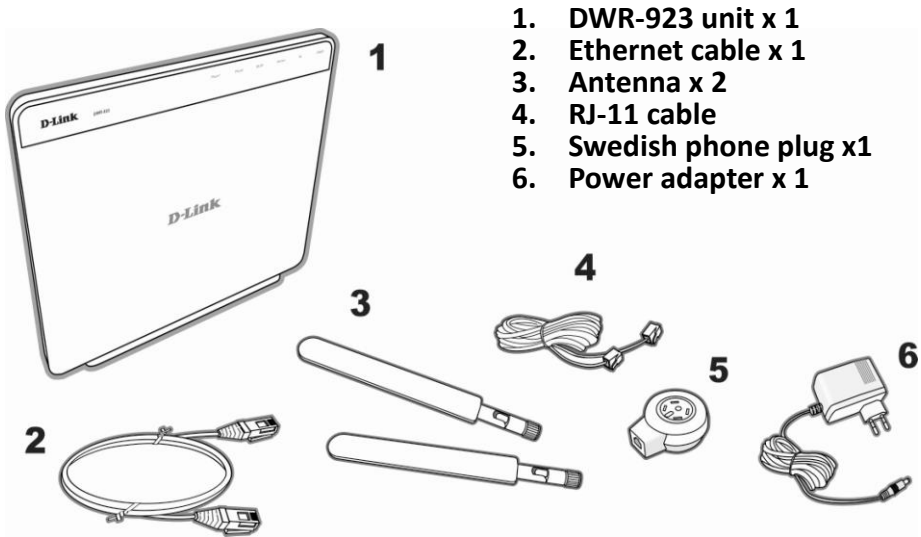
## 1.1 Introduction

The DWR-923 is a 4G Integrated Access Device (IAD) that integrates a range of methods for connecting to the Internet, allowing users to access 4G mobile network services via a single device. Once connected, you can easily share your network utilizing wireless Wi-Fi and wired Ethernet interfaces. The advanced 4G technology provides much better performance than traditional 3G networks.



## 1.2 Package Contents

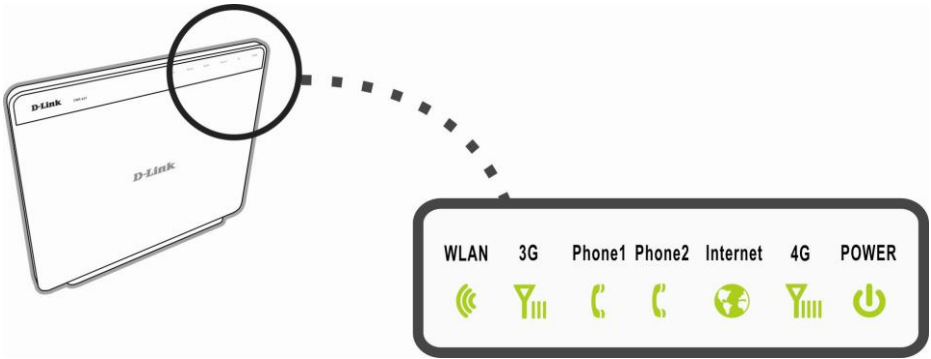
Thank you for purchasing the DWR-923. Before using the DWR-923, please confirm that the packaging includes the following items and accessories:



## 1.3 System Requirements

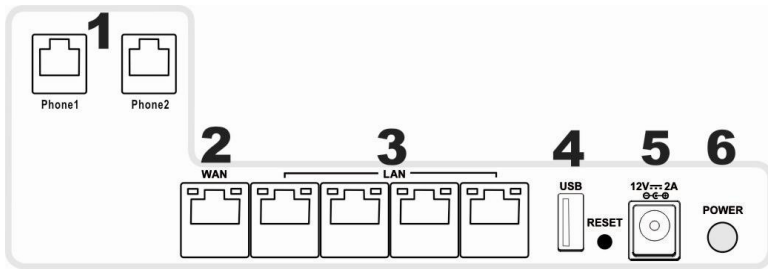
- 4G SIM card, with valid Internet service
- A computer with a Windows®, Macintosh®, or Linux-based operating system with an installed Ethernet adapter
- Internet Explorer Version 6.0 or above for configuration usage

# 1.4 Hardware Overview - Front Panel & LEDs



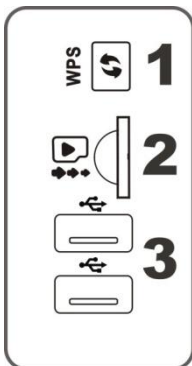
LED	Status	Description
<b>Power</b>	Green	System on
	Blinking Green	System booting
	Blinking Yellow	Firmware upgrading
	Red	Firmware upgrade error
<b>4G</b>	Off	No 4G signal received
	Red	Low 4G signal strength
	Yellow	Medium 4G signal strength
	Green	High 4G signal strength
<b>Internet</b>	Red	Invalid Internet connection
	Green	Valid Internet connection
<b>Phone1/2</b>	Red	Invalid VoIP server login
	Green	Successful VoIP server login
	Blinking Green	Off hook with successful VoIP server login
	Off	VoIP service is not subscribed
<b>3G</b>	Off	No 3G signal received
	Red	Low 3G signal strength
	Yellow	Medium 3G signal strength
	Green	High 3G signal strength
<b>WLAN</b>	Green	Local wireless network ready
	Blinking Green	Data transmission over local wireless network

## 1.5 Hardware Overview - Rear Panel



Item	Name	Description
1	Phone ports	Connects to your phones for SIP VoIP services
2	WAN port	N/A
3	LAN ports	Connects to your local network devices such as PC and laptop
4	USB port	Optional external device connections
5	Power input port	Connects to the power adapter
6	Power button	Turns device on

## 1.6 Hardware Overview - Side Panel



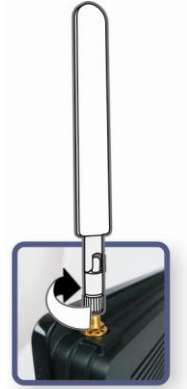
Item	Name	Description
1	WPS button	Quick wireless connection with other WPS supported devices
2	SIM card slot	4G or 3G SIM card connection
3	USB port	Optional external device connection

## 2. Installation

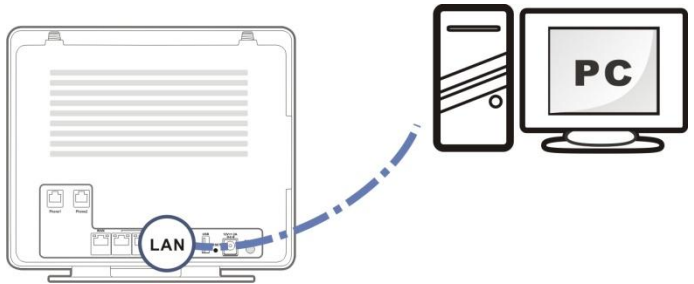
1. Insert the SIM card provided by your 4G mobile network operator.



2. Insert the antennas into the antenna connectors on the DWR-923. Rotate the connector end of the antenna to fasten it.



3. Insert the Ethernet cable into one of the LAN ports on the rear panel of the DWR-923. Insert the other end of this Ethernet cable into the port of the computer that you will use to configure the DWR-923.




## 3. User Configuration Interface

### 3.1 Accessing the User Configuration Interface

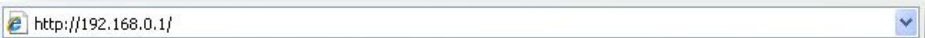
The User Configuration Interface allows you to configure the DWR-923 using your web browser. Follow the procedures below to log in and configure the settings:

1. Ensure that the computer you use for configuring the DWR-923 has the proper IP address settings for communicating with the DWR-923. The default LAN network settings and IP address of the DWR-923 are shown below:

**IP address:**            **192.168.0.1**  
**Subnet mask:**        **255.255.255.0.**


 **Note:** Set the IP address of this computer to obtain an IP address automatically or assign an IP address from 192.168.0.100 to 192.168.0.254. The IP address range can be modified through the User Configuration Interface, the default setting starts from 100. See **Appendix - Connected PC IP Address Configuration** for detailed procedures for setting your IP address.

