



300 Mbps Wireless Repeater

Model: REPW300



INSTRUCTION MANUAL

Contents

1	Safety Precautions.....	4
2	Overview	5
2.1	Product Introduction	5
2.2	Packing List	5
3	Mode Introduction	6
3.1	Bridge Mode.....	6
3.2	Router Mode	6
3.3	Wireless Universal Repeater/WDS Mode	6
3.4	Client Mode	6
4	Hardware Description and Requirements	6
4.1	Hardware Description.....	6
4.1.1	Front Panel and LED Status.....	6
4.1.2	Rear/Side Panel and Interface Description	8
4.2	Hardware Requirements.....	8
4.2.1	System Requirements	8
4.2.2	Before You Begin.....	9
4.3	Operation Range.....	9
5	PC Configuration and Wireless Configuration	10
5.1	PC Configuration.....	10
5.2	Wireless Configuration	12
6	Configure the Device	13
6.1	Bridge Mode Configuration	14
6.2	Router Mode Configuration.....	14
6.3	Repeater Mode Configuration	16
6.4	WDS Mode	17
6.4.1	Repeater Configuration in the WDS Mode.....	17
6.4.2	Central Base Station Configuration in the WDS Mode	18
6.4.3	WDS Application	19
6.5	Client Mode Configuration	20
7	Web Configuration in Bridge Mode.....	21
7.1	Running Status	21
7.1.1	Router Status	21
7.1.2	Clients List.....	22
7.2	Setup Wizard	22
7.3	Mode Setting.....	22
7.4	Network Settings	22
7.4.1	LAN Interface Settings	23
7.4.2	DHCP Server	23
7.5	Wireless Settings	24

7.5.1	Wireless Basic Settings	25
7.5.2	Guest Network.....	28
7.5.3	Wireless Advanced Settings.....	29
7.5.4	WPS Setup	32
7.6	Management Function	33
7.6.1	Backup Settings	34
7.6.2	Reboot Device.....	35
7.6.3	Set Password.....	35
7.6.4	Router Upgrade	35
8	Web Configuration in Router Mode	37
8.1	Running Status	37
8.1.1	Router Status	37
8.1.2	Clients List.....	38
8.2	Setup Wizard.....	39
8.3	Mode Setting.....	39
8.4	Network Settings.....	39
8.4.1	LAN Interface Settings	39
8.4.2	WAN Interface Settings.....	40
8.4.3	DHCP Server	47
8.4.4	NAT ALG	49
8.5	Wireless Settings	49
8.5.1	Wireless Basic Settings	50
8.5.2	Guest Network.....	50
8.5.3	Wireless Advanced Settings.....	51
8.5.4	WDS Function	51
8.5.5	WPS Setup	52
8.6	Network Application.....	52
8.6.1	Port Forwarding	52
8.6.2	Port Triggering	53
8.6.3	UPnP.....	55
8.6.4	IGMP Proxying	55
8.6.5	DMZ Server.....	56
8.6.6	Dynamic DNS	57
8.6.7	Static Routes	57
8.7	Security Options	58
8.7.1	Block Sites.....	59
8.7.2	Block Services	60
8.7.3	Protection	61
8.8	Management Function	62
8.8.1	Backup Settings	63

	8.8.2	Remote Management	63
	8.8.3	Schedules.....	63
	8.8.4	SNTP	64
	8.8.5	Reboot Device.....	65
	8.8.6	Set Password.....	65
	8.8.7	Router Upgrade	66
9		Web Configuration in Wireless Universal Repeater Mode	67
	9.1	Running Status	67
	9.1.1	Router Status	67
	9.1.2	Clients List.....	68
	9.2	Setup Wizard.....	68
	9.3	Repeater Mode Setting.....	68
	9.4	Network Settings	68
	9.5	Wireless Settings	68
	9.5.1	Wireless Universal Repeater	69
	9.5.2	WPS Setup	69
	9.5.3	Wireless Client Function	73
	9.6	Management Function	74
10		Web Configuration for the WDS Mode.....	74
	10.1	Running Status	74
	10.2	Setup Wizard.....	74
	10.3	Mode Setting.....	74
	10.4	Network Settings	75
	10.5	Wireless Settings	75
	10.5.1	WDS Function	75
	10.5.2	Wireless Basic Settings	76
	10.6	Management Function	76
11		Web Configuration in Client Mode.....	76
	11.1	Running Status	76
	11.1.1	Router Status	76
	11.1.2	Clients List.....	77
	11.2	Setup Wizard.....	77
	11.3	Network Settings	77
	11.4	Wireless Settings	77
	11.4.1	WPS Setup	77
	11.4.2	Wireless Client Function	77
	11.5	Management Function	77

1 Safety Precautions

Before operating the repeater, read the following precaution information carefully:

- Leave proper space for heat dissipation to avoid damage caused by device overheating. Heat dissipation holes enable the device to work normally. Do not cover heat dissipation holes.
- Keep the device away from heat outlets or high temperature places. Prevent the device from direct sunlight.
- Keep the device in dry places. Do not spill any liquid on this device.
- Do not connect the device to any PC or electronic product unless our customer engineer or your broadband provider instructs you to do this, because any wrong connection may cause power or fire risks.
- Do not place this device on an unstable surface.



This mark is applied to show the equipment conforms to European safety and electro-magnetic compatibility standards.

2 Overview

2.1 Product Introduction

The repeater, a pocket router, is case-shaped, easy to carry, and easy to install. Its wireless transmission rate is up to 300 Mbps. It is a high-performance and IEEE802.11b/g/n-compatible network access device that can provide reliable and convenient network access service for individual users and SOHO (Small Office, Home Office). It features Web-based GUI, allowing users to easily modify settings to connect the device to ISP (Internet Service Provider) and conveniently perform upgrade using the WEB page.

In addition, the device has a three-way switch on the side panel that enables users to change the device's working mode among AP, Repeater, and Client. In the AP mode, the device functions as a wireless router to achieve wireless connection for the wired LAN. In the Repeater mode, the device provides the URM (Universal Repeater Mode) function for users to expand wireless coverage of the existing AP in a quick and easy way. In the Client mode, the device functions as a wireless network adapter but it can provide a better transmission and connection performance.

2.2 Packing List

Please check whether your packing list includes the following items:

- 1 x 300 Mbps wireless repeater
- 1 x network cable
- 1 x User Manual (CD)

3 Mode Introduction

3.1 Bridge Mode

In the Bridge mode, the device works as a wireless router to achieve wireless connection for the wired LAN.

3.2 Router Mode

In the Router mode, the device works as a domestic gateway.

3.3 Wireless Universal Repeater/WDS Mode

In the Wireless Universal Repeater/WDS mode, the device expands wireless coverage of the existing AP. Computers can connect to the device in either a wired or wireless way.

3.4 Client Mode

In the Client mode, the device provides Internet access for a set-top box or a computer with a network adapter.

4 Hardware Description and Requirements

4.1 Hardware Description

4.1.1 Front Panel and LED Status

There are 4 LED indicators on the front panel of the device. By observing their status, you can check whether the device runs normally.



The following table describes indicator status of the device.

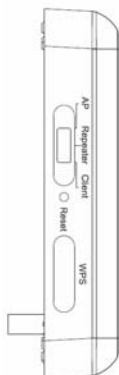
Indicator	Color	Status	Description
Power	Green	On	The device is working normally.
	Red	On	The system is in the process of self-inspection or fails the self-inspection. Or it is in the process of software upgrade.
WPS	Green	Off	The WPS session is down.
		On	The WPS indicator keeps on for 5 minutes after WPS (Wi-Fi Protected Setup) connection succeeds.
		Quick blink	A terminal is attempting to connect to the device through WPS but fails.
		Quick blink with a certain interval	Multiple terminals are connecting to the device through WPS at the same time. WPS sessions conflict.
		Slow blink	The WPS session is up.
Ethernet	Green	Off	The Ethernet port is in the non-communication state.
		On	The Ethernet port is in the communication state.
		Blink	The Ethernet port is transmitting and receiving data.
WLAN	Green	Off	The WLAN connection is in the non-communication state.
		On	The WLAN connection is in the communication state.
		Blink	Data is being transmitted and received in the WLAN.

4.1.2 Rear/Side Panel and Interface Description

Rear Panel



Side Panel



The following table describes interface and button status of the device.

Interface/Button	Description
WAN/LAN	If the device is set to AP mode, the interface is a WAN interface which connects it to WAN or uplink network devices. If the device is set to the Repeater/Client mode, the interface is a LAN interface.
Reset	Press the Reset button gently for 3-6 seconds and then release it. The system restores to the factory default settings.
AP/Repeater/Client	It is used for setting the device to the AP, Repeater, or Client mode. AP mode—including Bridge and router modes Repeater mode—to expand wireless network coverage Client mode—equivalent to a wireless network adapter
WPS	For enabling WPS PBC mode. For more information, refer to WPS descriptions for each mode.

4.2 Hardware Requirements

4.2.1 System Requirements

Before installing the device, please ensure that the following items are available:

- At least one Ethernet RJ45 cable (10Base-T/100Base-T)

- One wireless repeater
- A PC is already installed with the TCP/IP protocol and the PC can access the Internet.

4.2.2 Before You Begin

Before you install the device, please pay attention to the following items:

- The Ethernet cables that are used to connect the device to a computer, hub, router, or switch should be less than 100 meters.
- Do not place this device on an uneven or unstable surface. Do not put this device on the ground.
- Keep the device clean. Prevent the device from direct sunlight. Avoid any metal in the device.
- Place the device in the center of the area to optimize the wireless coverage.

4.3 Operation Range

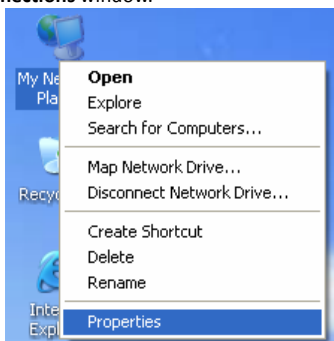
The operation range of the device depends on the actual environment. The path and effect of signal transmission vary with the deployment in a house or an office. For example, the outdoor straight transmission distance for a certain device can reach 300 meters and the indoor transmission distance can reach 100 meters.

5 PC Configuration and Wireless Configuration

5.1 PC Configuration

The following takes Windows XP as an example. Do as follows to manually set the network adapter:

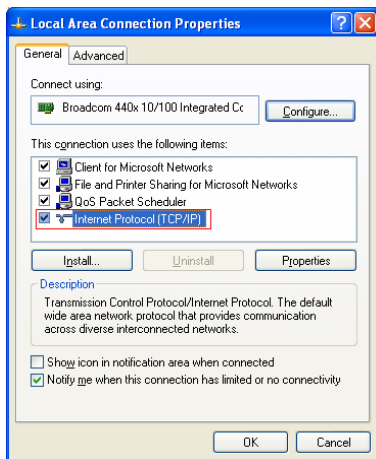
- Step 1** Right-click the icon of **My Network Places** and choose **Properties** to display the **Network Connections** window.



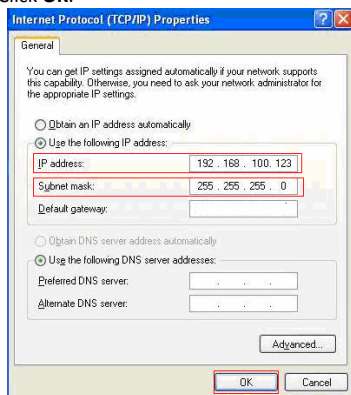
- Step 2** Right-click the icon of a network interface card or wireless network adapter and choose **Properties**. (Note: In the Client mode, computers can connect to the device through an Ethernet cable only.)



- Step 3** Double-click Internet Protocol (TCP/IP).



Step 4 Select **Obtain an IP address automatically** when the device is in Router mode. When the device is in other modes, set the IP address of your computer to **192.168.100.X** (X is an integer in the range of 2 to 253), and the MAC address to 255.255.255.0. Set the gateway and the IP address of the DNS server. You can leave them blank if you do not know information about the gateway and DNS server. Click **OK**.




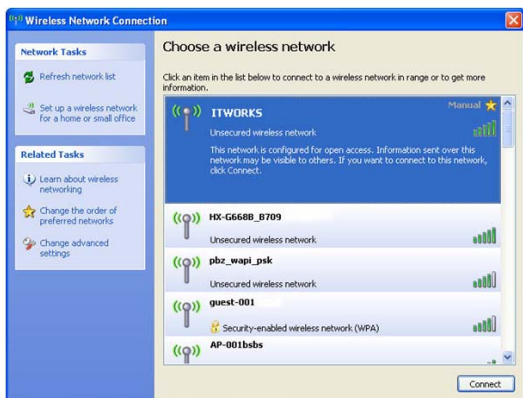
Note:

After finish configuring the device, the domestic gateway can set the Internet protocol for the PC's network adapter. Set the IP address and DNS server to obtain an IP address automatically as shown in the figure above.

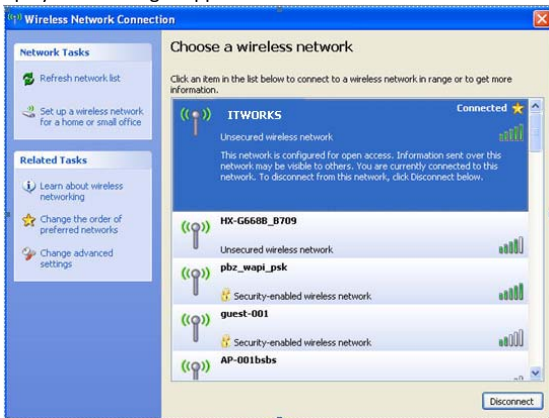
5.2 Wireless Configuration

Take Windows XP as an example; please do as follows to connect the wireless network adapter of your PC to the device:

- Step 1** Click the  icon displayed at the right bottom corner of the desktop (Note: Ensure that your PC is installed with a wireless network adapter).
- Step 2** In the **Wireless Network Connection** page, click the desired wireless network.



- Step 3** Your computer is connected to the wireless network when **Connected** is displayed on the right upper corner.



Note:

The default SSID of the repeater is ITWORKS.

6 Configure the Device

The following table describes the IP information of AP/Repeater/Client modes of the device.

Mode On the Case	Mode Available In the Web	Management IP Address	Subnet MAC Address	DHCP	Way of connecting to PC
AP	Bridge (default)	192.168.100.253	255.255.255.0	Disable	Ethernet cable /Wireless
	Router			Enable	Wireless only
Repeater	Wireless Universal Repeater (default)	192.168.100.253	255.255.255.0	Disable	Ethernet cable /Wireless
	WDS				
Client	Client (default)	192.168.100.253	255.255.255.0	Disable	Ethernet cable only

Step 1 Set the three-way switch on the case of the device to the mode you want.

Step 2 Run the Internet Explorer (IE). Enter the management IP address of **192.168.100.253** and press **Enter**. In the login window displayed below, enter the user name and password (both are **admin**).

Step 3 Click Login, the following page is displayed.

Click **Logout** to log out from the page.

 **Note:**

Language can be switched between English and French in the upper right corner.

Terminal devices can access the network through the repeater after finish the configuration by following procedures in the sections below.

6.1 Bridge Mode Configuration

- Step 1** Set the three-way switch on the side panel to **AP** after the device is powered on. Log in to the configuration page after the system is started.
- Step 2** Click **Setup Wizard** in the navigation bar on the left pane of the page. Set the SSID and encryption password and note them down. Click **Finish** to complete the settings.

Setup Wizard

This setup wizard helps you to configure wireless settings in bridge mode.

<input checked="" type="checkbox"/> Enable Wireless Router Radio	
Name(SSID)	
Name(SSID):	<input type="text" value="ITWORKS"/>
Security Options	
Security Options:	<input type="text" value="WPA2-PSK[AES]"/>
Security Options(WPA2-PSK)	
PassPhrase:	<input type="text"/> (8-63 characters or 64 hex digits)

6.2 Router Mode Configuration

- Step 1** Set the three-way switch on the side panel to **AP** after the device is powered on. Log in to the configuration page after the system is started.
- Step 2** Click **Mode Settings** and select **Router Mode** (The default one is **Bridge Mode**). Click **Apply** to reboot the device.

Mode Settings

Please choose your mode as follows:

Bridge Mode

Router Mode

In this mode, the port is used as a wan port.
You can only login web by using your wireless network card to connect this network.
Please remember SSID and Security Options of your wireless network before you change to this mode.

- Step 3** Take off the network cable and connect PC to the device by a wireless network adapter after the device is restarted. Log in to the configuration page. Click **Setup Wizard** in the navigation bar on the left pane of the page. Select **Yes** and click **Next**. The device will automatically detect the broadband type.

Setting up your internet

The smart setup wizard can detect the type of Internet connection that you have. Do you want the smart setup wizard to try and detect the connection type now?

- Yes.
 No. I Want To Configure The Router Myself.

Next

- Step 4** The device can detect three types of broadband: DHCP, Static IP, and PPPoE. Perform configurations according to the broadband type you are using.

(1) Parameter configuration for DHCP

Setup Wizard

Dynamic IP (DHCP) detected
Successfully detected the type of Internet connection you have.

Back Next

Dynamic IP Address

Account Name (If Required)

Apply Cancel

Enter the account name provided by your ISP. Leave it blank if your ISP does not provide the account name.

(2) Parameter configuration for static IP

Setup Wizard

Static IP (Fixed) detected
Successfully detected the type of Internet connection you have.
If you believe you have received this message in error, please power cycle your modem (unplug the modem and plug it back in). Then close this screen, and reopen a new Web browser (e.g., Internet Explorer)

Back Next

Static IP (Fixed) Addresses

Your Internet service provides the static IP (Fixed) settings.

Be sure to enter the correct IP address for each static IP settings. For example, be sure to enter the Gateway IP Address in the Gateway Address fields and the IP Address in the IP Address fields without mixing them up.

Internet IP Address	
IP Address	<input type="text"/>
IP Subnet Mask	<input type="text"/>
Gateway IP Address	<input type="text"/>
Domain Name Server (DNS) Address	
Primary DNS	<input type="text"/>
Secondary DNS	<input type="text"/>

Finish Cancel

(3) Parameter configuration for PPPoE

Setup Wizard

PPPoE detected
Successfully detected the type of Internet connection you have.

PPPoE

Password Setting

Login:

Password:

Service Name (if required):

Domain Name Server(DNS) Address:

Get Automatically From ISP

Use These DNS Servers

Primary DNS:

Secondary DNS:

Enter the account name and password for Internet connection.

Enter the DNS address provided by your ISP. If your ISP does not provide it, select Get Automatically From ISP.

Step 5 Click **Next**. Set the SSID and password and note them down. Click **Finish** to complete the settings.

Wireless Settings

Enable Wireless Device Radio

Name(SSID)

Name(SSID):

Security Options

Security Options:

You can use the default SSID. However, we suggest modifying the SSID.

Set the wireless encryption mode and password.

6.3 Repeater Mode Configuration

- Step 1** Set the three-way switch on the side panel to **Repeater** after the device is powered on. Connect the network cable to the device again and log in to the configuration page after the system is started.
- Step 2** Click **Setup Wizard** in the navigation bar on the left pane of the page. Select **Wireless Universal Repeater Mode** and click **Next**.

Setup Wizard

Step1: There are two modes to expand your wireless network of the Repeater Mode. You can choose anyone of WDS Mode or Wireless Universal Repeater Mode.

Please choose your repeater mode as follows:

WDS Mode

Wireless Universal Repeater Mode

- Step 3** Click **Site Survey** to search for the wireless network you want to connect. Select a desired network. Click **Next**.

Setup Wizard

Step2: Please configure the wireless client first. Click "Site Survey" button to survey wireless sites when client mode is enabled. If any Access Point or IBSS is found, the results will be displayed in the Site Survey List three seconds later, you could select anyone to connect it manually. Then click "Next".

Site Survey

Number of Sites Scanned:32

Site Survey List

#	SSID	BSSID	Channel	Signal	Encrypt	Select
1	TW-2B08	00:1F:A4:91:2A:60	10	100%	WPA-PSK(AES/TKIP)/ WPA2-PSK(AES/TKIP)	<input checked="" type="radio"/>
2	Zoltrix_ZW919	00:28:12:34:56:78	1	100%	None	<input type="radio"/>
3	SMC	00:1F:A4:90:87:50	3	100%	WPA-PSK(AES/TKIP)/ WPA2-PSK(AES/TKIP)	<input type="radio"/>

Back

Next

- Step 4** Configure the repeater with the same security option as its uplink network. (The following figure takes the security option of **None** as an example.) Set the encryption password and note it down. Click **Next**.

Setup Wizard

Step4: You should configure your wireless client manually so it has the same wireless security settings as the network which you selected. Then click "Next".

Wireless Client Security Options

Wireless Client Security Options :

None

Back

Next

- Step 5** The device provides wireless roaming function if **Synchronize Wireless Universal Repeater's and Uplink AP's SSID and Security Options** is selected. Otherwise, manually configure the SSID and security options for the repeater. Click **Finish** to complete setup wizard.

Setup Wizard

Step4: This page provides an easy way to configure wireless universal repeater. If you enable the function, your wireless universal repeater would use same SSID and security options with uplink AP, or you should configure SSID of Extended Interface and Security Options manually. Finally click "Finish".

Wireless Universal Repeater Settings

Synchronize Wireless Universal Repeater's And Uplink AP's SSID And Security Options

SSID of Extended Interface :

ITWORKS

Security Options :

none

Note: If you changed settings of wireless universal repeater, the wireless clients connecting to your wireless universal repeater need connect to wireless universal repeater with new SSID and security options again.

Back

Finish

Cancel

6.4 WDS Mode

6.4.1 Repeater Configuration in the WDS Mode

- Step 1** Set the three-way switch on the side panel to **Repeater** after the device is powered on. Log in to the configuration page after the system is started.

- Step 2** Click **Setup Wizard** in the navigation bar on the left pane of the page. Select **WDS Mode** and click **Next**. (Note: The WDS function cannot be enabled if the channel is set to **Auto**) Manually set all WDS devices to the same channel.

Setup Wizard

Step1: There are two modes to expand your wireless network of the Repeater Mode. You can choose anyone of WDS Mode or Wireless Universal Repeater Mode.

Please choose your repeater mode as follows:

WDS Mode

Wireless Universal Repeater Mode

Next

- Step 3** Set the IP address of the LAN port of the repeater and enter the MAC address of the basic station. Click **Next**.

Setup Wizard

Step2: In WDS Mode, the device would work as a Repeater and could communicate only with another Base Station-mode wireless station. You must enter the wireless MAC address of the other Base Station-mode wireless station in the field named "Basic Station MAC Address" and enter the wireless MAC address of router in the other Base Station-mode wireless station webpage. The change of Repeater IP Address would result the change of LAN IP Address.

WDS Settings

Wireless MAC of this router: 00:1E:E3:4B:06:6C

Repeater IP Address:

Basic Station MAC Address:

Back

Next

- Step 4** Set the SSID, channel, and security encryption for the repeater. The channel cannot be set to **Auto**. It is recommended to configure the repeater with the same security option as its base station. Set the encryption password and note it down. Click **Finish** to complete the settings.

Setup Wizard

Step3: WEP can (and should) be used to protect WDS communication. "Auto" channel can not be used.

Other Wireless Settings

Name(SSID):

ITWORKS

Channel:

1

Security Options:

None

Back

Finish

Cancel

6.4.2 Central Base Station Configuration in the WDS Mode

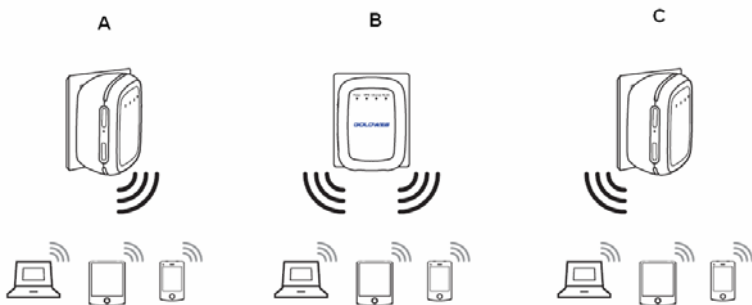
- Step 1** Set the device to Router mode.
- Step 2** Choose **Wireless Settings > WDS Function**, select **Enable WDS Function**, and enter the MAC address of the Repeater (Note: One basic station can connect to a maximum of 4 repeaters).

WDS Function

<input checked="" type="checkbox"/> Enable WDS Function	
<input type="checkbox"/> Disable Wireless Clients Association	
Wireless MAC of this router: 00:1E:E3:42:15:35	
Wireless Basic Station	
Repeater MAC Address 1:	<input type="text"/>
Repeater MAC Address 2:	<input type="text"/>
Repeater MAC Address 3:	<input type="text"/>
Repeater MAC Address 4:	<input type="text"/>

6.4.3 WDS Application

The following figure shows a wireless network for Humans Resource Department (marked as A in the figure), Finance Department (marked as B), and Marketing Department (marked as C) in an enterprise. If the three departments share one wireless router, signals searched by computers may be rather weak or even no signals are available. However, if each of the three departments uses a wireless router, we can use WDS to connect the three routers to provide perfect wireless coverage for the whole areas.



Configure the three routers in this way:

Wireless router B functions as the wireless basic station; wireless routers A and C connect to wireless router B by using WDS.

(1) **Configuring wireless router B as the wireless basic station**

Step 1 Log in to the Web management page of wireless router B. Choose **Wireless Settings > Wireless Basic Settings** and set the SSID, channel, and wireless encryption information. Write down the SSID, channel, and wireless encryption information that are required when you are configuring wireless router A and C.

Step 2 Choose **Wireless Settings > WDS Function** and enable the WDS function. Enter MAC addresses of repeaters (that is, wireless routers A and C in this example). Click **Apply** to save the settings.

(2) **Configuring wireless router A**

Do as follows to establish WDS connection between wireless routers A and B:

Step 1 Set wireless router A with the same channel and encryption information as wireless router B.

Step 2 Choose **Wireless Settings > WDS Function** and enable the WDS function. Set the IP address of wireless router B different from that of wireless router A to avoid IP address conflict (for example, change the IP address to 192.168.100.20 in the **LAN Interface Settings** page and log in to the Web management page again). Enter the MAC address of the wireless basic station.

Step 3 Click **Apply** to save the settings.

Then, WDS connection is established between wireless routers A and B.

(3) **Configuring wireless router C**

Configure wireless router C in the same way as wireless router A. Note that the IP address of the LAN interface must be changed to an IP address that does not conflict with IP addresses of existing computers or devices in the network.

6.5 Client Mode Configuration

Step 1 Click **Setup Wizard** in the navigation bar on the left pane of the page. Click **Site Survey** to search for the wireless network you want to connect.

Setup Wizard

Step1: This wizard help you to configure the wireless client. Click "Site Survey" button to survey wireless sites when client mode is enable d. If any Access Point or IBSS is found, the results will be displayed in the Site Survey List three seconds later, you could select anyone to connect it manually. Then click "Next".

#	SSID	BSSID	Channel	Signal	Encrypt	Select
1	Zoltnrk_ZW919	00:20:12:34:56:70	1	100%	None	<input checked="" type="radio"/>
2	TVI-2B008	00:1F:A4:91:2A:60	10	100%	WPA1-PSK(AES/TKIP) WPA2-PSK(AES/TKIP)	<input type="radio"/>
3	www24	00:1E:E3:C0:5F:60	9	95%	None	<input type="radio"/>

Step 2 Enter encryption information of the selected wireless network. Click **Finish** to complete the settings.

Setup Wizard

Step2: You should configure your wireless client manually so it has the same wireless security settings as the network which you selected. Then click "Finish".

Security Options :

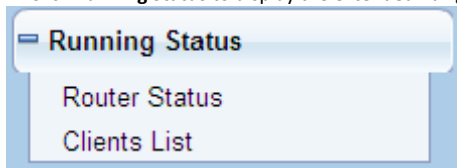
7 Web Configuration in Bridge Mode

Note:

Set the three-way switch on the side panel to **AP**, select **Bridge Mode** and restart the device. Log in to the configuration page after the device is restarted.

7.1 Running Status

Click **Running Status** to display the extended navigation menu.



Click the submenu to enter a specific configuration page.

7.1.1 Router Status

Choose **Running Status** > **Router Status** and the **Router Status** page is displayed.

Router Status

System Info	
Hardware Version	V1.0.0
Firmware Version	V1.0.0
Product Name	Wireless Router
Work Mode	Bridge Mode
Time and Date	1971-01-01 08:26:38
LAN Port	
MAC Address	00:1E:E3:4B:06:6D
IP Address	192.168.100.253
IP Subnet Mask	255.255.255.0
Wireless Port	
Wireless Network Name (SSID)	ITWORKS
Region	Europe
Wireless Channel	Auto
802.11 Mode	Mixed 802.11b/g/n
Wireless Radio	Enabled
Broadcast Name	ON
Wireless Isolation	OFF
Wi-Fi Protected Setup(WPS)	ON
Wireless Security Mode	None

In this page, you can view information about the current running status of the device, including system information, LAN port status, and wireless network status.

7.1.2 Clients List

Choose **Running Status > Clients List** and the **Clients List** page is displayed.

Clients List

Wired Devices			
#	IP Address	MAC Address	Device Name
1	192.168.100.10	48:02:2A:D1:A9:60	unknown

Wireless Devices(Wireless intruders also show up here)			
#	IP Address	MAC Address	Device Name

Refresh

This page displays information of computers connected to the router, including the IP address, and MAC address of each computer.

7.2 Setup Wizard

For settings, refer to section **6.1 Bridge Mode Configuration**.

7.3 Mode Setting

Click **Mode Settings** and the **Mode Settings** page is displayed.

Mode Settings

Please choose your mode as follows:

Bridge Mode

In this mode, the port is used as a lan port.
You can login web by either connecting you wired network card and the lan port with ethernet cable or using your wireless network card to connect this wireless network.

Router Mode

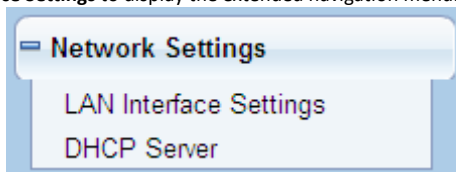
View Wireless Basic Config

Apply Cancel

- **Bridge Mode:** The interface on its case is an LAN interface. Users can connect the device and PC by an RJ45 cable or a wireless network card.
- **Router Mode:** Computers can connect to the device in wireless way only.

7.4 Network Settings

Click **LAN Interface Settings** to display the extended navigation menu.



7.4.1 LAN Interface Settings

Choose **Network Settings > LAN Interface Settings** and the **LAN Interface Settings** page is displayed.

LAN Interface Settings

LAN TCP/IP Setup					
IP Address		<input type="text" value="192"/>	<input type="text" value="168"/>	<input type="text" value="100"/>	<input type="text" value="253"/>
IP Subnet Mask		<input type="text" value="255"/>	<input type="text" value="255"/>	<input type="text" value="255"/>	<input type="text" value="0"/>

You can modify the IP address and IP subnet mask of the LAN port as required.



Note:

If you change the default IP address, you must use the new IP address to log in to the Web configuration page of the router and the default gateway of all hosts in the LAN must be set to the new IP address for Internet access.

The subnet mask of all hosts in the LAN must be the same as the subnet mask specified in the LAN Interface Settings page.

7.4.2 DHCP Server

Choose **Network Settings > DHCP Server** and the **DHCP Server** page is displayed.

DHCP refers to Dynamic Host Configuration Protocol. If **Use Device as DHCP Service** is selected, the device automatically assigns IP addresses to computers in the LAN. Users do not need to configure TCP/IP protocol parameters such as the IP address, the subnet mask, the gateway, and the DNS server information for computers connected to the router's LAN.

DHCP Server

<input type="checkbox"/> Use Router as DHCP Server					
Starting IP Address		<input type="text" value="192"/>	<input type="text" value="168"/>	<input type="text" value="100"/>	<input type="text" value="2"/>
Ending IP Address		<input type="text" value="192"/>	<input type="text" value="168"/>	<input type="text" value="100"/>	<input type="text" value="200"/>
DHCP Lease Time(1 - 160 hours)		<input type="text" value="24"/>			
Address Reservation					
#	IP Address	Device Name	MAC Address		
<input type="button" value="Add"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>					
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>					

7.4.2.1 Using the Router as a DHCP Server

- **Use Router as DHCP Server:** If you select the **Use Router as DHCP Server** check box, the device serves as a DHCP server to automatically assign IP addresses to computers connected to it.

- **Starting IP Address/Ending IP Address:** Set the starting and ending IP addresses to specify a pool of IP addresses to be assigned by the DHCP server. After you set **Starting IP Address/Ending IP Address**, hosts in the LAN obtain IP addresses that are in the range of the starting and ending IP addresses.
- **DHCP Lease Time:** The valid time for an IP address that is automatically assigned by the DHCP server to a host. The DHCP server does not assign the IP address to other hosts within the specified time.

7.4.2.2 Using Address Reservation

When you specify a reserved IP address for a computer in the LAN, the computer always receives the same IP address each time it accesses the router's DHCP server. Reserved IP addresses should be assigned to computers or servers that require permanent IP settings.

Address Reservation				
#	IP Address	Device Name	MAC Address	
<input type="button" value="Add"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>				

To reserve an IP address:

Step 1 Click **Add** to enter the **Address Reservation** page.

Address Reservation

Address Reservation Table				
#	IP Address	Device Name	MAC Address	
<input type="radio"/>	1			
<input type="radio"/>	2	192.168.100.10	dW5rIm93bg==	48:02:2A:D1:A9:60
IP Address	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
MAC Address	<input type="text"/>			
Device Name	<input type="text"/>			
<input type="button" value="Add"/> <input type="button" value="Cancel"/> <input type="button" value="Refresh"/>				

- Step 2** Select one item from **Address Reservation Table**, or enter the IP address in the **IP Address** field to assign to the computer or server (Choose an IP address from the IP address pool that you have specified, for example 192.168.100.x). Enter the MAC address and device name of the computer or server.
- Step 3** Click **Add** to add a new item into **Address Reservation**.
- Step 4** Click **Apply** to save the settings.

7.5 Wireless Settings

Set the three-way switch on the side panel to **AP**. Click **Wireless Settings** to display the extended navigation menu.

Wireless Settings

Wireless Basic Settings

Guest Network

Wireless Advanced Settings

WPS Setup

7.5.1 Wireless Basic Settings

Choose **Wireless Settings** > **Wireless Basic Settings** and the **Wireless Basic Settings** page is displayed.

Wireless Basic Settings

Region Selection	
Region :	Europe
Wireless Network	
<input checked="" type="checkbox"/> Enable SSID Broadcast	
<input type="checkbox"/> Enable Wireless Isolation	
Name(SSID) :	ITWORKS
Mode :	Mixed 802.11b/g/n
Channel:	Auto
Band Width :	Auto
Security Options	
Security Options :	None

Apply Cancel

- **Region:** Select the region where you are located.
- **Enable SSID Broadcast:** If enabled, the router broadcasts its SSID in the wireless network. Wireless clients can scan the SSID and access the wireless network under the SSID.
- **Enable Wireless Isolation:** If selected, wireless clients connected to the network of the same SSID can access the Internet only, but cannot communicate with each other.
- **Name (SSID):** Set the name for the wireless network. The SSID can contain up to 32 characters and can be letters, numerals, underlines, and any combinations of them. The SSID is case-sensitive.
- **Mode:** Select the wireless mode. **Mixed 802.11b/g/n** is recommended.

- **Channel:** The channel for transmitting wireless signals. The default channel is **Auto**. When **Auto** is selected, the device automatically selects the best channel from the available channels according to actual situations.
- **Band Width:** The bandwidth occupied for wireless signal transmission.
- **Max Transmission Rate:** The maximum transmission rate of the repeater.
- **Security Options:** Set the security encryption of the wireless network, to prevent unauthorized access and listening.

Security Options

– None

Data encryption is not adopted and the network is not secure. Any stations can access the network. This option is not recommended.

Security Options	
Security Options :	None

– WEP

Wired Equivalent Privacy, you can use WEP 64- or 128-bit encryption.

Security Options	
Security Options :	WEP
Security Encryption(WEP)	
Authentication Type :	Automatic
Encryption Type :	ASCII
Encryption Strength :	64 bits
Security Encryption(WEP) Key	
Key 1: <input checked="" type="radio"/>	<input type="text"/> (5 ASCII characters)
Key 2: <input type="radio"/>	<input type="text"/> (5 ASCII characters)
Key 3: <input type="radio"/>	<input type="text"/> (5 ASCII characters)
Key 4: <input type="radio"/>	<input type="text"/> (5 ASCII characters)

- **Authentication Type:** Select the authentication type that the system adopts. Three authentication types are available: Automatic, Open, and Shared keys.
 - **Automatic:** If selected, the router uses an authentication type of **Open** or **Shared keys** according to the request of the host.
 - **Open:** If selected, hosts in the wireless network can pass the authentication and connect to the wireless network without using a password. However, the password is required if you want to transmit data.

- **Shared keys:** If selected, hosts in the wireless network can pass authentication only when the correct password is entered. Otherwise, the hosts cannot connect to the wireless network.
- **Encryption Type:** The type of the key to be set. Hexadecimal and ASCII code are available.
 - **Hex:** Valid characters for keys contain 0–9 and A–F.
 - **ASCII:** Valid characters for keys contain all characters of the key board.
- **Encryption Strength:** The encryption strength determines the length of the key.
 - If **Encryption Strength** is set to **64 bits**, set the key to 10 hexadecimal digits or 5 ASCII characters.
 - If **Encryption Strength** is set to **128 bits**, set the key to 26 hexadecimal digits or 13 ASCII characters.
- **Key 1/2/3/4:** Set the key based on the selected encryption type and encryption strength.

– **WPA-PSK[TKIP] or WPA2-PSK[TKIP]**

WPA-PSK: Preshared key Wi-Fi protection access

WPA2-PSK: Preshared key Wi-Fi protection access version 2

TKIP: Temporal Key Integrity Protocol

Note that the 802.11n mode does not support the TKIP algorithm.

Security Options	
Security Options :	WPA-PSK[TKIP] ▼
Security Options(WPA-PSK)	
PassPhrase :	<input type="text"/> (8-63 characters or 64 hex digits)

- **PassPhrase:** Enter 8-63 ASCII characters or 64 hexadecimal digits.

– **WPA-PSK[AES] or WPA2-PSK[AES]**

WPA-PSK: Preshared key Wi-Fi protection access.

WPA2-PSK: Preshared key Wi-Fi protection access version 2.

AES: Advanced Encryption Standard

Security Options	
Security Options :	WPA2-PSK[AES] ▼
Security Options(WPA2-PSK)	
PassPhrase :	<input type="text"/> (8-63 characters or 64 hex digits)

- **PassPhrase:** Enter 8-63 ASCII characters or 64 hexadecimal digits.

– **WPA-PSK/WPA2-PSK+[TKIP]/[AES]**

It is allowed that the client uses either WPA-PSK[TKIP]/[AES] or WPA2-PSK[TKIP]/[AES].

Security Options	
Security Options :	WPA-PSK/WPA2-PSK+[TKIP]/[AES] ▼
Security Options(WPA-PSK+WPA2-PSK)	
PassPhrase :	<input type="text"/> (8-63 characters or 64 hex digits)

- **PassPhrase:** Enter 8-63 ASCII characters or 64 hexadecimal digits.



Note:

After complete configuring wireless settings for the device, only hosts that have the same wireless settings (for example, the SSID) as the device can connect to it. If you configure security settings for the device, hosts must have the same security settings (for example, the password) as the device in order to connect to it.

7.5.2 Guest Network

If you do not want visitors to know your wireless security key, you can use the guest network to allow them to use your Internet without knowing your wireless connection password.

Choose **Wireless Settings > Guest Network** and the **Guest Network** page is displayed.

Guest Network

Network Profiles					
	Scheme	SSID	Security	Apply	SSID Broadcast
<input checked="" type="radio"/>	1	ITWORKS-002	None	NO	YES
<input type="radio"/>	2	ITWORKS-003	None	NO	YES
<input type="radio"/>	3	ITWORKS-004	None	NO	YES
<input type="radio"/>	4	ITWORKS-005	None	NO	YES

Wireless Settings--Profile 1	
<input type="checkbox"/>	Enable Guest Network
<input checked="" type="checkbox"/>	Enable SSID Broadcast
<input type="checkbox"/>	Allow Guest to access My Local Network
<input type="checkbox"/>	Enable Wireless Isolation
Guest Wireless Network Name(SSID) :	<input type="text" value="ITWORKS-002"/>
Security Options--Profile 1	
Security Options :	None ▼

- **Network Profiles:** Brief description of the created guest network. You can create up to four guest networks. A network profile contains the SSID and encryption mode, whether to use the guest network, and whether to broadcast SSID. You can click the radio button of a profile to view detailed information or modify settings.
- **Enable Guest Network:** If enabled, both you and visitors can connect to the network by using the SSID of the guest network.

- **Enable SSID Broadcast:** If enabled, the device broadcasts its SSID to all wireless stations.
- **Allow Guest to access My Local Network:** If enabled, visitors using the SSID of a guest network can access not only the Internet but also LAN of the device, like users using the primary SSID of the network. If disabled, visitors using the SSID of a guest network cannot access LAN of the device.
- **Enable Wireless Isolation:** If selected, wireless clients connected to the guest network of the same SSID can access the Internet only, but cannot communicate with each other.
- **Guest Wireless Network Name (SSID):** Set the name of the guest network.
- **Security Options:** Refer to security option descriptions in section 8.5.2 **Wireless Basic Settings.**

After finishing, click **Apply** to save the settings.

7.5.3 Wireless Advanced Settings

Choose **Wireless Settings > Wireless Advanced Settings** and the **Wireless Advanced Settings** page is displayed.

Wireless Advanced Settings

Wireless Advanced Setting	
<input checked="" type="checkbox"/> Enable Wireless Router Radio	
Fragmentation Length (256-2346)	<input type="text" value="2346"/>
DTIM (1-255)	<input type="text" value="1"/>
Beacon Interval (20-1000)	<input type="text" value="100"/>
MAX Clients (0-12)	<input type="text" value="0"/>
CTS/RTS Threshold (1-2347)	<input type="text" value="2346"/>
Preamble Mode	<input type="text" value="Long preamble"/>
Guard Interval	<input type="text" value="Short GI"/>
Transmit Power Control	<input type="text" value="100%"/>
WPS Settings	
Router's PIN	<input type="text" value="12345670"/>
<input checked="" type="checkbox"/> Enable WPS <input type="checkbox"/> Disable Router's PIN	
Wireless Card Access List	
<input type="button" value="Setup Access List"/>	

- **Enable Wireless Router Radio:** If you disable the wireless router radio, wireless devices cannot connect to the repeater. If you do not use your wireless network

for a period of time, you can clear this check box and disable all wireless connectivity.

- **Fragmentation Length (256-2346):** Set the threshold of fragmentation length. If the length of a packet exceeds the set value, the packet is automatically fragmented into several packets. The value of **Fragmentation Length** cannot be too small because excessive packets reduce wireless network performance. The default value is 2346.
- **DTIM (1-255):** Set the interval for sending DTIM frames.
- **Beacon Interval (20-1000):** The beacon interval is the frequency of sending Beacon frames. Set the interval for sending Beacon frames. The unit is millisecond (ms). The default value is 100ms.
- **MAX Clients (0-12):** Set the maximum number of clients. 0 indicates the number of connected clients is not limited.
- **CTS/RTS Threshold (1-2347):** Set the CTS/RTS threshold. If the length of a packet is greater than the specified RTS value, the repeater sends an RTS frame to the destination station to negotiate. After receiving an RTS frame, the wireless station responds with a Clear to Send (CTS) frame to the repeater, notifying that they can communicate with each other.
- **Preamble Mode:** A preamble (especially the **802.11b High Rate/DSSS PHY** field; 56 digits synchronized field for short preamble) defines the length of the CRC correction block for communication between wireless devices. Short preamble should be applied in a network with intense traffics. It helps improve the efficiency of a wireless network responding to applications that have high requirement of real-time, such as streaming video and voice-over-IP telephony.
- **Guard Interval:**
 - Short GI: The interval is 400 ns. When short GI is enabled, the repeater can receive and send short-frame-interval packets. This helps improve the transmission rate of the repeater.
 - Long GI: The interval is 800 ns.
- **Transmit Power Control:** Set the transmit power of the wireless network. It is recommended to use the default setting of **100%**.
- **Router's PIN:** Display the PIN to be used for the wireless client when wireless settings of the router are configured through WPS.
- **Enable WPS:** Functions in the **WPS Setup** page are available only after the **Enable WPS** check box is selected. If the check box is not selected, the **WPS Setup** menu item is greyed out.
- **Disable Router's PIN:** The PIN mode function in the **WPS Setup** page is available only when the **Disable Router's PIN** check box is not selected. If the check box is selected, the PIN mode option is unavailable.

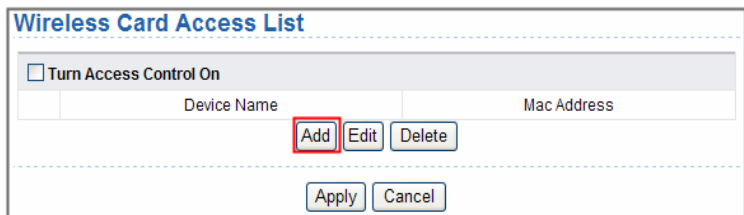
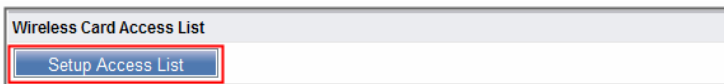
Restrict wireless access by MAC address

When a wireless card access list is configured and enabled, the router checks the MAC address of any wireless device attempting a connection and allows only connections to computers identified on the trusted computer list.

The MAC address is a network device's unique 12-character physical address, containing the hexadecimal characters 0–9, a–f, or A–F only. The MAC address is in the format of XX:XX:XX:XX:XX:XX.