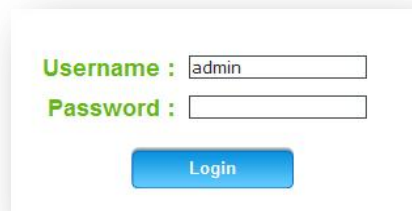
2. Open your web browser and type 192.168.0.1 in the address field:



3. An authentication screen appears. See the default username and password below:

**Username:**    **admin**  
**Password:**    **(blank)**

 **Note:** There is no default password. Please leave the password field blank.



Username :   
Password :



## 3.2 Interface Layout



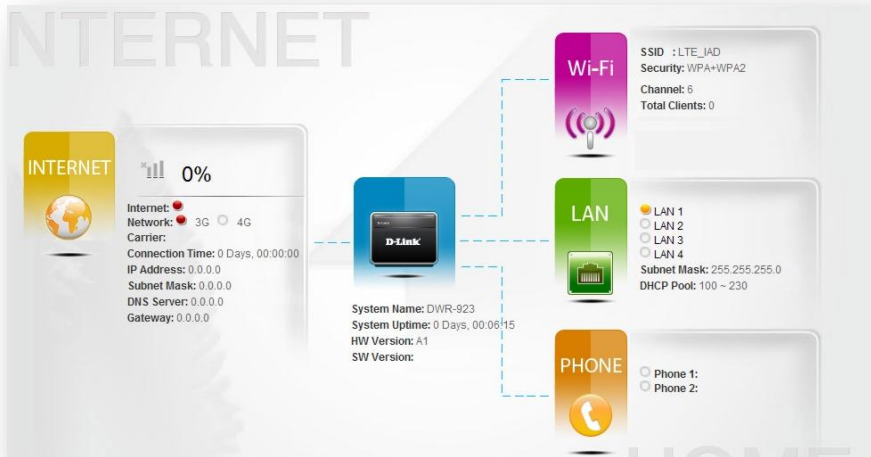
After logging in, the Home Screen appears. The **User Configuration Interface** consists of three parts:

- 1 This part is the displayed content. In the Home page, basic system status is displayed.
- 2 The menu bar of the User Configuration Interface. Click tabs to access configuration pages of each function. Additional selections will appear on the left hand side as you click the main tabs.
- 3 This part displays your Login status and provides links to refresh the page and open the Help page.

## 3.3 Using the User Configuration Interface

### 3.3.1 Home

The status page displays basic system Information including a summary of the Internet, system, Wi-Fi, Local Area Network (LAN) and connected VoIP phones.



#### ***Internet:***

**Network:** Provides the current status of the interface used to access the Internet.

**Carrier:** Provider name of your mobile network service.

**Connection Time:** Elapsed time the DWR-923 has been connected to the Internet.

**IP Address:** The DWR-923's Internet IP address.

**Subnet Mask:** The DWR-923's Internet subnet mask.

**DNS Server:** IP address of the DNS server that the DWR-923 uses.

**Gateway:** The Internet gateway IP address.



### ***System Information:***

System Name: Displays the DWR-923's configured name.

System Uptime: Elapsed time since the DWR-923 was last turned on or rebooted.

HW Version: Hardware version that the DWR-923 is currently using.

SW Version: Firmware version that the DWR-923 is currently using.

### ***Wi-Fi:***

SSID: Names of the DWR-923's wireless networks.

Security: Encryption and authentication settings of each wireless network.

Channel: Current channel that the DWR-923 uses.

Total Clients: Number of client devices connected via Wi-Fi.

### ***LAN:***

LAN1~4: Connection status of the four LAN ports of the DWR-923.

Subnet Mask: The DWR-923's LAN subnet mask.

DHCP Pool: IP address range that the DWR-923 will assign from within.

### ***Phone:***

Phone1 &2: Status of connected VoIP phones.

## 3.3.2 Internet

Internet → Status

4G Device Name	APN1	APN2
Registration State	Not Registered Searching	Not Registered Searching
Radio Interference	None	None
RSSI	1,(128,0)	1,(128,0)
Signal Strength	-128	-128
NetworkName	(null)	(null)
Mobile Country Code(MCC)	0	0
Mobile Network Code(MNC)	0	0
Cell ID	0	0

**Transmit**

4G Device Name	Tx Packets	Tx Errors	Tx Overflows	Tx Bytes
APN1	-1	-1	-1	-1
APN2	-1	-1	-1	-1

**Receive**


4G Device Name	Rx Packets	Rx Errors	Rx Overflows	Rx Bytes
APN1	-1	-1	-1	-1
APN2	-1	-1	-1	-1

[Refresh](#)

### ***4G Connection Status:***

Registration State: Status of connection to a network service.

Radio Interference: Any interference conditions that the DWR-923 has detected.



**RSSI:** Received Signal Strength Indicator (RSSI) measures the strength of received radio signals.

**Signal Strength:** Strength value of the received signal.

**Network Name:** Network name of the network connected to.

**Mobile Country Code (MCC):** Mobile country code of the connected network.

**Mobile Network Code (MNC):** Mobile network code of the connected network.

**Cell ID:** ID of the connected base transceiver station.

***Transmit:*** Displays transmission status and related statistics.

**Tx Packets:** Number of IP packets transmitted from the DWR-923.

**Tx Errors:** Number of error packets transmitted from the DWR-923.

**Tx Overflows:** Number of overflows transmitted from the DWR-923.

**Tx Bytes:** Number of bytes transmitted from the DWR-923.

***Receive:*** Displays receiving status and related statistics.

**Rx Packets:** Number of IP packets received by the DWR-923.

**Rx Errors:** Number of error packets received by the DWR-923.

**Rx Overflows:** Number of overflows received by the DWR-923.

**Rx Bytes:** Number of bytes received by the DWR-923.

Clicking Refresh will renew these data.

## Internet → PIN Configuration

**PIN Configuration**

This page is for you to configure pin code.

Use PIN:

Enable PIN Protection:  Yes  No

The selected PIN is disabled.

Enter PIN:

**Verify PIN**

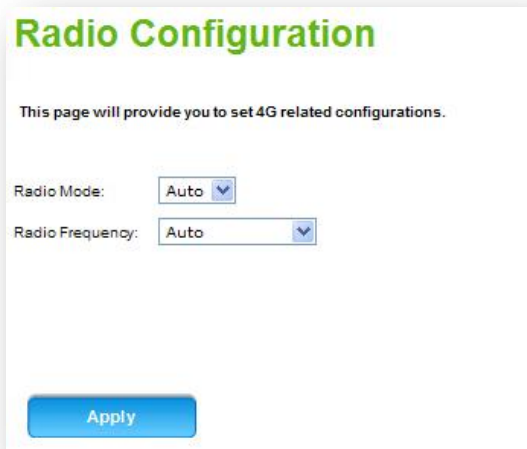
This page allows configuration of the PIN code of your SIM card.

**Use PIN:** Select a PIN code to use to protect your SIM card.

**Enable PIN Protection:** Choose to enable or disable PIN protection. If you choose Yes, you will be asked to enter the PIN code when you use the phone feature.

**Enter PIN:** Enter the PIN code.

Click Verify PIN to proceed.



**Radio Configuration**

This page will provide you to set 4G related configurations.

Radio Mode:

Radio Frequency:

**Radio Mode:** Select 3G or 4G for your mobile network or select Auto to switch between available 3G/4G mobile networks automatically.

**Radio Frequency:** Select a radio frequency according to your region and the frequency your service uses.

## Profile Configuration

This page displays current list of profiles.

### Network Profile List

	APN Index	Profile Name	Status
<input checked="" type="radio"/>	APN 1	profile1	Disconnected
<input type="radio"/>	APN 2	profile2	Connected to APN2

[Connect](#) [Edit](#)

This page displays the network profiles that are currently being used. Select one from the list and then click Connect to establish a connection, or click Edit to modify the selected profile.





This function scans for nearby network providers.

**4G Network Selection Method:** Choose Auto to scan for network providers automatically or choose Manual to scan manually.

After scanning, nearby network providers will be listed in the chart. Select your desired network provider and then click Apply to apply the changes or click Scan to scan again.

### 3.3.3 Wi-Fi

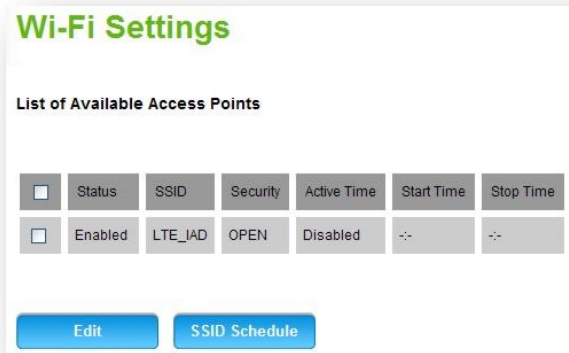
#### Wi-Fi → Device List



Host Name	IP Address	MAC Address	Signal Level
N/A	192.168.0.101	34:15:9e:77:dd:4c	-63 dBm

This page displays the client devices that are currently connected to the DWR-923 via Wi-Fi.

#### Wi-Fi → Wi-Fi Settings



<input type="checkbox"/>	Status	SSID	Security	Active Time	Start Time	Stop Time
<input type="checkbox"/>	Enabled	LTE_IAD	OPEN	Disabled	--	--

[Edit](#) [SSID Schedule](#)

You will need to establish a wireless local area network (WLAN) to connect your client devices with the DWR-923 wirelessly and to access the Internet. You can mark the box of the SSID and click Edit to modify its contents or click SSID Schedule to set a schedule rule for this network.

This page pops up when you click Edit in Wi-Fi → Wi-Fi Settings.

**Wi-Fi Settings Configuration**

In this section you can configure the wireless interface (access point) available on the router.  
» [Back to Wi-Fi Settings page](#)

Enable SSID  Enable  
 Disable

SSID

Security

Password

Show Plain Password

**Enable SSID:** Choose to Enable or Disable the function.

**SSID:** The Service Set Identifier (SSID) is the name of the wireless network broadcast from this system. In order for computers to connect to the local network over a wireless link, they must select this network name from the list of detected wireless networks in the area.

**Security:** Select one security method from the drop-down list.

**None:** No protection, open mode.

**WPA Personal:** Use WPA Personal for encryption.

**WPA2 Personal:** Use WPA2 Personal for encryption.

**WPA+WPA2 Personal:** Enables wireless with personal wireless protected access mode.

**WEP:** Enables wireless with WEP protection, provides a 5/13 character ASCII string to enable 64/128 bit encryption respectively. This option is only recommended when your network device does not support WPA or WPA2.

**Password:** Specify a password for your wireless network.

**Show Plain Password:** Check the box to make the password visible.

Click Apply to apply the changes. Or click Reset to undo your configurations. After this step, you can use your wireless client devices, such as your smart phone, to search for the WLAN with the SSID and password that you just specified.

**This page pops up when you choose to set a schedule rule for a wireless network in Wi-Fi → Wi-Fi Settings.**

**Wi-Fi Settings Schedules**

In this section you can configure the schedule rule(s) to enable/disable wireless functionality of the device.  
» [Back to Wi-Fi Settings page](#)

**List of Available Schedule rules**

<input type="checkbox"/>	Schedule Name	Start Time	End Time	Schedule Status
<input type="checkbox"/>	D-Link	: PM	: PM	Not active

[Add](#) [Edit](#) [Delete](#)

To set schedule rule for a network:

1. Click Add to add a new schedule rule.

Active Time: Mark the box to enable this schedule rule.

Schedule Name: Name of this schedule.

Start Time and Stop Time: The time that you wish to turn on or turn off this wireless network.

2. Click Apply to apply the changes.

## Wi-Fi → WPS

### WPS

#### Wi-Fi Protected Setup (WPS)

WPS is a standard for easy and secure setup of a wireless connection. In this section you can enable WPS for a client connection using WPA/WPA2 security.

Enable Wi-Fi Protected Setup (WPS)

Apply

Reset

#### Push Button Connect (PBC)

Press the WPS button on the client that supports WPS connectivity. Immediately after click the PBC button in this section to establish a wireless link to the routers AP.

Click for PBC

#### Personal Identification Number (PIN)

Enter the clients Personal Identification Number to establish a wireless link to this routers AP.

Client PIN

Submit PIN

**Wi-Fi Protected Setup (WPS):** WPS is a computing standard for easy and secure setup of a wireless connection. In this section you can enable WPS for a client connection using WPA/WPA2 security.

1. Check the box to enable WPS.
2. Click Apply to apply the changes. Or click Reset to undo your configurations.

**Push Button Connect (PBC):** If other wireless devices support the PBC WPS function, click on Click for PBC and then push the WPS button on the other device.

**Personal Information Number (PIN):** If other wireless devices support the PIN WPS function, specify the same PIN for the DWR-923 and the wireless device and then click Submit PIN to establish a connection.

## Wi-Fi → Wi-Fi Access Control

### Wireless Access Control

**Wireless Client Access Policy**

This page allows you configure the default Access Policy for all wireless clients. You can choose to block or allow specific wireless clients from associating with this gateways AP with the settings on this page.

Access Rule for Registered MAC Address

**List of MAC Addresses**

The wireless access policy is applied to the list of wireless clients, identified by their MAC Address and computer name, listed in this section.

MAC Address

Access control allows you to block or allow computer devices from establishing a wireless link to the DWR-923. The filtering is based on the wireless computer's unique hardware ID (MAC address). With this feature you can prevent unknown or unauthorized computers from accessing the DWR-923 and the services (like shares, DMC) it offers. In most cases you know which devices will be connecting to the DWR-923 through a wireless connection, which allows you to add these known devices to a list for authorized access. This feature helps in securing the wireless connectivity of the home network.



## ***Wireless Client Access Policy***

### Access Rule for Registered MAC Address:

*Allow Everybody:* Allows all devices to connect to the DWR-923 wirelessly regardless of the list of wireless computers defined below.

*Allow:* Allows devices that are added in the MAC address list to connect to the DWR-923.

*Deny:* Devices that are added in the MAC address list will be blocked when trying to connect to the DWR-923.

Click Apply to apply the changes. Or click Reset to undo your configurations.

***List of MAC Addresses:*** This is the list of wireless devices that have been added for the ACL policy.

MAC Address: The unique hardware ID of the local network wireless computer.

Click **Add** to add an access policy, or select an item and click **Delete** to delete the selected item.

## Advanced Wireless

Specify advanced configuration settings for the gateways radio from this page. AP security and association parameters can be modified from the default values if needed.

Disable Network Name Broadcast

Group Re-Key Interval  [Seconds]

Beacon Interval  [Milliseconds]

Fragmentation Threshold  [Bytes]

RTS Threshold  [Bytes]

Transmit Power

Channel

Wireless Mode


Bandwidth

This section allows you to configure and manage advanced settings of your wireless network. In most cases, however, the default wireless settings will be sufficient.

**Disable Network Name Broadcast:** By disabling SSID broadcasting, the DWR-923 will not broadcast its Network ID (SSID) to announce itself to wireless stations and other access points.

**Group Re-Key Interval:** Specify the timeout interval after which group keys are generated (only used if profile is configured with WPA or WPA2 security).