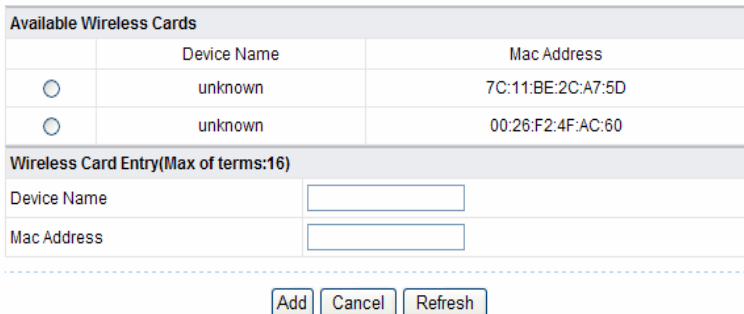
To restrict wireless access by MAC address:

- Step 1** Click **Setup Access List** button in the **Wireless Advanced Settings** page to display the **Wireless Card Access List** page.



- Step 2** Click **Add** to add a wireless device to the wireless access control list. The **Wireless Card Access Setup** page is displayed.

Wireless Card Access Setup



The screenshot shows the "Wireless Card Access Setup" page. At the top, there is a section titled "Available Wireless Cards" with a table containing two rows of data. Below the table is a section titled "Wireless Card Entry(Max of terms:16)" with two input fields for "Device Name" and "Mac Address". At the bottom of the page, there are three buttons: "Add", "Cancel", and "Refresh".

	Device Name	Mac Address
<input type="radio"/>	unknown	7C:11:BE:2C:A7:5D
<input type="radio"/>	unknown	00:26:F2:4F:AC:60

Wireless Card Entry(Max of terms:16)

Device Name

Mac Address

- Step 3** If the computer you want appears in the **Available Wireless Cards** list, you can select the radio button of that computer to obtain its MAC address. Otherwise, you can manually enter a name and MAC address of the computer to be

authorized. Generally, the MAC address is labeled on the bottom of the wireless device.

- Step 4** Click **Add** to add this wireless device to the wireless card access list. The page jumps to the list page.
- Step 5** Select **Turn Access Control On**. If selected, you can restrict PCs' access to the wireless network, only allowing specified PCs to access your network according to their MAC addresses.
- Step 6** Click **Apply** to save your Wireless Card Access List settings. Now, only devices on this list can wirelessly connect to the repeater.

7.5.4 WPS Setup

Choose **Wireless Settings > WPS Setup** to display the page below.

WPS Setup

New and easy way to connect to the Wireless Router via WiFi Protected setup (WPS)

A wireless client has to support WPS function in order to use this wizard to add the client to your WPS enabled Wireless Router. Please check the user manual and gift box of your wireless client to see whether it supports the WPS function. If your wireless client does not support the WPS function, you have to configure your wireless client manually so it has the same SSID and wireless security settings as on this router.

Next

WPS refers to Wi-Fi Protected Setup.

You can use WPS to establish wireless connection in a quick and secure way if the uplink AP or terminal (for example, the network adapter) has the WPS function. It is suggested to first configure wireless encryption for the uplink AP. If you change the wireless encryption mode after having establishing wireless connection using WPS, you must use WPS to establish wireless connection again. Note that if the wireless client does not support WPS you must manually configure the wireless client (such as SSID, security mode, and password) to make it have the same SSID and wireless security settings as the router.

Click Next to enter the **WPS Setup** page. The following describes how to configure WPS for the AP mode.

7.5.4.1 Using the WPS Button

In AP mode with WDS disabled, press the **WPS** button on the side panel of the device and the **WPS** button on the client device. The device can perform WPS encrypted connection to the downlink client device.

7.5.4.2 Using the Web Page

You can perform WPS settings using the Web page for configuration. Choose **Wireless Settings > WPS Setup** to display the **WPS Setup** page.

- Push Button

Step 1 Select **Push Button** and click **Start PBC**. WPS encrypted connection starts.

WPS Setup

As AP, Select a setup method:

Push Button (recommended)

You can either press the Push Button physically on the router or press the Button below (soft Push Button).

Start PBC

PIN (Personal Identification Number)

- Step 2** Press the **WPS** button on the network adapter or click the **PBC** button in the network adapter configuration tool within 2 minutes to start WPS connection. After WPS connection is established, the following page is displayed, indicating that the WPS connection is completed.

Success

The wireless client has been added to the network successfully.
Click OK to go back to the Wi-Fi Protected Setup page...

OK

- PIN mode

- Step 1** Select **PIN**, enter the PIN code of the network adapter (refer to the client of the network adapter), and click **Start PIN** to start WPS connection.

WPS Setup

As AP, Select a setup method:

Push Button (recommended)

PIN (Personal Identification Number)

If your Adapter supports WPS, please click on 'Generate a client Security Pin to input on the AP/Router/Gateway' and put the generated client PIN number here.

Enter Client's PIN:

Start PIN

- Step 2** Click the PIN button on the network adapter within 2 minutes to start WPS connection. After WPS connection is established, the following page is displayed, indicating that the WPS connection is completed.

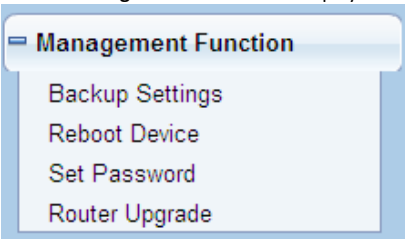
Success

The wireless client has been added to the network successfully.
Click OK to go back to the Wi-Fi Protected Setup page...

OK

7.6 Management Function

Click **Management Function** to display the extended navigation menu.



7.6.1 Backup Settings

Choose **Management Function > Backup Settings** and the **Backup Settings** page is displayed.

Backup Settings

Save a Copy of Current Settings	
	<input type="button" value="Backup"/>
Restore Saved Setting from a File	
<input type="text"/>	<input type="button" value="Browse..."/>
	<input type="button" value="Restore"/>
Revert to Factory Default Settings	
	<input type="button" value="Erase"/>

In this page, you can export configuration information of the router to the computer in the form of XML for later use, import a previously saved or a new configuration file, and restore the factory default settings of the router.

- Backup

Click **Backup** and save configuration information of the router as a local file.



Note:

Before saving your configuration file, change the administrator password to the default (admin) in case you forget your password. Then change it again after you have saved the configuration file. If you forget the password, you will need to reset the configuration to factory defaults.

- Restore

The Backup and Restore options in the **Backup Settings** page let you save and retrieve a file containing your router's configuration settings.

Click **Browse...** to select the configuration file restored in your computer and click **Restore** to load the file to the router.

- Erase

Under some circumstances (for example, if you move the router to a different network or if you have forgotten the password) you might want to erase the configuration and restore the factory default settings.

Click **Erase** to restore the factory default settings of the router. This operation has the same effect as pressing the **Reset** button on the side panel for 3-6 seconds.

7.6.2 Reboot Device

Choose **Management Function** > **Reboot Device** and the **Reboot Device** page is displayed.

Reboot Device

Reboot Device	
	<input type="button" value="Reboot"/>

Click **Reboot** to reboot the router. After the router is rebooted, the system jumps to the login page.

7.6.3 Set Password

Choose **Management Function** > **Set Password** and the **Set Password** page is displayed.

Set Password

Set Password	
Old Password	<input type="text"/>
Set Password	<input type="text"/>
Repeat New Password	<input type="text"/>
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

In this page, you can change the login password.



Note:

For security, it is strongly recommended to change the default password of the administrator. If you forget the password, you can restore the router to the default settings. The default password is admin.

7.6.4 Router Upgrade

Choose **Management Function** > **Router Upgrade** and the **Router Upgrade** page is displayed.

Router Upgrade

Locate and select the upgrade file from your hard disk:	
<input type="text"/>	<input type="button" value="Browse..."/> <input checked="" type="checkbox"/> Clear Config
<input type="button" value="Upload"/> <input type="button" value="Cancel"/>	

Follow the procedures below to upgrade the software of the router.

Step 1 Click **Browse...** to navigate to the latest software.

Step 2 Select the correct upgrade file. If you select **Clear Config**, the router restores to the default settings after upgrade is finished. If you do not select it, the current settings remain.

Step 3 Click **Upload** to start upgrade.

After the upgrade is completed, the router automatically reboots.



Note:

After the software upgrade, the device returns to the factory default settings. In case the previous configuration information is lost, please save settings before updating the software.

Do not power off the router during the upgrade.

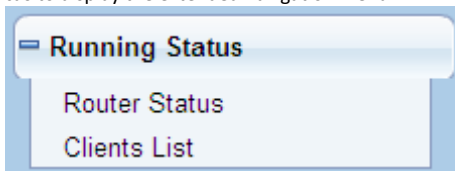
8 Web Configuration in Router Mode

Note:

Set the three-way switch on the side panel to **AP**, select **Router Mode** and restart the device. Log in to the configuration page after the device is restarted.

8.1 Running Status

Click **Running Status** to display the extended navigation menu.



8.1.1 Router Status

Choose **Running Status** > **Router Status** and the **Router Status** page is displayed.

Router Status

System Info	
Hardware Version	V1.0.0
Firmware Version	V1.0.0
Product Name	Wireless Router
Work Mode	Bridge Mode
Time and Date	1971-01-01 12:53:24
LAN Port	
MAC Address	00:1E:E3:4B:06:6D
IP Address	192.168.100.253
IP Subnet Mask	255.255.255.0
Wireless Port	
Wireless Network Name (SSID)	ITWORKS
Region	Europe
Wireless Channel	Auto
802.11 Mode	Mixed 802.11b/g/n
Wireless Radio	Enabled
Broadcast Name	ON
Wireless Isolation	OFF
Wi-Fi Protected Setup(WPS)	ON
Wireless Security Mode	None

In this page, you can view information about the current running status of the device, including system information, connection status of the Internet port, LAN port status, and wireless network status.

Click **Show Statistics** and the **Statistic Information** page as shown in the following figure is displayed:

Statistic Information

Port	Status	TxPkts	RxPkts	Collisions	Tx B/s	Rx B/s	Up Time
WAN	100M/Full	205	69	0	120402	6781	00:22:01
WLAN	Auto	6111	11483	0	3241546	1668284	00:21:55
System Up Time		00:22:10					
Poll Interval							
<input type="text" value="5"/> (1~86400 secs)		<input type="button" value="Set Interval"/>		<input type="button" value="Stop"/>			

In this page, you can view performance statistics information of the device, including the numbers of sent and received packets at each port.

- **Set Interval:** Set the interval for traffic statistics.
- **Stop:** If you click this button, this page always displays statistics information that was refreshed for the last time and it is not refreshed any more.

Click **Connection Status** in the **Router Status** page, and the **Connection Status** page is displayed. This page displays current connection information of the device.

The following takes WAN connection of **DHCP** as an example.

Connection Status

IP Address	0.0.0.0
Subnet Mask	0.0.0.0
Default Gateway	0.0.0.0
DHCP Server	0.0.0.0
DNS Server	0.0.0.0
Lease Obtained	0Day,0Hour,0Minute
Lease Expires	0Day,0Hour,0Minute

- **Release:** Click the button and the device sends a request to the ISP for releasing the IP address, the subnet mask, the default gateway, and DNS server settings.
- **Renew:** Click the button and the device dynamically obtains an IP address, a subnet mask, the default gateway, and DNS server settings from the ISP. The information will be displayed in this page.

For details of WAN connection modes, refer to section **8.4.2 WAN Interface Settings**.

8.1.2 Clients List

Choose **Running Status > Clients List** and the **Clients List** page is displayed.

Clients List

Wireless Devices(Wireless intruders also show up here)

#	IP Address	MAC Address	Device Name
1	192.168.100.2	00:1F:A4:91:F2:0E	gj2217d

Refresh

This page displays information of computers connected to the device, including the IP address and MAC address of each computer.

8.2 Setup Wizard

For settings, refer to section **6.2 Router Mode Configuration**.

8.3 Mode Setting

Click **Mode Settings** and the **Mode Settings** page is displayed.

Mode Settings

Please choose your mode as follows:

Bridge Mode

Router Mode

In this mode, the port is used as a wan port.

You can only login web by using your wireless network card to connect this network.

Please remember SSID and Security Options of your wireless network before you change to this mode.

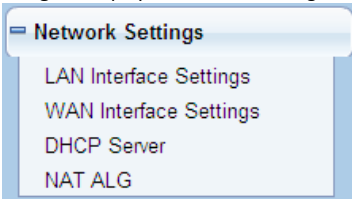
View Wireless Basic Config

Apply Cancel

- **Bridge Mode:** The interface is an LAN interface. Users can connect the device and PC by an RJ45 cable or a wireless network card.
- **Router Mode:** Computers can connect to the device in a wireless way only.

8.4 Network Settings

Click **Wired Network Settings** to display the extended navigation menu.



8.4.1 LAN Interface Settings

For details, refer to **7.4.1 LAN Interface Settings**.

8.4.2 WAN Interface Settings

Choose **Network Settings > WAN Interface Settings** and the **WAN Interface Settings** page is displayed.

The router supports 5 modes of WAN connection, including **Dynamic IP (DHCP)**, **Static IP**, **PPPoE**, **PPTP**, and **L2TP**. Select the WAN connection you use. Contact your ISP if you do not know your WAN connection mode.

(1) Dynamic IP (DHCP)

If dynamic IP (DHCP) is selected, the device automatically obtains the IP address from the ISP automatically. Select DHCP when the ISP does not provide any IP network parameters. See figure below:

WAN Interface Settings

Does your Internet Connection Require A Login?	<input type="radio"/> Yes <input checked="" type="radio"/> No
Account Name (If Required)	<input type="text"/>
Internet IP Address	
<input checked="" type="radio"/> Get Dynamically From ISP	
<input type="radio"/> Use Static IP Address	
IP Address	<input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/>
IP Subnet Mask	<input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/>
Gateway IP Address	<input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/>
Domain Name Server (DNS) Address	
<input checked="" type="radio"/> Get Automatically From ISP	
<input type="radio"/> Use These DNS Servers	
Primary DNS	<input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/>
Secondary DNS	<input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/>
MTU Setting	
MTU Size(616~1500 bytes)	<input type="text" value="1500"/>
Router MAC Address	
<input checked="" type="radio"/> Use Default Address	
<input type="radio"/> Use Computer MAC Address	
<input type="radio"/> Use This MAC Address	<input type="text" value="00:1E:E3:4B:06:6D"/>

- **Account Name:** The account name is provided by your ISP. If the ISP does not provide it, you can leave the item blank.
- **Domain Name Service (DNS) Address:** Select **Use These DNS Servers** if you know that your ISP does not automatically transmit DNS addresses to the router during

login. And enter the IP address of your ISP's primary DNS server. Enter a secondary DNS server address if available.

- **MTU Size:** Set the maximum transmission unit. The default value is recommended.
- **Router MAC Address:** Physical address of the router.
 - Generally, select **Use Default Address**.
 - If the ISP requires MAC address authentication, Select **Use Computer MAC Address** or **Use This MAC Address**. If you select **Use Computer MAC Address**, the MAC address of the current computer serves as the MAC address of the router. If you select **Use This MAC Address**, you need to enter the MAC address of another computer. The format of an MAC address is XX:XX:XX:XX:XX:XX.

After finishing settings, click **Apply** to save the settings.

(2) Static IP

If the ISP provides the IP address, subnet mask and information about the gateway and DNS server, select Static IP. Contact your ISP if you do not know the information.

WAN Interface Settings

Does your Internet Connection Require A Login?	<input type="radio"/> Yes <input checked="" type="radio"/> No
Account Name (If Required)	<input type="text"/>
Internet IP Address	
<input type="radio"/> Get Dynamically From ISP	
<input checked="" type="radio"/> Use Static IP Address	
IP Address	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>
IP Subnet Mask	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>
Gateway IP Address	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>
Domain Name Server (DNS) Address	
<input type="radio"/> Get Automatically From ISP	
<input checked="" type="radio"/> Use These DNS Servers	
Primary DNS	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>
Secondary DNS	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>
MTU Setting	
MTU Size(616~1500 bytes)	<input type="text" value="1500"/>
Router MAC Address	
<input checked="" type="radio"/> Use Default Address	
<input type="radio"/> Use Computer MAC Address	
<input type="radio"/> Use This MAC Address	<input type="text" value="00:1E:E3:4B:06:6D"/>

- **Account Name:** The account name is provided by your ISP. If the ISP does not provide it, you can leave the item blank.
- **IP Address:** Enter the WAN IP address provided by the ISP. The parameter must be entered.
- **IP Subnet Mask:** Enter the WAN subnet mask provided by the ISP. It varies with the network type. It is usually 255.255.255.0 (Class C).
- **Gateway IP Address:** Enter the IP address of the gateway provided by the ISP. It is the IP address used for connecting to the ISP.
- **Primary DNS:** Enter the IP address of the primary DNS server if necessary.
- **Secondary DNS:** Enter the IP address of that DNS server if the ISP provides another DNS server.
- **MTU Size:** Set the maximum transmission unit. The default value is recommended.
- **Router MAC Address:** See descriptions on setting **Router MAC Address** for DHCP.

After finishing, click **Apply** to save the settings.

(3) **PPPoE**

If the ISP provides the user name and password for PPPoE (Point-to-Point Protocol over Ethernet) dialup, click **Yes** and select **PPPoE**.

WAN Interface Settings

Does your Internet Connection Require A Login?	<input checked="" type="radio"/> Yes <input type="radio"/> No
Internet Service Provider	PPPoE ▾
Login	<input type="text"/>
Password	<input type="text"/>
Service Name (If Required)	<input type="text"/>
Connection Mode	Always On ▾
Idle Timeout (In minutes)	<input type="text" value="5"/>
Domain Name Server (DNS) Address	
<input checked="" type="radio"/> Get Automatically From ISP	
<input type="radio"/> Use These DNS Servers	
Primary DNS	<input type="text"/> . <input type="text"/> <input type="text"/> <input type="text"/>
Secondary DNS	<input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/>
MTU Setting	
MTU Size(616~1492 bytes)	<input type="text" value="1492"/>
Router MAC Address	
<input checked="" type="radio"/> Use Default Address	
<input type="radio"/> Use Computer MAC Address	
<input type="radio"/> Use This MAC Address	<input type="text" value="00:1E:E3:4B:06:6D"/>

- **Login:** Enter the user name for PPPoE dialup provided by the ISP.
- **Password:** Enter the password for PPPoE dialup provided by the ISP.
- **Service Name:** If several PPPoE servers are available, specify one in this field.
- **Connection Mode:**
 - **Always On:** If you select it, the system automatically establishes a connection. If the device is disconnected from the network because of external factors when you are using the Internet access service, the system attempts connection in an interval of the specified time (for example, 10 seconds) until the connection is established. If you pay for Internet access monthly, we recommend you to use this connection mode.
 - **Dial on Demand:** If you select it, the system automatically establishes a connection when a network access request from the LAN is received. If no network access request is sent from the LAN within the specified time of **Idle Timeout**, the system automatically interrupts the connection. If you pay for

Internet access by time, you are recommended to use this connection mode, which effectively saves the expense of Internet access.

- **Manually Connect:** If you select it, you need to manually set dialup connection after startup.
 - **Idle Timeout:** If the system does not detect any Internet access behavior within the specified time of **Idle Timeout**, the system interrupts the Internet connection.
 - **Domain Name Server (DNS) Address:** Select **Use These DNS Servers** if you know that your ISP does not automatically transmit DNS addresses to the router during login. And enter the IP address of your ISP's primary DNS server. Enter a secondary DNS server address if available.
 - **MTU Size:** Set the maximum transmission unit. The default value is recommended.
 - **Router MAC Address:** See descriptions on setting **Router MAC Address** for DHCP.
- After finishing, click **Apply** to save the settings.

(4) PPTP

If the ISP provides the user name and password for PPTP dialup, select **PPTP**.

WAN Interface Settings

Does your Internet Connection Require A Login?	<input checked="" type="radio"/> Yes <input type="radio"/> No
Internet Service Provider	PPTP ▾
Login	<input type="text"/>
Password	<input type="text"/>
Connection Mode	Always On ▾
Idle Timeout (In minutes)	<input type="text" value="5"/>
My IP Address	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>
Subnet Mask	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>
Server Address	<input type="text"/>
Gateway IP Address	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>
Domain Name Server (DNS) Address	
<input checked="" type="radio"/> Get Automatically From ISP	
<input type="radio"/> Use These DNS Servers	
Primary DNS	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>
Secondary DNS	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>
MTU Setting	
MTU Size(616~1450 bytes)	<input type="text" value="1450"/>
Router MAC Address	
<input checked="" type="radio"/> Use Default Address	
<input type="radio"/> Use Computer MAC Address	
<input type="radio"/> Use This MAC Address	<input type="text" value="00:1E:E3:4B:06:6D"/>

- **Login:** Enter the user name for PPTP dialup provided by the ISP.
- **Password:** Enter the password for PPTP dialup provided by the ISP.
- **Connection Mode:**
 - **Always On:** If you select it, the system automatically establishes a connection. If the device is disconnected from the network because of external factors when you are using the Internet access service, the system attempts connection in an interval of the specified time (for example, 10 seconds) until the connection is established. If you pay for Internet access monthly, we recommend you to use this connection mode.
 - **Dial on Demand:** If you select it, the system automatically establishes a connection when a network access request from the LAN is received. If no network access request is sent from the LAN within the specified time of **Idle**

Timeout, the system automatically interrupts the connection. If you pay for Internet access by time, you are recommended to use this connection mode, which effectively saves the expense of Internet access.

- **Manually Connect:** If you select it, you need to manually set dialup connection after startup.
 - **Idle Timeout:** If the system does not detect any Internet access behavior within the specified time of **Idle Timeout**, the system interrupts the Internet connection.
 - **My IP Address:** Enter your IP address. You can also leave this field blank.
 - **Subnet Mask:** Enter the subnet mask. You can also leave this field blank.
 - **Sever Address:** Enter the IP address of the server. You can also leave this field blank.
 - **Gateway IP Address:** Enter the IP address of the gateway. You can also leave this field blank.
 - **Domain Name Server (DNS) Address:** Select **Use These DNS Servers** if you know that your ISP does not automatically transmit DNS addresses to the router during login. And enter the IP address of your ISP's primary DNS server. Enter a secondary DNS server address if available.
 - **MTU Size:** Set the maximum transmission unit. The default value is recommended.
 - **Router MAC Address:** See descriptions on setting **Router MAC Address** for DHCP.
- After finishing settings, click **Apply** to save the settings.

(5) L2TP

If the ISP provides the user name and password for L2TP dialup, select **L2TP**.

WAN Interface Settings

Does your Internet Connection Require A Login?	<input checked="" type="radio"/> Yes <input type="radio"/> No
Internet Service Provider	L2TP ▾
Login	<input type="text"/>
Password	<input type="text"/>
Connection Mode	Always On ▾
Idle Timeout (In minutes)	<input type="text" value="5"/>
My IP Address	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>
Subnet Mask	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>
Server Address	<input type="text"/>
Gateway IP Address	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>
Domain Name Server (DNS) Address	
<input checked="" type="radio"/> Get Automatically From ISP	
<input type="radio"/> Use These DNS Servers	
Primary DNS	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>
Secondary DNS	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>
MTU Setting	
MTU Size(616~1450 bytes)	<input type="text" value="1450"/>
Router MAC Address	
<input checked="" type="radio"/> Use Default Address	
<input type="radio"/> Use Computer MAC Address	
<input type="radio"/> Use This MAC Address	<input type="text" value="00:1E:E3:4B:06:6D"/>

For details of parameter settings for this page, refer to previous parameter descriptions for **PPTP**.

8.4.3 DHCP Server

Choose **Network Settings** > **DHCP Server** and the **DHCP Server** page is displayed. DHCP refers to Dynamic Host Configuration Protocol. If **Use Device as DHCP Service** is selected, the device will automatically assign IP addresses to computers in the LAN. Users do not need to configure TCP/IP protocol parameters such as the IP address, the subnet mask, the gateway, and the DNS server information for computers connected to the router's LAN.

DHCP Server

<input checked="" type="checkbox"/> Use Router as DHCP Server					
Starting IP Address		192	168	100	2
Ending IP Address		192	168	100	200
DHCP Lease Time(1 - 160 hours)		24			
Address Reservation					
#	IP Address	Device Name		MAC Address	
		Add	Edit	Delete	
		Apply	Cancel		

8.4.3.1 Using the Router as a DHCP Server

- **Use Router as DHCP Server:** If the **Use Router as DHCP Server** check box is selected, the device serves as a DHCP server to automatically assign IP addresses to computers connected to it.
- **Starting IP Address/Ending IP Address:** Set the starting and ending IP addresses to specify a pool of IP addresses to be assigned by the DHCP server. After you set **Starting IP Address/Ending IP Address**, hosts in the LAN obtain IP addresses that are in the range of the starting and ending IP addresses.
- **DHCP Lease Time:** The valid time for an IP address that is automatically assigned by the DHCP server to a host. The DHCP server does not assign the IP address to other hosts within the specified time.

8.4.3.2 Using Address Reservation

When you specify a reserved IP address for a computer in the LAN, the computer always receives the same IP address each time it accesses the router's DHCP server. Reserved IP addresses should be assigned to computers or servers that require permanent IP settings.

Address Reservation				
#	IP Address	Device Name	MAC Address	
		Add	Edit	Delete

To reserve an IP address:

Step 1 Click **Add** to enter the **Address Reservation** page.

Address Reservation

Address Reservation Table				
	#	IP Address	Device Name	MAC Address
<input type="radio"/>	1			
<input type="radio"/>	2	192.168.100.2	Z2oyMJE3ZA==	00:1F:A4:91:F2:0E
IP Address		<input type="text"/>	<input type="text"/>	<input type="text"/>
MAC Address		<input type="text"/>		
Device Name		<input type="text"/>		
		Add	Cancel	Refresh

- Step 2** Select one item from **Address Reservation Table**, or enter the IP address in the **IP Address** field to assign to the computer or server (Choose an IP address from the IP address pool that you have specified, for example 192.168.100.x). Enter the MAC address and device name of the computer or server.
- Step 3** Click **Add** to add a new item into **Address Reservation**.
- Step 4** Click **Apply** to save the settings.

8.4.4 NAT ALG

Choose **Network Settings** > **NAT ALG** and the **NAT ALG** page is displayed.

NAT ALG

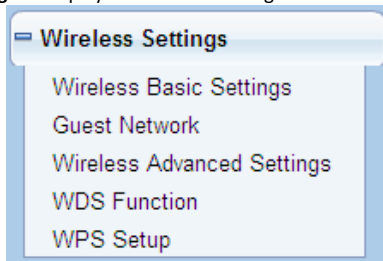
<input checked="" type="checkbox"/> Disable SIP ALG
<input type="checkbox"/> Disable IPSEC Pass-Through
<input type="checkbox"/> Disable L2TP Pass-Through
<input type="checkbox"/> Disable PPTP Pass-Through

- **Disable SIP ALG:** Certain SIP applications have special mechanisms for passing through the NAT firewall and SIP ALG may have conflicts with these mechanisms. In most cases, please disable SIP ALG.
- **Disable IPSEC/L2TP/PPTP Pass-Through:** IPSEC/PPTP/L2TP Pass-Through provides a secure communication method for remote computers in the wide area network (WAN) (for example, the Internet). Enable the corresponding VPN pass-through function if an intra-network host needs to use a VPN protocol (such as the PPTP, L2TP, IPSEC) to connect to a remote VPN network through the router.

After finishing settings, click **Apply** to save the settings.

8.5 Wireless Settings

Click **Wireless Settings** to display the extended navigation menu.



8.5.1 Wireless Basic Settings

For details, refer to **7.5.1 Wireless Basic Settings**.

8.5.2 Guest Network

If you do not want visitors to know your wireless security key, you can use the guest network to allow them to use your Internet without knowing your wireless connection password.

Choose **Wireless Settings > Guest Network** and the **Guest Network** page is displayed.

Guest Network

Network Profiles					
	Scheme	SSID	Security	Apply	SSID Broadcast
<input checked="" type="radio"/>	1	ITWORKS-002	None	NO	YES
<input type="radio"/>	2	ITWORKS-003	None	NO	YES
<input type="radio"/>	3	ITWORKS-004	None	NO	YES
<input type="radio"/>	4	ITWORKS-005	None	NO	YES

Wireless Settings--Profile 1

Enable Guest Network

Enable SSID Broadcast

Allow Guest to access My Local Network

Enable Wireless Isolation

Guest Wireless Network Name(SSID):

Security Options--Profile 1

Security Options:

- **Network Profiles:** Brief description of the created guest network. You can create up to four guest networks. A network profile contains the SSID and encryption mode, whether to use the guest network, and whether to broadcast SSID. You can click the radio button of a profile to view detailed information or modify settings.
- **Enable Guest Network:** If enabled, both you and visitors can connect to the network by using the SSID of the guest network.
- **Enable SSID Broadcast:** If enabled, the device broadcasts its SSID to all wireless stations.
- **Allow Guest to access My Local Network:** If enabled, visitors using the SSID of a guest network can access not only the Internet but also the LAN of the device, like users using the primary SSID of the network. If disabled, visitors using the SSID of a guest network cannot access the LAN of the device.
- **Enable Wireless Isolation:** If selected, wireless clients connected to the guest network of the same SSID can access the Internet only, but cannot communicate with each other.
- **Guest Wireless Network Name (SSID):** Set the name of the guest network.
- **Security Options:** Refer to security option descriptions in section **8.5.1 Wireless Basic Settings**.

After finishing, click **Apply** to save the settings.

8.5.3 Wireless Advanced Settings

For details, refer to section 7.5.3 **Wireless Advanced Settings**.

8.5.4 WDS Function

Wireless distribution system (WDS) enables interconnection between APs in an IEEE 802.11 wireless network. It extends the wireless network through several APs, without connection of the wired backbone network. If you want to use WDS to achieve wireless repeating or bridging, enable WDS.

Choose **Wireless Settings > WDS Function** and the **WDS Function** page is displayed.

WDS Function

<input type="checkbox"/> Enable WDS Function	
<input type="checkbox"/> Disable Wireless Clients Association	
Wireless MAC of this router: 00:1E:E3:4B:06:6C	
Wireless Basic Station	
Repeater MAC Address 1:	<input type="text"/>
Repeater MAC Address 2:	<input type="text"/>
Repeater MAC Address 3:	<input type="text"/>
Repeater MAC Address 4:	<input type="text"/>

- **Enable WDS Function:** Enable the WDS function if you want to use this function. Note that the WDS function cannot be enabled if the channel is set to **Auto**.
- **Enable Wireless Clients Association:** If not selected, the wireless basic station does not transmit any signals to clients that are directly connected to it.
- **Central Base Station:** In this mode, the router serves as a basic station to communicate with repeaters. The basic station forwards the data of communication between repeaters to the destination repeaters. Repeaters should be configured accordingly. Note that a wireless basic station can be configured with up to four repeaters.
- **Repeater MAC Address 1/2/3/4:** Enter the MAC address of the repeater.

After finishing settings, click **Apply** to save the settings.

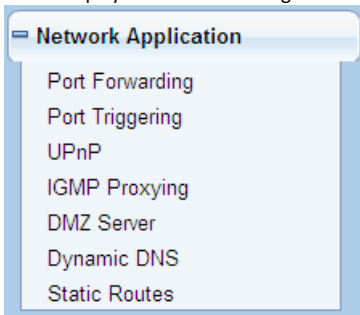
For WDS application description, refer to 6.4.3 **WDS Application**.

8.5.5 WPS Setup

For details, refer to **7.5.4 WPS Setup**.

8.6 Network Application

Click **Network Application** to display the extended navigation menu.



8.6.1 Port Forwarding

By default, the firewall function of the router hides your LAN. As a result, other users on the Internet can detect only the router, but cannot access a certain PC in the LAN directly. If you want to access a PC in a LAN, you need to configure port forwarding for the router and map the desired port to the corresponding PC in the LAN. The router forwards packets to the PC according to the port mapping rule after receiving an access request from the Internet. In this way, communication is successfully established between the Internet and the PC in the LAN.

Choose **Network Application > Port Forwarding** and the **Port Forwarding** page is displayed.

Port Forwarding

Service Name
FTP

Service IP Address
192 . 168 . 100 . Add

Service List
Max of rules: 32

#	Server Name	Start Port	End Port	Server IP Address
---	-------------	------------	----------	-------------------

Edit Service Delete Service

Add Custom Service

- **Service Name:** Select a service type.
- **Service IP Address:** Enter the IP address of the computer that provides services.

Click the **Add Custom Service** button and the **Ports - Custom Service** page is displayed:

Ports - Custom Service

Service Name:	<input type="text"/>
Protocol :	TCP <input type="button" value="v"/>
Starting Port	<input type="text"/> (1~65535)
Ending Port	<input type="text"/> (1~65535)
Server IP Address	<input type="text" value="192"/> . <input type="text" value="168"/> . <input type="text" value="100"/> . <input type="text"/>

- **Service Name:** Select a service type.
- **Protocol:** The protocol used at the mapping port. You can select **TCP/UDP**, **TCP**, or **UDP**. It is recommended to use **TCP/UDP** if you do not know which protocol should be used.
- **Starting Port:** After the connection to the mapping port is established, the corresponding port is open and the application can initiate subsequent connection requests to the open port.
- **Ending Port:** Set the end port of the mapping port range.
- **Service IP Address:** Enter the IP address of the computer that provides services.

After finishing, click **Apply** to save the settings.

8.6.2 Port Triggering

Certain applications, such as WAN network games, video conferences, and network calls, require multiple connections. Because of the firewall setting, these applications cannot work on a simple NAT router. However, certain special applications enable the applications to work on a NAT router. When an application sends a connection request to a trigger port, the corresponding ports are open for later connection and service provision.

Choose **Network Application > Port Triggering** and the **Port Triggering** page is displayed.

Port Triggering

Enable Port Triggering

Port Triggering Timeout(in minutes) (1-9999)

Max of rules: 32

#	Server Name	Service Type	Required Inbound Connection	Service User
<input type="button" value="Add Service"/> <input type="button" value="Edit Service"/> <input type="button" value="Delete Service"/>				

- **Enable Port Triggering:** If Enable Port Triggering box is not checked, the function will be disabled.

- **Port Triggering Timeout:** The timeout value controls the inactive timer at the specified ingress port. Upon timeout of the inactive timer, the ingress port is disabled.

Click the **Add Service** button and the **Port Triggering – Services** page is displayed:

Port Triggering - Services

Service Name	<input type="text"/>
Service User	Any <input type="button" value="v"/>
	<input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/>
Service Type	TCP <input type="button" value="v"/>
Triggering Starting Port	<input type="text"/> (1~65535)
Triggering Ending Port	<input type="text"/> (1~65535)
Required Inbound Connection	
Connection Type	TCP <input type="button" value="v"/>
Starting Port	<input type="text"/> (1~65535)
Ending Port	<input type="text"/> (1~65535)

- **Service Name:** Enter a service name.
- **Service User:**
 - **Any:** Allow everybody in the user network to use the service.
 - **Single address:** Enter the IP address of the network adapter on the PC. Then, the service is applied only on the specific network adapter of the PC.
- **Service Type:** The protocol used at the triggering port. You can select **TCP/UDP**, **TCP**, or **UDP**.
- **Triggering Starting Port:** The first port to which an application sends a connection request. All relevant ports can be open only after connection is established at this starting port. Otherwise, other relevant ports are not open.
- **Triggering Ending Port:** Set the end port of the triggering port range.
- **Starting Port:** The starting port of the port range.
- **Ending Port:** The ending port of the port range.

After finishing, click **Apply** to add a port triggering rule.

8.6.3 UPnP

By using the Universal Plug and Play (UPnP) protocol, a host in the LAN can ask the router to perform specific port conversion, to enable an external host to access resources on the internal host when necessary. For example, if MSN Messenger is installed on Windows ME and Windows XP operating systems, UPnP can be used for audio and video conversations. In this way, functions restricted by NAT can work properly.

Choose **Network Application > UPnP** and the **UPnP** page is displayed.

UPnP

Turn UPnP On

Advertisement Period(in minutes)

Advertisement Time To Live(in hops)

UPnP Portable Table

Active	Protocol	Int. Port	Ext. Port	IP Address	Description
--------	----------	-----------	-----------	------------	-------------

- **Turn UPnP On:** If selected, UPnP is enabled.
- **Advertisement Period (in minutes):** Set the broadcast interval. It indicates the interval for the router broadcasting its UPnP information. The value should be in the range of 1 to 1440 minutes and the default is 30 minutes.
- **Advertisement Time to Live (in hops):** The time for the broadcast to live. It is the number of hops after each UPnP packet is sent. The number of hops is the times that each packet can be broadcast before it vanishes. The value is in the range of 1 to 255 hops and the default is 4 hops.
- **UPnP Portable Table:** This table shows the IP addresses of UPnP devices that are connected to the router and open (internal and external) ports on the devices. It also lists the types and status of the open ports.



Note:

Only applications that support UPnP can use the UPnP function.

The functionality of UPnP requires support by the application and operating systems such as Windows ME, Windows XP, and Windows Vista.

8.6.4 IGMP Proxying

Click **Network Application > IGMP Proxying** and the **IGMP Proxying** page is displayed.

IGMP Proxying

Disable IGMP Proxying

Apply

Cancel

- **Enable IGMP proxying:** IGMP proxying enables a PC in the LAN to receive desired multicast traffic from the Internet. Disable IGMP proxying if you do not need this function.

After finishing, click **Apply** to apply the setting.

8.6.5 DMZ Server

DMZ (Demilitarized Zone), a special network zone that is different from the external network or the internal network. Servers that are allowed to access the external network, such as Web and e-mail, connect to the DMZ. The internal network is protected behind the Trust Zone interface, and is not allowed any user to access. Therefore, the internal and external networks are separated, which can meet user's secrecy demand. Usually, there are some public servers in DMZ, such as Web, Mail, and FTP. Users from the external network can access services in DMZ, but they cannot obtain the company's secret information or personal information that is stored on the internal network. Even though servers in the DMZ are damaged, it does not lead to secret information loss on the internal network.

Choose **Network Application > DMZ Server** and the **DMZ Server** page is displayed.

DMZ Server

Default DMZ Server

192

168

100

Apply

Cancel

- **Default DMZ Server:** Enter the IP address of a PC that serves as the DMZ server.



Note:

When PC on the internal network is set to be the DMZ host, all interfaces of the PC will be exposed to the Internet and the PC will risk great security. Unless necessary, please do not set the DMZ casually.

After the DMZ host is set, mappings of all the interfaces will point to the DMZ host and the port mappings that point to other hosts will be invalid.

8.6.6 Dynamic DNS

Dynamic domain name resolution (DDNS) is mainly used to achieve resolution between fixed domain names and dynamic IP addresses. For a user that uses a dynamic IP address, after the user obtains a new IP address in the Internet access, the dynamic domain name software installed in the host sends the IP address to the DDNS server provided by the DDNS service provider and updates the domain name resolution database. When another user on the Internet tries accessing the domain name, the dynamic domain name resolution server returns the correct IP address.

Choose **Network Application > Dynamic DNS** and the **Dynamic DNS** page is displayed.

Dynamic DNS

<input type="checkbox"/> Use a Dynamic DNS Service	
Service Provider	<input type="text" value="dyndns.org"/>
Host Name	<input type="text" value="myhostname"/>
User Name	<input type="text" value="User"/>
Password	<input type="password" value="••••••••"/>

- **Use a Dynamic DNS Service:** If you have registered with a DDNS service provider, select **Use a Dynamic DNS Service**.
- **Service Provider:** Select your DDNS service provider.
- **Host Name:** Enter the host name or domain name provided by your DDNS service provider.
- **User Name:** Enter the name of your DDNS account.
- **Password:** Enter the password of the DDNS account.

After finishing, click **Apply** to apply the settings.

8.6.7 Static Routes

Static routing is a special type of routing that can be applied in a network to reduce the problem of routing selection and data flow overload caused by routing selection so as to improve the packets forwarding speed. You can set the destination IP address, subnet mask, and gateway to specify a routing rule. The destination IP address and subnet mask determine a destination network or host to which the router sends packets through the gateway.

Choose **Network Application > Static Routes** and the **Static Routes** page is displayed.

Static Routes

Max of rules: 32

#	Active	Name	Destination	Gateway
---	--------	------	-------------	---------

Click **Add** to add a static routing rule.

Static Routes

Active	<input type="checkbox"/>
Route Name	<input type="text"/>
Destination IP Address	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>
IP Subnet Mask	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>
Gateway IP Address	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>
Metric	<input type="text"/>

- **Active:** The static routing rule can take effect only if the **Active** check box is selected.
- **Route Name:** Enter the name of the static route.
- **Destination IP Address:** The destination address or network that you want to access. This IP address cannot be in the same network segment as the IP address of the WAN or LAN interface of the device.
- **IP Subnet Mask:** This IP subnet mask together with the destination IP address identify the target network.
- **Gateway IP Address:** The IP address of the next node to which packets are sent. The gateway IP address must be in the same network segment as the IP address of the WAN or LAN interface of the device.
- **Metric:** The number of other routers in the user network. The value ranges from 2 to 15. Usually, the value of 2 or 3 leads to the best performance. If the route is direct connection, set **Metric** to 2.

After finishing settings, click **Apply** to save the settings.

8.7 Security Options

Click **Security Options** to display the extended navigation menu.

Security Options

Block Sites

Block Services

Protection

8.7.1 Block Sites

The repeater allows users to restrict access based on WEB addresses and WEB address keywords. When a user tries accessing a restricted website, a message is displayed, indicating that the firewall restricts access to the website.

Choose **Security Options** > **Block Sites** and the **Block Sites** page is displayed.

Block Sites

Keyword Blocking

Never

Per Schedule

Always

Type Keyword or Domain Name Here.

Add Keyword

Block Sites Containing these Keywords or Domain Names(Max of terms: 32) :

Delete Keyword

Clear List

Allow Trusted IP Address To Visit Blocked Sites

Trusted IP Address

Apply

Cancel

Follow the procedures below to block access to Internet sites.

Step 1 Select **Per Schedule** or **Always** to enable keyword blocking.

To block by schedule, be sure to specify a time period in the **Schedule** page. For more information about scheduling, refer to section **8.8.3 Schedules**.

Step 2 Enter keywords or domain names that you want to block in the keyword field and click **Add Keyword**. The keyword or domain name then appears in the **Block Sites Containing these Keywords or Domain Names** list.

Keyword application examples:

- If the keyword **XXX** is specified, the URL **www.aabccc.com/xxx.html** is blocked.
- If the keyword **.com** is specified, only websites with other domain suffixes (such as **.edu**, **.org**, or **.gov**) can be accessed.

Step 3 You can specify one trusted user, which is a computer that has no restriction in network access. To specify a trusted user, enter the computer's IP address in the **Trusted IP Address** field and select the **Allow Trusted IP Address to Visit Blocked Sites** check box.

Since the trusted user is identified by IP address, you should configure that computer with a fixed IP address.

Step 4 Click **Apply** to save the settings.

8.7.2 Block Services

The repeater allows users to block the use of certain Internet services by computers on your network.

Choose **Security Options > Block Services** and the **Block Services** page is displayed.

Block Services

Services Blocking

Never

Block List Per Schedule

Block List Always

Block Service Rules Table - Black List

Max of rules: 32

#	Service Name	Port	IP
<input type="button" value="Add"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>			

Block Service Rules Table - White List

Max of rules: 32

#	Service Name	Port	IP
<input type="button" value="Add"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>			

Follow the procedures below to specify a service for blocking.

Step 1 Select **Per Schedule** or **Always** to enable keyword blocking.

To block by schedule, be sure to specify a time period in the **Schedule** page. For more information about scheduling, refer to section **8.8.3 Schedules**.

- **Black List:** Indicates to prevent service that complies with the rule in the **Block Service Rules Table-Black List** area from being used.
- **White List:** Indicates to allow only service that complies with the rule in the **Block Service Rules Table-White List** area to be available for use.

Step 2 Click **Add** to specify a service for blocking. The **Block Services Setup** page is displayed:

Block Services Setup

Service Type	User Defined
Protocol	TCP
Starting Port	(1-65535)
Ending Port	(1-65535)
Service Type/User Defined	
Filter Service For:	
<input type="radio"/> Only This IP Address:	192 . 168 . 1 .
<input type="radio"/> IP Address Range:	192 . 168 . 1 .
	to 192 . 168 . 1 .
<input checked="" type="radio"/> All IP Address:	

Step 3 Set the parameters in this page.

- **Service Type:** Select a service type. If your desired type is not in the list, select **User defined**. Then, you need to select the protocol, enter the service name, and specify the port range. For services that exist in the drop-down list, the corresponding information is already preset.
- **Protocol:** Set the protocol used at service ports. If you are not sure about the protocol that the application uses, select **TCP/UDP**.
- **Starting Port/Ending Port:** The starting and ending ports of the port range where the specified service is blocked. If the application uses a single port number, enter the number in both fields.
- **Service Type/User Defined:** Enter the service name.
- **Filter Service For:** You can block the specified service for a single computer, computers within an IP address range, or all computers.

After finishing, click **Add** to add a new rule. Then, click **Apply** to save the settings.

8.7.3 Protection

Choose **Security Options > Protection** and the **Protection** page is displayed.

Protection

Disable Port Scan and DOS Protection

Respond to Ping on Internet Port

NAT Filtering

Secured

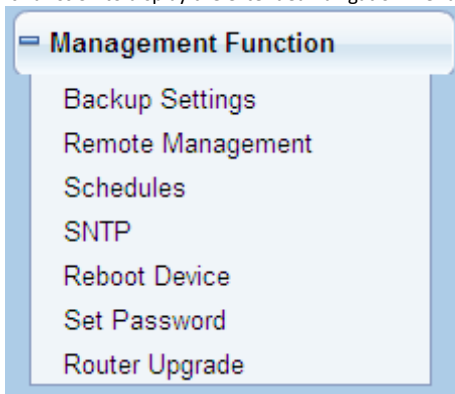
Apply Cancel

- **Disable port scan and DoS protection:** Denial of service (DoS) protection protects your LAN against DOS attacks. Generally, please enable the port scanning and DOS protection function.
- **Respond to Ping on Internet Port:** If enabled, the router responds to ping commands from the Internet. However, like the DMZ server, enabling this function can bring about security risks. Generally, please disable this function.
- **NAT Filtering:** NAT filtering determines the way that the router deals with incoming traffic.
 - **Secured:** This option provides a secured firewall to protect PCs on LAN from attacks from the Internet, but it may not allow some Internet games, point-to-point applications, or multimedia applications to work.
 - **Open:** This option provides a less secure firewall that allows almost all Internet applications to work.

After finishing, click **Apply** to apply the settings.

8.8 Management Function

Click **Management Function** to display the extended navigation menu.



8.8.1 Backup Settings

For details, refer to section 7.6.1 Backup Settings.