**Beacon Interval:** Enter the time in milliseconds between beacon transmissions. The default interval is 100 milliseconds.

**Fragmentation Threshold:** This is the maximum length of the frame, in bytes, beyond which packets must be broken up (fragmented) into two or more frames. Collisions occur more often for long frames because while sending them they occupy the channel for a longer time. The default value is 2346, which effectively disables fragmentation.


**RTS Threshold:** The Request to Send (RTS) threshold is the packet size in bytes above which the DWR-923 is required to check the transmitting frames to determine if RTS/Clear to Send (CTS) handshake is required with the receiving client. Using a small value causes RTS packets to be sent more often, consuming more of the available bandwidth, therefore reducing the apparent throughput of the network packets. The default value is 2346, which effectively disables RTS.

**Transmit Power:** Enter a value in dBm for the default transmit power level.

**Channel:** The wireless channel that the DWR-923 will broadcast on. This specifies the radio frequency used to transmit wireless frames. Select a channel from the list or choose Auto to let the system determine the best channel to use based on environmental noise levels for all available channels.

**Wireless Mode:** Select the 802.11 modulation technique. The DWR-923 supports 802.11 b/g/n Wi-Fi modes.

**Bandwidth:** When you choose “ng” as your wireless mode, you may choose a Wi-Fi bandwidth for this product from HT20, HT40- and HT40+. Higher bandwidth indicates a higher throughput of your

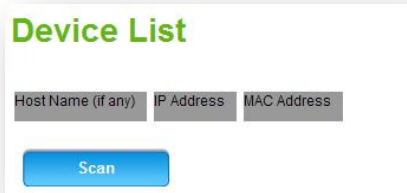


wireless network. However, there will also be a greater chance of signal interference from other network devices.

Click **Apply** to apply the changes. Or click **Reset** to undo your configurations.

## 3.3.4 LAN

### LAN → Device List



The screenshot shows a web interface titled "Device List". It features three input fields for "Host Name (if any)", "IP Address", and "MAC Address". Below these fields is a blue "Scan" button.

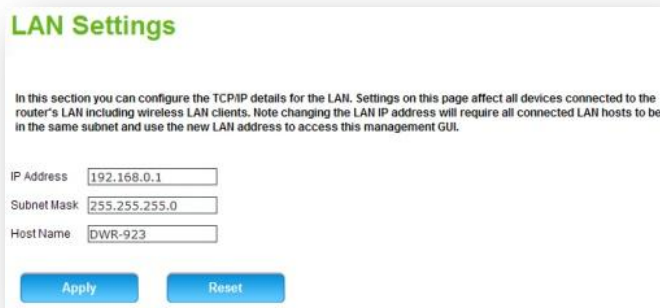
This page lists the information of client network devices that are connected via the DWR-923's LAN ports.

**Host Name:** Name of the client device.


**IP Address:** IP address that the client device is using.

**MAC Address:** MAC address of the client device.


### LAN → LAN Settings



The screenshot shows a web interface titled "LAN Settings". It contains a paragraph of text: "In this section you can configure the TCP/IP details for the LAN. Settings on this page affect all devices connected to the router's LAN including wireless LAN clients. Note changing the LAN IP address will require all connected LAN hosts to be in the same subnet and use the new LAN address to access this management GUI." Below the text are three input fields: "IP Address" with the value "192.168.0.1", "Subnet Mask" with the value "255.255.255.0", and "Host Name" with the value "DWR-923". At the bottom are two blue buttons: "Apply" and "Reset".



This page allows you to configure the local network settings of the DWR-923. In most cases the default settings should be sufficient. In this section you can configure the TCP/IP details for the LAN.

 **Note:** The settings on this page will affect all devices that are connected to the router's LAN including wireless LAN clients. All connected LAN hosts must be in the same subnet and use the new LAN address to access the User Configuration Interface.

**IP Address:** Enter the local network IP address for the DWR-923. The default IP address is 192.168.0.1.

**Subnet Mask:** The subnet mask along with the previously configured IP address defines the network. The default value for subnet mask is 255.255.255.0.

**Host Name:** The default host name is DWR-923.

Click Apply to apply the changes. Or click Reset to undo your configurations.

## Basic DHCP Configuration

### IPv4 Address Distribution

The local network has a DHCP server to offer IP address leases to connected devices. The range defined here will apply to wired and wireless clients in your local network.

Specify the number of devices/computers in your network:

Start IP distribution from 192.168.0.

Apply

Reset

By default, the DWR-923 will function as a DHCP (Dynamic Host Configuration Protocol) server. As such it will provide TCP/IP configuration to client computers connected to the local network.

### ***IPv4 Address Distribution:***

Specify the number of devices/computers in your network: Enter the number of local network computers (including those connecting over Wi-Fi) and the DHCP server will calculate the number of leases required for the network.

Start IP distribution from: Define the starting range of the IP address. The DHCP server will iterate the DHCP IP addresses to be given out by taking into account the starting IP address range and the configured number of devices in your network.

Click Apply to apply the changes. Or click Reset to undo your configurations.

## DHCP Reserved IP

To ensure certain local network devices always receive the same IP address from the gateway's DHCP server, you can bind the LAN device's MAC address to a preferred IP address. This IP address will only be assigned to the matching MAC address.

### List of Reserved IP Addresses

MAC Address IP Address

Add

Edit

Delete

IP addresses can be reserved so that a particular IP address is always allocated to a particular computer in the local network. This allows devices such as printers and VoIP phones to be assigned the same IP address from the DHCP server when they come online, which is critical for hostname mapping and port mapping rules. This is achieved by binding the unique hardware ID of the device, called the MAC address, to an IP address in the DHCP server reserved IP address list.

### ***List of Reserved IP Address:***

**MAC Address:** The MAC address of the computer or local network device.

**IP Address:** The reserved IP address to associate with the above MAC address.

Click Add to add a reserved IP, or select an item and click Edit to modify or click Delete to delete the selected item.

## 3.3.5 Advanced

Advanced → DNS&DynDNS

**DNS & DynDNS**

Domain Name Server (DNS), in this page you can define the system name and domain name of this gateway for DNS resolution.

Dynamic DNS (DDNS) is an Internet service that allows routers with varying public IP addresses to be located using Internet domain names. To use DDNS, you must setup an account with a DDNS provider such as DynDNS.org and set the required account details on this page.

**Domain Name Server (DNS) Address**

System Name:

Domain Name:

Description:

**DDNS (Dynamic DNS) Settings**

Dynamic DNS (DDNS) is an Internet service that allows routers with varying public IP addresses to be located using Internet domain names. To use DDNS, you must setup an account with a DDNS provider such as DynDNS.org and set the required account details on this page.

Select the Dynamic DNS Service:

Domain Name:


Username:

Password:

Use wildcards:

Update every 30 days:

The Domain Name Server (DNS) page allows you to define the system name and domain name of the DWR-923 for DNS resolution. You can assign a domain name to a particular computer with the use of Domain Name System (DNS) entries. DNS allows you to assign a readable system name to the DWR-923. All connected local network computers



will appear in the list of hosts as belonging to the domain configured on this page. Network hosts which are a part of a common domain can view the list of other computers that are part of that domain.

***Domain Name Server (DNS) Address:***

System Name: Enter the system name for the DWR-923.

Domain Name: Enter the domain name to define the common domain for computers connected to the DWR-923.

Description: Add a description about the system name.

***Dynamic DNS (DDNS)*** is an Internet service that allows routers with varying public IP addresses to be located using Internet domain names. To use DDNS, you must setup an account with a DDNS provider such as DynDNS.org and fill in the required account details including Domain Name, Username and Password on this page.

Select the Dynamic DNS Service: Select the DNS service that you are subscribed to.

Domain Name: Enter the domain name of the dynamic DNS account. This is the DNS domain name which will be used. An example is dyndns.org.

Username: Enter the username of the dynamic DNS account. This will be provided by the dynamic DNS service provider.

Password: Enter the password for the dynamic DNS account.

Use wildcards: Check this option to use wildcards.

Update every 30 days: Selecting this configures the DWR-923 to update the host information on DynDNS.com and keep the subscription active after the 30 day trial period.

Click Apply to apply the changes. Or click Reset to undo your configurations.



### Firewall

This page displays the firewall security setting of the gateway. At Maximum Security, all incoming requests from the Internet are blocked by default and the router allows limited Internet destined traffic from leaving the local network. In the Typical Security level, all incoming requests from the Internet are still blocked by default but the computers on the local network can access the Internet without restrictions. The No Security setting opens the firewall for all traffic to and from the Internet.

#### Security Mode Configuration

Security Level	Requests from the Internet (Incoming Traffic)	Requests from the local network (Outgoing Traffic)
<input type="radio"/>	Blocked - No access to local network from Internet, except as configured in the Port Mapping.	Limited - Only commonly used services, such as FTP, HTTP, HTTPS, DNS, POP, TELNET, IMAP, SMTP.
Maximum Security		
<input checked="" type="radio"/>	Blocked - No access to local network from Internet, except as configured in the Port Mapping.	Unrestricted - All services are permitted, except as configured in the Access Control screen.
Typical Security		
<input type="radio"/>	Unrestricted - Permits full access from Internet to local network; all connection attempts permitted.	Unrestricted - All services are permitted, except as configured in the Access Control screen.
No Security		

This section displays the firewall security settings of the DWR-923. The security levels are grouped into a set of rules corresponding to maximum, typical, and minimum security settings. Advanced users can supplement these rules with custom parental controls or port mapping rules as needed. Select from one of the three security modes to protect the local network from Internet intrusion:



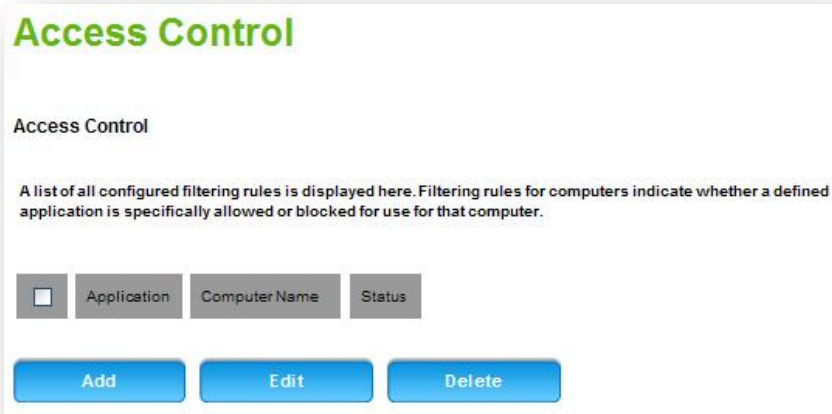
### ***Security Mode Configuration:***

**Maximum Security:** All incoming requests from the Internet are blocked by default and the router allows limited Internet destined traffic from leaving the local network. This mode is the strongest level of security. All traffic from the Internet is blocked from reaching the local network, except what is allowed via port mapping policies that apply to the local network. A limited set of commonly used services are permitted to be accessed from the local network such as web traffic (HTTP / HTTPS) or file transfer (FTP).

**Typical Security:** All incoming requests from the Internet are still blocked by default but the computers on the local network can access the Internet without restrictions. This is the default and generally most appropriate security setting for home networks. All traffic from the Internet is blocked from reaching the local network, thus blocking unwanted intrusion from the outside. At the same time local network users are given unrestricted access to the Internet regardless of service or application.

**No Security:** This setting opens the firewall for all traffic to and from the Internet. This mode provides unrestricted access from the local network to the Internet and vice-versa. It is not recommended to set the DWR-923 in this mode without additional parental controls as it makes the local network vulnerable to attack from the Internet.

Click Apply to apply the changes. Or click Reset to undo your configurations.



A list of all configured filtering rules is displayed in this section. Filtering rules for computers indicate whether a defined service is specifically allowed or blocked for use by that computer.

This is a security mechanism to selectively block or allow certain types of traffic in accordance with rules specified by network administrators. You can use this page to manage the firewall rules that control traffic to and from your network.

***Access Control:***

Application: The application on which the filtering rule is applied.

Computer Name: The name of the host on which the filtering rule is applied.

Status: Displays if the traffic is allowed or blocked.

Click Add to add an access rule, or select an item and click Edit to modify or click Delete to delete the selected item.



URL Blocking lets you block websites containing specific keywords from being accessed through this gateway. Displayed below is the list of blocking rules:

Filter Name: Unique identifier for the content filtering rule.

Keywords: The keywords that are used to filter websites accessed by local network users. The content filtering rule is based on these keywords.

Domains: The internet domain on which content filtering rules is applied.

Please follow the steps below to setup:

Step 1: Click Add to add a blocking rule. The image below uses *yahoo* to demonstrate: set *limit\_yahoo* as the filter name and *yahoo* as the keyword.

## URL Blocking

This security tool allows you to block access to Internet domains that contain certain defined keywords. Up to 32 keywords to check in a domain can be configured in a single filtering policy.

<input type="checkbox"/>	Filter Name	Keywords	Domains
<input type="checkbox"/>	limit_yahoo	yahoo	

Add

Edit

Delete

Step 2: Go to “Rules for schedule” page → Check the box to Enable Parental Control → Click Apply to enable the configurations for “List of Parental Control Profiles”.

## Schedules

### Parental Control Settings

By configuring some simple parental control profiles, you can protect local network computers from accessing undesirable content or reaching the internet during scheduled access times.

Enable Parental Control

Apply

Reset

### List of Parental Control Profiles

<input type="checkbox"/>	Profile Name	Description	Group	Session Timeout	Inactivity
<input type="checkbox"/>	test1		admin	5	3

Add

Edit

Delete

Step 3: Click Add to add profiles:

- (1) Enter Profile Name.
- (2) Select your Group membership (admin/guest).
- (3) Check the box to Enable Content Filtering.
- (4) Select a Filter Content.
- (5) Click Apply.

## Parental Control Profile Configuration

The profile consists of the identifier (Profile Name), a short description for what it does, and also the group of computers on the local network to which it applies. Content filtering will allow you to define internet content to block for the group. You can also define the time of the day when Internet access is disabled for the group. Be sure to set the system time for this schedule to be effective.

### Parental Control Profile Configuration

Profile Name	<input type="text" value="test1"/>
Description	<input type="text"/>
Group	<input type="text" value="admin"/>
Enable Content Filtering	<input checked="" type="checkbox"/>
Filter Content	<input type="text" value="limit_yahoo"/>
Restrict Internet Access Time	<input type="checkbox"/>
Internet Access Schedule	<input type="text"/>
Session Timeout	<input type="text" value="5"/> minutes
Inactivity Timeout	<input type="text" value="3"/> minutes

Apply

Reset

Step 4: Open browser and link to <http://www.yahoo.com.tw> . The webpage will ask you to login. Please login according to your Group membership setting on step 2 (admin/guest).



The image shows a login form titled "Web Access Login" in green text. Below the title, there are two input fields: "Username:" with the text "admin" entered, and "Password:" which is empty. Below these fields is a blue button with the text "Login".

Step 5: After logged in, link to <http://www.yahoo.com.tw> again. Since *yahoo* is the keyword for blocked webpage therefore you will see the denial message while accessing any content that include the keyword.

You have been denied access to this web page due to restrictions in your web browsing profile.

Please contact your administrator or follow this link (<http://192.168.0.1/platform.cgi?>

[page=urlFilterLogin.htm](#))

to login with a different web browsing profile.