8.8.2 Remote Management

The remote management function allows you to configure the router from the WAN through the Web browser. In this way, you can manage the router on a remote host.

Choose **Management Function > Remote Management** and the **Remote Management** page is displayed.

Remote Management

<input type="checkbox"/> Turn Remote Management On	
Remote Management Address :	http://0.0.0.0:8080
Port Number :	8080
Allow Remote Access By :	
<input type="radio"/> Only This Computer :	<input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/>
<input type="radio"/> IP Address Range :	From <input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/> To <input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/>
<input checked="" type="radio"/> Everyone	

- **Turn Remote Management On:** If selected, you can perform remote Web management for the router from the WAN.
- **Remote Management Address:** IP address that is used to access the router from the Internet. The default is http://0.0.0.0:8080. When accessing the router, you need to enter an address in the form of “the WAN IP address of the router” + “:” + “the port number” in the IE address bar. For example, if your external address is **10.0.0.123** and the used port number is **8080**, enter **10.0.0.123:8080** in your browser.
- **Port Number:** The port number for accessing the router through remote Web management.
- **Allow Remote Access By:** Set the IP address of the computer on which remote Web management is carried out to access the router.
 - **Only This Computer:** Only the specified IP address can access the router.
 - **IP Address Range:** A range of IP addresses on the Internet can access the router. You need to enter the starting and ending IP addresses to specify a range.
 - **Everyone:** Everyone on the Internet can access the router.

After finishing settings, click **Apply** to save the settings.

8.8.3 Schedules

Choose **Management Function > Schedules** and the **Schedule** page is displayed.

Schedule

Days to Block:	
<input checked="" type="checkbox"/> Every Day	
<input checked="" type="checkbox"/> Sunday	
<input checked="" type="checkbox"/> Monday	
<input checked="" type="checkbox"/> Tuesday	
<input checked="" type="checkbox"/> Wednesday	
<input checked="" type="checkbox"/> Thursday	
<input checked="" type="checkbox"/> Friday	
<input checked="" type="checkbox"/> Saturday	
Time of day to Block:(use 24-hour clock)	
<input checked="" type="checkbox"/> All Day	
Start Blocking	<input type="text" value="00"/> Hour <input type="text" value="00"/> Minute
End Blocking	<input type="text" value="23"/> Hour <input type="text" value="59"/> Minute

If you already set site filtering in the **Block Sites** page or set service filtering in the **Block Services** page, you can set a schedule to specify the time and mode of restricting Internet access.

- Days to Block: Select days on which you want to apply blocking by selecting the appropriate check boxes. Select **Every Day** to select the check boxes for all days.
- Time of Day to Block:
 - **All Day:** To perform 24-hour blocking.
 - **Start Blocking/End Blocking:** If you want to restrict access in a fixed period during the days you specify, enter the start and end time in 24-hour format.

After finishing settings, click **Apply** to save the settings.

8.8.4 SNTP

Choose **Management Function** > **SNTP** and the **SNTP** page is displayed.

Time Setting				
<input type="checkbox"/> Automatically synchronize with Internet time servers				
First NTP time server :	<input type="text" value="210.72.145.44"/>			
Second NTP time server :	<input type="text"/>			
Time Configuration				
Current Router Time :	1971-01-01 14:39:45			
Time Zone :	<input type="text" value="(GMT+01:00) Paris, Brussels, Copenhagen, Madrid"/>			
<input type="checkbox"/> Enable Daylight Saving				
Daylight Saving Offset :	<input type="text" value="0:00"/>			
Daylight Saving Dates : (Time interval must be greater than the days of start month)		Month	Week	Day
	Start	<input type="text" value="Apr"/>	<input type="text" value="2nd"/>	<input type="text" value="Sun"/>
	End	<input type="text" value="Sep"/>	<input type="text" value="2nd"/>	<input type="text" value="Sun"/>
		<input type="button" value="Apply"/>	<input type="button" value="Cancel"/>	

SNTP refers to Simple Network Time Protocol. In this page, you can set time information of your router. It is strongly recommended to set the correct time on the router first. This ensures proper functioning of log, site blocking, and schedule because their time settings are based on time information in this page.

- **Automatically synchronize with Internet time servers:** If selected automatic synchronization with the network time server is enabled.
- **First NTP time server:** Enter the IP address of the primary NTP server. The NTP server is a network time server that is used to synchronize the time of computers on the Internet. When you set the first NTP time server, the router obtains GMT time from the specified NTP server with priority after it is connected to the Internet.
- **Second NTP time server:** Enter the IP address of the secondary NTP server if available.
- **Current Router Time:** Display the current system time of the router.
- **Time Zone:** Select the time zone where you are located.
- **Enable Daylight Saving:** Enable or disable daylight saving time (DST).
- **Daylight Saving Offset:** Select a proper offset. If it is set to +1:00, 10:00 in the morning in standard time becomes 11:00 in the morning in DST.
- **Daylight Saving Dates:** Set the starting time and ending time of DST.

After finishing settings, click **Apply** to save the settings.

8.8.5 Reboot Device

For details, refer to section **7.6.2 Reboot Device**.

8.8.6 Set Password

For details, refer to section **7.6.3 Set Password**.

8.8.7 Router Upgrade

Choose **Management Function > Router Upgrade** and the **Router Upgrade** page is displayed.

Router Upgrade

Locate and select the upgrade file from your hard disk:

<input type="text"/>	<input type="button" value="Browse..."/>	<input checked="" type="checkbox"/> Clear Config
----------------------	--	--

Follow the procedures below to upgrade the software of the router.

- Step 1** Click **Browse...** to navigate to the latest software.
- Step 2** Select the correct upgrade file. If you select **Clear Config**, the router restores to the default settings after upgrade. If you do not select it, the current settings remain.
- Step 3** Click **Upload** to start upgrade.

After the upgrade is completed, the router automatically reboots.



Note:

After the software upgrade, the device returns to the factory default. In case the previous configuration information is lost, please save settings before updating the software.

Do not power off the router during the upgrade.

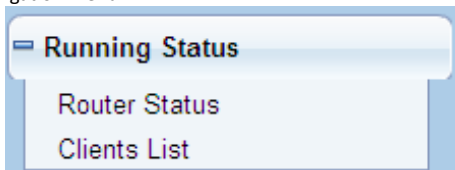
9 Web Configuration in Wireless Universal Repeater Mode

Note:

Set the three-way switch on the side panel to **Repeater**. Log in to the configuration page after the device is restarted.

9.1 Running Status

Set the three-way switch on the side panel to **Repeater**. Click **Running Status** to display the extended navigation menu.



9.1.1 Router Status

Choose **Running Status** > **Router Status** and the **Router Status** page is displayed.

Router Status

System Info	
Hardware Version	V1.0.0
Firmware Version	V1.0.0
Product Name	Wireless Router
Work Mode	Repeater Mode
Time and Date	1971-01-01 08:03:07
LAN Port	
MAC Address	00:1E:E3:4B:06:6C
IP Address	192.168.100.253
IP Subnet Mask	255.255.255.0
Wireless Client	
Wireless Network Selected Name (SSID)	TW-2B08
Wireless Channel	2.457GHz- CH10
Wi-Fi Protected Setup(WPS)	ON
Wireless Security Mode	None
Connect Status	Disconnected
Wireless Universal Repeater	
SSID of Extended Interface	TW-2B08
Wireless Security Mode	None

In this page, you can view information about the current running status of the device, including system information, LAN port status, wireless client information, and wireless universal repeater status.

9.1.2 Clients List

Choose **Running Status > Clients List** and the **Clients List** page is displayed.

Clients List

Wired Devices			
#	IP Address	MAC Address	Device Name
1	192.168.100.10	48:02:2A:D1:A9:60	unknown

Wireless Devices(Wireless intruders also show up here)

#	IP Address	MAC Address	Device Name
---	------------	-------------	-------------

Refresh

This page displays information of devices connected to the repeater, including the IP address, device name, and MAC address of each device.

9.2 Setup Wizard

For settings, refer to section **6.3 Repeater Mode Configuration**.

9.3 Repeater Mode Setting

Click **Repeater Mode Settings** and the **Repeater Mode Settings** page is displayed. Select **Wireless Universal Repeater Mode**.

Repeater Mode Settings

There are two modes to expand your wireless network of the Repeater Mode. You can choose anyone of WDS Mode or UR Mode.

Please choose your repeater mode as follows:

- WDS Mode
- Wireless Universal Repeater Mode

Apply

Cancel

9.4 Network Settings

For details, refer to section **7.4 Network Settings**.

9.5 Wireless Settings

Click **Wireless Settings** to display the extended navigation menu.

Wireless Settings

Wireless Universal Repeater

WPS Setup

Wireless Client Function

9.5.1 Wireless Universal Repeater

In universal repeater mode, the device acts as the AP and client simultaneously.

Choose **Wireless Settings > Wireless Universal Repeater** and the **Wireless Universal Repeater** page is displayed.

Wireless Universal Repeater

SSID of Extended Interface :	<input type="text" value="TW-2808"/>
Security Options	
Security Options :	<input type="text" value="none"/> ▼
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

- **SSID of Extended Interface:** Set the SSID of the repeater.
- **Security Options:** Set the security encryption mode for the repeater. It is recommended to configure the repeater with the same encryption mode as that of its uplink AP.

After finishing settings, click **Apply** to save the settings.

9.5.2 WPS Setup

Choose **Wireless Settings > WPS Setup** to display the page below.

WPS Setup

New and easy way to connect to the Wireless Router via WiFi Protected setup (WPS)

A wireless client has to support WPS function in order to use this wizard to add the client to your WPS enabled Wireless Router. Please check the user manual and gift box of your wireless client to see whether it supports the WPS function. If your wireless client does not support the WPS function, you have to configure your wireless client manually so it has the same SSID and wireless security settings as on this router.

WPS refers to Wi-Fi Protected Setup.

You can use WPS to establish wireless connection in a quick and secure way if the uplink AP or terminal (for example, the network adapter) has the WPS function. It is suggested to first configure wireless encryption for the uplink AP. If you change the wireless encryption mode after having established wireless connection by WPS, you must use WPS to establish wireless connection again. Note that if the wireless client does not support

WPS you must manually configure the wireless client (such as SSID, security mode, and password) to make it have the same SSID and wireless security settings as the router. In Repeater mode with WDS disabled, the device performs WPS encrypted connection to both the uplink AP and the downlink client device. Click Next to enter the **WPS Setup** page. Follow the description below to configure WPS for the Repeater mode.

9.5.2.1 Using the WPS Button

- WPS connection to the uplink AP

In Repeater mode with WDS disabled, press the **WPS** button on the side panel of the device in 3 seconds and release it. And press the **WPS** button on the uplink AP. Then they can start WPS session.

- WPS connection to the downlink client device

In Repeater mode with WDS disabled, press the **WPS** button on the side panel of the device for 3-10 seconds and release it. And press the **WPS** button on the client device. Then they can start WPS session.



Note:

The SSID, authentication and pre-shared key of the device will automatically change to the same as those of its uplink AP after the device succeeds in connecting to the uplink AP through the WPS button mode.

9.5.2.2 By the Web Page

You can perform WPS settings by the Web page for configuration.

Choose **Wireless Settings > WPS Setup** to display the **WPS Setup** page.

WPS Setup

As AP, Select a setup method:	
<input checked="" type="radio"/> Push Button (recommended)	
You can either press the Push Button physically on the router or press the Button below (soft Push Button).	<input type="button" value="Start PBC"/>
<input type="radio"/> PIN (Personal Identification Number)	
As Client, Select a setup method:	
<input checked="" type="radio"/> Push Button (recommended)	
You can either press the Push Button physically on the router or press the Button below (soft Push Button).	<input type="button" value="Start PBC"/>
<input type="radio"/> PIN (Personal Identification Number)	

– **As an AP**

You can perform WPS settings by the Web page for configuration.

Choose **Wireless Settings > WPS Setup** to display the WPS page.

- PBC mode

Step 1 Select **Push Button** and click **Start PBC**. WPS encrypted connection starts.

WPS Setup

As AP, Select a setup method:

Push Button (recommended)

You can either press the Push Button physically on the router or press the Button below (soft Push Button).

PIN (Personal Identification Number)

As Client, Select a setup method:

Push Button (recommended)

You can either press the Push Button physically on the router or press the Button below (soft Push Button).

PIN (Personal Identification Number)

Step 2 Press the **WPS** button on the network adapter or click the **PBC** button in the network adapter configuration tool within 2 minutes to start WPS connection. After WPS connection is established, the following page is displayed, indicating the WPS connection is completed.

Success

The wireless client has been added to the network successfully.
Click OK to go back to the Wi-Fi Protected Setup page...

- PIN mode

Step 1 Select **PIN**, enter the PIN code of the network adapter (refer to the client of the network adapter), and click **Start PIN** to start WPS connection.

WPS Setup

As AP, Select a setup method:

Push Button (recommended)

PIN (Personal Identification Number)

If your Adapter supports WPS, please click on 'Generate a client Security Pin to input on the AP/Router/Gateway' and put the generated client PIN number here.

As Client, Select a setup method:

Push Button (recommended)

You can either press the Push Button physically on the router or press the Button below (soft Push Button).

PIN (Personal Identification Number)

Step 2 Click the PIN button on the network adapter within 2 minutes to start WPS connection. After WPS connection is established, the following page is displayed, indicating that the WPS connection is completed.

Success

The wireless client has been added to the network successfully.
Click OK to go back to the Wi-Fi Protected Setup page...

OK

As a client

You can perform WPS settings using the Web page for configuration.

Choose **Wireless Settings > WPS** to display the WPS page.

- PBC mode

Step 1 Select **Push Button** and click **Start PBC**. WPS encrypted connection starts.

WPS Setup

As AP, Select a setup method:

- Push Button (recommended)

You can either press the Push Button physically on the router or press the Button below (soft Push Button).

Start PBC

- PIN (Personal Identification Number)

As Client, Select a setup method:

- Push Button (recommended)

You can either press the Push Button physically on the router or press the Button below (soft Push Button).

Start PBC

- PIN (Personal Identification Number)

Step 2 Start the WPS PBC process. After WPS connection is established, the following page is displayed, indicating that the WPS connection is completed.

Success

The wireless client has been added to the network successfully.
Click OK to go back to the Wi-Fi Protected Setup page...

OK

- PIN mode

Step 1 Select **PIN**, click **Generate New PIN**, and click **Start PIN** to start WPS connection.

WPS Setup

As AP, Select a setup method:

Push Button (recommended)

You can either press the Push Button physically on the router or press the Button below (soft Push Button). Start PBC

PIN (Personal Identification Number)

As Client, Select a setup method:

Push Button (recommended)

PIN (Personal Identification Number)

If your Adapter supports WPS, please click on 'Generate a client Security Pin to input on the AP/Router/Gateway' and put the generated client PIN number here.

Generate New PIN
Client's PIN: 12345670
Start PIN

- Step 2** Start the WPS PBC process within 2 minutes to start WPS connection. After WPS connection is established, the following page is displayed, indicating that the WPS connection is completed.

Success

The wireless client has been added to the network successfully.
Click OK to go back to the Wi-Fi Protected Setup page...

OK

9.5.3 Wireless Client Function

Choose **Wireless Settings > Wireless Client Function** and the **Wireless Client Function** page is displayed.

Wireless Client Function

This page help you to configure the wireless client.
Step1: Click "Site Survey" button to survey wireless sites when client mode is enabled. If any Access Point or IBSS is found, the results will be displayed in the Site Survey List three seconds later, you could select anyone to connect it manually. Then click "Next".

Site Survey

Number of Sites Scanned:32

#	SSID	BSSID	Channel	Signal	Encrypt	Select
1	Zoltrix_ZW919	00:28:12:34:56:78	1	100%	None	<input checked="" type="radio"/>
2	www24	00:1E:E3:C0:5F:6B	6	100%	None	<input type="radio"/>
3	TW-2B08	00:1F:A4:91:2A:60	10	100%	WPA-PSK(AES/TKIP)/ WPA2-PSK(AES/TKIP)	<input type="radio"/>

Next

- Step 1** Click **Site Survey** to search for the wireless network you want to connect.
- Step 2** Enter encryption information of the selected wireless network. Configure the client with the same security settings as the selected network. Click **Next**.

Wireless Client Function

Step2: You should configure your wireless client manually so it has the same wireless security settings as the network which you selected. Then click "Next".

Security Options

Security Options : 

- Step 3** The device provides the wireless roaming function if you select **Synchronize Wireless Universal Repeater's and Uplink AP's SSID and Security Options**. Click **Finish**. Then, the client can communicate with the selected network.

Wireless Client Function

Step3: This page provides an easy way to configure wireless universal repeater. If you enable the function, your wireless universal repeater would use same SSID and security options with uplink AP. Finally click "Finish".

Synchronize Wireless Universal Repeater's And Uplink AP's SSID And Security Options

Note: If you changed settings of wireless universal repeater, the wireless clients connecting to your wireless universal repeater need connect to wireless universal repeater with new SSID and security options again.

9.6 Management Function

For details, refer to section **7.6 Management Function**.

10 Web Configuration for the WDS Mode

10.1 Running Status

For details, refer to section **9.1 Running Status**.

10.2 Setup Wizard

For settings, refer to section **6.4 WDS Mode**.

10.3 Mode Setting

Click **Mode Settings** and the **Mode Settings** page is displayed.

Repeater Mode Settings

There are two modes to expand your wireless network of the Repeater Mode. You can choose anyone of WDS Mode or UR Mode.

Please choose your repeater mode as follows:

WDS Mode

Wireless Universal Repeater Mode

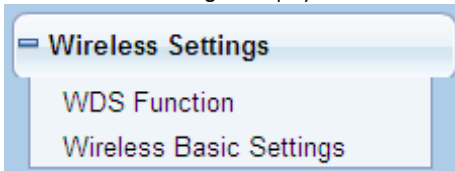
Select **WDS Mode**. Note that WDS function cannot be used if the channel is set to **Auto**.

10.4 Network Settings

For details, refer to section **7.4 Network Settings**.

10.5 Wireless Settings

Click **Wireless Settings** to display the extended navigation menu.



10.5.1 WDS Function

Wireless distribution system (WDS) enables interconnection between APs in an IEEE 802.11 wireless network. It extends the wireless network through several APs, without connection of the wired backbone network. Enable WDS if you want to use WDS to achieve wireless repeating or bridging.

Choose **Wireless Settings** > **WDS Function** and the **WDS Function** page is displayed.

WDS Function

<input type="checkbox"/> Disable Wireless Clients Association	
Wireless MAC of this router:	00:1E:E3:4B:06:6C
Wireless Repeater	
Repeater IP Address:	<input type="text" value="192"/> <input type="text" value="168"/> <input type="text" value="100"/> <input type="text" value="253"/>
Basic Station MAC Address:	<input type="text" value="00:1E:E3:4B:06:6C"/>

- **Disable Wireless Clients Association:** If selected, the repeater does not transmit any signals to clients that are connected to it. Generally, clear this check box. Generally, select this check box.
- **Repeater IP Address:** Set the repeater's IP address different from the wireless basic station and other repeaters to avoid IP address conflict. We suggest setting IP addresses of the same network segment for the wireless basic station and repeaters.
- **Basic Station MAC Address:** Enter the MAC address of the wireless basic station.

After finishing settings, click **Apply** to save the settings.

For WDS application description, refer to **6.4.3 WDS Application**.

10.5.2 Wireless Basic Settings

For details, refer to **7.5.1 Wireless Basic Settings**.

10.6 Management Function

For details, refer to section **7.6 Management Function**.

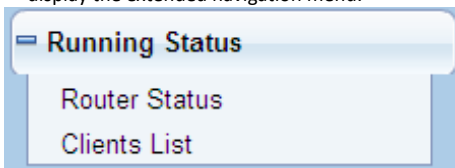
11 Web Configuration in Client Mode

Note:

Set the three-way switch on the side panel to **Client Mode**.

11.1 Running Status

Set the three-way switch on the case of the device to Client mode. Click **Running Status** to display the extended navigation menu.



11.1.1 Router Status

Choose **Running Status** > **Router Status** and the **Router Status** page is displayed.

Router Status

System Info	
Hardware Version	V1.0.0
Firmware Version	V1.0.0
Product Name	Wireless Router
Work Mode	Client Mode
Time and Date	1971-01-01 08:14:54
LAN Port	
MAC Address	00:1E:E3:4B:06:6C
IP Address	192.168.100.253
IP Subnet Mask	255.255.255.0
Wireless Client	
Wireless Network Selected Name (SSID)	
Wireless Channel	2.412GHz- CH1
Wi-Fi Protected Setup(WPS)	ON
Wireless Security Mode	None
Connect Status	Disconnected

In this page, you can view information about the current running status of the device, including system information, LAN port status, and wireless client status.

11.1.2 Clients List

Choose **Running Status > Clients List** and the **Clients List** page is displayed.

Clients List

Wired Devices			
#	IP Address	MAC Address	Device Name
1	192.168.100.10	48:02:2A:D1:A9:60	unknown

Refresh

This page displays information of wireless devices connected to the device, including the IP address and MAC address of each device.

11.2 Setup Wizard

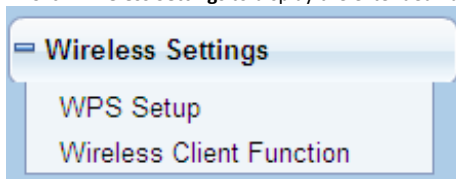
For details, refer to **6.5 Client Mode Configuration**.

11.3 Network Settings

For details, refer to section **7.4 Network Settings**.

11.4 Wireless Settings

Click **Wireless Settings** to display the extended navigation menu.



11.4.1 WPS Setup

For details, refer to **7.5.4 WPS Setup**.

11.4.2 Wireless Client Function

For details, refer to **9.5.3 Wireless Client Function**.

11.5 Management Function

For details, refer to section **7.6 Management Function**.

Appendix A FAQ

1	The device cannot be detected by the wireless network adapter.
	When the device which is in Client mode or Reaper mode but disconnected to the uplink AP does not support wireless client access and can be connected to through an Ethernet cable only. If the problem still remains, probably the device is far distant from the terminal device or there are obstacles block wireless signal. You can put the device in a place close to the terminal device or add a wireless repeater. In addition, place microwave ovens, Bluetooth devices, and wireless phones that interrupt WLAN signals far away from WLAN devices.
2	The wireless network adapter fails to connect to the device.
	Some early-version wireless network adapters may not support WPA2 authentication. You can set the authentication and encryption to WPA-AES, WPA-TKIP, or WEP.
3	The device in Repeater or Client mode fails to connect to the uplink AP, for example, the domestic gateway, to access the Internet, or it frequently gets disconnected from the Internet.
	Check the device is in the wireless signal coverage of its uplink device or not. Click Site Survey in the Wireless Client Function page and check whether the device can search out strong wireless signals from the uplink AP or not.
4	Wired connection to the device is abnormal.
	Check status of the Ethernet indicator on the device. If the Ethernet indicator turns off, check whether the Ethernet cable is connected properly. If the problem still remains, replace the Ethernet cable.
5	The Internet cannot be accessed.
	Check whether the network adapter connected to the device can automatically obtain an IP address. If it fails, enable DHCP for the domestic gateway or manually set the IP address of the network adaptor and DNS.
6	The device cannot be configured by the Web page.
	Check whether the IP address of the network adapter and that of the device are in the same network segment. Manually set the IP address of your network adapter in the network segment of 192.168.100.2/253 according to procedures described in Chapter 5 "Configuring Your Computer and Wireless Connection". Choose Network Settings > LAN Interface Settings and set the IP address of the device in the same network address as that of the domestic network gateway.
7	WPS connection fails.
	Ensure that one and the only WPS device connected to the device starts the WPS session within 2 minutes. Note the WPS difference between the device serving as the uplink AP and that as the downlink client device in the Repeater mode (see section 9.5.2 WPS Setup). Refer to Table 4.1 for description on WPS indicator status.

DISPOSAL



As a responsible retailer we care about the environment.

As such we urge you to follow the correct disposal procedure for the product, packaging materials and if applicable, accessories. This will help conserve natural resources and ensure that the materials are recycled in a manner that protects health and the environment.

You must follow laws and regulations about disposal. Waste electrical products must be disposed of separately from household waste when the product reaches the end of its life. Contact the store where you bought the product and your local authority to learn about disposal and recycling.

We apologise for any inconvenience caused by minor inconsistencies in these instructions, which may occur as a result of product improvement and development.

Darty Plc © UK: EC1N 6TE 21 / 11/ 2013

Declaration of Conformity

The following product has been deemed to comply with the requirements of the listed European Directives:-

R&TTE Directive (1999 / 5 / EC)

Electromagnetic Compatibility Directive (2004/108/EC)

Low Voltage Directive (2006/95/EC)

RoHS2 (2011/65/EU)

Product Description: 300 Mbps wireless repeater

Brand: I.T.Works

Model number: REPW300

The above listed products conform to the following EU Standards:

EN 62311: 2008

EN 301 489-17 V2.2.1

EN 300 328 V1.7.1

EN 301 489-1 V1.9.2

EN60950-1:2006 + A11:2009 + A1:2010+A12:2011

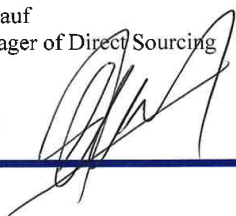
The person responsible for this declaration is:

Name: François Lemauf

Position: General Manager of Direct Sourcing

Signature:

Date: 6th January, 2014



EUROPEAN FRENCH

300 Mbps Répéteur WiFi

Modèle : REPW300



MODE D'EMPLOI

Index

1	Mises en garde	4
2	Introduction	5
2.1	Présentation du produit	5
2.2	Contenu de l'emballage.....	5
3	Présentation des modes	6
3.1	Mode pont.....	6
3.2	Mode routeur	6
3.3	Mode répéteur sans fil universel/WDS.....	6
3.4	Mode client	6
4	Description du matériel et configuration requise.....	6
4.1	Description du matériel.....	6
4.1.1	Panneau avant et états des LED	6
4.1.2	Description des panneaux arrière/latéral et de l'interface.....	10
4.2	Configuration matérielle requise.....	9
4.2.1	Configuration système requise	9
4.2.2	Avant de commencer.....	9
4.3	Portée de fonctionnement	9
5	Configuration PC et sans fil	10
5.1	Configuration PC.....	10
5.2	Configuration sans fil.....	12
6	Configuration de l'appareil.....	14
6.1	Configuration du mode pont	15
6.2	Configuration du mode routeur.....	15
6.3	Configuration du mode répéteur.....	17
6.4	Mode WDS	19
6.4.1	Configuration du répéteur en mode WDS	19
6.4.2	Configuration de la station de base centrale en mode WDS.....	20
6.4.3	Application WDS.....	20
6.5	Configuration du mode client.....	21
7	Configuration Web en mode pont	22
7.1	Statut fonctionnement	22
7.1.1	État du routeur	23
7.1.2	Liste clients	23
7.2	Assistant de configuration	24
7.3	Réglage du mode.....	24
7.4	Paramètres réseau.....	24
7.4.1	Paramètres de l'interface LAN	24
7.4.2	Serveur DHCP	25
7.5	Paramètres sans fil	26
7.5.1	Paramètres de base sans fil	27
7.5.2	Réseau invité	30
7.5.3	Paramètres sans fil avancés	31

	7.5.4	Configuration WPS.....	33
7.6		Fonction gestion.....	35
	7.6.1	Paramètres de sauvegarde.....	35
	7.6.2	Redémarrer.....	37
	7.6.3	Définir mot de passe.....	37
	7.6.4	Mise à jour du routeur.....	37
8		Configuration Web en mode routeur.....	39
8.1		Statut fonctionnement.....	39
	8.1.1	État du routeur.....	39
	8.1.2	Liste clients.....	41
8.2		Assistant de configuration.....	41
8.3		Réglage du mode.....	41
8.4		Paramètres réseau.....	41
	8.4.1	Paramètres de l'interface LAN.....	42
	8.4.2	Paramètres de l'interface WAN.....	42
	8.4.3	Serveur DHCP.....	49
	8.4.4	NAT ALG.....	51
8.5		Paramètres sans fil.....	51
	8.5.1	Paramètres de base sans fil.....	52
	8.5.2	Réseau invité.....	52
	8.5.3	Paramètres sans fil avancés.....	53
	8.5.4	Fonction WDS.....	53
	8.5.5	Configuration WPS.....	54
8.6		Application réseau.....	54
	8.6.1	Redirection de port.....	54
	8.6.2	Déclenchement de port.....	55
	8.6.3	UPnP.....	59
	8.6.4	Proxy IGMP.....	59
	8.6.5	Serveur DMZ.....	59
	8.6.6	DNS dynamique.....	59
	8.6.7	Routes statiques.....	59
8.7		Options de sécurité.....	60
	8.7.1	Bloquer des sites.....	61
	8.7.2	Bloquer des services.....	63
	8.7.3	Protection.....	64
8.8		Fonction gestion.....	64
	8.8.1	Paramètres de sauvegarde.....	65
	8.8.2	Gestion à distance.....	65
	8.8.3	Calendrier.....	66
	8.8.4	SNTP.....	67
	8.8.5	Redémarrer.....	68
	8.8.6	Définir mot de passe.....	68
	8.8.7	Mise à jour du routeur.....	68

9	Configuration Web en mode répéteur sans fil universel	69
9.1	Statut fonctionnement	69
9.1.1	État du routeur	69
9.1.2	Liste clients	70
9.2	Assistant de configuration	70
9.3	Réglage du mode de répétition	70
9.4	Paramètres réseau.....	70
9.5	Paramètres sans fil	70
9.5.1	Répéteur sans fil universel.....	71
9.5.2	Configuration WPS.....	71
9.5.3	Fonction client sans fil	75
9.6	Fonction gestion	76
10	Configuration Web pour le mode WDS	76
10.1	Statut fonctionnement	76
10.2	Assistant de configuration	76
10.3	Réglage du mode.....	76
10.4	Paramètres réseau.....	76
10.5	Paramètres sans fil	76
10.5.1	Fonction WDS	77
10.5.2	Paramètres de base sans fil.....	77
10.6	Fonction gestion	77
11	Configuration Web en mode client.....	78
11.1	Statut fonctionnement	78
11.1.1	État du routeur	79
11.1.2	Liste clients	79
11.2	Assistant de configuration	79
11.3	Paramètres réseau.....	79
11.4	Paramètres sans fil	79
11.4.1	Configuration WPS.....	79
11.4.2	Fonction client sans fil	79
11.5	Fonction gestion	79

1 Mises en garde

Avant d'utiliser le répéteur, veuillez lire attentivement les mises en garde suivantes:

- Laissez suffisamment d'espace autour de l'appareil pour permettre la dissipation de la chaleur: l'appareil peut être endommagé en cas de surchauffe. Les orifices de dissipation de la chaleur permettent à l'appareil de fonctionner normalement. Ne recouvrez pas ces orifices.
- Ne placez pas l'appareil dans un endroit à haute température, notamment à proximité d'une sortie d'air chaud. L'appareil doit rester à l'abri du soleil.
- Gardez l'appareil dans un endroit sec. Ne renversez en aucun cas du liquide sur l'appareil.
- Ne reliez pas l'appareil à un PC ni à tout autre appareil électronique, sauf indication contraire de notre ingénieur clientèle ou de votre fournisseur d'accès haut débit; toute connexion erronée peut entraîner une coupure de courant ou un risque d'incendie.
- Ne placez pas l'appareil sur une surface instable.



Ce symbole indique que l'appareil est conforme aux normes européennes de sécurité et de compatibilité électromagnétique.

2 Introduction

2.1 Présentation du produit

Ce répéteur est un routeur de poche; il est facile à installer et à transporter grâce à son format compact. Sa vitesse de transmission sans fil est de 300 Mbps maximum. Cet appareil haute performance est compatible avec les normes IEEE802.11b/g/n; il fournit des services d'accès à Internet pratiques et fiables pour les utilisateurs individuels et pour les TPE (très petites entreprises). Il comporte une interface basée sur le Web, permettant aux utilisateurs de modifier facilement les paramètres de connexion à l'ISP (fournisseur de services Internet) et d'effectuer facilement les mises à jour sur la page WEB.

En outre, le panneau latéral comporte un interrupteur à trois positions permettant de choisir le mode de fonctionnement: point d'accès, répéteur et client. En mode point d'accès, l'appareil fonctionne comme routeur sans fil permettant la connexion pour les réseaux LAN câblés. En mode répéteur, la fonction URM (mode répéteur universel) de l'appareil permet à l'utilisateur d'étendre la couverture sans fil du point d'accès existant de manière simple et rapide. En mode client, l'appareil fonctionne comme adaptateur réseau sans fil, à ceci près que la connexion et la transmission sont plus performantes.

2.2 Contenu de l'emballage

Le contenu de l'emballage doit être le suivant:

- 1 répéteur sans fil de 300 Mbps
- 1 câble réseau
- 1 mode d'emploi (CD)

3 Présentation des modes

3.1 Mode pont

En mode pont, l'appareil fonctionne comme routeur sans fil permettant la connexion pour les réseaux LAN câblés.

3.2 Mode routeur

En mode routeur, l'appareil fonctionne comme passerelle domestique.

3.3 Mode répéteur sans fil universel/WDS

En mode répéteur sans fil universel/WDS, l'appareil étend la couverture sans fil du point d'accès existant. Les ordinateurs peuvent se connecter à l'appareil avec ou sans fil.

3.4 Mode client

En mode client, l'appareil fournit l'accès à Internet pour les décodeurs ou les ordinateurs avec adaptateur réseau.

4 Description du matériel et configuration requise

4.1 Description du matériel

4.1.1 Panneau avant et états des LED

L'appareil comporte 4 témoins LED sur son panneau avant. Ceux-ci vous permettent de savoir si l'appareil fonctionne normalement ou non.



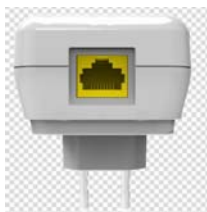
Le tableau suivant décrit les différents états des témoins de l'appareil.

Témoin lumineux	Couleur	État	Description
Alimentation	Vert	Allumé	L'appareil fonctionne normalement.
	Rouge	Allumé	L'auto-inspection du système est en cours ou vient d'échouer, ou la mise à jour du logiciel est en cours.
WPS (configuration protégée par Wi-Fi)	Vert	Éteint	La session WPS est terminée.
		Allumé	Le témoin WPS reste allumé pendant 5 minutes après l'établissement de la connexion WPS (Wi-Fi Protected Setup, "configuration protégée par Wi-Fi").
		Clignotement rapide	Un terminal a essayé de se connecter à l'appareil via WPS mais a échoué.
		Clignotement rapide, mais avec un intervalle plus long	Plusieurs terminaux essaient de se connecter en même temps à l'appareil via WPS. Conflit entre les sessions WPS.
		Clignotement lent	La session WPS est ouverte.

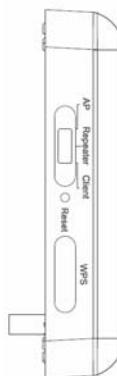
Ethernet	Vert	Éteint	Le port Ethernet est en état de non-communication.
		Allumé	Le port Ethernet est en état de communication.
		Clignotant	Transmission et réception de données en cours par le port Ethernet.
WLAN	Vert	Éteint	La connexion WLAN est en état de non-communication.
		Allumé	La connexion WLAN est en état de communication.
		Clignotant	Transmission et réception de données en cours sur le WLAN.

4.1.2 Description des panneaux arrière/latéral et de l'interface

Panneau arrière



Panneau latéral



APPUYEZ SUR = Point d'accès

Repeater = Répéteur

Client = Client

Reset = Réinitialisation

WPS = WPS

Le tableau suivant décrit l'interface et les boutons de l'appareil.

Interface/boutons	Description
WAN/LAN	Si l'appareil est en mode point d'accès, l'interface est une interface WAN pour une connexion à un réseau WAN ou à un réseau de liaison montante. Si l'appareil est en mode répéteur/client, l'interface est

	une interface LAN.
Reset (réinitialisation)	Appuyez délicatement sur la touche Reset pendant 3 à 6 secondes, puis relâchez-la. Les paramètres par défaut du système seront réinitialisés.
AP/Repeater/Client (point d'accès/répéteur/client)	Permet de régler l'appareil en mode point d'accès, répéteur ou client. Mode point d'accès: inclut les modes pont et routeur. Mode répéteur: permet d'étendre la couverture réseau sans fil. Mode client: équivalent à un adaptateur réseau sans fil.
WPS (configuration protégée par Wi-Fi)	Permet d'activer le mode WPS PBC. Pour plus de détails, veuillez vous référer aux descriptions de chaque mode WPS.

4.2 Configuration matérielle requise

4.2.1 Configuration système requise

Avant de procéder à l'installation de l'appareil, vous devez avoir à votre disposition:

- Au moins 1 câble Ethernet RJ45 (10Base-T/100Base-T)
- 1 répéteur sans fil
- Un PC installé avec le protocole TCP/IP et pouvant accéder à Internet.

4.2.2 Avant de commencer

Avant de procéder à l'installation, veuillez noter les points suivants:

- Les câbles Ethernet utilisés pour relier l'appareil à un ordinateur, à un hub, à un routeur ou à un interrupteur doivent faire moins de 100 m de long.
- Ne placez pas l'appareil sur une surface irrégulière ou instable. Ne le posez pas par terre.
- L'appareil doit rester propre. L'appareil doit rester à l'abri du soleil. Aucun objet métallique ne doit être introduit dans l'appareil.
- Placez l'appareil au centre de l'emplacement choisi afin d'optimiser la couverture sans fil.

4.3 Portée de fonctionnement

La portée de fonctionnement de l'appareil dépend des conditions de l'environnement. La trajectoire et l'effet de la transmission du signal dépendent de l'emplacement dans la maison ou le bureau. Par exemple, la portée en ligne droite peut atteindre 300 mètres à l'air libre pour certains appareils, mais seulement 100 mètres en intérieur.

5 Configuration PC et sans fil

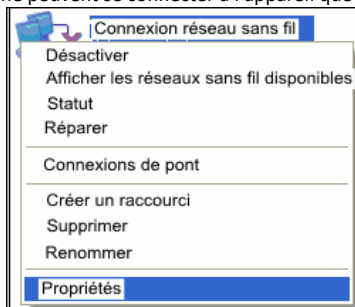
5.1 Configuration PC

L'exemple ci-dessous est valable pour Windows XP. Pour configurer manuellement l'adaptateur réseau, procédez de la manière suivante:

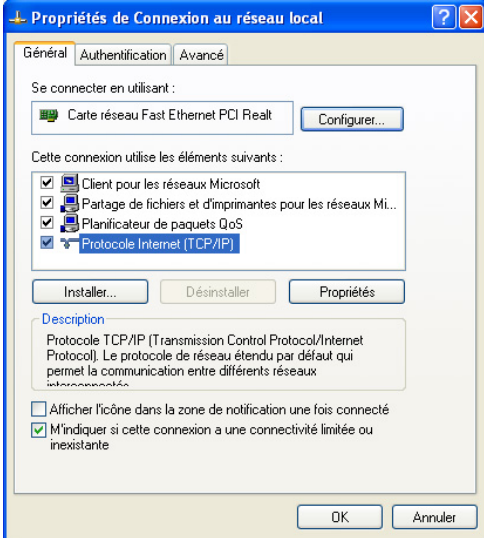
Etape 1 Faites un clic droit sur l'icône **Favoris réseau** puis allez dans **Propriétés**; la fenêtre **Connexions réseau** apparaît.



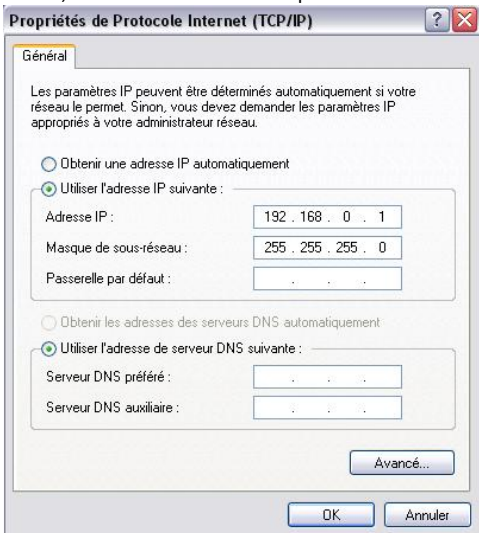
Etape 2 Faites un clic droit sur l'icône de carte d'interface réseau ou d'adaptateur réseau sans fil, puis allez dans **Propriétés**. (Remarque: en mode client, les ordinateurs ne peuvent se connecter à l'appareil que par câble Ethernet.)



Etape 3 Faites un double clic sur Protocole Internet (TCP/IP).



- Etape 4** Si l'appareil est en mode routeur, allez dans **Obtenir une adresse IP automatiquement**. Si l'appareil est dans un autre mode, réglez l'adresse IP de votre ordinateur sur **192.168.100.X** (X étant un nombre entier entre 2 et 253), et l'adresse MAC sur 255.255.255.0. Configurez la passerelle et l'adresse IP du serveur DNS. Si vous ne connaissez pas les données de la passerelle et du serveur DNS, laissez ces cases vides. Cliquez sur **OK**.






Remarque:

Une fois terminée la configuration de l'appareil, la passerelle domestique peut configurer le protocole Internet pour l'adaptateur réseau du PC. Configurez l'adresse IP et le serveur DNS pour vous faire attribuer une adresse IP automatiquement (voir figure ci-dessus).

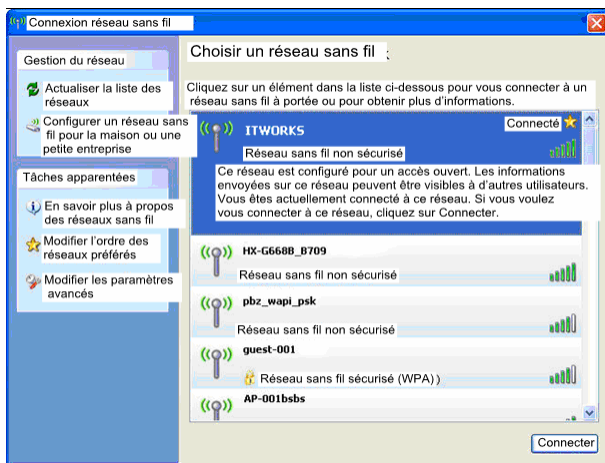
5.2 Configuration sans fil

L'exemple ci-dessous est valable pour Windows XP.

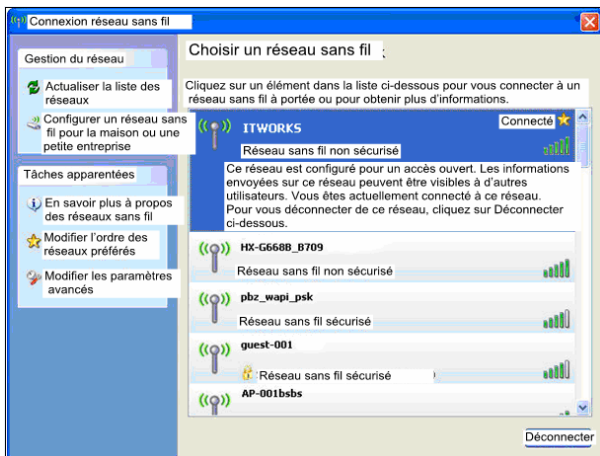
Pour connecter l'adaptateur réseau sans fil à votre PC, procédez de la manière suivante:

Etape 1 Cliquez sur l'icône  située en bas à droite du bureau. (Remarque: votre PC doit être installé avec un adaptateur réseau sans fil).

Etape 2 Dans la page **Connexion réseau sans fil**, cliquez sur le réseau sans fil souhaité.



Etape 3 Votre ordinateur est connecté au réseau sans fil lorsque le mot **Connecté** s'affiche en haut à droite.



Remarque:

Le SSID par défaut du répéteur est ITWORKS.

6 Configuration de l'appareil

Le tableau suivant contient les informations des modes point d'accès/répéteur/client de l'appareil.

Mode sur le boîtier	Mode disponible sur le Web	Adresse IP de gestion	Adresse MAC de sous-réseau	DHCP	Moyen de connexion au PC
AP (point d'accès)	Bridge (pont) (par défaut)	192.168.100.253	255.255.255.0	Désactivé	Câble Ethernet/sans fil
	Routeur			Activer	Sans fil seulement
Répéteur	Répéteur sans fil universel (par défaut)	192.168.100.253	255.255.255.0	Désactivé	Câble Ethernet/sans fil
	WDS				
Client	Client (par défaut)	192.168.100.253	255.255.255.0	Désactivé	Câble Ethernet seulement

Etape 1 Repérez l'interrupteur à trois positions sur le boîtier de l'appareil, et mettez-le sur le mode souhaité.

Etape 2 Lancez Internet Explorer (IE). Tapez l'adresse IP de gestion de **192.168.100.253** et appuyez sur **Enter**. Dans la fenêtre d'ouverture de session ci-dessous, tapez le nom d'utilisateur et le mot de passe (**admin** dans les deux cas).



it.WORKS

Langue: Français

Nom d'utilisateur:

Mot de passe:

Login Réinitialisation

La session a expiré

Etape 3 Cliquez sur Login, l'écran suivant apparaît.



it.WORKS

Assistant de configuration

Etape 1: Cet assistant a pour but de vous aider à configurer le client sans fil. Cliquez sur "Étude de sites" pour étudier les sites sans fil quand le mode client est activé. Si un point d'accès ou un BSS est trouvé, les résultats sont affichés dans la liste d'étude de sites très secondes plus tard; vous pouvez faire en sorte que n'importe qui se connecte manuellement. Puis cliquez sur "Suivant".

Étude de sites

Nombre de sites scannés: 32

Liste d'étude de sites

#	SSID	BSSID	Chaîne	Signal	Cryptage	Sélectionner
1	TW-2808	00:1F:A4:91:2A:50	9	100%	WPA-PSK(AES/TKIP) WPA2-PSK(AES/TKIP)	<input type="radio"/>
2	LIVCC	74:00:2B:3A:6B:C0	11	100%	WPA2-PSK(AES)	<input type="radio"/>
3	MT7620_AP_001123	88:88:88:88:88:88	4	99%	Jamais	<input type="radio"/>

Décconnexion

Aide - Assistant de configuration

Quand le mode client est activé, le routeur peut être utilisé comme client pour se connecter à n'importe quel point d'accès ou BSS.

Avec le bouton "Étude de sites", le client peut étudier les sites sans fil.

Configurez votre client sans fil manuellement, de manière à ce qu'il ait les mêmes paramètres de sécurité sans fil que le réseau choisi et puisse donc communiquer avec ce réseau.

Cliquez sur **Déconnexion** pour vous déconnecter de la page.

Remarque:

La langue se change en haut à droite de l'écran (anglais et français disponibles).

Les appareils à terminaux peuvent accéder au réseau par l'intermédiaire du répéteur une fois la configuration terminée (voir procédures ci-après).

6.1 Configuration du mode pont

Etape 1 Allumez l'appareil, puis mettez sur **AP** l'interrupteur à trois positions situé sur le panneau latéral. Une fois le système démarré, connectez-vous à la page de configuration.

Etape 2 Cliquez sur **Assistant de configuration** dans la barre de navigation située sur le panneau gauche de l'écran. Définissez le SSID et le mot de passe de cryptage, puis notez-les quelque part. Cliquez sur **Terminer** pour confirmer les paramètres.

Assistant de configuration

Cet assistant de configuration vous aide à configurer les paramètres sans fil en mode pont.

Activer la radio du routeur sans fil

Name(SSID)

Name(SSID) :

Options de sécurité

Options de sécurité :

Options de sécurité (WPA2-PSK)

Mot de passe : (8-63 caractères ou 64 caractères hexadécimaux)

6.2 Configuration du mode routeur

Etape 1 Allumez l'appareil, puis mettez sur **AP** l'interrupteur à trois positions situé sur le panneau latéral. Une fois le système démarré, connectez-vous à la page de configuration.

Etape 2 Cliquez sur **Réglage du mode** et choisissez **Mode routeur** (le réglage par défaut est **Mode pont**). Cliquez sur **Appliquer** pour redémarrer l'appareil.

Réglage du mode

Choisissez l'un des modes suivants:

Mode pont

Mode routeur

Dans ce mode, le port est utilisé comme port WAN.
Vous ne pouvez ouvrir votre session qu'en vous connectant au réseau correspondant à votre carte réseau sans fil.
Avant de passer à ce mode, veuillez mémoriser le SSID et les options de sécurité de votre réseau sans fil.

Etape 3 Une fois l'appareil redémarré, enlevez le câble réseau et connectez le PC à l'appareil à l'aide d'un adaptateur réseau sans fil. Connectez-vous à la page de configuration. Cliquez sur **Assistant de configuration** dans la barre de navigation

située sur le panneau gauche de l'écran. Choisissez **Oui** et cliquez sur **Suivant**.
L'appareil détectera automatiquement le type de connexion.

Configuration Internet

L'assistant de configuration intelligent peut détecter de quel type est votre connexion Internet.
Voulez-vous laisser l'assistant de configuration intelligent détecter le type de connexion maintenant?

- Oui.
 Non. Je souhaite configurer mon routeur moi-même.

Suivant

Etape 4 L'appareil peut détecter trois types de connexion: Adresse IP dynamique (DHCP), adresse IP statique et PPPoE. Effectuez la configuration correspondant au type de connexion que vous utilisez.

(1) Configuration de paramètres pour adresse IP dynamique (DHCP)

Assistant de configuration

Adresse IP dynamique (DHCP) détectée
Votre type de connexion a été détecté avec succès.

Retour Suivant



Adresse IP dynamique

Nom de compte (si nécessaire)

Suivant Annuler

(2) Configuration de paramètres pour adresse IP statique

Assistant de configuration

Adresse IP statique (fixe) détectée

Votre type de connexion a été détecté avec succès.

Si vous pensez avoir reçu ce message par erreur, débranchez votre modem puis rebranchez-le. Ensuite, fermez cet écran et ouvrez un autre navigateur Internet (ex: Internet Explorer)

Retour Suivant



Adresses IP statiques (fixes)

Votre fournisseur de service Internet fournit les paramètres d'adresse IP statique (fixe).

Entrez l'adresse IP exacte pour chaque paramètre d'adresse IP statique. Par exemple, entrez l'adresse IP de la passerelle dans le champ de l'adresse de la passerelle et celui de l'adresse IP.

Adresse IP Internet

Adresse IP

Masque de sous-réseau IP

Adresse IP de la passerelle

Adresse du serveur de nom de domaine (DNS)

DNS primaire

DNS secondaire

Suivant Annuler

(3) Configuration de paramètres pour PPOE

PPPoE détecté

Votre type de connexion a été détecté avec succès.

Retour Suivant



PPPoE

Réglage mot de passe

Login:

Password:

Service Name (if required):

Domain Name Server(DNS) Address

Get Automatically From ISP

Use These DNS Servers

Primary DNS:

Secondary DNS:

Suivant Annuler

Etape 5 Cliquez sur **Suivant**. Définissez le SSID et le mot de passe, puis notez-les quelque part. Cliquez sur **Terminer** pour confirmer les paramètres.

Paramètres sans fil

Activer la radio du routeur sans fil

Name(SSID)

Name(SSID):

Options de sécurité

Options de sécurité:

Options de sécurité (WPA2-PSK)

Mot de passe: (8-63 caractères ou 64 caractères hexadécimaux)

Retour Terminer Annuler

6.3 Configuration du mode répéteur

Etape 1 Allumez l'appareil, puis mettez sur **Repeater** l'interrupteur à trois positions situé sur le panneau latéral. Reliez le câble réseau à l'appareil et connectez-vous à la page de configuration une fois le système démarré.

Etape 2 Cliquez sur **Assistant de configuration** dans la barre de navigation située sur le panneau gauche de l'écran. Allez dans **Mode répéteur sans fil universel** et cliquez sur **Suivant**.

Assistant de configuration

Étape 1: Deux modes permettent d'étendre le réseau sans fil de votre mode de répétition. Vous avez le choix entre le mode WDS et le mode répéteur sans fil universel.

Choisissez l'un des modes de répétition suivants:

Mode WDS

Mode répéteur sans fil universel

Suivant

Etape 3 Cliquez sur **Étude de sites** pour rechercher le réseau sans fil auquel vous souhaitez vous connecter. Sélectionnez le réseau qui convient. Cliquez sur **Suivant**.

Assistant de configuration

Étape 2: Commencez par configurer le client sans fil. Cliquez sur "Étude de sites" pour étudier les sites sans fil quand le mode client est activé. Si un point d'accès ou un IBSS est trouvé, les résultats sont affichés dans la liste d'étude de sites trois secondes plus tard, vous pouvez faire en sorte qu'il importe qui se connecte manuellement. Puis cliquez sur "Suivant".

Étude de sites

Nombre de sites scannés :32

Liste d'étude de sites

#	SSID	BSSID	Chaîne	Signal	Cryptage	Sélectionner
1	LWCC	74:D0:2B:3A:6B:C0	1	100%	WPA2-PSK(AES)	<input type="radio"/>
2	TW-2B08	00:1F:A4:91:2A:60	9	96%	WPA-PSK(AES/TKIP) WPA2-PSK(AES/TKIP)	<input checked="" type="radio"/>
3	feifei002	00:1F:A4:92:56:3F	1	86%	WPA-PSK(AES/TKIP) WPA2-PSK(AES/TKIP)	<input type="radio"/>

Retour

Suivant

Etape 4 Configurez le répéteur avec les mêmes options de sécurité que son réseau de liaison montante. (la figure ci-dessous utilise comme exemple l'option de sécurité **Jamais**.) Définissez le mot de passe de cryptage, puis notez-le quelque part. Cliquez sur **Suivant**.

Assistant de configuration

Étape3: Vous devez configurer votre client sans fil manuellement, de manière à ce qu'il ait les mêmes paramètres de sécurité sans fil que le réseau choisi. Puis cliquez sur "Suivant".

Options de sécurité de client sans fil

Options de sécurité de client sans fil :

Jamais

Retour

Suivant

Etape 5 Si vous cochez la case **Synchroniser le SSID et les options de sécurité du répéteur universel sans fil et du point d'accès de liaison montante**, l'appareil fournit des services d'itinérance sans fil. Sinon, vous devrez configurer manuellement le SSID et les options de sécurité pour le répéteur. Cliquez sur **Terminer** pour refermer l'assistant de configuration.

Assistant de configuration

Étape 4: Cette page vous explique comment configurer le répéteur sans fil universel de manière simple. Si cette fonction est activée, le répéteur sans fil universel utilise le même SSID et les mêmes options de sécurité avec point d'accès de liaison montante; sinon, vous devrez configurer manuellement le SSID de l'interface étendue ainsi que les options de sécurité. Pour finir, cliquez sur "Terminer".

Paramètres de répéteur sans fil universel

Synchroniser le SSID et les options de sécurité du répéteur universel sans fil et du point d'accès de liaison montante

SSID de l'interface étendue :

TW-2B08

Options de sécurité :

aucune

Remarque: Si vous modifiez les paramètres du répéteur universel sans fil, les clients sans fil souhaitant s'y connecter devront utiliser un nouvel SSID et de nouvelles options de sécurité.

Retour

Terminer

Annuler

6.4 Mode WDS

6.4.1 Configuration du répéteur en mode WDS

Étape 1 Allumez l'appareil, puis mettez sur **Repeater** l'interrupteur à trois positions situé sur le panneau latéral. Une fois le système démarré, connectez-vous à la page de configuration.

Étape 2 Cliquez sur **Assistant de configuration** dans la barre de navigation située sur le panneau gauche de l'écran. Allez dans **Mode WDS** et cliquez sur **Suivant**. (Remarque: la fonction WDS ne peut pas être activée si le canal est réglé sur **Auto**) Réglez manuellement tous les appareils WDS sur le même canal.

Assistant de configuration

Étape 1: Deux modes permettent d'étendre le réseau sans fil de votre mode de répétition. Vous avez le choix entre le mode WDS et le mode répéteur sans fil universel.

Choisissez l'un des modes de répétition suivants:

Mode WDS

Mode répéteur sans fil universel

Suivant

Étape 3 Définissez l'adresse IP du port LAN du répéteur et tapez l'adresse MAC de la station de base. Cliquez sur **Suivant**.

Assistant de configuration

Étape 2: En mode WDS, l'appareil fonctionne comme répéteur et ne peut communiquer qu'avec une autre station sans fil en mode station de base. Tapez l'adresse MAC sans fil de l'autre station sans fil en mode station de base dans le champ intitulé "Adresse MAC de la station de base", puis tapez l'adresse MAC sans fil du routeur dans la page avec de l'autre station sans fil en mode station de base. Le changement de l'adresse IP du répéteur entraîne un changement de l'adresse IP LAN.

Réglages WDS

MAC sans fil de ce routeur: 00:1E:E3:4B:0E:6C

Adresse IP du répéteur:

Adresse MAC de la station de base:

Retour

Suivant

Étape 4 Définissez le SSID, le canal et le cryptage de sécurité pour le répéteur. Le canal ne peut pas être réglé sur **Auto**. Il est conseillé de configurer le répéteur avec les mêmes options de sécurité que sa station de base. Définissez le mot de passe de cryptage, puis notez-le quelque part. Cliquez sur **Terminer** pour confirmer les paramètres.

Assistant de configuration

Étape 3: Le WEP peut (et doit) être utilisé pour protéger la communication WDS. Le canal "auto" ne peut pas être utilisé.

Autres paramètres sans fil

Nom (SSID):

ITWORKS

Canal:

9

Options de sécurité:

Automatic

Retour

Terminer

Annuler

6.4.2 Configuration de la station de base centrale en mode WDS

Etape 1 Mettez l'appareil en mode Routeur.

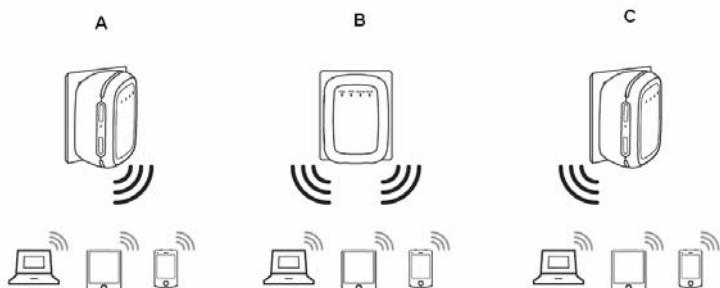
Etape 2 Allez dans **Paramètres sans fil > Fonction WDS**, choisissez **Activer la fonction WDS** puis tapez l'adresse MAC du répéteur (remarque: une même station de base peut se connecter à 4 répéteurs maximum).

Fonction WDS

<input type="checkbox"/> Activer la fonction WDS	
<input type="checkbox"/> Désactiver l'association de clients sans fil	
MAC sans fil de ce routeur: 00:1E:E3:4B:06:6C	
Station de base sans fil	
Adresse MAC du répéteur 1:	<input type="text"/>
Adresse MAC du répéteur 2:	<input type="text"/>
Adresse MAC du répéteur 3:	<input type="text"/>
Adresse MAC du répéteur 4:	<input type="text"/>

6.4.3 Application WDS

La figure ci-dessous montre le réseau sans fil du département des ressources humaines (A dans la figure), du département des finances (B) et du département marketing (C) dans une entreprise. Si les trois départements partagent un même routeur sans fil, les signaux recherchés par les ordinateurs risquent d'être plutôt faibles voire inexistants. Cependant, si chacun de ces trois départements utilise son propre routeur sans fil, la fonction WDS peut permettre de connecter ces trois routeurs afin de fournir une couverture sans fil parfaite pour la totalité des secteurs.



Pour configurer les trois routeurs, procédez de la manière suivante:

Le routeur sans fil B fonctionne comme station de base sans fil; les routeurs A et C se connectent au routeur B par WDS.

(1) Configuration du routeur sans fil B comme station de base sans fil

Etape 1 Connectez-vous à la page de gestion Web du routeur sans fil B. Allez dans **Paramètres sans fil > Paramètres de base sans fil** et définissez le SSID, le canal et les informations de cryptage sans fil. Notez quelque part le SSID, le canal et les informations de cryptage sans fil dont vous aurez besoin pour configurer les routeurs sans fil A et C.

Etape 2 Allez dans **Paramètres sans fil > Fonction WDS** et activez la fonction WDS. Tapez les adresses MAC des répéteurs (en l'occurrence, les routeurs sans fil A et C). Cliquez sur **Appliquer** pour sauvegarder les paramètres.

(2) Configuration du routeur sans fil A

Pour établir la connexion WDS entre les routeurs sans fil A et B, procédez de la manière suivante:

Etape 1 Paramétrez le routeur A avec le même canal et les mêmes informations de cryptage que le routeur B.

Etape 2 Allez dans **Paramètres sans fil > Fonction WDS** et activez la fonction WDS. Attribuez au routeur B une adresse IP différente de celle du routeur B afin d'éviter un conflit d'adresse IP (par exemple, changez l'adresse IP en 192.168.100.20 dans la page **Paramètres de l'interface LAN**, puis connectez-vous de nouveau à la page de gestion Web). Tapez l'adresse MAC de la station de base sans fil.

Etape 3 Cliquez sur **Appliquer** pour sauvegarder les paramètres. La connexion WDS est maintenant établie entre les routeurs A et B.

(3) Configuration du routeur sans fil C

Configurez le routeur C de la même manière que le routeur A. Veuillez noter que l'adresse IP de l'interface LAN doit au besoin être changée afin de ne pas entrer en conflit avec les adresses IP d'autres appareils ou ordinateurs déjà existants sur le réseau.

6.5 Configuration du mode client

Etape 1 Cliquez sur **Assistant de configuration** dans la barre de navigation située sur le panneau gauche de l'écran. Cliquez sur **Étude de sites** pour rechercher le réseau sans fil auquel vous souhaitez vous connecter.

Assistant de configuration

Étape 1: Cet assistant a pour but de vous aider à configurer le client sans fil. Cliquez sur "Étude de sites" pour étudier les sites sans fil quand le mode client est activé. Si un point d'accès ou un IBSS est trouvé, les résultats sont affichés dans la liste d'étude de sites trois secondes plus tard; vous pouvez faire en sorte que n'importe qui se connecte manuellement. Puis cliquez sur "Suivant".

Étude de sites

Nombre de sites scannés :32

#	SSID	BSSID	Chaîne	Signal	Cryptage	Sélectionner
1	LWCC	74:D0:2B:3A:6B:C0	11	100%	WPA2-PSK(AES)	<input type="radio"/>
2	TW-2B08	00:1F:A4:91:2A:60	9	100%	WPA-PSK(AES/TKIP)/ WPA2-PSK(AES/TKIP)	<input checked="" type="radio"/>
3	D-Link_DIR-815-5 G	00:0C:43:76:20:F8	11	96%	Jamais	<input type="radio"/>

Suivant

Étape 2 Tapez les informations de cryptage du réseau sans fil choisi. Cliquez sur **Terminer** pour confirmer les paramètres.

Assistant de configuration

Étape2: Vous devez configurer votre client sans fil manuellement, de manière à ce qu'il ait les mêmes paramètres de sécurité sans fil que le réseau choisi. Puis cliquez sur "Terminer".

Options de sécurité

Options de sécurité :

Jamais

Retour

Terminer

Annuler

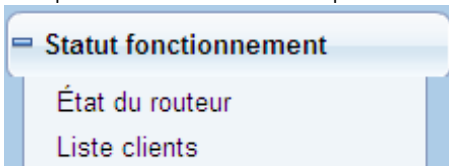
7 Configuration Web en mode pont

Remarque:

Mettez sur **AP** l'interrupteur à trois positions situé sur le panneau latéral, choisissez le **Mode pont** puis redémarrez l'appareil. Une fois l'appareil redémarré, connectez-vous à la page de configuration.

7.1 Statut fonctionnement

Cliquez sur **Statut fonctionnement** pour afficher le menu de navigation étendu.



Cliquez sur le sous-menu pour accéder à une page de configuration donnée.

7.1.1 État du routeur

Allez dans **Statut fonctionnement** > **Etat du routeur** pour accéder à la page **Etat du routeur**.

État du routeur

Infos système	
Version matériel	V1.0.0
Version micrologiciel	V1.0.0
Numéro de modèle	Wireless Router
Mode de travail	Mode routeur
Heure et date	1971-01-01 08:07:17
Port Internet	
Adresse MAC	00:1E:E3:4B:06:6D
Mode d'accès à Internet	Déconnecté(DHCP)
Adresse IP	0.0.0.0
Masque de sous-réseau IP	0.0.0.0
Passerelle par défaut	0.0.0.0
Serveur du nom de domaine	0.0.0.0
Port LAN	
Adresse MAC	00:1E:E3:4B:06:6C
Adresse IP	192.168.100.253
Masque de sous-réseau IP	255.255.255.0
Port sans fil	
Nom de réseau sans fil (SSID)	ITWORKS
Région	Europe
Canal sans fil	2.412GHz- CH1
Mode 802.11	802,11b/g/n mixte
Radio sans fil	Activé
Nom du diffuseur	ON
Isolation sans fil	OFF
Wi-Fi Protected Setup (WPS)	ON
Mode sécurité sans fil	Jamais

[Afficher les statistiques](#)[Statut connexion](#)

Sur cette page, vous trouverez des informations sur le statut de fonctionnement actuel de l'appareil (système, port LAN, réseau sans fil).

7.1.2 Liste clients

Allez dans **Statut fonctionnement** > **Liste clients** pour accéder à la page **Liste clients**.

Liste clients

Périphériques sans fil (les intrus apparaissent également ici)			
#	Adresse IP	Adresse MAC	Nom du périphérique
1	192.168.100.2	00:1F:A4:91:F2:0E	gl2217d

Actualiser

Sur cette page, vous trouverez des informations sur les ordinateurs connectés au routeur (adresse IP et adresse MAC de chacun des ordinateurs etc.).

7.2 Assistant de configuration

Pour la configuration, reportez-vous à la section **6.1 Configuration du mode pont**.

7.3 Réglage du mode

Cliquez sur **Réglage du mode** pour accéder à la page **Réglage du mode**.

Réglage du mode

Choisissez l'un des modes suivants:

Mode pont

Mode routeur

Dans ce mode, le port est utilisé comme port WAN.
Vous ne pouvez ouvrir votre session qu'en vous connectant au réseau correspondant à votre carte réseau sans fil.
Avant de passer à ce mode, veuillez mémoriser le SSID et les options de sécurité de votre réseau sans fil

Voir Configuration sans fil de base

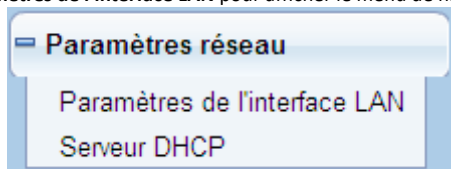
Appliquer

Annuler

- **Mode pont:** L'interface en question est une interface LAN. Les utilisateurs peuvent connecter l'appareil et le PC avec un câble RJ45 ou avec une carte réseau sans fil.
- **Mode routeur:** Les ordinateurs ne peuvent se connecter à l'appareil que par voie sans fil.

7.4 Paramètres réseau

Cliquez sur **Paramètres de l'interface LAN** pour afficher le menu de navigation étendu.



7.4.1 Paramètres de l'interface LAN

Allez dans **Paramètres réseau > Paramètres de l'interface LAN** pour accéder à la page des **Paramètres de l'interface LAN**.

Paramètres de l'interface LAN

Configuration TCP/IP LAN				
Adresse IP	<input type="text" value="192"/>	<input type="text" value="168"/>	<input type="text" value="100"/>	<input type="text" value="253"/>
Masque de sous-réseau IP	<input type="text" value="255"/>	<input type="text" value="255"/>	<input type="text" value="255"/>	<input type="text" value="0"/>

Vous pouvez maintenant modifier l'adresse IP et le masque de sous-réseau IP du port LAN selon les besoins.



Remarque:

Si vous changez l'adresse IP par défaut, vous devrez utiliser la nouvelle adresse IP pour vous connecter à la page de configuration Web du routeur, et la passerelle par défaut de tous les hôtes du réseau LAN devra être paramétrée sur la nouvelle adresse IP, afin de permettre l'accès à Internet.

Le masque de sous-réseau de tous les hôtes du réseau LAN doit être identique à celui spécifié sur la page des Paramètres de l'interface LAN.

7.4.2 Serveur DHCP

Allez dans **Paramètres réseau > Serveur DHCP** pour accéder à la page du **Serveur DHCP**. DHCP sont les initiales de Dynamic Host Configuration Protocol (protocole de configuration dynamique des hôtes). Si vous cochez la case **Utiliser le routeur comme serveur DHCP**, l'appareil attribue automatiquement les adresses IP aux ordinateurs du réseau LAN. Les utilisateurs n'ont alors pas besoin de configurer les paramètres du protocole TCP/IP comme l'adresse IP, le masque de sous-réseau, la passerelle et les informations du serveur DNS pour les ordinateurs connectés au réseau LAN du routeur.

Serveur DHCP

<input checked="" type="checkbox"/> Utiliser le routeur comme serveur DHCP	
Adresse IP de départ	<input type="text" value="192"/> <input type="text" value="168"/> <input type="text" value="100"/> <input type="text" value="2"/>
Adresse IP d'arrivée	<input type="text" value="192"/> <input type="text" value="168"/> <input type="text" value="100"/> <input type="text" value="200"/>
Durée d'autorisation DHCP (1-100 heures)	<input type="text" value="24"/>

7.4.2.1 Utilisation du routeur comme serveur DHCP

- **Utiliser le routeur comme serveur DHCP:** Si vous cochez la case **Utiliser le routeur comme serveur DHCP**, l'appareil prend la fonction de serveur DHCP et assigne automatiquement les adresses IP aux ordinateurs qui sont connectés à lui.
- **Adresse IP de départ/adresse IP d'arrivée:** Définissez des adresses IP de départ et d'arrivée si vous souhaitez spécifier un pool d'adresses devant être assignées par le serveur DHCP. Une fois définies l'**adresse IP de départ/adresse IP d'arrivée**, les hôtes du réseau LAN obtiendront des adresses IP situées entre l'adresse IP de départ et celle d'arrivée.

- **Durée d'autorisation DHCP:** Il s'agit de la durée de validité pour une adresse IP automatiquement attribuée par le serveur DHCP à un hôte. Le serveur DHCP ne peut pas attribuer une même adresse IP à d'autres hôtes pendant la durée spécifiée.

7.4.2.2 Réservez une adresse

Lorsque vous spécifiez une adresse IP réservée pour un ordinateur dans le réseau LAN, l'ordinateur en question reçoit toujours la même adresse IP chaque fois qu'il accède au serveur DHCP du routeur. Les adresses IP réservées doivent être attribuées aux ordinateurs ou aux serveurs nécessitant des paramètres IP permanents.

Réservation d'adresse			
#	Adresse IP	Nom du périphérique	Adresse MAC
<input type="button" value="Ajouter"/> <input type="button" value="Modifier"/> <input type="button" value="Supprimer"/>			

Pour réserver une adresse IP:

Etape 1 Cliquez sur **Ajouter** pour accéder à la page de **Réservation d'adresse**.

Réservation d'adresse

Tableau de réservation d'adresses				
	#	Adresse IP	Nom du périphérique	Adresse MAC
<input type="radio"/>	1			
<input type="radio"/>	2	192.168.100.2	Z2oYHjE3ZA==	00:1F:A4:91:F2:0E
Adresse IP		<input type="text"/>		
Adresse MAC		<input type="text"/>		
Nom du périphérique		<input type="text"/>		
<input type="button" value="Add"/> <input type="button" value="Cancel"/> <input type="button" value="Refresh"/>				

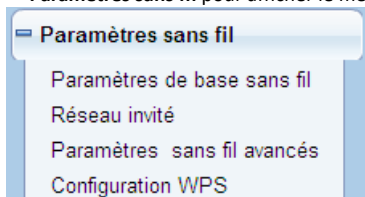
Etape 2 Choisissez dans le **Tableau de réservation d'adresses** l'adresse IP à attribuer à l'ordinateur ou au serveur, ou tapez l'adresse directement dans le champ **Adresse IP** (choisissez une adresse comprise dans le pool d'adresses que vous avez spécifié, par exemple 192.168.100.x). Tapez l'adresse MAC et le nom de périphérique de l'ordinateur ou du serveur.

Etape 3 Cliquez sur **Ajouter**; la nouvelle entrée est maintenant ajoutée dans **Réservation d'adresse**.

Etape 4 Cliquez sur **Appliquer** pour sauvegarder les paramètres.

7.5 Paramètres sans fil

Mettez sur **AP** l'interrupteur à trois positions situé sur le panneau latéral. Cliquez sur **Paramètres sans fil** pour afficher le menu de navigation étendu.



7.5.1 Paramètres de base sans fil

Allez dans **Paramètres sans fil** > **Paramètres de base sans fil** pour accéder à la page des **Paramètres de base sans fil**.

Paramètres de base sans fil

Sélection de région	
Région :	Europe ▼
Réseau sans fil	
<input checked="" type="checkbox"/> Activer la diffusion SSID	
<input type="checkbox"/> Activer l'isolation sans fil	
Nom (SSID) :	ITWORKS
Mode :	802.11b/g/n mixte ▼
Chaîne :	1 ▼
Bande passante :	Auto ▼
Options de sécurité	
Options de sécurité :	Jamais ▼

Appliquer Annuler

- **Région**: Sélectionnez la partie du monde dans laquelle vous vous trouvez.
- **Activer la diffusion SSID**: Si vous cochez cette case, le routeur diffusera son SSID dans le réseau sans fil. Les clients sans fil pourront alors scanner le SSID et s'en servir pour accéder au réseau sans fil.
- **Activer l'isolation sans fil**: Si vous cochez cette case, les clients sans fil connectés au réseau d'un même SSID pourront accéder à Internet mais ne pourront pas communiquer entre eux.
- **Nom (SSID)**: Définissez le nom du réseau sans fil. Le SSID peut contenir jusqu'à 32 caractères (lettres, chiffres ou tirets bas, seuls ou mélangés). Le SSID prend en compte les majuscules.
- **Mode**: Choisissez le mode sans fil. Il est conseillé d'utiliser le mode **802.11b/g/n mixte**.
- **Chaîne**: La chaîne permettant de transmettre les signaux sans fil. Le réglage par défaut est **Auto**. Avec le réglage **Auto**, l'appareil choisit automatiquement la meilleure chaîne parmi celles disponibles, selon la situation actuelle.
- **Bande passante**: Bande passante occupée pour la transmission du signal sans fil.
- **Débit de transmission max.:** Débit de transmission maximum du répéteur.
- **Options de sécurité**: Définissez le cryptage de sécurité du réseau sans fil afin d'empêcher toute possibilité d'accès et d'écoute non autorisés.

Options de sécurité

– Jamais

Aucun cryptage des données du réseau, qui n'est donc pas protégé. N'importe quelle station peut alors accéder au réseau. Cette option n'est pas conseillée.

Options de sécurité	
Options de sécurité :	Jamais ▼
<input type="button" value="Appliquer"/> <input type="button" value="Annuler"/>	

– WEP

Wired Equivalent Privacy; vous pouvez régler le cryptage des données sur 64 ou 128 bits.

Options de sécurité	
Options de sécurité :	WEP ▼
Cryptage de sécurité (WEP)	
Type d'authentification :	Automatique ▼
Type de cryptage :	ASCII ▼
Niveau de cryptage :	64 bits ▼
Clé de cryptage de sécurité (WEP)	
Clé 1: <input checked="" type="radio"/>	<input type="text"/> (5 caractères ASCII)
Clé 2: <input type="radio"/>	<input type="text"/> (5 caractères ASCII)
Clé 3: <input type="radio"/>	<input type="text"/> (5 caractères ASCII)
Clé 4: <input type="radio"/>	<input type="text"/> (5 caractères ASCII)

- **Type d'authentification:** Choisissez le type d'authentification pour le système. Trois types d'authentification sont possibles: Automatique, Ouverte et Clés partagées.
 - **Automatique:** Avec ce réglage, le routeur choisit lui-même le type d'authentification **Ouverte** ou à **Clés partagées** selon la requête de l'hôte.
 - **Ouverte:** Avec ce réglage, les hôtes du réseau sans fil peuvent ignorer l'authentification et se connecter au réseau sans mot de passe. Cependant, le mot de passe sera toujours requis pour transmettre des données.
 - **Clés partagées:** Avec ce réglage, les hôtes du réseau sans fil ont besoin de saisir le mot de passe correct pour passer l'authentification. Faute de quoi, ils ne peuvent pas accéder au réseau.
- **Type de cryptage:** Type de clé à utiliser. Le code peut contenir des caractères ASCII ou hexadécimaux.
 - **Hexadécimaux:** Les caractères valides pour les clés sont les chiffres de 0 à 9 et les lettres de A à F.
 - **ASCII:** N'importe quel caractère du clavier est valide pour les clés.
- **Niveau de cryptage:** Le niveau de cryptage détermine la longueur de la clé.
 - Si le **niveau de cryptage** est réglé à **64 bits**, tapez 10 caractères hexadécimaux ou 5 caractères ASCII.

- Si le **niveau de cryptage** est réglé à **128 bits**, tapez 26 caractères hexadécimaux ou 13 caractères ASCII.

- **Clé 1/2/3/4**: Définissez la clé selon le type et le niveau de cryptage choisis.

- **WPA-PSK[TKIP] ou WPA2-PSK[TKIP]**

WPA-PSK: Accès Wi-Fi protégé avec clé pré-partagée

WPA2-PSK: Accès Wi-Fi protégé version 2 avec clé pré-partagée

TKIP: Temporal Key Integrity Protocol (protocole d'intégrité par clé temporaire)

Veuillez noter que le mode 802.11n n'est pas compatible avec l'algorithme TKIP.

Options de sécurité	
Options de sécurité :	WPA-PSK[TKIP]
Options de sécurité (WPA-PSK)	
Mot de passe :	(8-63 caractères ou 64 caractères hexadécimaux)

- **Mot de passe**: Tapez 8 à 63 caractères ASCII ou 64 caractères hexadécimaux.

- **WPA-PSK[AES] ou WPA2-PSK[AES]**

WPA-PSK: Accès Wi-Fi protégé avec clé pré-partagée.

WPA2-PSK: Accès Wi-Fi protégé version 2 avec clé pré-partagée.

AES: Advanced Encryption Standard (standard de chiffrement avancé)

Options de sécurité	
Options de sécurité :	WPA-PSK[AES]
Options de sécurité (WPA-PSK)	
Mot de passe :	(8-63 caractères ou 64 caractères hexadécimaux)

- **Mot de passe**: Tapez 8 à 63 caractères ASCII ou 64 caractères hexadécimaux.

- **WPA-PSK/WPA2-PSK+[TKIP]/[AES]**

Le client a le droit d'utiliser l'une de ces deux options: WPA-PSK[TKIP]/[AES] ou

WPA2-PSK[TKIP]/[AES].

Options de sécurité	
Options de sécurité :	WPA-PSK/WPA2-PSK+[TKIP]/[AES]
Options de sécurité (WPA-PSK+WPA2-PSK)	
Mot de passe :	(8-63 caractères ou 64 caractères hexadécimaux)

- **Mot de passe**: Tapez 8 à 63 caractères ASCII ou 64 caractères hexadécimaux.



Remarque:

Une fois terminée la configuration des paramètres sans fil de l'appareil, seuls les hôtes ayant les mêmes paramètres sans fil (ex: le SSID) que l'appareil pourront s'y connecter. Si vous configurez des paramètres de sécurité pour l'appareil, seuls les hôtes ayant les mêmes paramètres de sécurité (ex: le mot de passe) que l'appareil pourront s'y connecter.

7.5.2 Réseau invité

Si vous ne souhaitez pas que les visiteurs connaissent votre clé de sécurité sans fil, vous pouvez utiliser le réseau invité pour leur permettre d'utiliser votre Internet sans les laisser connaître le mot de passe de votre connexion sans fil.

Allez dans **Paramètres sans fil > Réseau invité** pour accéder à la page du **Réseau invité**.

Réseau invité

Profils réseau					
	Régime	SSID	Sécurité	Appliquer	Diffusion SSID
<input checked="" type="radio"/>	1	PocketAP-002	None	NON	OUI
<input type="radio"/>	2	PocketAP-003	None	NON	OUI
<input type="radio"/>	3	PocketAP-004	None	NON	OUI
<input type="radio"/>	4	PocketAP-005	None	NON	OUI

Paramètres sans fil-- Profil1

Activer le réseau invité

Activer la diffusion SSID

Autoriser un invité à accéder à mon réseau local

Activer l'isolation sans fil

Nom de réseau sans fil invité (SSID):

Options de sécurité-- Profil1

Options de sécurité:

- **Profils réseau:** Brève description du réseau invité créé. Vous pouvez créer jusqu'à quatre réseaux invités. Un profil réseau contient le SSID, le mode de cryptage et les options d'utilisation du réseau invité et de diffusion du SSID. Pour afficher les détails d'un profil ou en modifier les paramètres, cliquez sur le bouton radio correspondant.
- **Activer le réseau invité:** Si vous cochez cette case, aussi bien vous que les visiteurs pourrez vous connecter au réseau en utilisant le SSID du réseau invité.
- **Activer la diffusion SSID:** Si vous cochez cette case, l'appareil diffusera son SSID à toutes les stations sans fil.
- **Autoriser un invité à accéder à mon réseau local:** Si vous cochez cette case, les visiteurs utilisant le SSID d'un réseau invité auront accès non seulement à Internet mais également au réseau LAN de l'appareil, comme les utilisateurs du SSID primaire du réseau. Si vous ne cochez pas cette case, les visiteurs utilisant le SSID d'un réseau invité n'auront pas accès au réseau LAN de l'appareil.
- **Activer l'isolation sans fil:** Si vous cochez cette case, les clients sans fil connectés au réseau invité d'un même SSID pourront accéder à Internet mais ne pourront pas communiquer entre eux.
- **Nom de réseau sans fil invité (SSID):** Définissez le nom du réseau invité.
- **Options de sécurité:** Reportez-vous aux options de sécurité décrites dans la section **8.5.2 Paramètres de base sans fil**.

Une fois les paramètres réglés, cliquez sur **Appliquer** pour les sauvegarder.

7.5.3 Paramètres sans fil avancés

Allez dans **Paramètres sans fil > Paramètres sans fil avancés** pour accéder à la page des **Paramètres de base sans fil avancés**.

Paramètres sans fil avancés

Paramètres sans fil avancés	
<input checked="" type="checkbox"/> Activer la radio du routeur sans fil	
Longueur de fragmentation (256-2346)	<input type="text" value="2346"/>
DTIM (1-255)	<input type="text" value="1"/>
Intervalle de balise (20-1000)	<input type="text" value="100"/>
Clients MAX (0-12)	<input type="text" value="0"/>
Seuil CTS/RTS (1-2347)	<input type="text" value="2346"/>
Mode préambule	<input type="text" value="Préambule long"/>
Intervalle de garde	<input type="text" value="Intervalle de garde court"/>
Commande de Puissance de Transmission	<input type="text" value="100%"/>
Paramètres WPS	
PIN routeur	<input type="text" value="12345670"/>
<input checked="" type="checkbox"/> Activer WPS <input type="checkbox"/> Désactiver le PIN pour le routeur	
Liste d'accès par carte sans fil	
<input type="button" value="Configuration de la liste d'accès"/>	
<input type="button" value="Appliquer"/> <input type="button" value="Annuler"/>	

- **Activer la radio du routeur sans fil:** Si vous désactivez la radio du routeur sans fil, les appareils sans fil ne pourront pas se connecter au répéteur. Si vous avez l'intention de laisser votre réseau sans fil inutilisé pendant un certain temps, vous pouvez décocher cette case et désactiver toute la connectivité sans fil.
- **Longueur de fragmentation (256-2346):** Définissez le seuil de la longueur de fragmentation. Si la longueur d'un paquet dépasse la valeur définie, ce paquet sera automatiquement fragmenté en plusieurs paquets. La valeur de la **longueur de fragmentation** ne doit pas être trop petite car un nombre trop important de paquets aurait pour effet de réduire la performance du réseau sans fil. La valeur par défaut est 2346.
- **DTIM (1-255):** Définissez l'intervalle d'envoi des trames DTIM.
- **Intervalle de balise (20-1000):** L'intervalle de balise correspondant à la fréquence d'envoi des trames de balise. Définissez l'intervalle d'envoi des trames de balise. L'unité est la milliseconde (ms). Le réglage par défaut est 100 ms.
- **Clients MAX (0-12):** Définissez le nombre maximum de clients. 0 signifie que le nombre de clients connectés n'est pas limité.
- **Seuil CTS/RTS (1-2347):** Définissez le seuil CTS/RTS. Si la longueur d'un paquet dépasse la valeur RTS spécifiée, le répéteur envoie une trame RTS à la station de destination pour négocier. Après avoir reçu une trame RTS, la station sans fil répond en envoyant une trame CTS (clear to send) au répéteur, signifiant qu'ils peuvent communiquer.

- **Mode préambule:** Un préambule (notamment le champ **802.11b High Rate/DSSS PHY**; champ synchronisé à 56 chiffres pour préambule court) définit la longueur du bloc de correction CRC pour la communication entre les appareils sans fil. Dans un réseau à trafic intense, un préambule court est préférable. Il permet d'améliorer l'efficacité d'un réseau sans fil devant faire face à des applications à haute exigence de temps réel comme par exemple la vidéo en streaming et la téléphonie voix sur IP.
- **Intervalle de garde:**
 - Intervalle de garde court: L'intervalle est de 400 ns. Lorsque l'intervalle court est activé, le répéteur peut recevoir et envoyer des paquets à intervalles courts. Cela permet d'améliorer le débit de transmission du répéteur.
 - Intervalle de garde long: L'intervalle est de 800 ns.
- **Commande de Puissance de Transmission:** Définissez la puissance de transmission du réseau sans fil. Il est conseillé d'utiliser le réglage par défaut, à savoir **100%**.
- **PIN routeur:** Afficher le code PIN à utiliser pour le client sans fil lorsque les paramètres sans fil du routeur sont configurés par WPS.
- **Activer WPS:** Les fonctions de la page **Configuration WPS** ne sont disponibles que si la case **Activer WPS** a été cochée. Si la case n'est pas cochée, le menu **Configuration WPS** est grisé.
- **Désactiver le PIN pour le routeur:** La fonction mode PIN de la page **Configuration WPS** n'est disponible que si la case **Désactiver le PIN pour le routeur** n'est pas cochée. Si cette case est cochée, l'option mode PIN n'est pas disponible.

Limiter l'accès sans fil par adresse MAC

Si une liste d'accès par carte sans fil est configurée et activée, le routeur vérifie l'adresse MAC de n'importe quel périphérique sans fil qui tente de se connecter, et n'autorise que les ordinateurs identifiés dans la liste des ordinateurs approuvés.

L'adresse MAC est l'adresse physique unique à 12 caractères d'un appareil du réseau, composée des caractères hexadécimaux 0-9, a-f, ou A-F seulement. Le format de l'adresse MAC est le suivant: XX:XX:XX:XX:XX:XX.

Pour limiter l'accès sans fil par adresse MAC:

Etape 1 Dans **Paramètres sans fil avancés**, cliquez sur **Configuration de la liste d'accès** pour accéder à la page **Liste d'accès par carte sans fil**.



Liste d'accès par carte sans fil

<input type="checkbox"/> Activer le contrôle d'accès	
Nom du périphérique	Adresse Mac
<input type="button" value="Ajouter"/> <input type="button" value="Modifier"/> <input type="button" value="Supprimer"/>	
<input type="button" value="Appliquer"/> <input type="button" value="Annuler"/>	

Etape 2 Cliquez sur **Ajouter** pour ajouter un périphérique sans fil à la liste de contrôle de l'accès sans fil. La page **Configuration d'accès par carte sans fil** s'affiche.

Configuration d'accès par carte sans fil

Cartes sans fil disponibles	
Nom du périphérique	Adresse Mac
Entrée carte sans fil (nombre max. de termes: 16)	
Nom du périphérique	<input type="text"/>
Adresse Mac	<input type="text"/>
<input type="button" value="Ajouter"/> <input type="button" value="Annuler"/> <input type="button" value="Actualiser"/>	

Etape 3 Si l'ordinateur recherché figure dans la liste **Cartes sans fil disponibles**, il vous suffit de cliquer sur le bouton radio de cet ordinateur pour obtenir son adresse MAC. Sinon, vous pouvez saisir manuellement le nom et l'adresse MAC de l'ordinateur à autoriser. En général, l'adresse MAC figure sur une étiquette collée sous le périphérique sans fil.

Etape 4 Cliquez sur **Ajouter** pour ajouter ce périphérique sans fil à la liste d'accès par carte sans fil. L'écran passe à la page de la liste.

Etape 5 Cochez la case **Activer le contrôle d'accès**. Une fois cette case cochée, vous pouvez limiter l'accès des PC au réseau sans fil, en n'autorisant que certains PC selon leur adresse MAC.

Etape 6 Cliquez sur Appliquer pour sauvegarder les paramètres de votre **Liste d'accès par carte sans fil**.

Désormais, seuls les périphériques de cette liste pourront se connecter sans fil au répéteur.

7.5.4 Configuration WPS

Allez dans **Paramètres sans fil > Configuration WPS**; la page ci-dessous s'affiche.

Configuration WPS

Nouveau moyen simple pour se connecter au routeur sans fil via WiFi Protected setup (WPS)

Un client sans fil doit accepter la fonctionnalité WPS pour pouvoir utiliser cet assistant d'ajout de clients sur votre routeur sans fil WPS. Reportez-vous au mode d'emploi ou à l'emballage de votre client sans fil pour vérifier s'il accepte ou non la fonctionnalité WPS. Si votre client sans fil n'accepte pas la fonctionnalité WPS, vous devrez le configurer manuellement afin qu'il ait le même SSID et les mêmes paramètres de sécurité que ceux du routeur.

Suivant

WPS signifie Wi-Fi Protected Setup (configuration protégée par Wi-Fi).

La fonctionnalité WPS permet d'établir une connexion sans fil de manière simple et rapide si le terminal ou le point d'accès de liaison montante (ex: l'adaptateur réseau) possèdent la fonctionnalité WPS. Il est conseillé de configurer d'abord le cryptage sans fil pour le point d'accès de liaison montante. Si vous changez le mode de cryptage sans fil après avoir établi la connexion par WPS, vous devrez utiliser la fonctionnalité WPS pour rétablir la connexion sans fil. Veuillez noter que si le client sans fil n'accepte pas la fonctionnalité WPS, vous devrez configurer manuellement le client sans fil (ex: SSID, mode de sécurité, mot de passe) afin qu'il ait le même SSID et les mêmes paramètres de sécurité sans fil que le routeur.

Cliquez sur Suivant pour accéder à la page de **Configuration WPS**. La section suivante explique comment configurer la fonctionnalité WPS pour le mode point d'accès.

7.5.4.1 Avec le bouton WPS

En mode point d'accès avec le WDS désactivé, appuyez sur le bouton **WPS** situé sur le panneau latéral de l'appareil, et sur le bouton **WPS** du périphérique client. L'appareil peut effectuer une connexion cryptée par WPS vers le périphérique client en aval.

7.5.4.2 Avec la page Web

Vous pouvez configurer les paramètres WPS en utilisant la page Web prévue à cet effet. Allez dans **Paramètres sans fil > Configuration WPS** pour accéder à la page **Configuration WPS**.

- Bouton-poussoir

Etape 1 Cochez la case **Bouton-poussoir** et cliquez sur **Start PBC**. La connexion cryptée par WPS commence.

Configuration WPS

Choisissez une méthode de configuration pour le point d'accès:

Bouton-poussoir (recommandé)

Vous pouvez soit appuyer manuellement sur le bouton-poussoir du routeur, soit appuyer sur la touche tactile ci-dessous.

Start PBC

PIN (code d'identification personnelle)

Etape 2 Appuyez sur la touche **WPS** de l'adaptateur réseau ou cliquez sur **PBC** dans l'outil de configuration de l'adaptateur réseau dans les 2 minutes qui suivent. Une fois établie la connexion WPS, la page suivante apparaît, indiquant que la connexion WPS a réussi.

Succès!

Le client sans fil vient d'être ajouté au réseau avec succès.
Cliquez sur OK pour revenir à la page de configuration Wi-Fi sécurisée.

OK

- Mode PIN

Etape 1 Cochez **PIN**, tapez le code PIN de l'adaptateur réseau (réf. client de l'adaptateur réseau) puis cliquez sur **Start PIN** pour lancer la connexion WPS.