## DoS Attacks

A denial-of-service attack (DoS attack) is an attempt to make a device resource unavailable to its intended users.

SYN Flood  [Max/Sec] (1-10000)  
Echo Storm  [Ping Pkts/Sec] (1-10000)  
ICMP Flood  [ICMP Pkts/Sec] (1-10000)

Apply

Reset

A denial-of-service attack (DoS attack) is an attempt to make a device resource unavailable to its intended users.

**SYN Flood:** Enter the maximum number of SYN packets per second the security appliance accepts before determining that a SYN Flood Intrusion is occurring. This value can range between 1 and 10,000 SYN packets per second. The default is 128 SYN packets per second.

**Echo Storm:** The security tool monitors the number of pings per second to determine when to declare an echo storm intrusion event. Echo storm intrusion events are not blacklisted. This value can range between 1 and 10,000 ping packets per second. The default is 15 ping packets per second.

**ICMP Flood:** The security tool monitors the number of ICMP packets per second, not including ping packets, to determine when to declare an ICMP flood intrusion event. ICMP flood events are not blacklisted. This value can range between 1 and 10,000 ICMP packets per second. The default is 100 ICMP packets per second.

Click Apply to apply the changes. Or click Reset to undo your configurations.



## Schedules

### Parental Control Settings

By configuring some simple parental control profiles, you can protect local network computers from accessing undesirable content or reaching the Internet during scheduled access times.

Enable Parental Control

Apply

Reset

### List of Parental Control Profiles

<input type="checkbox"/>	Profile Name	Description	Group	Session Timeout	Inactivity
<input type="button" value="Add"/>	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>			

### List of Schedules

Schedules are a very useful feature to allow security rules to be enabled or disabled based on the time of day or day of the week. Configured schedules will be available to select in the parental profile configuration page. All schedules will follow the configured system time.

<input type="checkbox"/>	ID	Name	Description
--------------------------	----	------	-------------


Add

Edit

Delete

This section allows you to determine what local network users can access on the Internet, and when. Parental control profiles enable you to restrict access to particular websites or block sites with specific keywords that you do not want home network users to access. Parental control configuration is accomplished in two steps. First content filtering rules or schedules are defined and then a parental control profile is created using a combination of content filtering rules and schedules.

**Parental Control Settings:** Check the box to enable parental control. You will be able to prevent local network computers from accessing



undesirable content or connecting to the Internet during scheduled access times.

***List of Parental Control Profiles:*** This section displays the parental control list you have set up.

Profile Name: A unique identifier for the parental control profile.

Description: This can be a short description of the purpose of the rule to allow DWR-923 administrators to remember the use and intent of this profile.

Group: The user group upon which the rule is applied.

Session Timeout: The elapsed time after which the user's session will expire.

Inactivity: The elapsed time that the system has been inactive.

***List of Schedules:*** Schedules are a very useful feature to allow security files to be enabled or disabled based on the time of day or day of the week. Configured schedules are available for selection in the firewall rule configuration page. All schedules follow the configured system time. When you create a parental control policy, you have the option to specify a time of day and duration when the rule is active. The table lists all the Available Schedules for this device and allows several operations on the Schedules.

ID: The user identification name.

Name: Name of the schedule for identification and management purposes.

Description: Describes the status of the schedule profile.

Click Add to add a parental control schedule rule, or select an item and click Edit to modify or click Delete to delete the selected item.

## Advanced → QoS Settings

### Sessions Limit

Limit Sessions  (1~4096)

Apply

Reset

### Bandwidth Management

Enable Bandwidth Management

Apply

Reset

### WAN Configuration

WAN Interface	Upstream Bandwidth in Kbps	Downstream Bandwidth in Kbps
LTE-WAN	80000	105000

### Bandwidth Queue Configuration

Priority	Upstream Bandwidth in Kbps	Downstream Bandwidth in Kbps
Urgent	<input type="text" value="10000"/>	<input type="text" value="30000"/>
High	<input type="text" value="10000"/>	<input type="text" value="20000"/>
Medium	<input type="text" value="10000"/>	<input type="text" value="10000"/>
Low	<input type="text" value="10000"/>	<input type="text" value="10000"/>

Apply

Reset

### Bandwidth Profiles



Name


IP Address

Priority

Add

Edit

Delete



**Sessions Limit:** Enter the upper limit of the number of sessions that other devices may connect to the device. The number ranges from 1~4096.


**Bandwidth Management:** Bandwidth management controls the rate and priority of the traffic on your Internet link, allowing you to efficiently utilize Internet bandwidth. Configuring bandwidth management will allow you to control the rate and priority of traffic going to the Internet, ensuring that high priority traffic, such as voice, is assured of a certain quality of service, and also limiting low priority traffic.

You can manage the bandwidth on both Dedicated and Optional WAN ports. For bandwidth management on the Optional port, the port has to be configured as a WAN port.

Enable Bandwidth management: Check the box and click Apply to enable adding, editing and deleting of bandwidth profiles. Add profiles in the List of Bandwidth Profiles table first.

**WAN Configuration:** The WAN configuration table allows you to set the values of the upstream and downstream bandwidth as specified by your ISP.

**Bandwidth Queue Configuration:** Specify the bandwidth queue priority. Packets that are tagged with different priority will be delivered using different throughput what you specified here.



**Bandwidth Profiles:** The table lists the Bandwidth Profiles for this device and allows several operations on the Bandwidth Profiles.

Name: The user-defined name for this bandwidth profile.

IP Address: The range of the IP address set in the profile.

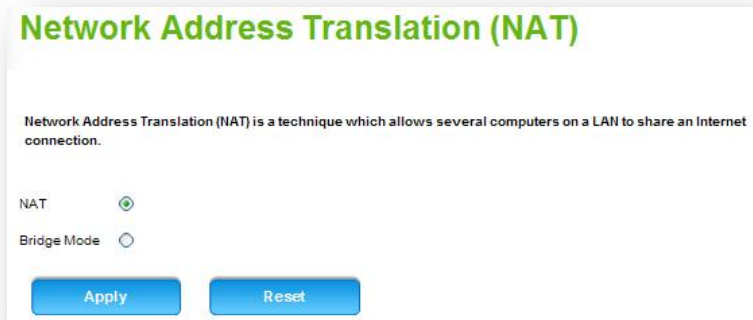
Priority: Priority of the bandwidth profile.

Actions that can be carried out on bandwidth profiles are:

Checking the box in the first column will select all the bandwidth profiles in the table.

Click Add to add a bandwidth profile, or click Edit to open the Bandwidth Profiles Configuration page to edit the selected bandwidth profile. Or click Delete to delete the selected item.

## Advanced → NAT



Network Address Translation (NAT) is a technique which allows several computers on a LAN to share an Internet connection. The computers on the LAN use a "private" IP address range while the WAN port on the DWR-923 is configured with a single "public" IP address.

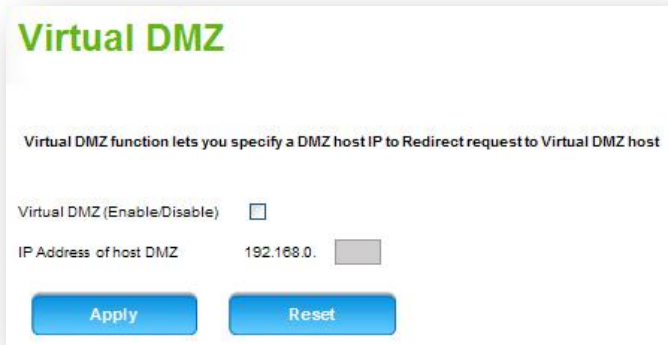
Along with connection sharing, NAT also hides internal IP addresses from computers on the Internet.

**NAT:** Select NAT if your ISP has assigned you only one IP address. The computers that connect through the DWR-923 will need to be assigned IP addresses from a private subnet (e.g. 192.168.10.0).