Configuration WPS

Choisissez une méthode de configuration pour le point d'accès:

Bouton-poussoir (recommandé)

PIN (code d'identification personnelle)

Si votre adaptateur est compatible avec WPS, cliquez sur "Créer un code PIN client de sécurité pour entrer dans le point d'accès, le routeur ou la passerelle", puis entrez ce code PIN client créé.

Saisissez le code PIN client:

Etape 2 Cliquez sur la touche PIN de l'adaptateur réseau dans les 2 minutes pour lancer la connexion WPS. Une fois établie la connexion WPS, la page suivante apparaît, indiquant que la connexion WPS a réussi.

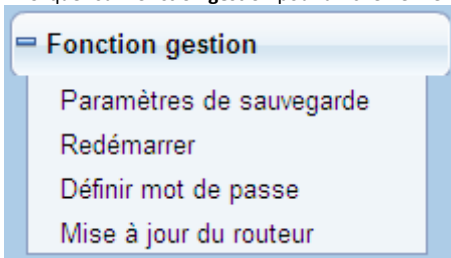
Succès!

Le client sans fil vient d'être ajouté au réseau avec succès.
Cliquez sur OK pour revenir à la page de configuration Wi-Fi sécurisée.

OK

7.6 Fonction gestion

Cliquez sur **Fonction gestion** pour afficher le menu de navigation étendu.



7.6.1 Paramètres de sauvegarde

Allez dans **Fonction gestion** > **Paramètres de sauvegarde** pour accéder à la page **Paramètres de sauvegarde**.

Paramètres de sauvegarde

Sauvegarder une copie des paramètres actuels	
<input type="text"/>	<input type="button" value="Sauvegarder"/>
Restaurer les paramètres sauvegardés à partir d'un fichier	
<input type="text"/>	<input type="button" value="Parcourir..."/>
	<input type="button" value="Réinitialiser"/>
Rétablir tous les paramètres par défaut	
	<input type="button" value="Effacer"/>

Sur cette page, vous pouvez exporter les informations de configuration du routeur vers l'ordinateur sous format XML pour les utiliser ultérieurement, importer un fichier de configuration nouveau ou sauvegardé auparavant, ou encore restaurer tous les paramètres par défaut du routeur.

- Sauvegarder

Cliquez sur **Sauvegarder** pour sauvegarder les informations de configuration du routeur en tant que fichier local.



Remarque:

Avant de sauvegarder votre fichier de configuration, rétablissez le mot de passe d'administrateur par défaut (admin) au cas où vous oublieriez votre mot de passe. Puis changez-le à nouveau une fois le fichier de configuration sauvegardé. Si vous oubliez votre mot de passe, vous serez obligé de rétablir les paramètres de configuration par défaut.

- Restaurer

Dans la page **Paramètres de sauvegarde**, les options Sauvegarder et Restaurer vous permettent de sauvegarder ou de restaurer un fichier contenant les paramètres de configuration de votre routeur.

Cliquez sur **Parcourir...** pour rechercher le fichier de configuration restauré dans votre ordinateur, puis cliquez sur **Restaurer** pour charger le fichier dans le routeur.

- Effacer

Dans certaines circonstances (par exemple, si vous déplacez le routeur vers un réseau différent ou si vous avez oublié le mot de passe), il peut être utile d'effacer la configuration et de restaurer les paramètres par défaut.

Cliquez sur **Effacer** pour rétablir tous les paramètres par défaut du routeur. Cette manipulation a les mêmes effets que l'appui long sur la touche **Reset** (réinitialisation) du panneau latéral pendant 3-6 secondes.

7.6.2 Redémarrer

Allez dans **Fonction gestion** > **Redémarrer** pour accéder à la page **Redémarrer**.

Redémarrer

Redémarrer	
	<input type="button" value="Redémarrer"/>

Cliquez sur **Redémarrer** pour redémarrer le routeur. Une fois le routeur redémarré, le système affiche la page de connexion.

7.6.3 Définir mot de passe

Allez dans **Fonction gestion** > **Définir mot de passe** pour accéder à la page **Définir mot de passe**.

Définir mot de passe

Définir mot de passe	
Ancien mot de passe	<input type="text"/>
Définir mot de passe	<input type="text"/>
Confirmer nouveau mot de passe	<input type="text"/>
<input type="button" value="Appliquer"/> <input type="button" value="Annuler"/>	

Sur cette page, vous pouvez changer le mot de passe d'ouverture de session.



Remarque:

Pour des raisons de sécurité, il est fortement recommandé de changer le mot de passe d'administrateur par défaut. Si vous oubliez le mot de passe, vous pouvez restaurer les paramètres par défaut du routeur. Le mot de passe par défaut est admin.

7.6.4 Mise à jour du routeur

Allez dans **Fonction gestion** > **Mise à jour du routeur** pour accéder à la page **Mise à jour du routeur**.

Mise à jour du routeur

Repérer et sélectionner le fichier de mise à jour à partir du disque dur:

Parcourir... Effacer config

Téléverser

Annuler

Suivez la procédure ci-dessus pour mettre à jour le logiciel du routeur.

Etape 1 Cliquez sur **Parcourir...** pour retrouver le dernier logiciel.

Etape 2 Choisissez le fichier de mise à jour qui convient. Si vous cochez la case **Effacer config**, le routeur rétablira les paramètres par défaut après chaque mise à jour. Si vous ne cochez pas cette case, les paramètres actuels resteront inchangés.

Etape 3 Cliquez sur **Téléverser** pour lancer la mise à jour.

Une fois la mise à jour terminée, le routeur redémarre automatiquement.



Remarque:

Après la mise à jour du logiciel, les paramètres par défaut de l'appareil sont restaurés. N'oubliez pas de sauvegarder les paramètres avant de mettre à jour le logiciel, pour le cas où les informations de la configuration précédente seraient perdues.

N'éteignez pas le routeur pendant que la mise à jour est en cours.

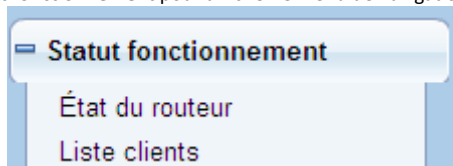
8 Configuration Web en mode routeur

Remarque:

Mettez sur **AP** l'interrupteur à trois positions situé sur le panneau latéral, choisissez le **Mode routeur** puis redémarrez l'appareil. Une fois l'appareil redémarré, connectez-vous à la page de configuration.

8.1 Statut fonctionnement

Cliquez sur **Statut fonctionnement** pour afficher le menu de navigation étendu.



8.1.1 État du routeur

Allez dans **Statut fonctionnement > Statut routeur** pour accéder à la page **Statut routeur**.

État du routeur

Infos système	
Version matériel	V1.0.0
Version micrologiciel	V1.0.0
Numéro de modèle	Wireless Router
Mode de travail	Mode routeur
Heure et date	1971-01-01 08:03:14
Port Internet	
Adresse MAC	00:1E:E3:4B:06:6D
Mode d'accès à Internet	Déconnecté(DHCP)
Adresse IP	0.0.0.0
Masque de sous-réseau IP	0.0.0.0
Passerelle par défaut	0.0.0.0
Serveur du nom de domaine	0.0.0.0
Port LAN	
Adresse MAC	00:1E:E3:4B:06:6C
Adresse IP	192.168.100.253
Masque de sous-réseau IP	255.255.255.0
Port sans fil	
Nom de réseau sans fil (SSID)	ITWORKS
Région	Europe
Canal sans fil	2.412GHz- CH1
Mode 802.11	802.11b/g/n mixte
Radio sans fil	Activé
Nom du diffuseur	ON
Isolation sans fil	OFF
Wi-Fi Protected Setup (WPS)	ON
Mode sécurité sans fil	Jamais

Afficher les statistiques

Statut connexion

Sur cette page, vous trouverez des informations sur le statut de fonctionnement actuel de l'appareil (système, connexion du port Internet, port LAN, réseau sans fil).

Cliquez sur **Afficher les statistiques**; la page **Infos statistiques** ci-dessous apparaît.

Infos statistiques

Port	Statut	TxPkts	RxPkts	Collisions	Tx B/s	Rx B/s	Temps d'activité
WAN	100M/Full	175	1104	0	102702	141941	00:18:35
WLAN	Auto	16508	89367	0	14280719	18854046	00:18:29
Temps d'activité système		00:18:44					
Intervalle Poll							
<input type="text" value="5"/>	(1-86400 s)	<input type="button" value="Régler intervalle"/>	<input type="button" value="Arrêt"/>				

Sur cette page, vous trouverez les statistiques de fonctionnement de l'appareil, avec notamment les nombres de paquets envoyés et reçus par chaque port.

- **Régler intervalle:** Permet de régler l'intervalle pour les statistiques de trafic.
- **Arrêt:** Si vous cliquez sur ce bouton, la page affichera toujours les statistiques mises à jour la dernière fois et qui ne sont plus mises à jour.

Dans la page **État du routeur**, cliquez sur **Statut connexion** pour accéder à la page **Statut connexion**. Cette page contient les informations actualisées sur la connexion.

L'exemple ci-dessous est celui de la connexion WAN en DHCP.

Statut connexion

Adresse IP	0.0.0.0
Masque de sous-réseau	0.0.0.0
Passerelle par défaut	0.0.0.0
Serveur DHCP	0.0.0.0
Serveur DNS	0.0.0.0
Obtention d'autorisation	0Jour,0Heures,0Minutes
Expiration d'autorisation	0Jour,0Heures,0Minutes

- **Libérer:** Cliquez sur ce bouton pour envoyer une requête à l'ISP pour libérer l'adresse IP, le masque de sous-réseau, la passerelle par défaut et les paramètres du serveur DNS.
- **Renouveler:** Cliquez sur ce bouton pour obtenir de manière dynamique une adresse IP, un masque de sous-réseau, une passerelle par défaut et les paramètres du serveur DNS de la part de l'ISP. Ces informations apparaîtront sur cette page.

Pour les détails des modes de connexion WAN, veuillez vous référer à la section **8.4.2 Paramètres de l'interface WAN**.

8.1.2 Liste clients

Allez dans **Statut fonctionnement > Liste clients** pour accéder à la page **Liste clients**.

Liste clients

Périphériques sans fil (les intrus apparaissent également ici)			
#	Adresse IP	Adresse MAC	Nom du périphérique
1	192.168.100.2	00:1F:A4:91:F2:0E	gl2217d

Actualiser

Sur cette page, vous trouverez des informations sur les ordinateurs connectés à l'appareil (adresse IP et adresse MAC de chacun des ordinateurs etc.).

8.2 Assistant de configuration

Pour la configuration, reportez-vous à la section **6.2 Configuration du mode routeur**.

8.3 Réglage du mode

Cliquez sur **Réglage du mode** pour accéder à la page **Réglage du mode**.

Réglage du mode

Choisissez l'un des modes suivants:

Mode pont

Mode routeur

Dans ce mode, le port est utilisé comme port WAN.
Vous ne pouvez ouvrir votre session qu'en vous connectant au réseau correspondant à votre carte réseau sans fil.
Avant de passer à ce mode, veuillez mémoriser le SSID et les options de sécurité de votre réseau sans fil

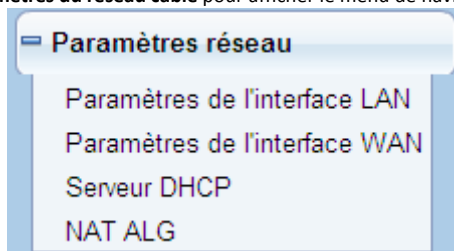
Voir Configuration sans fil de base

Appliquer Annuler

- **Mode pont:** L'interface en question est une interface LAN. Les utilisateurs peuvent connecter l'appareil et le PC avec un câble RJ45 ou avec une carte réseau sans fil.
- **Mode routeur:** Les ordinateurs ne peuvent se connecter à l'appareil que par voie sans fil.

8.4 Paramètres réseau

Cliquez sur **Paramètres du réseau câblé** pour afficher le menu de navigation étendu.



8.4.1 Paramètres de l'interface LAN

Pour plus de détails, reportez-vous à la section **7.4.1 Paramètres de l'interface LAN**.

8.4.2 Paramètres de l'interface WAN

Allez dans **Paramètres réseau > Paramètres de l'interface WAN** pour accéder à la page des **Paramètres de l'interface WAN**.

Le routeur accepte 5 modes de connexion WAN: **IP dynamique (DHCP)**, **IP statique**, **PPPoE**, **PPTP** et **L2TP**. Choisissez la connexion WAN à utiliser. Si vous ne savez pas quel est votre mode de connexion WAN, contactez votre ISP.

(1) IP dynamique (DHCP)

Si vous choisissez l'option IP dynamique (DHCP), l'appareil obtient automatiquement l'adresse IP de la part de l'ISP. Choisissez DHCP si l'ISP ne fournit aucun paramètre de réseau IP. Voir ci-dessous:

Paramètres de l'interface WAN

Votre connexion Internet nécessite-t-elle un login?	<input type="radio"/> Oui <input checked="" type="radio"/> Non
Nom de compte (si nécessaire)	<input type="text"/>
Adresse IP Internet	
<input checked="" type="radio"/> Obtention dynamique sur ISP	
<input type="radio"/> Utiliser une adresse IP statique	
Adresse IP	<input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/>
Masque de sous-réseau IP	<input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/>
Adresse IP de la passerelle	<input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/>
Adresse du serveur de nom de domaine (DNS)	
<input checked="" type="radio"/> Obtention automatique sur ISP	
<input type="radio"/> Utiliser ces serveurs DNS	
DNS primaire	<input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/>
DNS secondaire	<input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/>
Réglage MTU	
Taille MTU(616-1500 bytes)	<input type="text" value="1500"/>
Adresse MAC routeur	
<input checked="" type="radio"/> Utiliser l'adresse par défaut	
<input type="radio"/> Utiliser l'adresse MAC de l'ordinateur	
<input type="radio"/> Utiliser cette adresse MAC	<input type="text" value="00:1E:E3:4B:06:6D"/>

Appliquer

Annuler

- **Nom de compte:** Le nom de compte est fourni par votre ISP. S'il n'est pas fourni par votre ISP, vous pouvez laisser cette case vide.
- **Adresse du serveur de nom de domaine (DNS):** Cochez la case **Utiliser ces serveurs DNS** si vous savez que votre ISP ne transmet pas automatiquement les adresses DNS au routeur au moment de l'ouverture de session. Puis tapez l'adresse IP du serveur DNS primaire de votre ISP. Le cas échéant, tapez également l'adresse du serveur DNS secondaire.
- **Taille MTU:** Permet de définir l'unité de transmission maximale. Il est conseillé de garder la valeur par défaut.
- **Adresse MAC du routeur:** Adresse physique du routeur.
 - De manière générale, choisissez **Utiliser l'adresse par défaut**.
 - Si l'ISP nécessite l'authentification de l'adresse MAC, cochez la case **Utiliser l'adresse MAC de l'ordinateur** ou **Utiliser cette adresse MAC**. Si vous cochez la case **Utiliser l'adresse MAC de l'ordinateur**, l'adresse MAC de l'ordinateur actuel servira d'adresse MAC pour le routeur. Si vous cochez la case **Utiliser cette adresse MAC**, vous devrez taper l'adresse MAC d'un autre ordinateur. Le format requis pour l'adresse MAC est XX:XX:XX:XX:XX:XX.

Une fois les paramètres réglés, cliquez sur **Appliquer** pour les sauvegarder.

(2) IP statique

Si l'adresse IP, le masque de sous-réseau et les informations de la passerelle et du serveur DNS sont fournis par l'ISP, choisissez l'option IP statique. Si vous ne connaissez pas ces informations, contactez votre ISP.

Paramètres de l'interface WAN

Votre connexion Internet nécessite-t-elle un login?	<input type="radio"/> Oui <input checked="" type="radio"/> Non
Nom de compte (si nécessaire)	<input type="text"/>
Adresse IP Internet	
<input type="radio"/> Obtention dynamique sur ISP	
<input checked="" type="radio"/> Utiliser une adresse IP statique	
Adresse IP	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>
Masque de sous-réseau IP	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>
Adresse IP de la passerelle	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>
Adresse du serveur de nom de domaine (DNS)	
<input type="radio"/> Obtention automatique sur ISP	
<input checked="" type="radio"/> Utiliser ces serveurs DNS	
DNS primaire	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>
DNS secondaire	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>
Réglage MTU	
Taille MTU(616-1500 bytes)	<input type="text" value="1500"/>
Adresse MAC routeur	
<input checked="" type="radio"/> Utiliser l'adresse par défaut	
<input type="radio"/> Utiliser l'adresse MAC de l'ordinateur	
<input type="radio"/> Utiliser cette adresse MAC	<input type="text" value="00:1E:E3:4B:06:6D"/>

Appliquer

Annuler

- **Nom de compte:** Le nom de compte est fourni par votre ISP. S'il n'est pas fourni par votre ISP, vous pouvez laisser cette case vide.
- **Adresse IP:** Tapez l'adresse IP WAN fournie par l'ISP. Ce paramètre est obligatoire.
- **Masque de sous-réseau IP:** Tapez le masque de sous-réseau WAN fourni par l'ISP. Celui-ci dépend du type de réseau. Il est en général le suivant: 255.255.255.0 (classe C).
- **Adresse IP de la passerelle:** Tapez l'adresse IP de la passerelle, fournie par l'ISP. Il s'agit de l'adresse IP utilisée pour la connexion à l'ISP.
- **DNS primaire:** Tapez l'adresse IP du serveur DNS primaire, le cas échéant.
- **DNS secondaire:** Si l'ISP fournit un autre serveur DNS, tapez l'adresse IP du serveur en question.
- **Taille MTU:** Permet de définir l'unité de transmission maximale. Il est conseillé de garder la valeur par défaut.

- **Adresse MAC du routeur:** Reportez-vous aux descriptions de configuration de l'**Adresse MAC du routeur** pour le DHCP.

Une fois les paramètres réglés, cliquez sur **Appliquer** pour les sauvegarder.

(3) PPPoE

Si le nom d'utilisateur et le mot de passe du PPPoE (Point-to-Point Protocol over Ethernet, "protocole point-à-point sur Ethernet") sont fournis par l'ISP, cliquez sur **Oui** et choisissez **PPPoE**.

Paramètres de l'interface WAN

Votre connexion Internet nécessite-t-elle un login?	<input checked="" type="radio"/> Oui <input type="radio"/> Non
Fournisseur de services Internet	PPPoE ▼
Login	<input type="text"/>
Mot de passe	<input type="text"/>
Nom de service (si nécessaire)	<input type="text"/>
Mode de connexion	Toujours allumé ▼
Délai d'inactivité (en minutes)	<input type="text" value="5"/>
Adresse du serveur de nom de domaine (DNS)	
<input checked="" type="radio"/> Obtention automatique sur ISP	
<input type="radio"/> Utiliser ces serveurs DNS	
DNS primaire	<input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/>
DNS secondaire	<input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/>
Réglage MTU	
Taille MTU(616-1492 bytes)	<input type="text" value="1492"/>
Adresse MAC routeur	
<input checked="" type="radio"/> Utiliser l'adresse par défaut	
<input type="radio"/> Utiliser l'adresse MAC de l'ordinateur	
<input type="radio"/> Utiliser cette adresse MAC	<input type="text" value="00:1E:E3:4B:06:6D"/>

Appliquer

Annuler

- **Login:** Tapez le nom d'utilisateur pour l'accès par PPPoE, fourni par l'ISP.
- **Mot de passe:** Tapez le mot de passe pour l'accès par PPPoE fourni par l'ISP.
- **Nom de service:** Si plusieurs PPPoE sont disponibles, spécifiez-en un dans ce champ.
- **Mode connexion:**
 - **Toujours allumé:** Si vous choisissez ce réglage, le système établit la connexion de manière automatique. Lorsque vous utilisez les services d'accès à Internet, si l'appareil est déconnecté du réseau en raison de facteurs extérieurs, le système tente de se reconnecter au bout d'un délai spécifié (par exemple 10

secondes) jusqu'à ce que la connexion soit rétablie. Si vous payez un forfait mensuel pour votre connexion Internet, nous vous conseillons d'utiliser ce mode de connexion.

- **Connexion à la demande:** Si vous choisissez cette option, le système établit automatiquement la connexion lorsque le réseau LAN envoie une demande d'accès au réseau. Si le réseau LAN n'envoie aucune demande d'accès au réseau, le système interrompt la connexion automatiquement au bout de la durée définie dans le champ **Délai d'inactivité**. Si vous payez l'accès à Internet à la durée, nous vous conseillons d'utiliser ce mode de connexion qui vous permet d'économiser vos dépenses d'Internet de manière efficace.
- **Connexion manuelle:** Si vous choisissez cette option, vous devrez configurer manuellement la connexion par ligne commutée après le démarrage.
- **Délai d'inactivité:** Si le système ne détecte aucune tentative d'accès à Internet, il interrompt la connexion au bout de la durée spécifiée dans le champ **Délai d'inactivité**.
- **Adresse du serveur de nom de domaine (DNS):** Cochez la case **Utiliser ces serveurs DNS** si vous savez que votre ISP ne transmet pas automatiquement les adresses DNS au routeur au moment de l'ouverture de session. Puis tapez l'adresse IP du serveur DNS primaire de votre ISP. Le cas échéant, tapez également l'adresse du serveur DNS secondaire.
- **Taille MTU:** Permet de définir l'unité de transmission maximale. Il est conseillé de garder la valeur par défaut.
- **Adresse MAC routeur:** Reportez-vous aux descriptions de configuration de l'**Adresse MAC routeur** pour le DHCP.

Une fois les paramètres réglés, cliquez sur **Appliquer** pour les sauvegarder.

(4) PPTP

Si le nom d'utilisateur et le mot de passe pour la connexion par PPTP sont fournis par l'ISP, choisissez l'option **PPTP**.

Paramètres de l'interface WAN

Votre connexion Internet nécessite-t-elle un login?	<input checked="" type="radio"/> Oui <input type="radio"/> Non
Fournisseur de services Internet	PPTP
Login	
Mot de passe	
Mode de connexion	Toujours allumé
Délai d'inactivité (en minutes)	5
Mon adresse IP	
Masque de sous-réseau	
Adresse du serveur	
Adresse IP de la passerelle	
Adresse du serveur de nom de domaine (DNS)	
<input checked="" type="radio"/> Obtention automatique sur ISP	
<input type="radio"/> Utiliser ces serveurs DNS	
DNS primaire	
DNS secondaire	
Réglage MTU	
Taille MTU(616-1450 bytes)	1450
Adresse MAC routeur	
<input checked="" type="radio"/> Utiliser l'adresse par défaut	
<input type="radio"/> Utiliser l'adresse MAC de l'ordinateur	
<input type="radio"/> Utiliser cette adresse MAC	00:1E:E3:4B:06:6D

- **Login:** Tapez le nom d'utilisateur pour l'accès par PPTP, fourni par l'ISP.
- **Mot de passe:** Tapez le mot de passe pour l'accès par PPTP, fourni par l'ISP.
- **Mode connexion:**
 - **Toujours allumé:** Si vous choisissez ce réglage, le système établit la connexion de manière automatique. Lorsque vous utilisez les services d'accès à Internet, si l'appareil est déconnecté du réseau en raison de facteurs extérieurs, le système tente de se reconnecter au bout d'un délai spécifié (par exemple 10 secondes) jusqu'à ce que la connexion soit rétablie. Si vous payez un forfait mensuel pour votre connexion Internet, nous vous conseillons d'utiliser ce mode de connexion.
 - **Connexion à la demande:** Si vous choisissez cette option, le système établit automatiquement la connexion lorsque le réseau LAN envoie une demande d'accès au réseau. Si le réseau LAN n'envoie aucune demande d'accès au réseau,

le système interrompt la connexion automatiquement au bout de la durée définie dans le champ **Délai d'inactivité**. Si vous payez l'accès à Internet à la durée, nous vous conseillons d'utiliser ce mode de connexion qui vous permet d'économiser vos dépenses d'Internet de manière efficace.

- **Connexion manuelle:** Si vous choisissez cette option, vous devrez configurer manuellement la connexion par ligne commutée après le démarrage.
- **Délai d'inactivité:** Si le système ne détecte aucune tentative d'accès à Internet, il interrompt la connexion au bout de la durée spécifiée dans le champ **Délai d'inactivité**.
- **Mon adresse IP:** Tapez votre adresse IP. Vous pouvez également laisser ce champ vide.
- **Masque de sous-réseau:** Tapez le masque de sous-réseau. Vous pouvez également laisser ce champ vide.
- **Adresse du serveur:** Tapez l'adresse IP du serveur. Vous pouvez également laisser ce champ vide.
- **Adresse IP de la passerelle:** Tapez l'adresse IP de la passerelle. Vous pouvez également laisser ce champ vide.
- **Adresse du serveur de nom de domaine (DNS):** Cochez la case **Utiliser ces serveurs DNS** si vous savez que votre ISP ne transmet pas automatiquement les adresses DNS au routeur au moment de l'ouverture de session. Puis tapez l'adresse IP du serveur DNS primaire de votre ISP. Le cas échéant, tapez également l'adresse du serveur DNS secondaire.
- **Taille MTU:** Permet de définir l'unité de transmission maximale. Il est conseillé de garder la valeur par défaut.
- **Adresse MAC routeur:** Reportez-vous aux descriptions de configuration de l'**Adresse MAC routeur** pour le DHCP.

Une fois les paramètres réglés, cliquez sur **Appliquer** pour les sauvegarder.

(5) L2TP

Si le nom d'utilisateur et le mot de passe pour la connexion par L2TP sont fournis par l'ISP, choisissez l'option **L2TP**.

Paramètres de l'interface WAN

Votre connexion Internet nécessite-t-elle un login?	<input checked="" type="radio"/> Oui <input type="radio"/> Non
Fournisseur de services Internet	L2TP
Login	
Mot de passe	
Mode de connexion	Toujours allumé
Délai d'inactivité (en minutes)	5
Mon adresse IP	
Masque de sous-réseau	
Adresse du serveur	
Adresse IP de la passerelle	
Adresse du serveur de nom de domaine (DNS)	
<input checked="" type="radio"/> Obtention automatique sur ISP	
<input type="radio"/> Utiliser ces serveurs DNS	
DNS primaire	
DNS secondaire	
Réglage MTU	
Taille MTU(616-1450 bytes)	1450
Adresse MAC routeur	
<input checked="" type="radio"/> Utiliser l'adresse par défaut	
<input type="radio"/> Utiliser l'adresse MAC de l'ordinateur	
<input type="radio"/> Utiliser cette adresse MAC	00:1E:E3:4B:06:6D

Pour plus de détails sur la configuration des paramètres pour cette page, veuillez vous reporter à la description des paramètres **PPTP** dans la section précédente.

8.4.3 Serveur DHCP

Allez dans **Paramètres réseau > Serveur DHCP** pour accéder à la page du **Serveur DHCP**. DHCP sont les initiales de Dynamic Host Configuration Protocol (protocole de configuration dynamique des hôtes). Si vous cochez la case **Utiliser le routeur comme serveur DHCP**, l'appareil attribue automatiquement les adresses IP aux ordinateurs du réseau LAN. Les utilisateurs n'ont alors pas besoin de configurer les paramètres du protocole TCP/IP comme l'adresse IP, le masque de sous-réseau, la passerelle et les informations du serveur DNS pour les ordinateurs connectés au réseau LAN du routeur.

Utiliser le routeur comme serveur DHCP

Adresse IP de départ

Adresse IP d'arrivée

Durée d'autorisation DHCP (1-150 heures)

#	Adresse IP	Nom du périphérique	Adresse MAC
<input type="button" value="Ajouter"/> <input type="button" value="Modifier"/> <input type="button" value="Supprimer"/>			

8.4.3.1 Utilisation du routeur comme serveur DHCP

- **Utiliser le routeur comme serveur DHCP:** Si vous cochez la case **Utiliser le routeur comme serveur DHCP**, l'appareil prend la fonction de serveur DHCP et assigne automatique les adresses IP aux ordinateurs qui sont connectés à lui.
- **Adresse IP de départ/adresse IP d'arrivée:** Définissez des adresses IP de départ et d'arrivée si vous souhaitez spécifier un pool d'adresses devant être assignées par le serveur DHCP. Une fois définis l'**adresse IP de départ/adresse IP d'arrivée**, les hôtes du réseau LAN obtiendront des adresses IP situées entre l'adresse IP de départ et celle d'arrivée.
- **Durée d'autorisation DHCP:** Il s'agit de la durée de validité pour une adresse IP automatiquement attribuée par le serveur DHCP à un hôte. Le serveur DHCP ne peut pas attribuer une même adresse IP à d'autres hôtes pendant la durée spécifiée.

8.4.3.2 Réserve d'adresse

Lorsque vous spécifiez une adresse IP réservée pour un ordinateur dans le réseau LAN, l'ordinateur en question reçoit toujours la même adresse IP chaque fois qu'il accède au serveur DHCP du routeur. Les adresses IP réservées doivent être attribuées aux ordinateurs ou aux serveurs nécessitant des paramètres IP permanents.

#	Adresse IP	Nom du périphérique	Adresse MAC
<input type="button" value="Ajouter"/> <input type="button" value="Modifier"/> <input type="button" value="Supprimer"/>			

Pour réserver une adresse IP:

Etape 1 Cliquez sur **Ajouter** pour accéder à la page de **Réserve d'adresse**.

Réserve d'adresse

Tableau de réservation d'adresses

#	Adresse IP	Nom du périphérique	Adresse MAC
<input type="radio"/>	1		
<input checked="" type="radio"/>	2	192.168.100.2	Z2yMjE3Z4== 09:1F:A4:91:F2:0E

Adresse IP

Adresse MAC

Nom du périphérique

Etape 2 Choisissez dans le **Tableau de réservation d'adresses** l'adresse IP à attribuer à l'ordinateur ou au serveur, ou tapez l'adresse directement dans le champ **Adresse IP** (choisissez une adresse comprise dans le pool d'adresses que vous avez spécifié, par

exemple 192.168.100.x). Tapez l'adresse MAC et le nom de périphérique de l'ordinateur ou du serveur.

Etape 3 Cliquez sur **Ajouter**; la nouvelle entrée est maintenant ajoutée dans **Réservation d'adresse**.

Etape 4 Cliquez sur **Appliquer** pour sauvegarder les paramètres.

8.4.4 NAT ALG

Allez dans **Paramètres réseau > NAT ALG** pour accéder à la page du **NAT ALG**.

NAT ALG

Désactiver SIP ALG

Désactiver le tunnel IPSEC

Désactiver le tunnel L2TP

Désactiver le tunnel PPTP

Appliquer

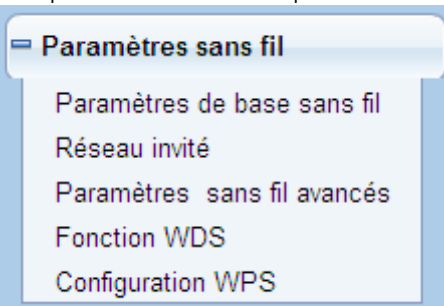
Annuler

- **Désactiver SIP ALG:** Certaines applications SIP contournent le pare-feu NAT de leur propre manière, et le SIP ALG peut entrer en conflit avec les solutions en question. Dans la plupart des cas, le SIP ALG doit rester désactivé.
- **Désactiver les tunnels IPSEC/L2TP/PPTP:** Les tunnels IPSEC/L2TP/PPTP offrent une méthode de communication sécurisée par WAN (wide area network) (ex: Internet) entre les ordinateurs distants. Si un hôte intra-réseau a besoin d'utiliser un protocole VPN (PPTP, L2TP ou IPSEC) pour se connecter à un réseau VPN distant par l'intermédiaire du routeur, activez la fonction tunnel VPN correspondante.

Une fois les paramètres réglés, cliquez sur **Appliquer** pour les sauvegarder.

8.5 Paramètres sans fil

Cliquez sur **Paramètres sans fil** pour afficher le menu de navigation étendu.



8.5.1 Paramètres de base sans fil

Pour plus de détails, reportez-vous à la section **7.5.1 Paramètres de base sans fil**.

8.5.2 Réseau invité

Si vous ne souhaitez pas que les visiteurs connaissent votre clé de sécurité sans fil, vous pouvez utiliser le réseau invité pour leur permettre d'utiliser votre Internet sans les laisser connaître le mot de passe de votre connexion sans fil.

Allez dans **Paramètres sans fil > Réseau invité** pour accéder à la page du **Réseau invité**.

Réseau invité

Profils réseau					
	Régime	SSID	Sécurité	Appliquer	Diffusion SSID
<input checked="" type="radio"/>	1	PocketAP-002	None	NON	OUI
<input type="radio"/>	2	PocketAP-003	None	NON	OUI
<input type="radio"/>	3	PocketAP-004	None	NON	OUI
<input type="radio"/>	4	PocketAP-005	None	NON	OUI

Paramètres sans fil-- Profil1

Activer le réseau invité

Activer la diffusion SSID

Autoriser un invité à accéder à mon réseau local

Activer l'isolation sans fil

Nom de réseau sans fil invité (SSID) :

Options de sécurité-- Profil1

Options de sécurité :

- **Profils réseau:** Brève description du réseau invité créé. Vous pouvez créer jusqu'à quatre réseaux invités. Un profil réseau contient le SSID, le mode de cryptage et les options d'utilisation du réseau invité et de diffusion du SSID. Pour afficher les détails d'un profil ou en modifier les paramètres, cliquez sur le bouton radio correspondant.
- **Activer le réseau invité:** Si vous cochez cette case, aussi bien vous que les visiteurs pourrez vous connecter au réseau en utilisant le SSID du réseau invité.
- **Activer la diffusion SSID:** Si vous cochez cette case, l'appareil diffusera son SSID à toutes les stations sans fil.
- **Autoriser un invité à accéder à mon réseau local:** Si vous cochez cette case, les visiteurs utilisant le SSID d'un réseau invité auront accès non seulement à Internet mais également au réseau LAN de l'appareil, comme les utilisateurs du SSID primaire du réseau. Si vous ne cochez pas cette case, les visiteurs utilisant le SSID d'un réseau invité n'auront pas accès au réseau LAN de l'appareil.
- **Activer l'isolation sans fil:** Si vous cochez cette case, les clients sans fil connectés au réseau invité d'un même SSID pourront accéder à Internet mais ne pourront pas communiquer entre eux.
- **Nom de réseau sans fil invité (SSID):** Définissez le nom du réseau invité.
- **Options de sécurité:** Référez-vous aux options de sécurité décrites dans la section **8.5.1 Wireless Basic Settings**.

Une fois les paramètres réglés, cliquez sur **Appliquer** pour les sauvegarder.

8.5.3 Paramètres sans fil avancés

Pour plus de détails, reportez-vous à la section **7.5.3 Paramètres sans fil avancés**.

8.5.4 Fonction WDS

La fonction WDS (Wireless distribution system, "système de distribution sans fil") permet l'interconnexion entre les différents points d'accès dans un réseau sans fil IEEE 802.11. Elle étend le réseau sans fil par plusieurs points d'accès, sans connexion du réseau central câblé. Activez la fonction WDS si vous souhaitez permettre la répétition ou le pontage sans fil.

Allez dans **Paramètres sans fil > Fonction WDS** pour accéder à la page **Fonction WDS**.

Fonction WDS

<input type="checkbox"/> Activer la fonction WDS	
<input type="checkbox"/> Désactiver l'association de clients sans fil	
MAC sans fil de ce routeur: 00:1E:E3:4B:06:6C	
Station de base sans fil	
Adresse MAC du répéteur 1:	<input type="text"/>
Adresse MAC du répéteur 2:	<input type="text"/>
Adresse MAC du répéteur 3:	<input type="text"/>
Adresse MAC du répéteur 4:	<input type="text"/>

Appliquer

Annuler

- **Activer la fonction WDS:** Cochez cette case si vous souhaitez utiliser la fonction WDS. Veuillez noter que la fonction WDS ne peut pas être activée si le canal est réglé sur **Auto**.
- **Désactiver l'association de clients sans fil:** Si cette case n'est pas cochée, la station de base sans fil ne transmet pas les signaux aux clients qui lui sont directement connectés.
- **Station centrale de base:** Dans ce mode, le routeur sert de station de base pour communiquer avec les répéteurs. La station de base transmet les données de communication entre les répéteurs aux répéteurs destinataires. Les répéteurs doivent être configurés en conséquence. Veuillez noter qu'une station de base sans fil peut être configurée avec quatre répéteurs maximum.
- **Adresse MAC des répéteurs 1/2/3/4:** Tapez l'adresse MAC du répéteur.

Une fois les paramètres réglés, cliquez sur **Appliquer** pour les sauvegarder.

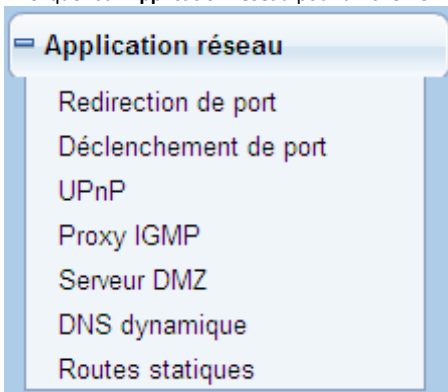
Pour une description de l'application WDS, reportez-vous à la section **6.4.3**

8.5.5 Configuration WPS

Pour les détails, reportez-vous à la section **7.5.4 Configuration WPS**.

8.6 Application réseau

Cliquez sur **Application réseau** pour afficher le menu de navigation étendu.



8.6.1 Redirection de port

Par défaut, la fonction pare-feu du routeur cache votre LAN. Il s'ensuit que les autres utilisateurs sur Internet peuvent seulement détecter le routeur sans pouvoir accéder directement à un PC donné du réseau LAN. Si vous souhaitez accéder à un PC du réseau LAN, vous devrez configurer la redirection de port pour le routeur et rediriger le port souhaité vers le PC correspondant dans le réseau LAN. Le routeur redirige les paquets vers le PC selon les règles de redirection définies, après avoir reçu une requête d'accès depuis Internet. De cette manière, la communication peut s'établir entre Internet et le PC du réseau LAN.

Allez dans **Application réseau > Redirection de port** pour accéder à la page **Redirection de port**.

Port Forwarding

Service Name
FTP

Service IP Address
192 . 168 . 100 .

Service List
Max of rules: 32

#	Server Name	Start Port	End Port	Server IP Address
---	-------------	------------	----------	-------------------

- **Nom de service:** Choisissez un type de service.
- **Adresse IP de service:** Tapez l'adresse IP de l'ordinateur fournissant les services.

Cliquez sur **Ajouter service personnalisé** pour accéder à la page **Ports - Service personnalisé:**

Redirection de port

Nom de service

FTP ▼

Adresse IP de service

192 . 168 . 100 Ajouter

Liste de services

Nombre max. de règles: 32

#	Nom du serveur	Port de départ	Port d'arrivée	Adresse IP du serveur
Éditer service Supprimer service Ajouter service personnalisé				

- **Nom de service:** Choisissez un type de service.
 - **Protocole:** Le protocole utilisé au port de redirection. Les options disponibles sont **TCP/UDP**, **TCP** et **UDP**. Si vous ne savez pas quel protocole utiliser, utilisez de préférence l'option **TCP/UDP**.
 - **Port de départ:** Une fois la connexion établie avec le port de redirection, le port correspondant est ouvert et l'application peut rediriger les demandes de connexion ultérieures vers le port ouvert.
 - **Port d'arrivée:** Définissez le port d'arrivée de la plage des ports de redirection.
 - **Adresse IP de service:** Tapez l'adresse IP de l'ordinateur fournissant les services.
- Une fois les paramètres réglés, cliquez sur **Appliquer** pour les sauvegarder.

8.6.2 Déclenchement de port

Certaines applications nécessitent plusieurs connexions, par exemple les jeux en réseau WAN, les conférences vidéo ou encore les appels en réseau. Du fait du pare-feu, ces applications ne peuvent pas fonctionner sur un routeur NAT simple. Cependant, certaines applications spéciales permettent à ces applications de fonctionner sur un routeur NAT. Lorsqu'une application adresse une demande de connexion à un port de déclenchement, les ports correspondants sont ouverts pour permettre une connexion ultérieure et une fourniture de services.

Allez dans **Application réseau > Déclenchement de port** pour accéder à la page **Déclenchement de port**.

Déclenchement de port

Activer le déclenchement de port

Délai de déclenchement de port (en minutes) (1-9999)

Nombre max. de règles: 32

#	Nom du serveur	Type de service	Connexion entrante requise	Service User
---	----------------	-----------------	----------------------------	--------------

- **Activer le déclenchement de port:** Si la case Activer le déclenchement de port n'est pas cochée, cette fonction est désactivée.
- **Délai de déclenchement de port:** Cette valeur détermine le délai d'inactivité pour le port d'entrée spécifié. Une fois expiré le délai d'inactivité, le port d'entrée est désactivé.

Cliquez sur **Ajouter service** pour accéder à la page **Déclenchement de port – Services**.

Déclenchement de port - Services

Nom de service	<input type="text"/>
Utilisateur de service	Tous <input type="button" value="v"/> <input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/>
Type de service	TCP <input type="button" value="v"/>
Port de déclenchement de départ	<input type="text"/> (1~65535)
Port de déclenchement d'arrivée	<input type="text"/> (1~65535)
Connexion entrante requise	
Type de connexion	TCP <input type="button" value="v"/>
Port de départ	<input type="text"/> (1~65535)
Port d'arrivée	<input type="text"/> (1~65535)

- **Nom de service:** Tapez un nom de service.
- **Utilisateur de service:**
 - **Tous:** Permettre à tous les utilisateurs du réseau d'utiliser le service.
 - **Adresse unique:** Tapez l'adresse IP de l'adaptateur réseau sur le PC. Par la suite, le service s'appliquera seulement à l'adaptateur réseau spécifié du PC.
- **Type de service:** Le protocole utilisé au port de déclenchement. Les options disponibles sont **TCP/UDP**, **TCP** et **UDP**.
- **Port de déclenchement de départ:** Le premier port vers lequel une application envoie une demande de connexion. Tous les ports concernés peuvent être ouverts

seulement une fois la connexion établie à ce port de départ. Dans le cas contraire, les autres ports concernés ne sont pas ouverts.

- **Port de déclenchement d'arrivée:** Définissez le port d'arrivée de la plage des ports de déclenchement.
- **Port de départ:** Définissez le port de départ de la plage des ports.
- **Port d'arrivée:** Définissez le port d'arrivée de la plage des ports.

Quand vous avez fini, cliquez sur **Appliquer** pour ajouter la nouvelle règle de déclenchement de port.

8.6.3 UPnP

Par l'intermédiaire du protocole UPnP (Universal Plug and Play), un hôte du réseau LAN peut demander au routeur d'effectuer une conversion de port spécifique, afin de permettre à un hôte extérieur d'accéder aux ressources de l'hôte intérieur en cas de besoin. Par exemple, si MSN Messenger est installé sur un système d'exploitation Windows ME ou Windows XP, le protocole UPnP peut être utilisé pour les conversations audio et vidéo. De cette manière, les fonctions bloquées par NAT peuvent fonctionner normalement.

Allez dans **Application réseau > UPnP** pour accéder à la page **UPnP**.

UPnP

Activer UPnP

Intervalle de diffusion(en minutes)

TTL de diffusion(en hop)

Tableau portable UPnP					
Actif	Protocole	Port int.	Port ext.	Adresse IP	Description

- **Activer UPnP:** Cochez cette case pour activer le protocole UPnP.
- **Intervalle de diffusion (en minutes):** Définir l'intervalle de diffusion. Celui-ci correspond à l'intervalle auquel le routeur diffuse ses informations UPnP. La valeur est réglable de 1 à 1440 minutes (valeur par défaut: 30 minutes).
- **TTL de diffusion (en hop):** Durée de la diffusion. Il s'agit du nombre de hops après l'envoi de chaque paquet UPnP. Le nombre de hops correspond à la durée de diffusion d'un paquet avant sa disparition. La valeur est réglable de 1 à 255 hops (valeur par défaut: 4 hops).
- **Tableau portable UPnP:** Ce tableau indique les adresses IP des périphériques UPnP connectés au routeur, ainsi que les ports (intérieurs et extérieurs) ouverts des périphériques. Il contient également les types et les statuts des ports ouverts.



Remarque:

Seules les applications compatibles avec le protocole UPnP peuvent accepter cette fonction.

La fonctionnalité UPnP nécessite la compatibilité avec l'application, et un système d'exploitation de type Windows ME, Windows XP ou Windows Vista.

8.6.4 Proxy IGMP

Allez dans **Application réseau > Proxy IGMP** pour accéder à la page **Proxy IGMP**.

Proxy IGMP

Désactiver proxy IGMP

Appliquer

Annuler

- **Désactiver proxy IGMP:** La fonction de proxy IGMP permet à un ordinateur connecté au réseau LAN de recevoir le trafic multidiffusion à partir d'Internet. Désactivez le proxy IGMP si vous n'avez pas besoin de cette fonction.

Une fois les paramètres réglés, cliquez sur **Appliquer** pour les appliquer.

8.6.5 Serveur DMZ

DMZ (zone démilitarisée), zone spéciale du réseau, différente à la fois du réseau externe et du réseau interne. Les serveurs autorisés à accéder au réseau externe, comme par exemple le Web et les e-mails, se connectent au serveur DMZ. Le réseau interne est protégé par l'interface Zone de confiance; aucun utilisateur n'y a accès. C'est pourquoi les réseaux interne et externe sont séparés, de manière à mieux répondre aux besoins de confidentialité de l'utilisateur. En général, il existe quelques serveurs publics dans le DMZ, comme le Web, les e-mails et le FTP. Les utilisateurs du réseau externe peuvent accéder aux services en DMZ, mais ne peuvent pas obtenir les informations secrètes ou personnelles de la compagnie, qui sont stockées dans le réseau interne. Même si les serveurs du DMZ sont endommagés, aucune fuite d'informations secrètes ne peut se produire dans le réseau interne.

Allez dans **Paramètres réseau > Serveur DMZ** pour accéder à la page du **Serveur DMZ**.

Serveur DMZ

Serveur DMZ par défaut

192

168

100

Appliquer

Annuler

- **Serveur DMZ par défaut:** Tapez l'adresse IP du PC devant servir de serveur DMZ.



Remarque:

Lorsqu'un PC du réseau interne est configuré comme hôte DMZ, toutes les interfaces de ce PC sont exposées à Internet et les risques sont élevés en termes de sécurité. Évitez de configurer le DMZ à la légère, sauf en cas de nécessité.

Une fois configuré l'hôte DMZ, les mappings de toutes les interfaces seront dirigés vers lui et les mappings des ports dirigés vers d'autres hôtes seront invalides.

8.6.6 DNS dynamique

Le DDNS (Dynamic domain name resolution) est principalement utilisé pour la résolution entre les noms de domaines fixes et les adresses IP dynamiques. Pour un utilisateur d'adresse IP dynamique ayant obtenu une nouvelle adresse IP par accès à Internet, le logiciel de nom de domaine dynamique installé dans l'hôte envoie l'adresse IP au serveur DDNS fourni par le fournisseur de services DDNS, puis met à jour la résolution de nom de domaine. Lorsqu'un autre utilisateur d'Internet tente d'accéder au nom de domaine en question, le serveur de résolution de nom de domaine dynamique renvoie l'adresse IP correcte.

Allez dans **Application réseau > DNS dynamique** pour accéder à la page **DNS dynamique**.

DNS dynamique

<input type="checkbox"/> Utiliser un service de DNS dynamique	
Fournisseur de services	dyndns.org
Nom d'hôte	myhostname
Nom d'utilisateur	User
Mot de passe	••••••

Appliquer

Annuler

- **Utiliser un service de DNS dynamique:** Si vous êtes abonné à un fournisseur de services DDNS, cochez la case **Utiliser un service de DNS dynamique**.
- **Fournisseur de services:** Choisissez votre fournisseur de services DDNS.
- **Nom d'hôte:** Tapez le nom d'hôte ou de domaine fourni par votre fournisseur de services DDNS.
- **Nom d'utilisateur:** Tapez le nom de votre compte DDNS.
- **Mot de passe:** Tapez le mot de passe de votre compte DDNS.

Une fois les paramètres réglés, cliquez sur **Appliquer** pour les appliquer.

8.6.7 Routes statiques

Les routes statiques sont un type de routes pouvant être appliquées dans un réseau pour réduire le problème du choix de routes et de la surcharge du flux de données qui en découle, ce afin d'améliorer la vitesse de transmission des paquets. Vous pouvez spécifier une règle de route en

définissant l'adresse IP de destination, le masque de sous-réseau et la passerelle. L'adresse IP de destination et le masque de sous-réseau déterminent un hôte ou réseau de destination auquel le routeur enverra les paquets via la passerelle.

Allez dans **Application réseau > Routes statiques** pour accéder à la page **Routes statiques**.

Routes statiques

Nombre max. de règles: 32

#	Actif	Nom	Destination	Passerelle
---	-------	-----	-------------	------------

[Ajouter](#) [Modifier](#) [Supprimer](#)

Cliquez sur **Ajouter** pour ajouter une règle de route statique.

Routes statiques

Actif	<input type="checkbox"/>
Nom de route	<input type="text"/>
Adresse IP de destination	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>
Masque de sous-réseau IP	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>
Adresse IP de la passerelle	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>
Métrique	<input type="text"/>

[Appliquer](#) [Annuler](#)

- **Actif:** La règle de route statique ne peut prendre effet que si la case **Actif** est cochée.
- **Nom de route:** Tapez le nom de la route statique.
- **Adresse IP de destination:** Le réseau ou l'adresse IP de destination auquel vous voulez accéder. Cette adresse IP ne peut pas être dans le même segment de réseau que l'adresse IP de l'interface WAN ou LAN de l'appareil.
- **Masque de sous-réseau IP:** Le masque de sous-réseau IP constitue l'autre identifiant du réseau cible avec l'adresse IP de destination.
- **Adresse IP de la passerelle:** L'adresse IP du nœud suivant vers lequel les paquets sont envoyés. L'adresse IP de la passerelle doit être dans le même segment de réseau que l'adresse IP de l'interface WAN ou LAN de l'appareil.
- **Métrique:** Le nombre d'autres routeurs dans le réseau de l'utilisateur. Le nombre peut être compris entre 2 et 15. En général, un fonctionnement optimal s'obtient avec 2 ou 3. Pour une connexion directe, réglez le nombre **Métrique** sur 2.

Une fois les paramètres réglés, cliquez sur **Appliquer** pour les sauvegarder.

8.7 Options de sécurité

Cliquez sur **Options de sécurité** pour afficher le menu de navigation étendu.

Options de sécurité

Bloquer des sites

Bloquer des services

Protection

8.7.1 Bloquer des sites

Le répéteur pose des restrictions d'accès aux utilisateurs en fonction des adresses WEB et des mots-clés contenus dans ces adresses. Lorsqu'un utilisateur tente d'accéder à un site Web bloqué, un message s'affiche, indiquant que le pare-feu bloque l'accès au site en question.

Allez dans **Options de sécurité** > **Bloquer des sites** pour accéder à la page **Bloquer des sites**.

Bloquer des sites

Blocage du mot de passe
<input type="radio"/> Jamais
<input type="radio"/> Selon le calendrier
<input checked="" type="radio"/> Toujours
Tapez ici le mot-clé ou le nom de domaine.
<input type="text"/>
<input type="button" value="Ajouter un mot-clé"/>
Bloquer les sites contenant ces mots-clés ou noms de domaines(Nombre max. de termes: 32) :
<input type="text"/>
<input type="button" value="Supprimer un mot-clé"/> <input type="button" value="Supprimer la liste"/>
<input type="checkbox"/> Permettre à une adresse IP de confiance de visiter les sites bloqués
Adresse IP de confiance
<input type="text" value="192"/> <input type="text" value="168"/> <input type="text" value="100"/> <input type="text"/>

Suivez la procédure ci-dessous pour bloquer l'accès à des sites Internet.

Etape 1 Cochez **Selon le calendrier** ou **Toujours** pour activer le blocage de mots-clés. Pour un blocage selon le calendrier, vous devrez préciser un intervalle de temps dans la page **Calendrier**. Pour plus d'informations sur le calendrier, veuillez vous reporter à la section **8.8.3 Calendrier**.

Etape 2 Tapez les mots-clés ou les noms de domaines que vous souhaitez bloquer dans le champ prévu à cet effet, puis cliquez sur **Ajouter un mot-clé**. Le mot-clé ou nom de domaine apparaît ensuite dans la liste **Bloquer les sites contenant ces mots-clés ou noms de domaines**.

Exemples d'application de mots-clés:

- Si vous avez spécifié le mot-clé **XXX**, l'URL `www.aabbcc.com/xxx.html` sera bloquée.
- Si vous avez spécifié le mot-clé **.com**, seuls les sites comportant d'autres suffixes de noms de domaines (.edu, .org, .gov etc.) ne seront pas bloqués.

Etape 3 Vous pouvez spécifier un utilisateur de confiance, qui sera un ordinateur libre de toute restriction d'accès. Pour spécifier un utilisateur de confiance, tapez l'adresse IP de l'ordinateur en question dans le champ **Adresse IP de confiance** puis cochez la case **Permettre à une adresse IP de confiance de visiter les sites bloqués**.

Étant donné que l'utilisateur de confiance sera identifié par son adresse IP, l'ordinateur en question doit être configuré avec une adresse IP fixe.

Etape 4 Cliquez sur **Appliquer** pour sauvegarder les paramètres.

8.7.2 Bloquer des services

Le répéteur permet aux utilisateurs de bloquer l'utilisation de certains services Internet par des ordinateurs sur votre réseau.

Allez dans **Options de sécurité > Bloquer des services** pour accéder à la page **Bloquer des services**.

Bloquer des services

Never

Black List Per Schedule

Black List Always

Block Service Rules Table - Black List

Max of rules: 32

#	Nom du services	Port	IP
<input type="button" value="Ajouter"/> <input type="button" value="Modifier"/> <input type="button" value="Effacer"/>			

Block Service Rules Table - White List

Max of rules: 32

#	Nom du services	Port	IP
<input type="button" value="Ajouter"/> <input type="button" value="Modifier"/> <input type="button" value="Effacer"/>			

Suivez la procédure ci-dessous pour spécifier un service devant être bloqué.

Etape 1 Cochez **Selon le calendrier** ou **Toujours** pour activer le blocage de mots-clés. Pour un blocage selon le calendrier, vous devrez préciser un intervalle de temps dans la page **Calendrier**. Pour plus d'informations sur le calendrier, veuillez vous reporter à la section **8.8.3 Calendrier**.

- **Liste noire:** Permet de bloquer l'accès aux services correspondant aux règles définies dans **Tableau des règles de blocage de services - Liste noire**.
- **Liste blanche:** Permet d'autoriser seulement l'accès aux services correspondant aux règles définies dans **Tableau des règles de blocage de services - Liste blanche**.

Etape 2 Cliquez sur **Ajouter** pour spécifier un service à bloquer. La page **Configuration du blocage de services** s'affiche.

Configuration du blocage de services

Type de service	User Defined
Protocole	TCP
Port de départ	<input type="text"/> (1~65535)
Port d'arrivée	<input type="text"/> (1~65535)
Type de service/utilisateur défini	<input type="text"/>
Filtrer les services pour:	
<input type="radio"/> Seulement cette adresse IP:	<input type="text"/> 192 . <input type="text"/> 168 . <input type="text"/> 100 . <input type="text"/>
<input type="radio"/> Plage d'adresses IP:	<input type="text"/> 192 . <input type="text"/> 168 . <input type="text"/> 100 . <input type="text"/>
	vers <input type="text"/> 192 . <input type="text"/> 168 . <input type="text"/> 100 . <input type="text"/>
<input checked="" type="radio"/> Toutes les adresses IP:	

Etape 3 Définissez les paramètres sur cette page.

- **Type de service:** Choisissez un type de service. Si le type recherché ne figure pas dans cette liste, choisissez **Défini par l'utilisateur**. Ensuite, choisissez le protocole puis tapez le nom et la plage de numéros de ports utilisés par le service. Pour les services figurant dans le menu déroulant, les informations correspondantes seront déjà prédéfinies.
- **Protocole:** Définir le protocole utilisé aux ports de service. En cas d'incertitude concernant le protocole utilisé par l'application, choisissez **TCP/UDP**.
- **Port de départ/port d'arrivée:** Les ports de départ et d'arrivée de la plage dans laquelle le service en question sera bloqué. Si l'application utilise un seul et même port, tapez le numéro correspondant dans les deux champs.
- **Type de service/utilisateur défini:** Tapez le nom de service.
- **Filtrer les services pour:** Vous pouvez bloquer le service en question pour un seul ordinateur, pour tous les ordinateurs ou pour ceux de la plage d'adresses IP définie. Quand vous avez fini, cliquez sur **Ajouter** pour ajouter la nouvelle règle. Puis cliquez sur **Appliquer** pour sauvegarder les paramètres.

8.7.3 Protection

Allez dans **Options de sécurité > Protection** pour accéder à la page **Protection**.

Protection

Désactiver le scan de ports et la protection DOS

Répondre au ping sur le port Internet

Filtrage NAT

Sécurisé

Appliquer

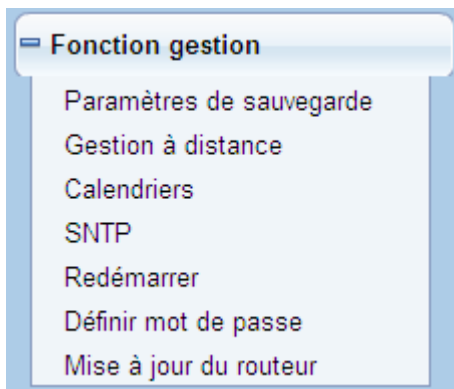
Annuler

- **Désactiver le scan de ports et la protection DoS:** La protection DoS (denial of service, "refus de service") protège votre réseau LAN contre les attaques DOS. De manière générale, il est préférable d'activer le scan de ports et la protection DOS.
- **Répondre au ping sur le port Internet:** Si vous cochez cette case, le routeur répondra aux pings à partir d'Internet. Cependant, comme pour le serveur DMZ, cette fonction comporte des risques de sécurité une fois activée. Il est donc préférable de la désactiver, de manière générale.
- **Filtrage NAT:** Le filtrage NAT détermine la manière dont le routeur gère le trafic entrant.
 - **Sécurisé:** Cette option fournit un pare-feu sécurisé pour protéger les ordinateurs du réseau local contre les attaques depuis Internet. Cependant, ce pare-feu peut empêcher les jeux en ligne et les applications point à point ou multimédia de fonctionner normalement.
 - **Ouverte:** Cette option fournit un pare-feu moins sécurisé, qui permet à presque toutes les applications d'Internet de fonctionner.

Une fois les paramètres réglés, cliquez sur **Appliquer** pour les appliquer.

8.8 Fonction gestion

Cliquez sur **Fonction gestion** pour afficher le menu de navigation étendu.



8.8.1 Paramètres de sauvegarde

Pour plus de détails, reportez-vous à la section **7.6.1 Paramètres de sauvegarde**.

8.8.2 Gestion à distance

La fonction de gestion à distance vous permet de configurer le routeur à partir du réseau WAN, via le navigateur Web. De cette manière, vous pouvez gérer le routeur en tant qu'hôte distant.

Allez dans **Fonction gestion** > **Gestion à distance** pour accéder à la page **Gestion à distance**.

Gestion à distance

<input type="checkbox"/> Activer la gestion à distance	
Adresse de gestion à distance :	<input type="text" value="http://0.0.0.0:8080"/>
Numéro de port :	<input type="text" value="8080"/>
Autoriser l'accès à distance par :	
<input type="radio"/>	Pour cet ordinateur seulement : <input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/>
<input type="radio"/>	Plage d'adresses IP : <input type="text"/> De <input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/> À <input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/>
<input checked="" type="radio"/>	Tous

- **Activer la gestion à distance**: Si vous cochez cette case, vous pourrez gérer le routeur à distance sur Internet, à partir du réseau WAN.
- **Adresse de gestion à distance**: L'adresse IP utilisée pour accéder au routeur depuis Internet. L'adresse par défaut est `http://0.0.0.0:8080`. Pour accéder au routeur, vous devrez taper une adresse sous la forme suivante dans la barre d'adresse IE: **"adresse IP WAN du routeur" + ":" + "numéro de port"**. Par exemple, si votre adresse externe est **10.0.0.123** et si le numéro du port utilisé est **8080**, tapez **10.0.0.123:8080** dans votre navigateur.

- **Numéro de port:** Le numéro de port permettant d'accéder au routeur par gestion Web à distance.
- **Autoriser l'accès à distance par:** Définir l'adresse IP de l'ordinateur à partir duquel la gestion Web à distance aura lieu pour accéder au routeur.
 - **Pour cet ordinateur seulement:** Seule l'adresse IP spécifiée peut accéder au routeur.
 - **Plage d'adresses IP:** Une plage d'adresses IP sur Internet peut accéder au routeur. Vous devrez taper les adresses IP de départ et d'arrivée de la plage en question.
 - **Tous:** Tout le monde sur Internet peut accéder au routeur.

Une fois les paramètres réglés, cliquez sur **Appliquer** pour les sauvegarder.

8.8.3 Calendrier

Allez dans **Fonction gestion > Calendrier** pour accéder à la page **Calendrier**.

Programme

Jours à bloquer:	
<input checked="" type="checkbox"/>	Tous les jours
<input checked="" type="checkbox"/>	Dimanche
<input checked="" type="checkbox"/>	Lundi
<input checked="" type="checkbox"/>	Mardi
<input checked="" type="checkbox"/>	Mercredi
<input checked="" type="checkbox"/>	Jeudi
<input checked="" type="checkbox"/>	Vendredi
<input checked="" type="checkbox"/>	Samédi
Moment de la journée à bloquer (heure au format 24h)	
<input checked="" type="checkbox"/>	Toute la journée
Début du blocage	00 Heures 00 Minutes
Fin du blocage	23 Heures 59 Minutes
<input type="button" value="Appliquer"/> <input type="button" value="Annuler"/>	

Si vous avez déjà défini un filtrage de sites sur la page **Bloquer des sites**, ou de services sur la page **Bloquer des services**, vous pouvez maintenant définir un calendrier des jours et du mode de restriction d'accès à Internet.

- **Jours à bloquer:** Choisissez les jours auxquels vous souhaitez appliquer le blocage, en cochant les cases correspondantes. Cochez la case **Tous les jours** si vous souhaitez sélectionner tous les jours de la semaine.
- **Moment de la journée à bloquer:**
 - **Toute la journée:** Blocage 24h/24.
 - **Début du blocage/fin du blocage:** Si vous souhaitez limiter l'accès sur un laps de temps précis aux jours spécifiés, tapez les heures de début et de fin du blocage en format 24 h.

Une fois les paramètres réglés, cliquez sur **Appliquer** pour les sauvegarder.

8.8.4 SNTP

Allez dans **Fonction gestion > SNTP** pour accéder à la page **SNTP**.

SNTP

Réglage heure				
<input type="checkbox"/> Synchronisation automatique avec les serveurs d'horaire sur Internet				
Premier serveur horaire NTP :	<input type="text" value="210.72.145.44"/>			
Deuxième serveur horaire NTP :	<input type="text"/>			
Configuration heure				
Heure actuelle du routeur:	1971-01-01 22:42:20			
Fuseau horaire:	<input type="text" value="(GMT+01:00) Paris, Bruxelles, Copenhague, Madrid"/>			
<input type="checkbox"/> Activer l'heure d'été				
Décalage d'heure d'été:	<input type="text" value="0:00"/>			
Dates de l'heure d'été: (l'intervalle doit être supérieur au nombre de jours du mois de départ)	Mois	Semaine	Jour	
	Démarrage	<input type="text" value="Avr"/>	<input type="text" value="2"/>	<input type="text" value="Dim"/>
	Fin	<input type="text" value="Sep"/>	<input type="text" value="2"/>	<input type="text" value="Dim"/>
<input type="button" value="Appliquer"/> <input type="button" value="Annuler"/>				

SNTP sont les initiales de Simple Network Time Protocol (protocole de synchronisation horaire par réseau simple). Sur cette page, vous pouvez définir les paramètres d'horloge de votre routeur. Il est fortement conseillé de régler d'abord l'heure exacte sur le routeur. Cela permet d'assurer le bon fonctionnement du journal, du blocage des sites et du calendrier, car tous les paramètres d'horaires de ces fonctions dépendent des réglages de l'horloge sur cette page.

- **Synchronisation automatique avec les serveurs d'horaire sur Internet:** Si vous cochez cette case, la synchronisation automatique avec les serveurs d'horaire sur Internet est activée.
- **Premier serveur horaire NTP:** Tapez l'adresse IP du serveur NTP primaire. Le serveur NTP est un serveur horaire en réseau utilisé pour la synchronisation de l'heure des ordinateurs sur Internet. Une fois paramétré le premier serveur horaire NTP, le routeur obtient l'heure GMT à partir du serveur NTP spécifié une fois qu'il est connecté à Internet.
- **Deuxième serveur horaire NTP:** Tapez l'adresse IP du serveur NTP secondaire, le cas échéant.
- **Heure actuelle du routeur:** Affiche l'heure actuelle du système du routeur.
- **Fuseau horaire:** Sélectionnez le fuseau horaire dans lequel vous vous trouvez.
- **Activer l'heure d'été:** Activer ou désactiver l'heure d'été.
- **Décalage d'heure d'été:** Choisissez le décalage d'heure d'été qui convient. Si celui-ci est réglé à +1:00, 10:00 du matin en heure standard devient 11:00 du matin en heure d'été.
- **Dates de l'heure d'été:** Dates de début et de fin de l'heure d'été.

Une fois les paramètres réglés, cliquez sur **Appliquer** pour les sauvegarder.

8.8.5 Redémarrer

Pour plus de détails, reportez-vous à la section **7.6.2 Redémarrer**.

8.8.6 Définir mot de passe

Pour plus de détails, reportez-vous à la section **7.6.3 Définir mot de passe**.

8.8.7 Mise à jour du routeur

Allez dans **Fonction gestion > Mise à jour du routeur** pour accéder à la page **Mise à jour du routeur**.

Mise à jour du routeur

Repérer et sélectionner le fichier de mise à jour à partir du disque dur:

<input type="text"/>	<input type="button" value="Parcourir..."/>	<input checked="" type="checkbox"/> Effacer config
<input type="button" value="Téléverser"/> <input type="button" value="Annuler"/>		

Suivez la procédure ci-dessus pour mettre à jour le logiciel du routeur.

Etape 1 Cliquez sur **Parcourir...** pour retrouver le dernier logiciel.

Etape 2 Choisissez le fichier de mise à jour qui convient. Si vous cochez la case **Effacer config**, le routeur rétablira les paramètres par défaut après chaque mise à jour. Si vous ne cochez pas cette case, les paramètres actuels resteront inchangés.

Etape 3 Cliquez sur **Téléverser** pour lancer la mise à jour.

Une fois la mise à jour terminée, le routeur redémarre automatiquement.



Remarque:

Après la mise à jour du logiciel, les paramètres par défaut de l'appareil sont restaurés. N'oubliez pas de sauvegarder les paramètres avant de mettre à jour le logiciel, pour le cas où les informations de la configuration précédente seraient perdues.

N'éteignez pas le routeur pendant que la mise à jour est en cours.

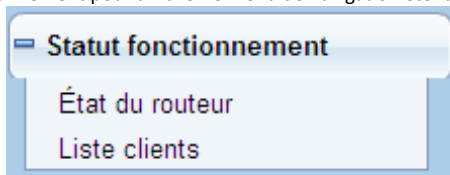
9 Configuration Web en mode répéteur sans fil universel

Remarque:

Mettez sur **Répéteur** l'interrupteur à trois positions situé sur le panneau latéral. Une fois l'appareil redémarré, connectez-vous à la page de configuration.

9.1 Statut fonctionnement

Mettez sur **Répéteur** l'interrupteur à trois positions situé sur le panneau latéral. Cliquez sur **Statut fonctionnement** pour afficher le menu de navigation étendu.



9.1.1 État du routeur

Allez dans **Statut fonctionnement** > **Etat du routeur** pour accéder à la page **Etat du routeur**.

État du routeur

Infos système	
Version matériel	V1.0.0
Version micrologiciel	V1.0.0
Numéro de modèle	Wireless Router
Mode de travail	Mode répéteur
Heure et date	1971-01-01 08:01:34
Port LAN	
Adresse MAC	00:1E:E3:4B:06:6C
Adresse IP	192.168.100.253
Masque de sous-réseau IP	255.255.255.0
Client sans fil	
Nom choisi de réseau sans fil (SSID)	TW-2B08
Canal sans fil	2.452GHz- CH9
Wi-Fi Protected Setup (WPS)	ON
Mode sécurité sans fil	Jamais
Statut connexion	Déconnecté
Répéteur sans fil universel	
SSID de l'interface étendue	TW-2B08
Mode sécurité sans fil	Jamais

Sur cette page, vous trouverez des informations sur le statut de fonctionnement actuel de l'appareil (système, port LAN, client sans fil, répéteur sans fil universel).

9.1.2 Liste clients

Allez dans **Statut fonctionnement** > **Liste clients** pour accéder à la page **Liste clients**.

Liste clients

Appareils reliés			
#	Adresse IP	Adresse MAC	Nom du périphérique
1	192.168.100.10	48:02:2A:D1:A9:60	unknown

Périphériques sans fil (les intrus apparaissent également ici)			
#	Adresse IP	Adresse MAC	Nom du périphérique

Actualiser

Sur cette page, vous trouverez des informations sur les périphériques connectés au répéteur (nom, adresse IP et adresse MAC de chacun des périphériques etc.).

9.2 Assistant de configuration

Pour la configuration, reportez-vous à la section **6.3 Configuration du mode répéteur**.

9.3 Réglage du mode de répétition

Cliquez sur **Réglage du mode de répétition** pour accéder à la page **Réglage du mode de répétition**. Cochez la case **Mode répéteur sans fil universel**.

Réglage du mode de répétition

Deux modes permettent d'étendre le réseau sans fil de votre mode de répétition. Vous avez le choix entre le mode WDS et le mode UR.

Choisissez l'un des modes de répétition suivants:

Mode WDS

Mode répéteur sans fil universel

Appliquer

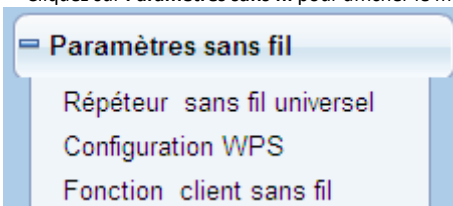
Annuler

9.4 Paramètres réseau

Pour plus de détails, reportez-vous à la section **7.6**.

9.5 Paramètres sans fil

Cliquez sur **Paramètres sans fil** pour afficher le menu de navigation étendu.



9.5.1 Répéteur sans fil universel

En mode répéteur universel, l'appareil se comporte à la fois comme client et comme point d'accès.

Allez dans **Paramètres sans fil > Répéteur sans fil universel** pour accéder à la page des **Répéteur sans fil universel**.

Répéteur sans fil universel

SSID de l'interface étendue :	<input type="text" value="TW-2B08"/>
Options de sécurité	
Options de sécurité :	<input type="text" value="aucune"/>

- **SSID de l'interface étendue:** SSID du répéteur.
- **Options de sécurité:** Réglage du mode de cryptage de sécurité pour le répéteur. Il est recommandé de configurer le répéteur avec le même mode de cryptage que son point d'accès de liaison montante.

Une fois les paramètres réglés, cliquez sur **Appliquer** pour les sauvegarder.

9.5.2 Configuration WPS

Allez dans **Paramètres sans fil > Configuration WPS**; la page ci-dessous s'affiche.

Configuration WPS

Nouveau moyen simple pour se connecter au routeur sans fil via WiFi Protected setup (WPS)

Un client sans fil doit accepter la fonctionnalité WPS pour pouvoir utiliser cet assistant d'ajout de clients sur votre routeur sans fil WPS. Reportez-vous au mode d'emploi ou à l'emballage de votre client sans fil pour vérifier s'il accepte ou non la fonctionnalité WPS. Si votre client sans fil n'accepte pas la fonctionnalité WPS, vous devrez le configurer manuellement afin qu'il ait le même SSID et les mêmes paramètres de sécurité que ceux du routeur.

WPS signifie Wi-Fi Protected Setup (configuration protégée par Wi-Fi).

La fonctionnalité WPS permet d'établir une connexion sans fil de manière simple et rapide si le terminal ou le point d'accès de liaison montante (ex: l'adaptateur réseau) possèdent la fonctionnalité WPS. Il est conseillé de configurer d'abord le cryptage sans fil pour le point d'accès de liaison montante. Si vous changez le mode de cryptage sans fil après avoir établi la connexion sans fil par WPS, vous devrez utiliser la fonctionnalité WPS pour rétablir de nouveau la connexion sans fil. Veuillez noter que si le client sans fil n'accepte pas la fonctionnalité WPS, vous devrez configurer manuellement le client sans fil (ex: SSID, mode de sécurité, mot de passe) afin qu'il ait le même SSID et les mêmes paramètres de sécurité sans fil que le routeur.

En mode répéteur avec le WDS désactivé, l'appareil effectue une connexion WPS cryptée à la fois avec le point d'accès de liaison montante et avec le périphérique client en aval.

Cliquez sur Suivant pour accéder à la page de **Configuration WPS**. La section suivante explique comment configurer la fonctionnalité WPS pour le mode répéteur.

9.5.2.1 Avec le bouton WPS

- Connexion WPS avec le point d'accès de liaison montante

En mode répéteur avec le WDS désactivé, appuyez pendant 3 secondes sur le bouton **WPS** situé sur le panneau latéral de l'appareil, puis relâchez-le. Ensuite, appuyez sur le bouton **WPS** du point d'accès de liaison montante. La session WPS peut maintenant commencer.

- Connexion WPS avec le périphérique client en aval

En mode répéteur avec le WDS désactivé, appuyez pendant 3 à 10 secondes sur le bouton **WPS** situé sur le panneau latéral de l'appareil, puis relâchez-le. Ensuite, appuyez sur le bouton **WPS** du périphérique client. La session WPS peut maintenant commencer.



Remarque:

Une fois l'appareil connecté au point d'accès de liaison montante avec le mode bouton WPS, le SSID, l'authentification et la clé pré-partagée de l'appareil seront automatiquement alignés sur ceux de son point d'accès de liaison montante.

9.5.2.2 Avec la page Web

Vous pouvez configurer les paramètres WPS en utilisant la page Web prévue à cet effet.

Allez dans **Paramètres sans fil > Configuration WPS** pour accéder à la page **Configuration WPS**.

Configuration WPS

Choisissez une méthode de configuration pour le point d'accès:	
<input checked="" type="radio"/> Bouton-poussoir (recommandé)	
Vous pouvez soit appuyer manuellement sur le bouton-poussoir du routeur, soit appuyer sur la touche tactile ci-dessous.	<input type="button" value="Start PBC"/>
<input type="radio"/> PIN (code d'identification personnelle)	
Sélectionnez une méthode de configuration pour le client:	
<input checked="" type="radio"/> Bouton-poussoir (recommandé)	
Vous pouvez soit appuyer manuellement sur le bouton-poussoir du routeur, soit appuyer sur la touche tactile ci-dessous.	<input type="button" value="Start PBC"/>
<input type="radio"/> PIN (code d'identification personnelle)	

En tant que point d'accès

Vous pouvez configurer les paramètres WPS en utilisant la page Web prévue à cet effet. Allez dans **Paramètres sans fil > Configuration WPS** pour accéder à la page **WPS**.

- Mode PBC

Etape 1 Cochez la case **Bouton-poussoir** et cliquez sur **Start PBC**. La connexion cryptée par WPS commence.

Configuration WPS

Choisissez une méthode de configuration pour le point d'accès:

Bouton-poussoir (recommandé)

Vous pouvez soit appuyer manuellement sur le bouton-poussoir du routeur, soit appuyer sur la touche tactile ci-dessous.

Start PBC

PIN (code d'identification personnelle)

Sélectionnez une méthode de configuration pour le client:

Bouton-poussoir (recommandé)

Vous pouvez soit appuyer manuellement sur le bouton-poussoir du routeur, soit appuyer sur la touche tactile ci-dessous.

Start PBC

PIN (code d'identification personnelle)

Etape 2 Appuyez sur la touche **WPS** de l'adaptateur réseau ou cliquez sur **PBC** dans l'outil de configuration de l'adaptateur réseau dans les 2 minutes qui suivent. Une fois établie la connexion WPS, la page suivante apparaît, indiquant que la connexion WPS à réussi.

Succès!

Le client sans fil vient d'être ajouté au réseau avec succès.
Cliquez sur OK pour revenir à la page de configuration Wi-Fi sécurisée.

OK

● Mode PIN

Etape 1 Cochez **PIN**, tapez le code PIN de l'adaptateur réseau (réf. client de l'adaptateur réseau) puis cliquez sur **Start PIN** pour lancer la connexion WPS.

Configuration WPS

Choisissez une méthode de configuration pour le point d'accès:

Bouton-poussoir (recommandé)

PIN (code d'identification personnelle)

Si votre adaptateur est compatible avec WPS, cliquez sur "Créer un code PIN client de sécurité pour entrer dans le point d'accès, le routeur ou la passerelle", puis entrez ici le code PIN client créé.

Saisissez le code PIN client:

Start PIN

Sélectionnez une méthode de configuration pour le client:

Bouton-poussoir (recommandé)

Vous pouvez soit appuyer manuellement sur le bouton-poussoir du routeur, soit appuyer sur la touche tactile ci-dessous.

Start PBC

PIN (code d'identification personnelle)

Etape 2 Cliquez sur la touche PIN de l'adaptateur réseau dans les 2 minutes pour lancer la connexion WPS. Une fois établie la connexion WPS, la page suivante apparaît, indiquant que la connexion WPS a réussi.

Succès!

Le client sans fil vient d'être ajouté au réseau avec succès.
Cliquez sur OK pour revenir à la page de configuration Wi-Fi sécurisée.

OK

– **En tant que client**

Vous pouvez configurer les paramètres WPS en utilisant la page Web prévue à cet effet. Allez dans **Paramètres sans fil > WPS** pour accéder à la page **WPS**.

- Mode PBC

Etape 1 Cochez la case **Bouton-poussoir** et cliquez sur **Start PBC**. La connexion cryptée par WPS commence.

Configuration WPS

Choisissez une méthode de configuration pour le point d'accès:

Bouton-poussoir (recommandé)

Vous pouvez soit appuyer manuellement sur le bouton-poussoir du routeur, soit appuyer sur la touche tactile ci-dessous.

PIN (code d'identification personnelle)

Sélectionnez une méthode de configuration pour le client:

Bouton-poussoir (recommandé)

Vous pouvez soit appuyer manuellement sur le bouton-poussoir du routeur, soit appuyer sur la touche tactile ci-dessous.

PIN (code d'identification personnelle)

Etape 2 Lancez le processus PBC par WPS. Une fois établie la connexion WPS, la page suivante apparaît, indiquant que la connexion WPS a réussi.

Succès!

Le client sans fil vient d'être ajouté au réseau avec succès.
Cliquez sur OK pour revenir à la page de configuration Wi-Fi sécurisée.

OK

- Mode PIN

Etape 1 Cochez la case **PIN**, cliquez sur **Générer un nouveau code PIN**, puis cliquez sur **Start PIN** pour lancer la connexion WPS.

Configuration WPS

Choisissez une méthode de configuration pour le point d'accès:

Bouton-poussoir (recommandé)

Vous pouvez soit appuyer manuellement sur le bouton-poussoir du routeur, soit appuyer sur la touche tactile ci-dessous.

PIN (code d'identification personnelle)

Sélectionnez une méthode de configuration pour le client:

Bouton-poussoir (recommandé)

PIN (code d'identification personnelle)

Si votre adaptateur est compatible avec WPS, cliquez sur "Créer un code PIN client de sécurité pour entrer dans le point d'accès, le routeur ou la passerelle", puis entrez ici le code PIN client créé.

Générer un nouveau code PIN

Code PIN client:12345670

Start PIN

Etape 2 Lancez le processus PBC par WPS dans les 2 minutes qui suivent pour établir la connexion WPS. Une fois établie la connexion WPS, la page suivante apparaît, indiquant que la connexion WPS a réussi.

Succès!

Le client sans fil vient d'être ajouté au réseau avec succès.
Cliquez sur OK pour revenir à la page de configuration Wi-Fi sécurisée.

OK

9.5.3 Fonction client sans fil

Allez dans **Paramètres sans fil > Fonction client sans fil** pour accéder à la page **Fonction client sans fil**.

Fonction client sans fil

Cette page a pour but de vous aider à configurer le client sans fil.

Étape 1: Cliquez sur "Étude de sites" pour étudier les sites sans fil quand le mode client est activé. Si un point d'accès ou un IBSS est trouvé, les résultats sont affichés dans la liste d'étude de sites trois secondes plus tard; vous pouvez faire en sorte que n'importe qui se connecte manuellement. Puis cliquez sur "Suivant".

Étude de sites

Nombre de sites scannés :32

Liste d'étude de sites

#	SSID	BSSID	Chaîne	Signal	Cryptage	Sélectionner
1	TW-2B08	00:1F:A4:91:2A:60	9	100%	WPA-PSK(AES/TKIP)/ WPA2-PSK(AES/TKIP)	<input checked="" type="radio"/>
2	feifei002	00:1F:A4:92:56:3F	1	91%	WPA-PSK(AES/TKIP)/ WPA2-PSK(AES/TKIP)	<input type="radio"/>
3	CHENQL_NETGEAR	4C:60:DE:E1:E7:20	8	86%	WPA-PSK(AES/TKIP)/ WPA2-PSK(AES/TKIP)	<input type="radio"/>

Suivant

Étape 1 Cliquez sur **Étude de sites** pour rechercher le réseau sans fil auquel vous souhaitez vous connecter.

Étape 2 Tapez les informations de cryptage du réseau sans fil choisi. Configurez le client avec les mêmes paramètres de sécurité que le réseau choisi. Cliquez sur **Suivant**.

Fonction client sans fil

Étape 2: Vous devez configurer votre client sans fil manuellement, de manière à ce qu'il ait les mêmes paramètres de sécurité sans fil que le réseau choisi. Puis cliquez sur "Suivant".

Options de sécurité

Options de sécurité :

- Jamais
- Jamais
- WEP
- WPA-PSK(TKIP)
- WPA-PSK(AES)
- WPA2-PSK(TKIP)
- WPA2-PSK(AES)

Étape 3 Si vous cochez la case **Synchroniser le SSID et les options de sécurité du répéteur universel sans fil et du point d'accès de liaison montante**, l'appareil fournit des services d'itinérance sans fil. Cliquez sur **Terminer**. Le client peut maintenant communiquer avec le réseau choisi.

Fonction client sans fil

Étape 3: Cette page vous explique comment configurer le répéteur sans fil universel de manière simple. Si cette fonction est activée, le répéteur sans fil universel utilise le même SSID et les mêmes options de sécurité avec point d'accès de liaison montante. Pour finir, cliquez sur "Terminer".

Synchroniser le SSID et les options de sécurité du répéteur universel sans fil et du point d'accès de liaison montante

Remarque: Si vous modifiez les paramètres du répéteur universel sans fil, les clients sans fil souhaitant s'y connecter devront utiliser un nouvel SSID et de nouvelles options de sécurité.

Retour

Terminer

9.6 Fonction gestion

Pour plus de détails, reportez-vous à la section **7.6 Fonction gestion**.

10 Configuration Web pour le mode WDS

10.1 Statut fonctionnement

Pour plus de détails, reportez-vous à la section **9.1 Statut fonctionnement**.

10.2 Assistant de configuration

Pour la configuration, reportez-vous à la section **6.4 WDS Mode**.

10.3 Réglage du mode

Cliquez sur **Réglage du mode** pour accéder à la page **Réglage du mode**.

Réglage du mode de répétition

Deux modes permettent d'étendre le réseau sans fil de votre mode de répétition. Vous avez le choix entre le mode WDS et le mode UR.

Choisissez l'un des modes de répétition suivants:

Mode WDS

Mode répéteur sans fil universel

Appliquer

Annuler

Cochez la case **Mode WDS**. Veuillez noter que la fonction WDS est inaccessible si le canal est réglé sur **Auto**.

10.4 Paramètres réseau

Pour plus de détails, reportez-vous à la section **7.6**.

10.5 Paramètres sans fil

Cliquez sur **Paramètres sans fil** pour afficher le menu de navigation étendu.

Paramètres sans fil

Fonction WDS

Paramètres de base sans fil

10.5.1 Fonction WDS

La fonction WDS (Wireless distribution system, "système de distribution sans fil") permet l'interconnexion entre les différents points d'accès dans un réseau sans fil IEEE 802.11. Elle étend le réseau sans fil par plusieurs points d'accès, sans connexion du réseau central câblé. Activez la fonction WDS si vous souhaitez permettre la répétition ou le pontage sans fil.

Allez dans **Paramètres sans fil > Fonction WDS** pour accéder à la page **Fonction WDS**.

Fonction WDS

Désactiver l'association de clients sans fil

MAC sans fil de ce routeur: 00:1E:E3:4B:06:6C

Répéteur sans fil

Adresse IP du répéteur:

Adresse MAC de la station de base:

Appliquer

Annuler

- **Désactiver l'association de clients sans fil:** Si cette case est cochée, le répéteur ne transmet pas les signaux aux clients qui lui sont connectés. De manière générale, laissez cette boîte vide. De manière générale, cochez cette boîte.
- **Adresse IP du répéteur:** L'adresse IP du répéteur doit être différente de celle de la station de base sans fil et des autres répéteurs, afin d'éviter tout conflit. Nous vous conseillons d'utiliser des adresses IP du même segment de réseau pour les répéteurs et la station de base sans fil.
- **Adresse MAC de la station de base:** Tapez l'adresse MAC de la station de base sans fil.

Une fois les paramètres réglés, cliquez sur **Appliquer** pour les sauvegarder.

Pour une description de l'application WDS, reportez-vous à la section **6.4.3**

10.5.2 Paramètres de base sans fil

Pour plus de détails, reportez-vous à la section **7.5.1 Paramètres de base sans fil**.

10.6 Fonction gestion

Pour plus de détails, reportez-vous à la section **7.6 Fonction gestion**.

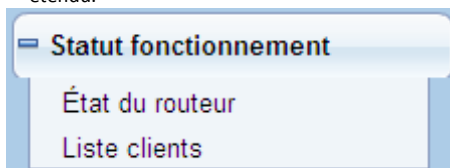
11 Configuration Web en mode client

Remarque:

Mettez sur **Client** l'interrupteur à trois positions situé sur le panneau latéral.

11.1 Statut fonctionnement

Repérez l'interrupteur à trois positions sur le boîtier de l'appareil, et mettez-le sur le mode Client. Cliquez sur **Statut fonctionnement** pour afficher le menu de navigation étendu.



11.1.1 État du routeur

Allez dans **Statut fonctionnement** > **Statut routeur** pour accéder à la page **Statut routeur**.

État du routeur

Infos système	
Version matériel	V1.0.0
Version micrologiciel	V1.0.0
Numéro de modèle	Wireless Router
Mode de travail	Mode client
Heure et date	1971-01-01 08:01:30
Port LAN	
Adresse MAC	00:1E:E3:4B:06:6C
Adresse IP	192.168.100.253
Masque de sous-réseau IP	255.255.255.0
Client sans fil	
Nom choisi de réseau sans fil (SSID)	
Canal sans fil	2.412GHz- CH1
Wi-Fi Protected Setup (WPS)	ON
Mode sécurité sans fil	Jamais
Statut connexion	Déconnecté

Sur cette page, vous trouverez des informations sur le statut de fonctionnement actuel de l'appareil (système, port LAN, client sans fil).

11.1.2 Liste clients

Allez dans **Statut fonctionnement > Liste clients** pour accéder à la page **Liste clients**.

Liste clients

Appareils reliés			
#	Adresse IP	Adresse MAC	Nom du périphérique
1	192.168.100.10	48:02:2A:D1:A9:60	unknown

Sur cette page, vous trouverez des informations sur les périphériques sans fil connectés à l'appareil (adresse IP et adresse MAC de chacun des périphériques etc.).

11.2 Assistant de configuration

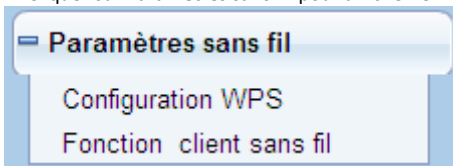
Pour plus de détails, reportez-vous à la section **6.5**.

11.3 Paramètres réseau

Pour plus de détails, reportez-vous à la section **7.6**.

11.4 Paramètres sans fil

Cliquez sur **Paramètres sans fil** pour afficher le menu de navigation étendu.



11.4.1 Configuration WPS

Pour les détails, reportez-vous à la section **7.5.4 Configuration WPS**.

11.4.2 Fonction client sans fil

Pour plus de détails, reportez-vous à la section **9.5.3 Fonction client sans fil**.

11.5 Fonction gestion

Pour plus de détails, reportez-vous à la section **7.6 Fonction gestion**.

Appendix A Questions-réponses

1	L'appareil n'est pas détecté par l'adaptateur réseau sans fil. Lorsque l'appareil est en mode client ou répéteur mais déconnecté du point d'accès de liaison montante, il n'accepte pas l'accès client sans fil et ne peut être connecté que par câble Ethernet. Si le problème persiste, l'appareil est probablement situé trop loin du terminal, à moins que le signal sans fil ne soit bloqué par un obstacle. Mettez l'appareil dans un emplacement près du terminal ou ajoutez un répéteur sans fil. D'autre part, les fours micro-ondes, les appareils Bluetooth et les téléphones sans fil doivent rester à distance des appareils WLAN, car ils sont de nature à interrompre les signaux WLAN.
2	L'adaptateur réseau sans fil n'arrive pas à se connecter à l'appareil. Certaines versions anciennes d'adaptateurs réseau sans fil peuvent être incompatibles avec l'authentification WPA2. Les réglages possibles de cryptage et d'authentification sont les suivants: WPA-AES, WPA-TKIP ou WEP.
3	En mode répéteur ou en mode client, l'appareil n'arrive pas à se connecter à Internet par l'intermédiaire du point d'accès de liaison montante (ex: la passerelle domestique), ou il se déconnecte très souvent. Vérifiez si l'appareil est actuellement en couverture de signal sans fil de son appareil en amont. Dans Fonction client sans fil , cliquez sur Étude de sites et vérifiez si l'appareil est capable ou non de trouver les signaux sans fil puissants en provenance du point d'accès de liaison montante.
4	La connexion câblée avec l'appareil est anormale. Vérifiez l'état du témoin Ethernet de l'appareil. Si le témoin Ethernet est éteint, cela signifie peut-être que le câble Ethernet est mal branché. Si le problème persiste, changez le câble Ethernet.
5	Impossible d'accéder à Internet. Vérifiez si l'adaptateur réseau connecté à l'appareil peut obtenir une adresse IP automatiquement. En cas d'échec, activez le DHCP pour la passerelle domestique, ou configurez manuellement l'adresse IP de l'adaptateur réseau et du DNS.
6	Impossible de configurer l'appareil sur la page Web. Vérifiez si l'adresse IP de l'adaptateur réseau et celle de l'appareil sont sur le même segment de réseau. Configurez l'adresse IP de votre adaptateur réseau dans le segment de réseau de 192.168.100.2/253, en suivant la procédure décrite dans la section 5 "PC Configuration and Wireless Con". Allez dans Paramètres réseau > Paramètres de l'interface LAN et mettez comme adresse IP de l'appareil la même adresse réseau que celle de la passerelle du réseau domestique.
7	Connexion WPS impossible. Assurez-vous qu'un seul périphérique WPS connecté à l'appareil initie la session WPS dans les 2 minutes. Veuillez noter la différence de WPS lorsque l'appareil sert de point d'accès de liaison montante et lorsqu'il sert de périphérique client en aval en mode répéteur (voir section 9.5.2 WPS Setup). Veuillez vous reporter au tableau 4.1 pour une description détaillée du témoin WPS.

MISE AU REBUT



En tant que distributeurs responsables, nous sommes soucieux de l'environnement.

Nous vous prions donc de bien vouloir respecter la procédure de mise au rebut de votre produit, de l'emballage et, le cas échéant, des accessoires, afin de contribuer à la préservation des ressources naturelles et de garantir le recyclage des matériaux d'une manière respectueuse de la santé et de l'environnement.

Ce produit doit être mis au rebut d'une manière conforme aux lois et réglementations locales. Les produits électriques usagés ne doivent pas être jetés avec les ordures ménagères à la fin de leur durée de vie.