**Bridge Mode:** The DWR-923 in bridge mode can act as a bridge and also filter/inspect packets. It has all the interfaces belonging to the same LAN segment and you do not have to change other network settings when you add a transparent device to the network. Select this option to add your WAN interface to the LAN segment.

Click Apply to apply the changes. Or click Reset to undo your configurations.

## Advanced → NAT → Virtual DMZ



**Virtual DMZ**

Virtual DMZ function lets you specify a DMZ host IP to Redirect request to Virtual DMZ host

Virtual DMZ (Enable/Disable)

IP Address of host DMZ 192.168.0.

Virtual DMZ (De-Militarized Zone) allows you to specify a DMZ host IP to redirect requests to a Virtual DMZ host in order to enhance the security of the local area network.

**Virtual DMZ (Enable/Disable):** Enable or disable the Virtual DMZ function. If this function is enabled, threats from external networks will be directed to the Virtual DMZ instead of the network.

**IP Address of host DMZ:** Enter the IP address of host DMZ.

Click Apply to apply the changes. Or click Reset to undo your configuration.

## Advanced → NAT → Port Mapping



Port Mapping can be used to translate the common service port to a custom port inside your local network such as web or FTP.

***List of Port Mapping Services:*** Displays all the port mapping rules for the DWR-923.

**Service:** The name of the service for which the port mapping rule has been created.

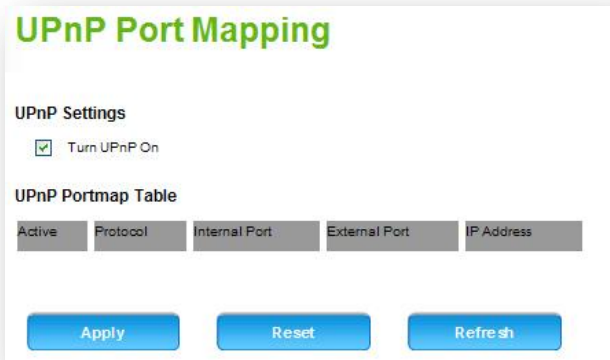
**IP Address:** The IP address of the computer on the local network to which the traffic will be forwarded.

**Port Translation:** The port number of the destination host for traffic forwarding.

Click Add to add a port mapping rule, or select an item and click Edit to modify or click Delete to delete the selected item.



## Advanced → NAT → UPnP Port Mapping



**UPnP Port Mapping**

**UPnP Settings**

Turn UPnP On

**UPnP Portmap Table**

Active	Protocol	Internal Port	External Port	IP Address
--------	----------	---------------	---------------	------------

**Apply**   **Reset**   **Refresh**

For devices that support Universal Plug and Play (UPnP), enabling the UPnP Port Mapping function will allow automatic port forwarding that helps your UPnP devices communicate with the Internet.

**UPnP Settings:** Check the box and click Apply to enable UPnP port mapping function.

**UPnP Portmap Table:** UPnP devices that are applied with the UPnP port mapping function will be listed in this chart.

## Special Applications

While common applications use known TCP/UDP ports, many custom or uncommon applications require traffic to be sent through the firewall. This section allows you to define the traffic type and static ports for a unique application and then create security policies for this user-defined application.

### List of Services

<input type="checkbox"/>	Service Name	Protocol	Start Port	End Port
<input type="checkbox"/>	HTTP	TCP	80	80
<input type="checkbox"/>	DNS	UDP	53	53
<input type="checkbox"/>	FTP	TCP	21	21
<input type="checkbox"/>	HTTPS	TCP	443	443
<input type="checkbox"/>	ICQ	TCP	5190	5190
<input type="checkbox"/>	IRC	TCP	6660	6669

While common services use known TCP/UDP ports, many custom or uncommon applications require traffic to be sent through the firewall. This section introduces the custom services of the DWR-923.

**Service Name:** Name of the service for identification and management purposes.

**Protocol:** The layer 4 protocol that the service uses: TCP, UDP.

**Start Port:** The start of the port range for the custom service.

**End port:** The end of the port range for the custom service.

Click Add to add a special application, or select an item and click Edit to modify or click Delete to delete the selected item.



Static routing is a data communication concept describing one way of determining packet path selection of routers in your networks. The table lists all static routes that have been added manually and allows several operations on the static routes.

**Name:** The name of the route for identification and management purposes.

**Destination Network:** The destination host or network to which the route leads.

**IP Subnet Mask:** Subnet Mask for the destination.

**Network:** Displays the network to which the route belongs, and can be either wired or wireless.

**Gateway:** The IP Address of the gateway through which the destination host or network can be reached.

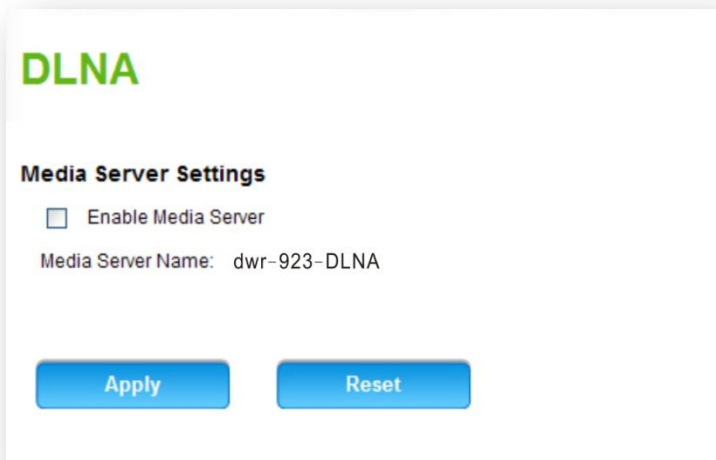
Click Add to add a static route, or select an item and click Edit to modify or click Delete to delete the selected item.

## Advanced → USB → USB Storage

### USB Storage

Directory	Total	Used	Available	Percent
-----------	-------	------	-----------	---------

Show information of the USB storage device connecting to this product, which includes the directory it mounts, its capacity and the used percentage.



Turning this function on allows use of this product as a media server. DLNA compatible client devices will be able to read or play files that are stored in the USB storage device connecting to this product.

**Enable Media Server:** Check this option to enable the media server function.

## 3.3.6 System

System → Time Settings

### Time Settings

Network Time Protocol (NTP) is a protocol that is used to synchronize computer clock time in a network of computers. This page allows setting the date, time and NTP servers. Accurate time across a network is important for logging, scheduled upgrade and scheduled policies.

Current Time Thursday, January 01, 1970, 02:16:42 (GMT +0100)

Automatically get date and time

Time Zone

Enable Daylight Saving

NTP Server1

NTP Server2

NTP Server3


Configure date and time manually

Year	Month	Day	Hours	Min	Sec
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

Network Time Protocol (NTP) is a protocol that is used to synchronize computer clock time in a network of computers. This page allows you to set the date, time and NTP (Network Time Protocol) servers. Accurate time across a network is important for logging and execution of scheduled upgrades and scheduled policies.

**Current Time:** Displays the current time of the DWR-923.

**Time Zone:** Select the local time zone. This is required in order for the



firewall schedules to work.

**Enable Daylight Saving:** If supported by the NTP servers for your region, you can check Automatically Adjust for Daylight Savings Time.