Contactez le magasin d'achat et les autorités locales pour plus d'informations concernant les procédures de mise au rebut et de recyclage.

En raison des mises au point et améliorations constamment apportées à nos produits, de petites incohérences peuvent apparaître dans le mode d'emploi. Veuillez nous excuser pour la gêne occasionnée.

Darty Plc © UK: EC1N 6TE 21 / 11/ 2013

Declaration of Conformity

The following product has been deemed to comply with the requirements of the listed European Directives:-

R&TTE Directive (1999 / 5 / EC)

Electromagnetic Compatibility Directive (2004/108/EC)

Low Voltage Directive (2006/95/EC)

RoHS2 (2011/65/EU)

Product Description: 300 Mbps wireless repeater

Brand: I.T.Works

Model number: REPW300

The above listed products conform to the following EU Standards:

EN 62311: 2008

EN 301 489-17 V2.2.1

EN 300 328 V1.7.1

EN 301 489-1 V1.9.2

EN60950-1:2006 + A11:2009 + A1:2010+A12:2011

The person responsible for this declaration is:

Name: François Lemauf

Position: General Manager of Direct Sourcing

Signature:

Date: 6th January, 2014



DUTCH

300 Mbps WiFi-versterker

Model: REPW300



HANDLEIDING

Inhoudsopgave

1	Veiligheidsvoorzorgen	4
2	Overzicht van het apparaat	5
2.1	Voorstelling van uw apparaat	5
2.2	Paklijst	5
3	Voorstelling van de verschillende modi	6
3.1	Brugmodus	6
3.2	Router-modus	6
3.3	Draadloze universele repeater/WDS-modus	6
3.4	Cliëntmodus	6
4	Beschrijving van de hardware en vereisten	6
4.1	Beschrijving van de hardware	6
4.1.1	Voorpaneel en LED-status	6
4.1.2	Beschrijving van het achter/zijpaneel en de interface	8
4.2	Hardware-vereisten	9
4.2.1	Systeemvereisten	9
4.2.2	Voordat u van start gaat	9
4.3	Werkingsbereik	9
5	Pc-configuratie en configuratie van de draadloze verbinding	10
5.1	Pc-configuratie	10
5.2	Configuratie van de draadloze verbinding	12
6	Het apparaat configureren	14
6.1	Configuratie van de brugmodus	15
6.2	Configuratie van de router-modus	16
6.3	Configuratie van de repeater-modus	18
6.4	WDS-modus	19
6.4.1	Configuratie van de repeater in de WDS-modus	19
6.4.2	Configuratie van het centraal basisstation in de WDS-modus	20
6.4.3	WDS-toepassing	21
6.5	Configuratie van de cliëntmodus	22
7	Webconfiguratie in de Brugmodus	23
7.1	Werkingsstatus	23
7.1.1	Router-status	23
7.1.2	Cliëntenlijst	24
7.2	Installatie-wizard	24
7.3	Modusinstelling	25
7.4	Netwerkinstellingen	25
7.4.1	Instellingen van de LAN-interface	25
7.4.2	DHCP-server	26

7.5	Draadloze instellingen	27
7.5.1	Draadloze basisinstellingen.....	28
7.5.2	Gastnetwerk	31
7.5.3	Draadloze geavanceerde instellingen.....	32
7.5.4	WPS-instelling.....	36
7.6	Managementfunctie.....	37
7.6.1	Back-up-instellingen	38
7.6.2	Apparaat heropstarten	39
7.6.3	Wachtwoord instellen.....	39
	Router-upgrade	40
8	Webconfiguratie in router-modus	41
8.1	Werkingsstatus	41
8.1.1	Router-status	41
8.1.2	Cliëntenlijst.....	42
8.2	Installatie-wizard	43
8.3	Modusinstelling.....	43
8.4	Netwerkinstellingen	43
8.4.1	Instellingen van de LAN-interface	44
8.4.2	Instellingen van de WAN-interface	44
8.4.3	DHCP-server.....	51
8.4.4	NAT ALG	52
8.5	Draadloze instellingen	53
8.5.1	Draadloze basisinstellingen.....	53
8.5.2	Gastnetwerk	53
8.5.3	Draadloze geavanceerde instellingen.....	54
8.5.4	WDS-functie.....	54
8.5.5	WPS-instelling.....	55
8.6	Netwerktoepassing.....	55
8.6.1	Poort-forwarding	55
8.6.2	Poort-triggering	56
8.6.3	UPnP	58
8.6.4	IGMP-proxying	59
8.6.5	DMZ-server	59
8.6.6	Dynamische DNS.....	60
8.6.7	Statische routes	61
8.7	Beveiligingsopties.....	62
8.7.1	Sites blokkeren.....	62
8.7.2	Services blokkeren	63
8.7.3	Beveiliging	65
8.8	Managementfunctie.....	65

8.8.1	Back-up-instellingen	66
8.8.2	Management op afstand.....	66
8.8.3	Tijdsschema's	67
8.8.4	SNTP	68
8.8.5	Apparaat heropstarten	69
8.8.6	Wachtwoord instellen.....	69
8.8.7	Router-upgrade.....	69
9	Webconfiguratie in de draadloze universele repeater-modus	70
9.1	Werkingsstatus	70
9.1.1	Router-status	70
9.1.2	Cliëntenlijst.....	70
9.2	Installatie-wizard	71
9.3	Instelling van de repeater-modus	71
9.4	Netwerkinstellingen	71
9.5	Draadloze instellingen	71
9.5.1	Draadloze universele repeater	72
9.5.2	WPS-instelling.....	72
9.5.3	Draadloze cliëntfunctie	76
9.6	Managementfunctie	77
10	Webconfiguratie voor de WDS-modus	77
10.1	Werkingsstatus	77
10.2	Installatie-wizard	77
10.3	Modusinstelling	77
10.4	Netwerkinstellingen	77
10.5	Draadloze instellingen	77
10.5.1	WDS-functie.....	77
10.5.2	Draadloze basisinstellingen.....	78
10.6	Managementfunctie	78
11	Webconfiguratie in de cliëntmodus	79
11.1	Werkingsstatus	79
11.1.1	Router-status	79
11.1.2	Cliëntenlijst	79
11.2	Installatie-wizard	80
11.3	Netwerkinstellingen	80
11.4	Draadloze instellingen	80
11.4.1	WPS-instelling.....	80
11.4.2	Draadloze cliëntfunctie	80
11.5	Managementfunctie.....	80

1 Veiligheidsvoorzorgen

Lees de onderstaande veiligheidsvoorzorgen aandachtig voordat u repeater begint te gebruiken:

- Laat voldoende ruimte voor warmteafvoer rondom het apparaat om schade door oververhitting te voorkomen. De openingen voor de warmteafvoer stellen het apparaat in staat normaal te werken, dek deze dus niet af.
- Houd dit apparaat uit de buurt van warmte-uitlaten of plaatsen waar de temperatuur hoog is. Voorkom dat het apparaat wordt blootgesteld aan rechtstreeks zonlicht.
- Bewaar dit apparaat in een droge plaats. Mors geen vloeistof op dit apparaat.
- Sluit dit apparaat niet aan op een pc of elektronisch product als uw techniker of breedband-provider u deze instructie niet geeft, omdat een foutieve aansluiting tot stroomproblemen of brandgevaar kan leiden.
- Zet dit apparaat niet neer op een onstabiele ondergrond.



Deze markering wordt aangebracht op producten die conform zijn de Europese veiligheidsnormen en de normen voor elektromagnetische congruentie.

2 Overzicht van het apparaat

2.1 Voorstelling van uw apparaat

Deze repeater of router in zakformaat, is doosvormig, makkelijk mee te nemen en eenvoudig te installeren. De draadloze transmissiesnelheid ervan bedraagt tot 300 Mbps. Het is een high-performance en IEEE802.11b/g/n-compatibel apparaat dat individuele gebruikers en SOHO (klein kantoor, thuishkantoor) een betrouwbare en handige netwerktoegang biedt. Het biedt web-gebaseerde GUI, dat gebruikers toestaat de instellingen voor verbinding van het apparaat met de ISP (internetservice provider) gemakkelijk te wijzigen en upgrades via de webpagina eenvoudig uit te voeren. Daarnaast beschikt dit apparaat over een driewegschakelaar op het zijpaneel, waarmee gebruikers voor de werkmodus van het apparaat kunnen kiezen uit onder meer AP, repeater en cliënt. In de AP-modus functioneert het apparaat als een draadloze router om een draadloze verbinding te maken met draadgebonden LAN. In de Repeater-modus biedt het apparaat de functie URM (universele repeater-modus), waarmee gebruikers de draadloze dekking van de bestaande AP snel en gemakkelijk kunnen uitbreiden. In de Cliëntmodus functioneert het apparaat dan weer als een draadloze netwerkadapter, maar dan met een betere performance qua transmissie en verbindingsskwaliteit.

2.2 Paklijst

Controleer of de onderstaande items in de verpakking aanwezig zijn:

- 1 x 300 Mbps draadloze repeater
- 1 x netwerkkabel
- 1 x handleiding (CD)

3 Voorstelling van de verschillende modi

3.1 Brugmodus

In de Brugmodus functioneert dit apparaat als een draadloze router om draadloze verbinding te maken met de draadgebonden LAN.

3.2 Router-modus

In de Router-modus werkt het apparaat als een domestic gateway.

3.3 Draadloze universele repeater/WDS-modus

In de Draadloze universele repeater/WDS-modus breidt dit apparaat de draadloze dekking van de bestaande AP uit. Computers kunnen zowel draadgebonden als draadloos met het apparaat verbinden.

3.4 Cliëntmodus

In de Cliëntmodus biedt dit apparaat Internettoegang voor een settopbox of een computer met een netwerkadapter.

4 Beschrijving van de hardware en vereisten

4.1 Beschrijving van de hardware

4.1.1 Voorpaneel en LED-status

Er zijn 4 LED-indicatoren op het voorpaneel van het apparaat. Aan hun status kunt u zien of het apparaat normaal werkt of niet.



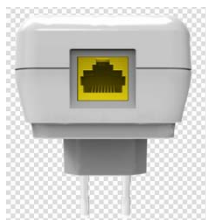
De onderstaande tabel geeft een overzicht van de indicator-statussen van het apparaat.

Indicator	Kleur	Status	Beschrijving
Power	Groen	Aan	Het apparaat functioneert normaal.
	Rood	Aan	Het systeem is bezig met een zelf-inspectie of de zelf-inspectie is mislukt. Of het is bezig de software te upgraden.
WPS	Groen	Uit	De WPS-sessie is afgelopen.
		Aan	The WPS -indicator blijft nog 5 minuten branden nadat de WPS-verbinding (Wi-Fi beveiligde instelling) tot stand is gebracht.
		Snel knipperend	Een terminal probeert met het apparaat te verbinden via WPS maar dit mislukt.
		Snel knipperend met een bepaalde tussentijd	Meerdere terminals proberen tegelijkertijd via WPS met het apparaat te verbinden. Conflict tussen WPS-sessies.
		Langzaam knipperend	De WPS-sessie is afgelopen.
Ethernet	Groen	Uit	De Ethernetpoort bevindt zich in de non-communicatieve status.
		Aan	De Ethernetpoort bevindt zich in de communicatieve status.

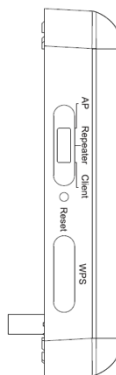
		Knipperend	De Ethernetpoort is bezig data te verzenden en ontvangen.
WLAN	Groen	Uit	De WLAN-verbinding bevindt zich in de non-communicatieve status.
		Aan	De WLAN-verbinding bevindt zich in de communicatieve status.
		Knipperend	Data wordt in de WLAN verzonden en ontvangen.

4.1.2 Beschrijving van het achter/zijpaneel en de interface

Achterpaneel



Zijpaneel



De onderstaande tabel geeft een overzicht van de interface- en toetsenstatus van het apparaat.

Interface/toets	Beschrijving
WAN/LAN	Als het apparaat is ingesteld op de AP-modus is de interface een WAN-interface die WAN- of uplink-netwerkapparaten met elkaar verbindt. Als het apparaat is ingesteld op de Repeater/cliëntmodus is de interface een LAN-interface.
Terugstellen	Houd de toets Terugstellen (Reset) 3-6 seconden zacht ingedrukt en laat dan los. Het systeem stelt zich terug naar de standaardfabrieksinstellingen.
AP/repeater/cliënt	Wordt gebruikt om het apparaat in te stellen op de AP-, Repeater- of Cliëntmodus. AP-modus—waaronder de Brug- en Routermodus Repeater-modus—om de dekking van het draadloze

	<p>netwerk uit te breiden</p> <p>Cliëntmodus—equivalent aan een draadloze netwerkadapter</p>
WPS	<p>Voor het inschakelen van de WPS PBC-modus. Verwijs voor meer informatie naar de WPS-beschrijvingen voor elke modus.</p>

4.2 Hardware-vereisten

4.2.1 Systeemvereisten

Zorg voordat u het apparaat installeert dat de onderstaande items beschikbaar zijn:

- Tenminste één Ethernet RJ45 kabel (10Base-T/100Base-T)
- Eén draadloze repeater
- Een pc met het TCP/IP-protocol reeds geïnstalleerd en met internettoegang.

4.2.2 Voordat u van start gaat

Besteed aandacht aan de volgende items voordat u het apparaat installeert:

- De ethernetkabels die worden gebruikt om het apparaat op een computer, hub, router of schakelaar aan te sluiten mogen niet langer zijn dan 100 meter.
- Zet dit apparaat niet neer op een oneffen of onstabiele ondergrond. Leg het apparaat niet op de grond.
- Houd dit apparaat schoon. Stel dit apparaat niet bloot aan rechtstreeks zonlicht. Let erop dat geen metaal in het apparaat terecht komt.
- Zet dit apparaat in het midden van de ruimte voor een optimale draadloze dekking.

4.3 Werkingsbereik

Het werkingsbereik van het apparaat is afhankelijk van omgevingsfactoren. Het pad en effect van de signaaltransmissie varieert naargelang men het apparaat thuis gebruikt of in een kantoor. Buiten kan de transmissie in rechte lijn voor een bepaald apparaat bijvoorbeeld tot 300 meter reiken, terwijl de transmissie binnen 100 meter kan bedragen.

5 Pc-configuratie en configuratie van de draadloze verbinding

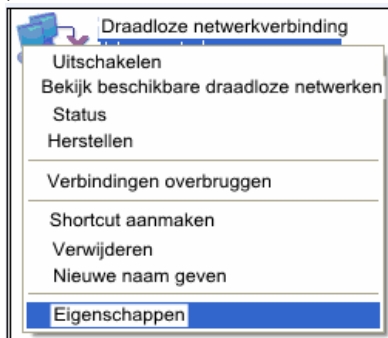
5.1 Pc-configuratie

Hieronder nemen we Windows XP als voorbeeld. Ga als volgt te werk om de netwerkadapter handmatig in te stellen:

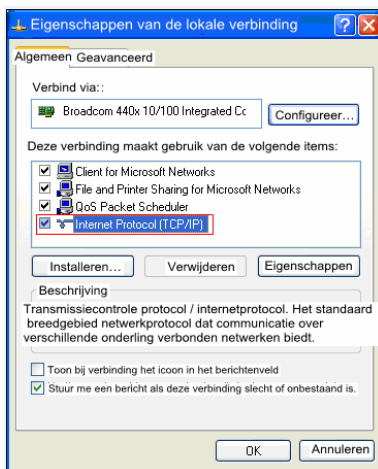
Stap 1 Klik met de rechtermuisknop op het icoon van **Mijn netwerkplaatsen** en kies **Eigenschappen** om het venster van de **Netwerkverbindingen** op de display te zien.



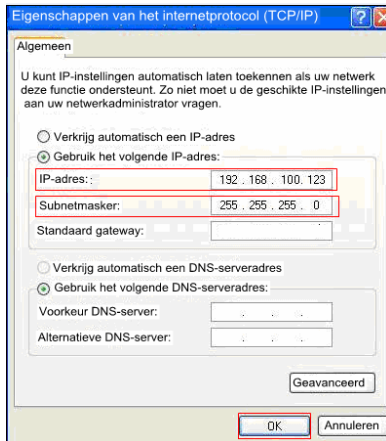
Stap 2 Klik met de rechtermuisknop op het icoon van een netwerk interface-kaart of draadloze netwerkadapter en kies **Eigenschappen**. (Opmerking: in de Cliëntmodus kunnen computers alleen via een ethernetkabel met het apparaat verbinden.)



Stap 3 Dubbelklik op Internet-protocol (TCP/IP).



Stap 4 Selecteer **Verkrijg automatisch een IP-adres** wanneer het apparaat in de Router-modus is geschakeld. In de andere modi van het apparaat stelt u **192.168.100.X** (X is een geheel getal tussen 2 en 253) in als het IP-adres van uw computer, en 255.255.255.0 als het MAC-adres. Stel de gateway en het IP-adres van de DNS-server in. U kunt deze leeg laten als u geen informatie heeft over de gateway en DNS-server. Klik op **OK**.




Opmerking:

Nadat het apparaat is geconfigureerd kan de domestic gateway het internet-protocol voor de netwerkadapter van de pc instellen. Stel het IP-adres en de DNS-server in om automatisch een IP-adres te verkrijgen als aangegeven in de bovenstaande figuur.

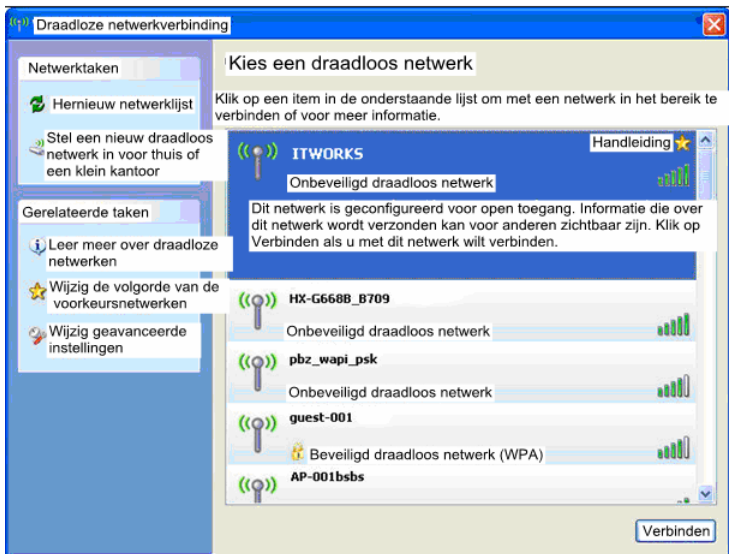
5.2 Configuratie van de draadloze verbinding

We nemen Windows XP als voorbeeld. Ga als volgt te werk om de draadloze netwerkadapter van uw pc met het apparaat te verbinden:

Stap 1

Stap 1 Klik op het icoon  in de rechter benedenhoek van het bureaublad (Opmerking: zorg ervoor dat een draadloze netwerkadapter op uw pc is geïnstalleerd).

Stap 2 Klik in de pagina van de **Draadloze netwerkverbinding** op het gewenste draadloze netwerk.



Stap 3 Uw computer is verbonden met het draadloze netwerk wanneer **Verbonden** in de rechterbovenhoek van de display is aangegeven.

Draadloze netwerkverbinding

Kies een draadloos netwerk

Klik op een item in de onderstaande lijst om met een netwerk in het bereik te verbinden of voor meer informatie.

Netwerktaken

- Hernieuw netwerklijst
- Stel een nieuw draadloos netwerk in voor thuis of een klein kantoor

Gerelateerde taken

- Leer meer over draadloze netwerken
- Wijzig de volgorde van de voorkeursnetwerken
- Wijzig geavanceerde instellingen

ITWORKS verbonden

Onbeveiligd draadloos netwerk

Dit netwerk is geconfigureerd voor open toegang. Informatie die over dit netwerk wordt verzonden kan ook voor anderen zichtbaar zijn. U bent momenteel met dit netwerk verbonden. Klik op Loskoppelen als u de verbinding met dit netwerk ongedaan wilt maken.

HX-G668B_B709

Onbeveiligd draadloos netwerk

pbz_wapi_psk

Beveiligd draadloos netwerk (WPA)

guest-001

Beveiligd draadloos netwerk (WPA)

AP-001bsbs

Loskoppelen



Opmerking:


De standaard SSID van de repeater is ITWORKS.

6 Het apparaat configureren

De onderstaande tabel geeft een overzicht van the IP-informatie van de AP/repeater/cliëntmodi van het apparaat.

Modus op de behuizing	Beschikbare modus op het Web	Management IP-adres	Subnet MAC-adres	DHCP	Methode van verbinding met pc
AP	Brug (standaard)	192.168.100.253	255.255.255.0	Uitschakelen	Ethernetkabel /draadloos
	Router			Inschakelen	Alleen draadloos
Repeater	Draadloze universele repeater (standaard)	192.168.100.253	255.255.255.0	Uitschakelen	Ethernetkabel / draadloos
	WDS				
Cliënt	Cliënt (standaard)	192.168.100.253	255.255.255.0	Uitschakelen	Alleen ethernetkabel

- Stap 1** Schakel de driewegschakelaar op de behuizing van het apparaat naar de gewenste modus.
- Stap 2** Open Internet Explorer (IE). Voer het management IP-adres of **192.168.100.253** in en druk op **Enter**. Voer de gebruikersnaam en het wachtwoord (beide zijn **admin**) in het aanmeldvenster als hieronder aangegeven.



- Stap 3** Klik op Inloggen, zodat de onderstaande pagina verschijnt.

Klik op **Uitloggen** om uit te loggen op deze pagina.

Opmerking:

U kunt in de rechterbovenhoek kiezen uit de talen Engels en Frans.

Terminal-apparaten verkrijgen door de onderstaande stappen te volgen toegang tot het netwerk via de repeater nadat de configuratie is voltooid.

6.1 Configuratie van de brugmodus

Stap 1 **Stap 1** Schakel het apparaat in en schakel de driewegschakelaar op het zijpaneel naar **AP**. Log in op de configuratiepagina nadat het systeem is opgestart.

Stap 2 **Stap 2** Klik op **Installatie-wizard** in de navigatiebalk in het linkerveld van de pagina. Stel de SSID en het encryptie-wachtwoord in en noteer deze. Klik op **Voltoeien** om de instelling te beëindigen.

Installatie-wizard

Deze installatie-wizard helpt u bij het configureren van uw draadloze instellingen in de Brugmodus.

Schakel de draadloze router-radio in

Naam (SSID)

Naam (SSID)

:Beveiligingsopties

Beveiligingsopties

Beveiligingsopties (WPA2-PSK)

Geheime frase: 8-63 tekens of 64 hex-tekens

[Voltoeien](#) [Annuleren](#)

6.2 Configuratie van de router-modus

Stap 1 **Stap 1** Schakel het apparaat in en schakel de driewegschakelaar op het zijpaneel naar **AP**. Log in op de configuratiepagina nadat het systeem is opgestart.

Stap 2 **Stap 2** Klik op **Modusinstellingen** en selecteer **Router-modus** (de standaard is de **Brugmodus**). Klik op **Toepassen** om het apparaat te heropstarten.

Modusinstellingen:

Kies de gewenste modus als volgt:

Brugmodus

Router-modus

In deze modus wordt de poort als een WAN-poort gebruikt.
U kunt alleen op het web inloggen met behulp van uw draadloze netwerkkaart om met dit netwerk te verbinden.
Onthoud de SSID en de beveiligingsopties van uw draadloze netwerk voordat u deze modus wijzigt.

Bekijk draadloze basisconfig.

Toepassen Annuleren

Stap 3 **Stap 3** Ontkoppel de netwerkkabel en sluit de pc aan op het apparaat met behulp van de draadloze netwerkadapter nadat het apparaat is heropgestart. Log in op de configuratiepagina. Klik op **Installatie-wizard** in de navigatiebalk op het linkerveld van de pagina. Selecteer **Ja** en klik op **Volgende**. Het apparaat zal het breedband type automatisch detecteren.

Uw internet installeren

De slimme installatie-wizard detecteert automatisch het type internetverbinding dat u heeft.
Wilt u de slimme installatie-wizard het verbindingsstype nu laten detecteren?

Ja

Neen, ik wil de router zelf configureren

Volgende

Stap 4 **Stap 4** Dit apparaat kan drie types breedband detecteren: DHCP, Statische IP en PPPoE. Voer de configuraties uit in overeenstemming met het type breedband dat u gebruikt.

(1) Parameterconfiguratie voor DHCP

Installatie-wizard

Dynamische IP (DHCP) gedetecteerd
Het type internetverbinding dat u heeft is met succes gedetecteerd

Terug Volgende

Dynamisch IP-adres

Accountnaam (indien nodig)

Toepassen Annuleren

Voer de accountnaam van uw ISP in.
Laat dit leeg als uw ISP geen accountnaam heeft aangeboden.

(2) Parameterconfiguratie voor statische IP

Installatie-wizard

Statische IP (vast) gedetecteerd
Het type internetverbinding dat u heeft is met succes gedetecteerd.

Als u gelooft dat u dit bericht verkeerdelijk heeft ontvangen, moet u uw modem powercyclen (de modem loskoppelen en weer aansluiten). Sluit dan dit venster en heropen een nieuwe webbrowser (vb. Internet Explorer)

Terug **Volgende**

Statische (vaste) IP-adressen

Uw internet-service biedt instellingen voor statische (vaste) IP aan.

Let erop het correcte IP-adres in te voeren voor elke statische IP-instelling. Voer bijvoorbeeld het gateway IP-adres in het veld van het gateway IP-adres en het IP-adres in het veld van het IP-adres zonder deze te verwisselen.

Internet IP-adres

IP-adres	<input type="text"/>	→ Vereist
IP-subnetmasker	<input type="text"/>	
Gateway IP-adres	<input type="text"/>	

Domeinnaam (DNS) server-adres

Primaire DNS	<input type="text"/>	→ Optioneel
Secundaire DNS	<input type="text"/>	

Voltoeien Annuleren

(3) Parameterconfiguratie voor PPPoE

Installatie-wizard

PPPoE gedetecteerd
Het type internetverbinding dat u heeft is met succes gedetecteerd.

Terug **Volgende**

PPPoE

Wachtwoord instellen

Gebbruikersnaam:	<input type="text"/>	→ Voer de accountnaam en het wachtwoord in voor internetverbinding.
Wachtwoord:	<input type="text"/>	

Service-naam (indien nodig):

Domeinnaam (DNS) server-adres

Verkrijg automatisch van ISP

Gebruik deze DNS-servers

Primaire DNS	<input type="text"/>	→ Voer het DNS-adres in dat u van uw ISP heeft gekregen. Kies Verkrijg automatisch van ISP als uw ISP dit niet heeft gegeven.
Secundaire DNS	<input type="text"/>	

Toepassen **Annuleren**

Stap 5 **Stap 5** Klik op **Volgende**. Stel de SSID en het wachtwoord in en noteer deze. Klik op **Apply** om de installatie te voltooien.

Draadloze instellingen

Schakel de draadloze apparaat-radio in

Naam (SSID)

Naam (SSID):

Beveiligingsopties

Beveiligingsopties:

U kunt de standaard SSID gebruiken. Wij raden u echter aan de SSID te wijzigen.

Stel de draadloze encryptiemodus en het wachtwoord in.

6.3 Configuratie van de repeater-modus

- Stap 1** Schakel het apparaat in en schakel de driewegschakelaar op het zijpaneel naar **Repeater**. Sluit de netwerkkabel opnieuw aan op het apparaat en meld u aan op de configuratiepagina nadat het systeem is opgestart.
- Stap 2** Klik op **Installatie-wizard** in de navigatiebalk op het linkerveld van de pagina. Selecteer **draadloze universele repeater-modus** en klik op **Volgende**.

Installatie-wizard

Stap1: er zijn twee methodes om uw draadloze netwerk van de repeater-modus uit te breiden. U kunt de WDS-modus of de Draadloze universele repeater-modus kiezen.

Kies uw repeater-modus als volgt:

WDS-modus

Draadloze universele repeater-modus

Figure 1

- Stap 3** Klik op **Site-onderzoek** om te zoeken naar het draadloze netwerk waarmee u wilt verbinden. Selecteer het gewenste netwerk. Klik op **Volgende**.

Installatie-wizard

Stap2: configureer eerst de draadloze cliënt. Klik op de button "Site-onderzoek" om draadloze sites te onderzoeken terwijl de cliëntmodus is ingeschakeld Als een access-point of IBSS is gevonden worden de resultaten drie seconden later aangegeven de Lijst van het site-onderzoek. U kunt een van beide kiezen om deze handmatig te verbinden. Klik daarna op "Volgende".

Aantal sites gescand: 32

Lijst van het site-onderzoek

#	SSID	BSSID	rKanaal	Signaal	Encryptie	Selecteer
1	TW-2B08	00:1F:A4:91:2A:60	10	100%	WPA-PSK(AES/TKIP)/ WPA2-PSK(AES/TKIP)	<input checked="" type="radio"/>
2	Zoltrix_ZW919	00:28:12:34:56:78	1	100%	Geen	<input type="radio"/>
3	SMC	00:1F:A4:90:87:50	3	100%	WPA-PSK(AES/TKIP)/ WPA2-PSK(AES/TKIP)	<input type="radio"/>

- Stap 4** Configureer de repeater met dezelfde beveiligingsoptie als zijn uplink-netwerk. (In de onderstaande figuur wordt de beveiligingsoptie **Geen** als voorbeeld genomen.) Stel het encryptiewachtwoord en noteer dit ergens. Klik op **Volgende**.

Installatie-wizard

Stap3: u moet uw draadloze cliënt handmatig configureren zodat deze dezelfde draadloze beveiligingsinstellingen heeft als het netwerk dat u selecteerde. Klik daarna op "Volgende".

Beveiligingsopties draadloze cliënt

Beveiligingsopties draadloze cliënt

- Stap 5** Het apparaat biedt een draadloze roaming-functie wanneer **Synchroniseer de SSID en Beveiligingsopties van de draadloze universele repeater en Uplink AP** is geselecteerd. Zo niet moet u de SSID en beveiligingsopties voor de repeater handmatig configureren. Klik op **Voltoeien** om de installatie-wizard te voltooien.

Installatie-wizard

Stap4: deze pagina biedt een gemakkelijke manier om de draadloze universele repeater te configureren. Als u deze functie activeert, zal uw draadloze universele repeater dezelfde SSID en beveiligingsopties met uplink-AP gebruiken, of configureert u de SSID van de Uitgebreide Interface en Beveiligingsopties handmatig. Klik tenslotte op "Voltoeien".

Instellingen van de draadloze universele repeater

Synchroniseer de SSID en beveiligingsopties van de draadloze universele repeater en uplink-AP

SSID van de Uitgebreide Interface:

Beveiligingsopties:

Opmerking: als u de instellingen van de draadloze universele repeater heeft gewijzigd, zal de draadloze cliënt die met uw draadloze universele repeater verbindt dit opnieuw moeten doen met de nieuwe SSID en beveiligingsopties.

6.4 WDS-modus

6.4.1 Configuratie van de repeater in de WDS-modus

- Stap 1** **Stap 1** Schakel het apparaat in en schakel de driewegschakelaar op het zijpaneel naar **Repeater**. Log in op de configuratiepagina nadat het systeem is opgestart.
- Stap 2** **Stap 2** Klik op **Installatie-wizard** in de navigatiebalk op het linkerveld van de pagina. Selecteer **WDS-modus** en klik op **Volgende**. (Opmerking: de WDS-functie kan niet geactiveerd worden als het kanaal is ingesteld op **Auto**.) Stel alle WDS-apparaten handmatig in op hetzelfde kanaal.

Installatie-wizard

Stap1: er zijn twee methodes voor het uitbreiden van uw draadloze netwerk van de Repeater-modus. U kunt kiezen uit de WDS-modus of de Draadloze universele repeater-modus.

Kies uw repeater-modus als volgt:

WDS-modus

Draadloze universele repeater-modus

Volgende

Stap 3 **Stap 3** Stel het IP-adres van de LAN-poort van de repeater in en voer het MAC-adres van het basisstation in. Klik op **Volgende**.

Installatie-wizard

Stap2: in de WDS-modus functioneert het apparaat als een repeater en kan het alleen in de basisstation-modus communiceren met een ander draadloos station. U moet het draadloze MAC-adres van het andere draadloze station in de basisstation-modus invoeren in het veld genaamd "Basisstation Mac-adres" en het draadloze MAC-adres van de router in de webpagina van het andere draadloze station in de basisstation-modus. Het wijzigen van het IP-adres van de repeater veroorzaakt een wijziging van het LAN IP-adres.

WDS-instellingen

Draadloze MAC van deze router: 00:1E:E3:4B:06:6C

IP-adres van de repeater

MAC-adres van het basisstation

Terug Volgende

Stap 4 **Stap 4** Stel de SSID, het kanaal en de beveiligingsencryptie voor de repeater in. Het kanaal mag niet op **Auto** worden ingesteld. Het is raadzaam de repeater te configureren met dezelfde beveiligingsoptie als het basisstation ervan. Stel het encryptie-wachtwoord in en noteer dit ergens. Klik op **Voltoeien** om de installatie te voltooien.

Installatie-wizard

Stap3: WEP kan (en moet) worden gebruikt om de WDS-communicatie te beveiligen. Het kanaal "Auto" mag niet worden gebruikt.

Andere draadloze instellingen

Naam (SSID): ITWORKS

Kanaal: 1

Beveiligingsopties: Geen

Terug Voltoeien Annuleren

6.4.2 Configuratie van het centraal basisstation in de WDS-modus

Stap 1 **Stap 1** Schakel het apparaat in de Router-modus.

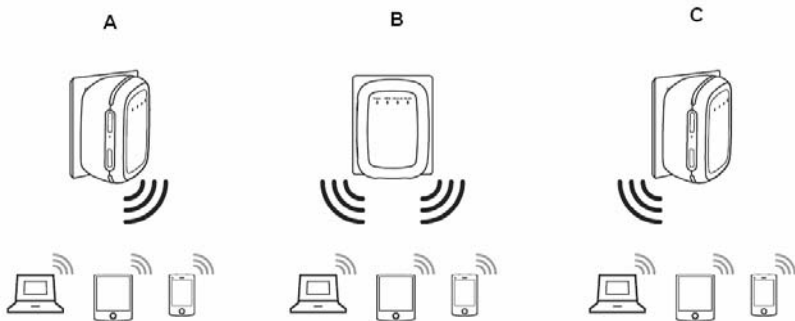
Stap 2 **Stap 2** Kies **Draadloze instellingen > WDS-functie**, selecteer **WDS-functie activeren** en voer het MAC-adres van de repeater in. (Opmerking: één basisstation kan met maximaal 4 repeaters verbinden).

WDS-functie

<input checked="" type="checkbox"/> WDS-functie activeren
<input type="checkbox"/> WDS-functie deactiveren
Draadloze MAC van deze router: 00:1E:E3:42:15:35
Draadloos basisstation
MAC-adres 1 van repeater: <input type="text"/>
MAC-adres 2 van repeater: <input type="text"/>
MAC-adres 3 van repeater: <input type="text"/>
MAC-adres 4 van repeater: <input type="text"/>

6.4.3 WDS-toepassing

De onderstaande figuur toont een draadloos netwerk voor een personeelsafdeling (gemarkeerd als A in de figuur), een financiële afdeling (gemarkeerd als B) en een marketingafdeling (gemarkeerd als C) in een bedrijf. Als de drie afdelingen één draadloze router delen, is het mogelijk dat de signalen die door de computers worden gevonden eerder zwak zijn, of zelfs dat geen signalen worden gevonden. Wanneer elk van de drie afdelingen echter gebruik maken van een draadloze router, kunnen we WDS gebruiken om de drie routers te verbinden voor een perfecte draadloze dekking van alle afdelingen.



Configureer de drie routers als volgt:

Draadloze router B functioneert als draadloos basisstation; draadloze routers A en C staan via WDS in verbinding met de draadloze router B.

(1) **De draadloze router B als het draadloze basisstation configureren**

Stap 1 Log in op de pagina van het web-management van draadloze router B. Kies **Draadloze instellingen > Draadloze basisinstellingen** en stel de SSID, het

kanaal en de draadloze encryptie-informatie in. Schrijf de SSID, het kanaal en de draadloze encryptie-informatie op, omdat u deze nog nodig heeft voor het configureren van draadloze routers A en C.

Stap 2 **Stap 2** Kies **Draadloze instellingen > WDS-functie** en schakel de WDS-functie in. Voer de MAC-adressen van de repeaters in (d.w.z. de draadloze routers A en C van dit voorbeeld). Klik op **Toepassen** om de instellingen op te slaan.

(2) **Draadloze router A configureren**

Doe het volgende om een WDS-verbinding tussen draadloze routers A en B tot stand te brengen:

Stap 1 **Stap 1** Stel draadloze router A in op hetzelfde kanaal en encryptie-informatie als draadloze router B.

Stap 2 **Stap 2** Kies **Draadloze instellingen > WDS-functie** en schakel de WDS-functie in. Stel een ander IP-adres voor draadloze router B in dan dat van draadloze router A om conflicten van IP-adressen te voorkomen (verander bijvoorbeeld het IP-adres naar 192.168.100.20 in de pagina van de **Instellingen van de LAN-interface** en log opnieuw in op de pagina van het Web-management). Voer het MAC-adres van het draadloze basisstation in.

Stap 3 Klik op **Toepassen** om de instellingen op te slaan.

De WDS-verbinding tussen draadloze routers A en B is dan tot stand gebracht.

(3) **Draadloze router C configureren**

Configureer draadloze router C op dezelfde manier als draadloze router A. Noteer dat het IP-adres van de LAN-interface moet worden gewijzigd naar een IP-adres dat niet conflicteert met de IP-adressen van bestaande computers of apparaten in het netwerk.

6.5 Configuratie van de cliëntmodus

Stap 1 Klik op **Installatie-wizard** in de navigatiebalk op het linkerveld van de pagina. Klik op **Site-onderzoek** om te zoeken naar het draadloze netwerk waarmee u verbinding wilt.

Installatie-wizard

Stap1: deze wizard helpt u bij het configureren van de draadloze cliënt. Klik op de button "Site-onderzoek" om de draadloze sites te onderzoeken terwijl de cliënt-modus is ingeschakeld. Zodra een access point of IBSS is gevonden, worden de resultaten drie seconden later in de lijst van het site-onderzoek weergegeven, en kunt u er een uit selecteren om er handmatig mee te verbinden. Klik dan op "Volgende".

Site-onderzoek

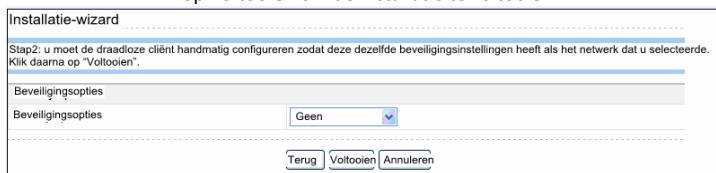
Aantal sites gescand: 32

Lijst van het site-onderzoek

#	SSID	BSSID	Kanaal	Signaal	Encrypteer	Selecteer
1	Zoltrix_ZW919	00:28:12:34:56:78	1	100%	Geen	<input checked="" type="radio"/>
2	TW-2B08	00:1F:A4:91:2A:60	10	100%	WPA-PSK(AES/TKIP) WPA2-PSK(AES/TKIP)	<input type="radio"/>
3	www24	00:1E:E3:C0:5F:6B	9	96%	Geen	<input type="radio"/>

Volgende

Stap 2 Voer de encryptie-informatie van het geselecteerde draadloze netwerk in. Klik op **Voltooien** om de installatie te voltooien.



Installatie-wizard


Stap2: u moet de draadloze cliënt handmatig configureren zodat deze dezelfde beveiligingsinstellingen heeft als het netwerk dat u selecteerde. Klik daarna op "Voltooien".

Beveiligingsopties

Beveiligingsopties Geen

Terug Voltooien Annuleren

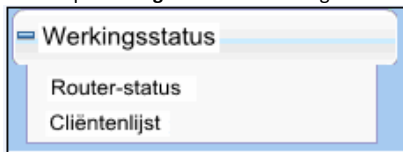
7 Webconfiguratie in de Brugmodus

 **Opmerking:**

Schakel de driewegschakelaar op het zijpaneel naar AP, selecteer de Brugmodus en herstart het apparaat. Meld aan op de configuratiepagina nadat het apparaat is heropgestart.

7.1 Werkingsstatus

Klik op **Werkingsstatus** om het uitgebreide navigatiemenu op de display te zien.



Klik op het submenu om een specifieke configuratiepagina binnen te gaan.

7.1.1 Router-status

Kies **Werkingsstatus** > **Router-status** om de pagina van de **Router-status** op de display te zien.

Router-status	
Systeeminfo	
Hardware-versie	V1.0.0
Firmware-versie	V1.0.0
Productnaam	Draadloze router
Werkmodus	Brugmodus
Tijd en datum	1971-01-01 08:26:38
LAN-poort	
MAC-adres	00:1E:E3:4B:06:6D
IP-adres	192.168.100.253
IP-subnetmasker	255.255.255.0
Draadloze poort	
Naam van draadloze netwerk (SSID)	ITWORKS
Regio	Gemixt 802.11/b/g/n
Draadloos kanaal	Auto
802.11-modus	Mixed 802.11b/g/n
Draadloze radio	Ingeschakeld
Uitzendnaam	AAN
Draadloze isolatie	UIT
Wi-Fi-beveiligde installatie (WPS)	AAN
Draadloze beveiligingsmodus	Geen

U kunt in deze pagina informatie over de huidige werkingsstatus van het apparaat zien, met onder meer de systeeminformatie, de status van de LAN-poort en de status van het draadloze netwerk.

7.1.2 Cliëntenlijst

Kies **Werkingsstatus > Cliëntenlijst** zodat de pagina van de **Cliëntenlijst** op de display verschijnt.

Cliëntenlijst			
Draadgebonden apparatuur			
#	IP-adres	MAC-adres	Apparaat naam
1	192.168.100.10	48:02:2A:D1:A9:60	unknown
Draadloze apparaten (draadloze indringers verschijnen hier ook)			
#	IP-adres	MAC-adres	Device Name
Hernieuwen			

Deze pagina toont informatie van computers die met de router zijn verbonden, met onder meer de IP-adressen en het MAC-adres van elke computer.

7.2 Installatie-wizard

Verwijs voor de instellingen naar paragraaf **6.1 Configuratie van de brugmodus**.

7.3 Modusinstelling

Klik op **Modusinstellingen** om de pagina van de **Modusinstellingen** op de display te zien.

Modusinstellingen

Kies uw modus als volgt:

Brugmodus

In deze modus wordt de poort gebruikt als een LAN-poort.
U kunt op het web inloggen door ofwel uw draadgebonden netwerkkaart en de LAN-poort met ethernetkabel te verbinden ofwel uw draadloze netwerkkaart te gebruiken om dit draadloze netwerk te verbinden.

Router-modus

[Bekijk de Draadloze basisconfiguratie](#)

[Toepassen](#) [Annuleren](#)

- **Brugmodus:** de interface op de behuizing ervan is een LAN-interface. Gebruikers kunnen het apparaat met de pc verbinden door middel van een RJ45-kabel of draadloze netwerkkaart.
- **Router-modus:** computers kunnen alleen op een draadloze manier met het apparaat verbinden.

7.4 Netwerkinstellingen

Klik op **Instellingen van de LAN-interface** om het uitgebreide navigatiemenu op de display te zien.



7.4.1 Instellingen van de LAN-interface

Kies **Netwerkinstellingen** > **Instellingen van de LAN-interface** om de pagina van de **Instellingen van de LAN-interface** op de display te zien.

Instellingen van de LAN-interface

Instellingen van LAN TCP/IP

IP-adres:

IP-subnetmasker

[Toepassen](#) [Annuleren](#)

U kunt zo nodig het IP-adres en IP-subnetmasker van de LAN-poort wijzigen.



Opmerking:

Als u het standaard IP-adres wijzigt, moet u het nieuwe IP-adres gebruiken om in te loggen op de Webconfiguratie-pagina van de router en moet de standaard gateway van alle hosts in de LAN worden ingesteld op het nieuwe IP-adres voor internettoegang.

Het subnetmasker van alle hosts in de LAN moet hetzelfde zijn als het subnetmasker dat is vooropgesteld in de pagina Instellingen van de LAN-interface.

7.4.2 DHCP-server

Kies **Netwerkinstellingen > DHCP-server** om de pagina van de **DHCP-server** op de display te zien.

DHCP staat voor Dynamische Host Configuratieprotocol. Als **Gebruik apparaat als DHCP-service** is geselecteerd, kent het apparaat automatisch IP-adressen toe aan computers in de LAN. Gebruikers hoeven de parameters van het TCP/IP-protocol niet te configureren, zoals daar zijn het IP-adres, het subnetmasker, de gateway en de DNS-serverinformatie voor computers die zijn verbonden met de LAN van de router.

DHCP-server

Gebruik router als DHCP-server

Startend IP-adres

Eindigend IP-adres

DHCP-leasetijd (1-160 uur)

Adresreservatie

#	IP-adres	Apparaat-naam	MAC-adres
Toevoegen Bewerken Verwijderen			

Toepassen | Annuleren

7.4.2.1 De router als een DHCP-server gebruiken

- **Om de router als DHCP-server te gebruiken:** als u het vakje bij **Gebruik router als DHCP-server** aanvinkt doet het apparaat dienst als een DHCP-server om automatisch IP-adressen toe te kennen aan computers die ermee zijn verbonden.
- **Startend IP-adres/eindigend IP-adres:** stel de startende en eindigende IP-adressen in om een poel van IP-adressen te specificeren die de DHCP-server zal toekennen. Nadat u het **Startend IP-adres/eindigend IP-adres** heeft ingesteld verkrijgen hosts in de LAN IP-adressen die binnen de reikwijdte van het startende en eindigende IP-adres liggen.
- **DHCP-leasetijd:** de geldigheidsduur van een IP-adres dat automatisch door de DHCP-server aan een host is toegekend. De DHCP-server kent dit IP-adres binnen de ingestelde periode niet aan andere hosts toe.

7.4.2.2 Adresreservatie gebruiken

Wanneer u een gereserveerd IP-adres voor een computer in de LAN specificeert, zal deze computer altijd hetzelfde IP-adres krijgen telkens wanneer hij de DHCP-server van de router binnegaat. Gereserveerde IP-adressen moeten worden toegekend aan computers of servers die permanente IP-instellingen vereisen.