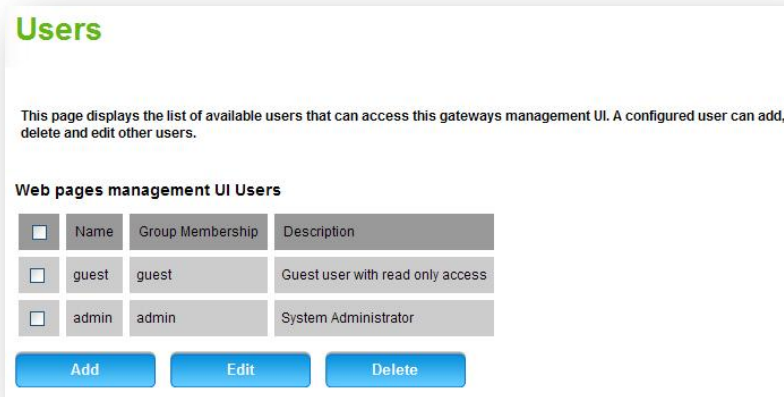
**NTP Server1:** The NTP server to sync. Default is 0.us.pool.ntp.org

**NTP Server2:** The second NTP server to sync in case the first one does not respond. Default is 1.us.pool.ntp.org.

**NTP Server3:** The third NTP server to sync in case the first and second does not respond. Default is 2.us.pool.ntp.org.

**Configure date and time manually:** Select this if you would like to set time manually.

Click Apply to apply the changes. Or click Reset to undo your configurations.



This page lists the users that have been configured on the DWR-923 for accessing shares, the Internet or even managing the device. The default guest or administrator user has access to the DWR-923’s web management. A newly configured user (along with the default guest / admin) can be assigned to a group, upon which common parental control and content sharing policies can be applied. Custom users are not able to access the web management interface.

**Name:** Unique identifier for this user

**Group Membership:** Group to which the user belongs.

**Description:** Description of the user.

Click Add to add a user account, or select a user and click Edit to modify or click Delete to delete the selected item.



## Reboot


On clicking the button to reboot the device, you will see a countdown timer through the reboot period. At the end of the timer the login page of the browser will be shown.

Reboot

Apply

**Reboot:** Select Reboot and click Apply, a countdown timer will appear and count down the reboot period. After the device reboots, the Login page will be displayed.

**Revert to factory reset configuration:** Select revert to factory reset configuration and click Apply. The DWR-923 will restore all configuration settings to the original factory default settings.

 **Note:** Restoring factory default settings will erase all of your existing settings.

## Firmware Upgrade

### 4G Router Firmware Upgrade

The gateways firmware can be upgraded by locating it on your computer and uploading it to the system.

Select firmware

### 4G Model Firmware Upgrade

The 4G Module firmware can be upgraded by locating it on your computer and uploading it to the system.

Select 4G Model firmware

Firmware will be continually updated as more features are added and known issues are resolved. This section helps you to upgrade your firmware to the latest version available online.

Select to upgrade firmware for the DWR-923 system or the LTE module:

1. Click Browse to locate the firmware file from the directory on the local host.
2. Click Router Upgrade/ 4G Upgrade to begin firmware upgrade.

**Remote Management**

This feature can be used to manage the box remotely from WAN side.

Enable Remote Management:

Access Type: All IP Addresses

IP Address: 0.0.0.0

Enable Remote SNMP:

Apply Reset

**Multiple IP ranges Configuration**

Start IP Address End IP Address


Add Edit Delete

This feature can be used to manage the device remotely from the WAN side. By default, Remote Management is disabled. To enable WAN access to the Configuration Utility, check the box.

**IMPORTANT:** When Remote Management is enabled, the security appliance is accessible to anyone who knows its IP address. Since a malicious WAN user can reconfigure the DWR-923 and misuse it in many ways, it is **HIGHLY RECOMMENDED** that you change the admin and guest passwords before continuing.

Permission for Remote Management can be given to the following:

**Enable Remote Management:** Check the box to enable remote management.



**Access Type:** Select an access type. If you choose All IP Addresses the DWR-923 will access all IPs automatically. If IP Address Range is selected, you will have to specify the starting and ending IP addresses from the following column. If Only this PC is selected, you will have to specify your PC IP address.

**IP Address:** IP address of the PC given remote management permissions

**Enable Remote SNMP:** Check the box to enable remote SNMP.

Click Apply to apply the changes. Or click Reset to undo your configurations.

### ***Multiple IP Range Configuration***

Start IP Address: Displays the starting IP address for the allowed range.

End IP Address: Displays the ending IP address for the allowed range.

Click Add to add an IP address, or select an item and click Edit to modify or click Delete to delete the selected item.

## System → System Logs

**System Logs**

Enable Logging

Log Category: All

Apply Reset

**View Logs**

Refresh Log Clear Log

**Download tar log files**

Select file: logfile.tar Download

**Remote Logging**

Enable Remote Logging

IP Address

Apply Reset

**System Logs:** As the DWR-923 manages network traffic and communication, it continuously generates logs for troubleshooting and network analysis by the home network administrator. The logging features for various sections can be enabled for desired features (such as network, security, applications and administration) to analyze the actions performed in these sections of the DWR-923.

1. Check Enable Logging box to enable log collection on the DWR-923.
2. Select a Log Category from All, Network, Security, Administration or



Applications to display the appropriate logs in the View Logs section.

3. Click Apply to apply the changes. Or click Reset to undo your configurations.

**View Logs:** The logs are displayed in this section. Click Refresh Log to view the most up-to-date log information. Or click Clear Log to erase all of the log information.

**Download Tar Log Files:** Select a tar log file and then click Download to download the selected file to your computer.

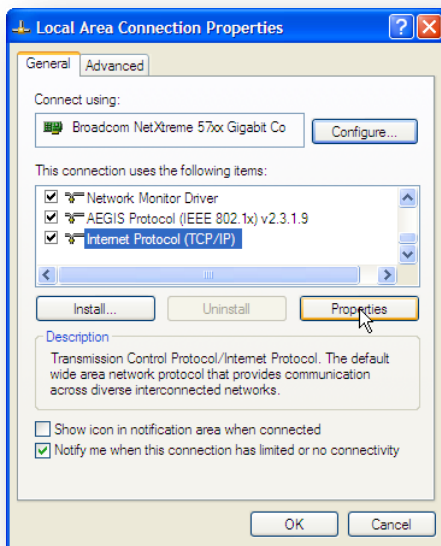
**Remote Logging:** You can write and maintain the log data to a remote computer using the remote logging function. Enable this function and enter the IP address of this computer.

## 4. Appendix

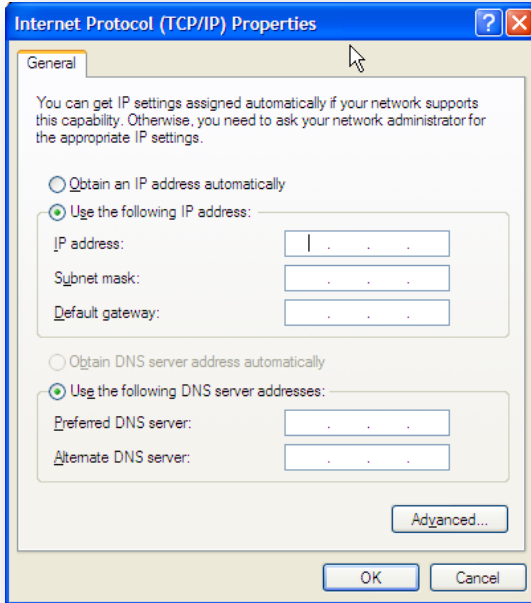
### 4.1 Connected PC IP Address Configuration

Appropriate IP address settings are required to communicate with the DWR-923. The following instructions use Windows XP to demonstrate the IP setup steps.

1. In the Windows Start menu, click Control Panel.
2. Double-click Network Connections (if required, switch to Classic View first).
3. Right-click Local Area Connection and then click Properties.
4. The Local Area Connection Properties window will appear:



- From the “This connection uses the following items” list, select Internet Protocol (TCP/IP) and then click Properties. The Internet Protocol (TCP/IP) window will appear:



- If you select “Obtain an IP address automatically,” click the OK button to finish your configuration.
- If you select “Use the following IP address,” ensure that your IP address is from 192.168.0.100 to 192.168.0.254. The subnet mask is 255.255.255.0.
- Click OK → OK to apply this IP address setting.