Adresreservatie			
#	IP-adres _s	Apparaat-naam	MAC-adres
<input type="button" value="Toevoegen"/> <input type="button" value="Bewerken"/> <input type="button" value="Verwijderen"/>			

Om een IP-adres te reserveren:

Stap 1 **Stap 1** Klik op **Toevoegen** om de pagina van de **adresreservatie** binnen te gaan.

Adresreservatie

Tabel van de adresreservatie			
#	IP-adres _s	Apparaat naam	MAC-adres _i
<input type="radio"/>	1		
<input type="radio"/>	2	192.168.100.10	dW5rBm93bg==

IP-adres:

MAC-adres:

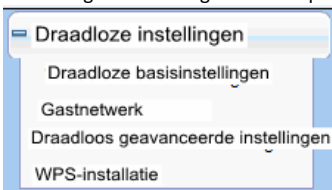
Apparaat naam:

Figure 2

- Stap 2** **Stap 2** Selecteer één item uit de **Tabel van de adresreservatie** of voer het IP-adres in het veld voor het **IP-adres** in om dat toe te kennen aan de computer of server (Kies een IP-adres uit de IP-adressenpoel die u heeft gespecificeerd, bijv. 192.168.100.x). Voer het MAC-adres en de apparaat-naam van de computer of server in.
- Stap 3** **Stap 3** Klik op **Toevoegen** om een nieuw item aan **adresreservatie** toe te voegen.
- Stap 4** **Stap 4** Klik op **Toepassen** om de instellingen op te slaan.

7.5 Draadloze instellingen

Schakel de driewegschakelaar op het zijpaneel naar **AP**. Klik op **Draadloze instellingen** om het uitgebreide navigatiemenu op de display te zien.



7.5.1 Draadloze basisinstellingen

Kies **Draadloze instellingen** > **Draadloze basisinstellingen** om de pagina van de **Draadloze basisinstellingen** op de display te zien.

Draadloze basisinstellingen

Regioselectie	
Regio:	Europa
Draadloos netwerk	
<input checked="" type="checkbox"/> Activeer SSID-uitzending	
<input type="checkbox"/> Activeer draadloze isolatie	
Naam (SSID):	ITWORKS
Modus:	Mixed 802.11b/g/n
Kanaal:	Auto
Bandbreedte:	Auto
Beveiligingsopties	
Beveiligingsopties:	Geen

Toepassen Annuleren

- **Regio:** selecteer de regio waar u zich bevindt.
- **Activeer SSID-uitzending:** indien ingeschakeld stuurt de router zijn SSID uit in het draadloze netwerk. Draadloze cliënten kunnen de SSID scannen en toegang krijgen tot het draadloze netwerk onder de SSID.
- **Activeer draadloze isolatie:** als dit is geselecteerd kunnen draadloze cliënten die met het netwerk van dezelfde SSID zijn verbonden alleen toegang hebben tot het internet, maar niet met elkaar communiceren.
- **Naam (SSID):** stel de naam voor het draadloze netwerk in. De SSID kan tot 32 tekens bevatten en kan uit letters, cijfers, onderlijningen en eender welke combinatie daarvan bestaan. De SSID is hoofdlettergevoelig.
- **Modus:** selecteer de draadloze modus. **Gemixt 802.11b/g/n** is aanbevolen.
- **Kanaal:** het kanaal voor het versturen van draadloze signalen. Het standaardkanaal is **Auto**. Wanneer **Auto** is geselecteerd, selecteert het apparaat automatisch het beste kanaal uit de beschikbare kanalen in overeenstemming met de eigenlijke situatie.
- **Bandbreedte:** de bandbreedte die wordt ingenomen voor draadloze signaaltransmissie.
- **Max. transmissiesnelheid:** de maximale transmissiesnelheid van de repeater.

- **Beveiligingsopties:** stel de beveiligingsencryptie van het draadloze netwerk in om ongeoorloofde toegang en meeluisteren te voorkomen.

Beveiligingsopties

– Geen

De data-encryptie is niet geadopteerd en het netwerk is niet beveiligd. Alle stations kunnen het netwerk binnenkomen. Deze optie is niet aanbevolen.

Beveiligingsopties	
Beveiligingsopties:	Geen

– WEP

Draadgebonden equivalente privacy, u kunt de WEP 64- of 128-bitencryptie gebruiken.

Beveiligingsopties	
Beveiligingsopties:	WEP
Beveiligingsencryptie (WEP)	
Authenticatie-type: :	Automatisch
Encryptie-type: :	ASCII
Encryptie-sterkte:	64 bits
Sleutel beveiligingsencryptie (WEP)	
Sleutel 1:	<input type="text"/> (5 ASCII-teken)
Sleutel 2:	<input type="text"/> (5 ASCII-tekens)
Sleutel 3:	<input type="text"/> (5 ASCII-tekens)
Sleutel 4:	<input type="text"/> (5 ASCII-tekens)

- **Authenticatie-type:** selecteer het authenticatie-type dat het systeem adopteert. Drie authenticatie-types zijn beschikbaar: **automatisch**, **open** en **gedeelde sleutels**.
 - **Automatisch:** als dit is geselecteerd gebruikt de router het authenticatie-type **open** of **gedeelde sleutels** naargelang het verzoek van de host.
 - **Open:** als dit is geselecteerd kunnen hosts in het draadloze netwerk doorheen de authenticatie en zonder wachtwoord met het draadloze netwerk verbinden. Het wachtwoord is echter vereist voor het verzenden van data.
 - **Gedeelde sleutels:** als dit is geselecteerd kunnen hosts in het draadloze netwerk alleen doorheen de authenticatie nadat het correcte wachtwoord is ingevoerd. Zo niet kunnen de hosts niet met het draadloze netwerk verbinden`.

- **Encryptie-type:** het type van de sleutel die zal worden ingesteld. Hexadecimale en ASCII-codes zijn beschikbaar.
 - **Hex:** geldige tekens voor sleutels bevatten 0–9 en A–F.
 - **ASCII:** geldige tekens voor sleutels bevatten alle tekens van het toetsenbord.
- **Encryptie-sterkte:** de encryptie-sterkte bepaalt de lengte van de sleutel.
 - Als de **Encryptie-sterkte** is ingesteld op **64 bits** stelt u de sleutel in op 10 hexadecimale tekens of 5 ASCII-tekens.
 - Als de **Encryptie-sterkte** is ingesteld op **128 bits** stelt u de sleutel in op 26 hexadecimale tekens of 13 ASCII-tekens.
- **Sleutel 1/2/3/4:** stel de sleutel in op basis van het geselecteerde encryptie-type en de encryptie-sterkte.

– **WPA-PSK[TKIP] of WPA2-PSK[TKIP]**

WPA-PSK: vooraf-gedeelde sleutel Wi-Fi beveiligde toegang

WPA2-PSK: vooraf-gedeelde sleutel Wi-Fi beveiligde toegang versie 2

TKIP: tijdelijke sleutel integriteitsprotocol

Noteer dat de 802.11n-modus het TKIP-algoritme niet ondersteunt.

Beveiligingsopties	
Beveiligingsopties:	WPA-PSK[TKIP] ▼
Beveiligingsopties (WPA-PSK)	
Geheime frase	<input type="text"/> (8-63 tekens of 64 hex-tekens)

- **Geheime frase:** voer 8-63 ASCII-tekens of 64 hexadecimale tekens in.

– **WPA-PSK[AES] or WPA2-PSK[AES]**

WPA-PSK: vooraf-gedeelde sleutel Wi-Fi beveiligde toegang.

WPA2-PSK: vooraf-gedeelde sleutel Wi-Fi beveiligde toegang versie 2.

AES: geavanceerde encryptie-standaard

Beveiligingsopties	
Beveiligingsopties:	WPA2-PSK[TKIP] ▼
Beveiligingsopties (WPA2-PSK)	
Geheime frase	<input type="text"/> (8-63 tekens of 64 hex-tekens)

- **Geheime frase:** voer 8-63 ASCII-tekens of 64 hexadecimale tekens in.

– **WPA-PSK/WPA2-PSK+[TKIP]/[AES]**

De cliënt mag ofwel WPA-PSK[TKIP]/[AES] of WPA2-PSK[TKIP]/[AES] gebruiken.

Beveiligingsopties	
Beveiligingsopties:	WPA-PSK/WPA2-PSK
Beveiligingsopties (WPA-PSK/WPA2-PSK)	
Geheime frase	<input type="text"/> (8-63 tekens of 64 hex-tekens)

- **Geheime frase:** voer 8-63 ASCII-tekens of 64 hexadecimale tekens in.



Opmerking:

Nadat de configuratie van de draadloze instellingen voor het apparaat is voltooid kunnen alleen hosts met dezelfde draadloze instellingen (bijv. de SSID) als het apparaat ermee verbinden. Als u de beveiligingsinstellingen voor apparaat configureert, moeten hosts dezelfde beveiligingsinstellingen (bijv. het wachtwoord) hebben als het apparaat om ermee te kunnen verbinden.

7.5.2 Gastnetwerk

Als u niet wilt dat bezoekers uw draadloze beveiligingssleutel kennen, kunt u het gastnetwerk gebruiken om hen van uw internet gebruik te laten maken zonder uw wachtwoord van de draadloze verbinding te kennen.

Kies **Draadloze instellingen > Gastnetwerk** om de pagina van het **Gastnetwerk** op de display te zien.

Gastnetwerk

Netwerkprofielen					
	Schema	SSID	Beveiliging	Toepassen	SSID-uitzending
<input checked="" type="radio"/>	1	ITWORKS-002	None	NEEN	JA
<input type="radio"/>	2	ITWORKS-003	None	NEEN	JA;
<input type="radio"/>	3	ITWORKS-004	None	NEEN	JA;
<input type="radio"/>	4	ITWORKS-005	None	NEEN	JA

Draadloze instellingen – Profiel 1

Activeer gastnetwerk

Activeer SSID-uitzending

Sta gasten toegang tot mijn plaatselijk netwerk toe

Activeer draadloze isolatie

Draadloos gastnetwerk naam (SSID):

Beveiligingsopties- Profiel 1

Beveiligingsopties:

- **Netwerkprofielen:** korte beschrijving van het aangemaakte gastnetwerk. U kunt tot vier gastnetwerken aanmaken. A netwerkprofiel bevat de SSID en

encryptie-modus, of het gastnetwerk wordt gebruikt of niet of de SSID wordt uitgezonden of niet. U kunt op de radiobutton van een profiel klikken voor gedetailleerde informatie of om instellingen te wijzigen.

- **Activeer gastnetwerk:** als dit geactiveerd is hebben zowel uzelf als uw gasten toegang tot het netwerk via de SSID van het gastnetwerk.
- **Activeer SSID-uitzending:** als dit geactiveerd is zendt het apparaat zijn SSID uit naar alle draadloze stations.
- **Sta gasten toegang tot mijn plaatselijk netwerk toe:** als dit geactiveerd is hebben gasten die de SSID van een gastnetwerk gebruiken niet alleen toegang tot het internet maar ook tot de LAN van het apparaat, zoals gebruikers die de primaire SSID van het netwerk gebruiken. Als dit uitgeschakeld is hebben gasten die de SSID van een gastnetwerk gebruiken geen toegang tot de LAN van het apparaat.
- **Activeer draadloze isolatie:** als dit geactiveerd is hebben gasten die met het gastnetwerk van dezelfde SSID zijn verbonden alleen toegang tot het internet, maar kunnen niet met elkaar communiceren.
- **Draadloos gastnetwerk naam (SSID):** stel de naam van het gastnetwerk in.
- **Beveiligingsopties:** verwijst naar de beschrijvingen van de beveiligingsoptie in de paragraaf **8.5.2 Draadloze basisinstellingen**.

Klik als u klaar bent op **Toepassen** om de instellingen op te slaan.

7.5.3 Draadloze geavanceerde instellingen

Kies **Draadloze instellingen > Draadloze geavanceerde instellingen** om de pagina van **Draadloze geavanceerde instellingen** op de display te zien.

Draadloze geavanceerde instellingen

Draadloze geavanceerde instelling	
<input checked="" type="checkbox"/> Activeer draadloze router-radio	
Fragmentatielengte (256-2346)	<input type="text" value="2346"/>
DTIM (1-255)	<input type="text" value="1"/>
Bakeninterval (20-1000)	<input type="text" value="100"/>
MAX. cliënten (0-12)	<input type="text" value="0"/>
CTS/RTS-drempel (1-2347)	<input type="text" value="2346"/>
Proloogmodus	<input type="text" value="Long preamble"/>
Lange proloog	<input type="text" value="Short GI"/>
Verzendkracht controle	<input type="text" value="100%"/>
WPS-instellingen	
Router-PIN	<input type="text" value="12345670"/>
<input checked="" type="checkbox"/> Activeer WPS <input type="checkbox"/> Deactiveer Router-PIN	
Toegangslijst van draadloze kaart	
<input type="text" value="Toegangslijst instellen"/>	

- **Activeer draadloze router-radio:** als u de draadloze router-radio uitschakelt kunnen draadloze apparaten niet met de repeater verbinden. Als u uw draadloze netwerk een tijd lang niet gebruikt, kunt u dit vakje ontvinken en alle draadloze verbindingsmogelijkheden uitschakelen.
- **Fragmentatielengte (256-2346):** stel de drempel van de fragmentatielengte in. Als de lengte van een pakket groter is dan de ingestelde waarde, wordt het pakket automatisch gefragmenteerd tot verschillende pakketten. De waarde van de **Fragmentatielengte** mag niet te klein zijn omdat een te groot aantal van pakketten de performance van het draadloze netwerk zou aantasten. De standaard waarde is 2346.
- **DTIM (1-255):** stel het interval voor het versturen van DTIM-frames in.
- **Bakeninterval (20-1000):** het bakeninterval is de frequentie van het versturen van baken-frames. Stel het interval voor het versturen van baken-frames in. De eenheid is milliseconde (ms). De standaardwaarde is 100ms.
- **MAX. cliënten (0-12):** stel het maximale aantal cliënten in. 0 geeft aan dat het aantal verbonden cliënten onbeperkt is.
- **CTS/RTS-drempel (1-2347):** stel de CTS/RTS-drempel in. Als de lengte van een pakket groter is dan de gespecificeerde RTS-waarde, stuurt de repeater een RTS-frame naar het bestemmingsstation om te negotiëren. Na ontvangst van een RTS-frame antwoordt het draadloze station de repeater met een frame Vrij voor verzending (CTS) en de melding dat zij met elkaar kunnen communiceren.

- **Proloogmodus:** een proloog (in het bijzonder het veld **802.11b hoge snelheid/DSSS PHY**; 56 tekens gesynchroniseerd veld voor een korte proloog) definieert de lengte van de CRC-correctieblokkade voor communicatie tussen draadloos apparaten. Een korte proloog moet worden gebruikt in een netwerk met intensief verkeer. Dit helpt de doeltreffendheid van een draadloze netwerk verbeteren bij het reageren op applicaties met hoge real-time vereisten, zoals het streamen van video en voice-over-IP telefonie.
- **Bewakingsinterval (GI):**
 - Korte GI: het interval bedraagt 400 ns. Wanneer de korte GI is geactiveerd, kan de repeater korte-frame-interval pakketten versturen en ontvangen. Dit helpt voor een betere de transmissiesnelheid van de repeater.
 - Lange GI: het interval bedraagt 800 ns.
- **Transmissiekracht controle:** stel de transmissiekracht van het draadloze netwerk in. Het is raadzaam de standaard instelling **100%** te gebruiken.
- **Router-PIN:** toon de PIN die zal worden gebruikt voor de draadloze cliënt wanneer de draadloze instellingen van de router via WPS worden geconfigureerd.
- **Activeer WPS:** de functies in de pagina van de **WPS-instelling** zijn alleen beschikbaar als het vakje van **Activeer WPS** is aangevinkt. Als dit vakje niet is aangevinkt is het menu-item **WPS-instelling** grijs en uitgeschakeld.
- **Uitschakelen router-PIN:** de functie PIN-modus in de pagina van de **WPS-instelling** is alleen beschikbaar als het vakje bij **Uitschakelen router-PIN** niet is aangevinkt. Als het vakje is aangevinkt is de optie PIN-modus niet beschikbaar.

Draadloze toegang via MAC-adres beperken

Wanneer de toegangslijst voor een draadloze kaart wordt geconfigureerd en geactiveerd, controleert de router het MAC-adres van alle draadloze apparaten die verbinding proberen te maken en staat alleen verbinding toe met computers die op de lijst van vertrouwde computer zijn geïdentificeerd.

Het MAC-adres is een uniek fysiek adres van een netwerkkapparaat bestaande uit 12 tekens, dat alleen de hexadecimale tekens 0–9, a–f, of A–F bevat. Het MAC-adres is in de format XX:XX:XX:XX:XX:XX.

Om de draadloze toegang via MAC-adres te verhinderen:

- Stap 1** **Stap 1** Klik op de button **Toegangslijst aanmaken** in de pagina van de **Draadloze geavanceerde instellingen** om de pagina van de **Toegangslijst draadloze kaart** op de display te zien.

Toegangslijst draadloze kaart

Toegangslijst aanmaken



Toegangslijst draadloze kaart

Toegangscontrole inschakelen

Apparaat-naam	MAC-adres

- Stap 2** **Stap 2** Klik op **Toevoegen** om een draadloos apparaat toe te voegen aan de lijst van de draadloze toegangscontrole. De pagina van de **Draadloze kaart toegangsinstellingen** is op de display te zien.

Toegangsinstellingen draadloze kaarten

Beschikbare draadloze kaarten

	Apparaat-naam	MAC-adres
<input type="radio"/>	Onbekend	7C:11:BE:2C:A7:5D
<input type="radio"/>	Onbekend	00:26:F2:4F:AC:60

Toegang draadloze kaart (max. termen: 16)

Apparaat-naam

MAC-adres

- Stap 3** **Stap 3** Als de gewenste computer in de lijst van **Beschikbare draadloze kaarten** staat, kunt u de radio-button van die computer selecteren om het MAC-adres ervan te verkrijgen. Zo niet kunt een naam handmatig invoeren en het MAC-adres van de computer toestemming geven. Over het algemeen is het MAC-adres gelabeld op de onderzijde van een draadloos apparaat.
- Stap 4** **Stap 4** Klik op **Toevoegen** om dit draadloze apparaat toe te voegen aan de Toegangslijst draadloze kaarten. Het systeem verspringt naar de pagina van de lijst.
- Stap 5** **Stap 5** Selecteer **Toegangscontrole inschakelen**. Als dit geselecteerd is kunt u de toegang van pc's tot het draadloze netwerk beperken, en alleen specifieke pc's toegang op uw netwerk toelaten op basis van hun MAC-adressen.

Stap 6 Klik op **Toepassen** om uw instellingen voor de Toegangslijst draadloze kaart op te slaan.

Nu kunnen alleen de apparaten in deze lijst draadloos met de repeater verbinden.

7.5.4 WPS-instelling

Kies **Draadloze instellingen > WPS-instelling** om de onderstaande pagina op de display te zien.

WPS-instelling

Nieuwe en gemakkelijke manier om met de draadloze router te verbinden via WiFi-beveiligde instelling (WPS)

Een draadloze cliënt moet de WPS-functie ondersteunen om deze wizard voor het toevoegen van een cliënt aan uw WPS-geactiveerde draadloze router te kunnen gebruiken.

Kijk de handleiding en verpakking van uw draadloze cliënt na om te zien of hij de WPS-functie ondersteunt.

Als uw draadloze cliënt de WPS-functie niet ondersteunt moet u uw draadloze client handmatig configureren zodat hij dezelfde SSID en draadloze beveiligingsinstellingen heeft als deze router.

[Volgende](#)

WPS staat voor Wi-Fi beveiligde instelling.

U kunt WPS gebruiken om snel en veilig een draadloze verbinding tot stand te brengen als de uplink-AP of terminal (bijv. de netwerkadapter) is uitgerust met de WPS-functie. Het is raadzaam om eerst de draadloze encryptie voor de uplink-AP te configureren. Als u de draadloze encryptie-modus na het tot stand brengen van de draadloze verbinding via WPS wijzigt, moet u WPS gebruiken om opnieuw een draadloze verbinding tot stand te kunnen brengen. Noteer dat als de draadloze cliënt WPS niet ondersteunt, u hem handmatig moet configureren (onder meer SSID, beveiligingsmodus en wachtwoord) met dezelfde SSID en draadloze beveiligingsinstellingen als de router.

Klik op **Volgende** om de pagina van de **WPS-instelling** binnen te gaan. Het onderstaande beschrijft hoe u WPS voor de AP-modus kunt configureren.

7.5.4.1 Via de WPS-toets

Druk in de AP-modus met WDS uitgeschakeld op de toets **WPS** op het zijpaneel van het apparaat en op de toets **WPS** van het cliëntapparaat. Het apparaat kan een WPS-geëncrypteerde verbinding naar het downlink-cliëntapparaat uitvoeren.

7.5.4.2 Via de webpagina

U kunt de WPS-instellingen ook via de webpagina configureren.

Kies **Draadloze instellingen > WPS-instelling** om de pagina van de **WPS-instelling** op de display te zien.

- Druk op toets

Stap 1 **Stap 1** Selecteer **Druktoets** en klik op **Start PBC**. De WPS-geëncrypteerde verbinding start op.

WPS-instellingen

Als AP, selecteer een instelmethode:

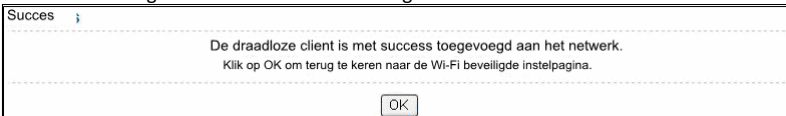
Druk op toets (aanbevolen)

U kunt ofwel fysiek op de Druktoets van de router drukken of op de onderstaande button drukken (soft-push button).

Start PBC

PIN (persoonlijke identificatienummer)

- Stap 2** Druk binnen de 2 minuten op de **WPS**-toets van de netwerkadapter of klik op de **PBC**-button in het hulpprogramma voor de configuratie van de netwerkadapter om de WPS-verbinding te maken. Nadat de WPS-verbinding tot stand is gebracht verschijnt de onderstaande pagina op de display, aangevend dat de WPS-verbinding is voltooid.



- PIN-modus

- Stap 1** Selecteer **PIN**, voer de PIN-code van de netwerkadapter in (verwijs naar de cliënt van de netwerkadapter) en klik op **Start PIN** om de WPS-verbinding te starten.

WPS-instellingen

Als AP, selecteer een instelmethode:

Druktoets (aanbevolen)

PIN (persoonlijke identificatienummer)

Als uw adapter WPS ondersteunt, klikt u op "Genereer een cliënt-veiligheidspín om in te voeren op de AP/router/gateway" en voer het gegenereerde PIN-nummer hier in.

Voer PIN van cliënt in:

Start PIN

- Stap 2** Klik binnen de 2 minuten op the PIN-toets van de netwerkadapter om de WPS-verbinding te starten. Nadat de WPS-verbinding tot stand is gebracht verschijnt de onderstaande pagina op de display, aangevend dat de WPS-verbinding is voltooid.



7.6 Managementfunctie

Klik op **Managementfunctie** om het uitgebreide navigatiemenu op de display te zien.

Managementfunctie

Back-up-instellingen

Apparaat heropstarten

Wachtwoord instellen

Router-upgrade

7.6.1 Back-up-instellingen

Kies **Managementfunctie** > **Back-up-instellingen** om de pagina van de **Back-up-instellingen** op de display te zien.

Back-up-instellingen

Bewaar een kopie van de huidige instellingen

Back-up maken

Herstel een opgeslagen instelling van een bestand

Bladeren ..

Herstellen

Revert to Factory Default Settings

Verwijderen

U kunt in deze pagina configuratie-informatie van de router voor later gebruik exporteren naar de computer in de vorm XML, een eerder opgeslagen of nieuw configuratiebestand importeren en de router terugstellen naar de standaard fabrieksinstellingen.

- Back-up maken

Klik op **Back-up maken** om de configuratie-informatie van de router op te slaan als een lokaal bestand.



Opmerking:

Voordat u uw configuratiebestand opslaat moet u het wachtwoord van de administrator wijzigen naar de standaard (admin) voor het geval u uw wachtwoord vergeet. Wijzig dit dan opnieuw nadat u het configuratiebestand heeft opgeslagen. Als u het wachtwoord vergeet moet u de configuratie terugstellen naar de standaard fabrieksinstellingen.

- Herstellen

Met de opties Back-up maken en Herstellen in de pagina van de **Back-up-instellingen** kunt u een bestand met de configuratie-instellingen van uw router opslaan en ophalen. Klik op **Bladeren...** om het configuratiebestand dat in uw computer is opgeslagen te selecteren en klik op **Herstellen** om dat bestand op de router te uploaden.

- Verwijderen

In bepaalde omstandigheden (bijvoorbeeld wanneer u de router naar een ander netwerk verplaatst of het wachtwoord bent vergeten) is het nodig om de configuratie te verwijderen en terug te stellen naar de standaard fabrieksinstellingen.

Klik op **Verwijderen** om de router terug te stellen naar de standaard fabrieksinstellingen. Deze bewerking heeft dezelfde gevolgen als wanneer u de toets **Terugstellen** (Reset) op het zijpaneel 3-6 seconden lang ingedrukt houdt.

7.6.2 Apparaat heropstarten

Kies **Managementfunctie > Apparaat heropstarten** om de pagina van **Apparaat heropstarten** op de display te zien.

Apparaat heropstarten

Apparaat heropstarten
<input type="button" value="Heropstarten"/>

Klik op **Heropstarten** om de router te heropstarten. Nadat de router is heropgestart gaat het systeem over naar de aanmeldpagina.

7.6.3 Wachtwoord instellen

Kies **Managementfunctie > Wachtwoord instellen** om de pagina van **Wachtwoord instellen** op de display te zien.

Wachtwoord instellen

Wachtwoord instellen	
Oude wachtwoord	<input type="text"/>
Wachtwoord instellen	<input type="text"/>
Herhaal nieuw wachtwoord	<input type="text"/>
	<input type="button" value="Toepassen"/> <input type="button" value="Annuleren"/>

U kunt in deze pagina het wachtwoord voor het aanmelden wijzigen.



Opmerking:

Voor de veiligheid is het sterk aangewezen het standaard wachtwoord van de administrator te wijzigen. Als u het wachtwoord vergeet kunt u de router terugstellen naar de standaardinstellingen. Het standaard wachtwoord is admin.

Router-upgrade

Kies **Managementfunctie > Router-upgrade** om de pagina van de **Router-upgrade** op de display te zien.

Router-upgrade

Zoek en selecteer het upgrade-bestand in uw harde schijf:

Volg de onderstaande werkwijze om de software van de router te upgraden.

- Stap 1** **Stap 1** Klik op **Bladeren...** om te navigeren naar de meest recente software.
- Stap 2** **Stap 2** Selecteer het correcte upgrade-bestand. Als u **Config. verwijderen** kiest, stelt de router na het voltooien van de upgrade terug naar de standaardinstellingen. Als u dit niet selecteert blijven de huidige instellingen in voege.
- Stap 3** **Stap 3** Klik op **Uploaden** om de upgrade te starten.

Na het voltooien van de upgrade start de router automatisch opnieuw op.



Opmerking:

Na de software-upgrade keert het apparaat terug naar de standaard fabrieksinstellingen. Voor het geval de vorige configuratie-informatie verloren gaat, is het altijd beter de instellingen op te slaan voordat u de software updatet.

Schakel de router tijdens het upgraden niet uit.

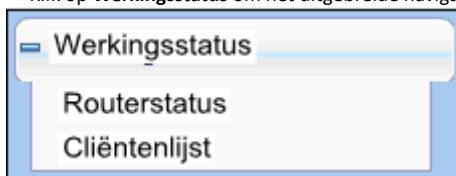
8 Webconfiguratie in router-modus

Opmerking:

Stel de driewegschakelaar op het zijpaneel in op **AP**, selecteer **Router-modus** en herstart het apparaat. Meld aan op de configuratiepagina nadat het apparaat is heropgestart.

8.1 Werkingsstatus

Klik op **Werkingsstatus** om het uitgebreide navigatiemenu op de display te zien.



8.1.1 Router-status

Kies **Werkingsstatus > Router-status** om de pagina van de **Router-status** op de display te zien.

Router-status

Systeeminformatie	
Hardware-versie	V1.0.0
Firmware-versie	V1.0.0
Productnaam	Draadloze router
Werkmodus	Brugmodus
Tijd en datum	1971-01-01 12:53:24
LAN-poort	
MAC-adres	00:1E:E3:4B:06:6D
IP-adres	192.168.100.253
IP-subnetmasker	255.255.255.0
Draadloze poort	
Draadloos netwerknaam (SSID)	ITWORKS
Regio	Europa
Draadloos kanaal	Auto
802.11-modus	Gemixt 802.11b/g/n
Draadloze radio	Ingeschakeld
Uitzendnaam	AAN
Draadloze isolatie	UIT
Wi-Fi-beveiligde instellingen (WPS)	AAN
Draadloze beveiligingsmodus	Geen

U kunt in deze pagina informatie bekijken over de huidige werkingsstatus van het apparaat, met onder meer de systeeminformatie, verbindingstatus van de internet-poort, de status van de LAN-poort en de status van het draadloze netwerk.

Klik op **Statistieken tonen** om de pagina met de **Statistische informatie** als in de onderstaande afbeelding op de display te zien:

Statistische informatie

Poort	Status	TxPkts	RxPkts	Botsingen	Tx B/s	Rx B/s	Op-tijd
WAN	100M/vol	205	69	0	120402	6781	00:22:01
WLAN	Auto	6111	11483	0	3241546	1668284	00:21:55
Systeem op-tijd		00:22:10					
Poll-interval							
<input type="text" value="5"/> (1~86400 secs) <input type="button" value="Interval instellen"/> <input type="button" value="Stop"/>							

U kunt op deze pagina de prestatiestatistieken van het apparaat bekijken, met onder meer de aantallen verzonden en ontvangen pakketten per poort.

- **Interval instellen:** stel het interval voor verkeersstatistieken in.
- **Stop:** als u op deze button klikt, toont deze pagina altijd de laatst hernieuwde statistiekinformatie en wordt niet meer opnieuw hernieuwd.

Klik op **Verbindingsstatus** in de pagina van de **Router-status** om de pagina van de **Verbindingsstatus** op de display te zien. Deze pagina toont informatie over de huidige verbinding van het apparaat.

Hieronder wordt de WAN-verbinding van **DHCP** als voorbeeld genomen.

Verbindingsstatus

IP-adres	0.0.0.0
Subnetmasker	0.0.0.0
Standaard gateway	0.0.0.0
DHCP-server	0.0.0.0
DNS-server	0.0.0.0
Lease verkregen	0Day,0Hour,0Minute
Lease verstrijkt	0Day,0Hour,0Minute

- **Vrijgeven:** klik op deze button om het apparaat een verzoek aan de ISP te laten versturen voor het vrijgeven van het IP-adres, het subnetmasker, de standaard gateway en de DNS-server-instellingen.
- **Hernieuwen:** klik op deze button om het apparaat op dynamische wijze een IP-adres, een subnetmasker, de standaard gateway en DNS-server-instellingen van de ISP te laten verkrijgen. De informatie zal in deze pagina op de display te zien zijn.

Verwijs voor meer details over WAN-verbindingsmethoden naar de paragraaf **8.4.2 Instellingen van de WAN-interface**.

8.1.2 Cliëntenlijst

Kies **Werkingstatus** > **Cliëntenlijst** om de pagina van **Cliëntenlijst** op de display te zien.

Clëntenlijst

Draadloze apparaten (draadloze indringers worden hier ook aangegeven)

#	IP-adres s	MAC-adres	Apparaat-naam
1	192.168.100.2	00:1F:A4:91:F2:0E	gj2217d

[Hernieuwen](#)

Deze pagina toont informatie over computers die met het apparaat zijn verbonden, met inbegrip van de IP-adressen en het MAC-adres van elke computer.

8.2 Installatie-wizard

Verwijs voor de instellingen naar de paragraaf **6.2 Configuratie van de router-modus**

8.3 Modusinstelling

Klik op **Modusinstellingen** om de pagina van de **Modusinstellingen** op de display te zien.

Modusinstellingen

Kies uw modus als volgt:

Brugmodus

Router-modus

In deze modus wordt de poort als een WAN-poort gebruikt.
U kunt alleen op het web inloggen door middel van uw draadloze netwerkkaart voor een verbinding met dit netwerk.

Onthoud de SSID en beveiligingsopties van uw draadloze netwerk voordat u naar deze modus overschakelt.

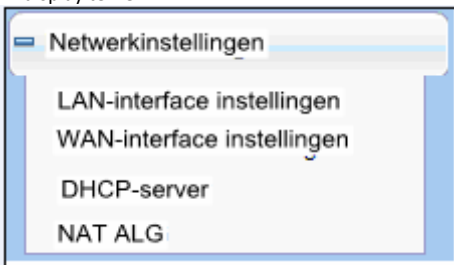
[Toon draadloze basisconf.](#)

[Toepassen](#) [Annuleren](#)

- **Brugmodus:** de interface is een LAN-interface. Gebruikers kunnen het apparaat en de pc verbinden via een RJ45-kabel of een draadloze netwerkkaart.
- **Router-modus:** computers kunnen alleen draadloos met het apparaat verbinden.

8.4 Netwerkinstellingen

Klik op **Draadgebonden Netwerkinstellingen** om het uitgebreide navigatiemenu op de display te zien.



8.4.1 Instellingen van de LAN-interface

Verwijs voor details naar [7.4.1 Instellingen van de LAN-interface](#).

8.4.2 Instellingen van de WAN-interface

Kies **Netwerkinstellingen > Instellingen van de WAN-interface** om de pagina van de **Instellingen van de WAN-interface** op de display te zien.

De router ondersteunt 5 modi voor de WAN-verbinding, waaronder de **dynamische IP (DHCP)**, **statische IP**, **PPPoE**, **PPTP** en **L2TP**. Selecteer de WAN-verbinding die u gebruikt. Neem contact op met uw ISP als u de modus van uw WAN-verbinding niet kent.

(1) Dynamische IP (DHCP)

Als dynamische IP (DHCP) is geselecteerd verkrijgt het apparaat automatisch het IP-adres van de ISP. Selecteer DHCP als de ISP geen IP-netwerkparameters aanbiedt. Zie onderstaande figuur:

WAN-interface instellingen	
Vergt uw internetverbinding een gebruikersnaam?	<input type="radio"/> Ja <input checked="" type="radio"/> Neen
Accountnaam (indien vereist)	<input type="text"/>
Internet IP-adres	
<input checked="" type="radio"/> Haal dynamisch van ISP	
<input type="radio"/> Gebruik statisch IP-adres	
IP-adres	<input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/>
IP-subnetmasker	<input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/>
Gateway IP-adres	<input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/>
Domeinnaam (DNS) server-adres	
<input checked="" type="radio"/> Haal automatisch van ISP	
<input type="radio"/> Gebruik deze DNS-servers	
Primaire DNS	<input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/>
Secundaire DNS	<input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/>
MTU-instelling	
MTU-grootte (616-1500 bytes)	<input type="text" value="1500"/>
Router MAC-adres	
<input checked="" type="radio"/> Gebruik standaardadres	
<input type="radio"/> Gebruik MAC-adres van computer	
<input type="radio"/> Gebruik dit MAC-adres	<input type="text" value="00:1E:E3:4B:06:6D"/>
<input type="button" value="Toepassen"/> <input type="button" value="Annuleren"/>	

- **Accountnaam:** de accountnaam wordt aangeboden door de ISP. Als de ISP dit niet aanbiedt kunt u het item leeg laten.
- **Domeinnaam-service (DNS) adres:** selecteer **Gebruik deze DNS-server** als u weet dat uw ISP tijdens het inloggen niet automatisch DNS-adressen naar de router stuurt. En voer het IP-adres van de primaire DNS-server van uw ISP in. Voer een secundair DNS-server adres in als dat beschikbaar is.
- **MTU-grootte:** stel de maximale transmissie-eenheid in. De standaardwaarde is aanbevolen.
- **Router MAC-adres:** het fysieke adres van de router.
 - Selecteer normaal gezien **Gebruik standaardadres**.
 - Als de ISP authenticatie van het MAC-adres vereist, selecteert u **Gebruik MAC-adres van computer** of **Gebruik dit MAC-adres**. Als u **Gebruik MAC-adres van computer** selecteert, zal het MAC-adres van de huidige computer dienen als MAC-adres van de router. Als u **Gebruik dit MAC-adres** selecteert, moet u het MAC-adres van een andere computer invoeren. De opmaak van een MAC-adres is XX:XX:XX:XX:XX:XX.

Klik na het voltooiën van de instellingen op **Toepassen** om de instellingen op te slaan.

(2) Statische IP

Selecteer **Statische IP** als de ISP het IP-adres, subnetmasker en informatie over de gateway en DNS-server aanbiedt. Neem contact op met uw ISP als u niet over deze informatie beschikt.

WAN-interface instellingen

Vergt uw internetverbinding een gebruikersnaam? Ja Neen

Accountnaam (indien vereist)

Internet IP-adres

Haal dynamisch van ISP

Gebruik statisch IP-adres

IP-adres

IP-subnetmasker

Gateway IP-adres

Domeinnaam (DNS) server-adres

Haal automatisch van ISP

Gebruik deze DNS-servers

Primaire DNS

Secundaire DNS

MTU-instelling

MTU-grootte (616-1500 bytes)

Router MAC-adres

Gebruik standaardadres

Gebruik MAC-adres van computer

Gebruik dit MAC-adres

- **Accountnaam:** de accountnaam wordt door uw ISP geleverd. Laat dit leeg als de ISP dit niet aanbiedt.
- **IP-adres:** voer het WAN IP-adres dat u van de ISP kreeg in. De parameter moet worden ingevoerd.
- **IP-subnetmasker:** voer het WAN-subnetmasker dat u van de ISP kreeg in. Dit verschilt naargelang het netwerktype. Het is gewoonlijk 255.255.255.0 (Klasse C).
- **Gateway IP-adres:** voer het IP-adres van de gateway dat u van de ISP kreeg in. Dit is het IP-adres dat wordt gebruikt voor het verbinden met de ISP.
- **Primaire DNS:** voer het IP-adres van de primaire DNS-server indien nodig in.
Secundaire DNS: voer het IP-adres van die DNS-server in als de ISP een andere DNS-server aanbiedt.
- **MTU-grootte:** stel de maximale transmissie-eenheid in. De standaardwaarde is aanbevolen.
- **Router MAC-adres:** verwijst naar de beschrijvingen over het instellen van het **Router MAC-adres** voor DHCP.

Klik na het voltooiën op **Toepassen** om de instellingen op te slaan.

(3) PPPoE

Als de ISP de gebruikersnaam en het wachtwoord voor PPPoE (point-to-point protocol via ethernet) dialup aanbiedt, klikt u op **Ja** en selecteert u **PPPoE**.

WAN-interface instellingen;

Vergt uw internetverbinding een gebruikersnaam?	<input checked="" type="radio"/> Ja <input type="radio"/> Neen
Internet serviceprovider	PPPoE
Gebruikersnaam	<input type="text"/>
Wachtwoord	<input type="text"/>
Service-naam (indien nodig)	<input type="text"/>
Verbindingsmodus	Altijd ingeschakeld
Time-out na inactiviteit (in minuten)	5
Domeinnaam (DNS) server-adres	
<input checked="" type="radio"/> Haal dynamisch van ISP	
<input type="radio"/> Gebruik deze DNS-servers	
Primaire DNS	<input type="text"/>
Secondaire DNS	<input type="text"/>
MTU-instelling	
MTU-grootte (616-1492 bytes)	1492
Router MAC-adres	
<input checked="" type="radio"/> Gebruik standaardadres	
<input type="radio"/> Gebruik MAC-adres van computer	
<input type="radio"/> Gebruik dit MAC-adres	00:1E:E3:4B:06:6D

- **Inloggen:** voer de gebruikersnaam voor de PPPoE-dialup in die werd opgegeven door de ISP.
- **Wachtwoord:** voer het wachtwoord voor de PPPoE-dialup in die werd opgegeven door de ISP.
- **Service-naam:** als meerdere PPPoE-servers beschikbaar zijn kunt u er één van in dit veld specificeren.
- **Verbindingsmodus:**
 - **Altijd ingeschakeld:** als u dit selecteert brengt het systeem automatisch een verbinding tot stand. Als het apparaat omwille van externe factoren van het netwerk wordt losgekoppeld terwijl u de internettoegang-service gebruikt, zal het systeem met gespecificeerde tussentijden (bijv. 10 seconden) proberen te herverbinden tot de verbinding weer tot stand is gebracht. Als u maandelijks voor de internettoegang betaalt bevelen we deze verbindingmodus aan.

- **Bellen op aanvraag:** als u dit selecteert brengt het systeem automatisch een verbinding tot stand telkens wanneer een verzoek tot netwerktoegang van de LAN wordt ontvangen. Als de LAN geen verzoek tot netwerktoegang verstuurt binnen de gespecificeerde tijd van **Time-out bij inactiviteit**, zal het systeem de verbinding automatisch verbreken. Als u per tijd voor de internettoegang betaalt bevelen we deze verbindingsmodus aan, omdat het doeltreffend kosten van internettoegang bespaart.
- **Handmatig verbinden:** als u dit selecteert moet u de dial-upverbinding na het opstarten handmatig instellen.
- **Time-out bij inactiviteit:** als het systeem binnen de gespecificeerde tijd van **Time-out bij inactiviteit** geen enkel signaal met betrekking tot internettoegang ontvangt, zal het de verbinding automatisch verbreken.
- **Domeinnaam (DNS) server-adres:** selecteer **Gebruik deze DNS-servers** als u weet dat uw ISP bij het aanmelden niet automatisch DNS-adressen naar de router verstuurt. Voer dan het IP-adres van de primaire DNS-server van uw ISP in. Voer indien beschikbaar een secundair DNS-server adres in.
- **MTU-grootte:** stel de maximale transmissie-eenheid in. De standaardwaarde is aanbevolen.
- **Router MAC-adres:** verwijst naar de beschrijvingen voor het instellen van een **Router MAC-adres** voor DHCP.

Klik als u klaar bent op **Toepassen** om de instellingen op te slaan.

(4) PPTP

Selecteer **PPTP** als de ISP een gebruikersnaam en wachtwoord voor PPTP-dialup aanbiedt.

WAN-interface instellingen

Vergt uw internetverbinding een gebruikersnaam? Ja Neen

Internet serviceprovider	PPTP
Gebruikersnaam	<input type="text"/>
Wachtwoord	<input type="text"/>
Service-naam (indien nodig)	<input type="text"/>
Verbindingsmodus	Altijd ingeschakeld
Time-out na inactiviteit (in minuten)	5
Domeinnaam (DNS) server-adres	
<input checked="" type="radio"/> Haal dynamisch van ISP	
<input type="radio"/> Gebruik deze DNS-servers	
Primaire DNS	<input type="text"/>
Secundaire DNS	<input type="text"/>
MTU-instelling	
MTU-grootte (616-1492 bytes)	1450
Router MAC-adres	
<input checked="" type="radio"/> Gebruik standaardadres	
<input type="radio"/> Gebruik MAC-adres van computer	
<input type="radio"/> Gebruik dit MAC-adres	
	00:1E:E3:4B:06:6D

- **Aanmelden:** voer de gebruikersnaam voor PPTP-dialup in als geleverd door de ISP.
- **Wachtwoord:** voer het wachtwoord voor PPTP-dialup in als geleverd door de ISP.
- **Verbindingsmodus:**
 - **Altijd ingeschakeld:** als u dit selecteert brengt het systeem automatisch een verbinding tot stand. Als het apparaat omwille van externe factoren van het netwerk werd losgekoppeld terwijl u de internettoegang gebruikte, zal het systeem met tussenpauzes van de gespecificeerde tijd (bijv. 10 seconden) proberen te verbinden tot de verbinding opnieuw tot stand is gebracht. Als u maandelijks voor uw internettoegang betaalt bevelen we deze verbindingsmodus aan.
 - **Bellen op aanvraag:** als u dit selecteert brengt het systeem automatisch een verbinding tot stand telkens wanneer een verzoek tot netwerktoegang van de LAN wordt ontvangen. Als de LAN binnen de gespecificeerde tijd van **Time-out bij inactiviteit** geen verzoek tot netwerktoegang verstuurt, zal het systeem de verbinding automatisch verbreken. Als u per tijd voor de internettoegang betaalt bevelen we deze verbindingsmodus aan, omdat het doeltreffend kosten van internettoegang bespaart.
 - **Handmatig verbinden:** als u dit selecteert moet u na het opstarten de dialup-verbinding handmatig instellen.

- **Time-out bij inactiviteit:** als het systeem binnen de gespecificeerde tijd van **Time-out bij inactiviteit** geen enkel signaal met betrekking tot internettoegang ontvangt, zal het de verbinding verbreken.
- **Mijn IP-adres:** voer uw IP-adres in. U kunt dit veld ook leeg laten.
- **Subnetmasker:** voer het subnetmasker in. U kunt dit veld ook leeg laten.
- **Server-adres:** voer het IP-adres van de server in. U kunt dit veld ook leeg laten.
- **Gateway IP-adres:** voer het IP-adres van de gateway in. U kunt dit veld ook leeg laten.
- **Domeinnaam (DNS) server-adres:** selecteer **Gebruik deze DNS-server** als u weet dat uw ISP bij het inloggen niet automatisch DNS-adressen naar de router stuurt. Voer dan het IP-adres van de primaire DNS-server van uw ISP in. Voer indien beschikbaar een secundair DNS-server adres in.
- **MTU-grootte:** stel de maximale transmissie-eenheid in. De standaardwaarde is aanbevolen.
- **Router MAC-adres:** Verwijs naar de beschrijvingen voor het instellen van **Router MAC-adres** voor DHCP.

Klik als u klaar bent met de instellingen op **Toepassen** om de instellingen op te slaan.

(5) L2TP

Selecteer **L2TP** als de ISP een gebruikersnaam en wachtwoord voor L2TP-dialup aanbiedt. WAN-interface instellingen;

Vergt uw internetverbinding een gebruikersnaam?	<input checked="" type="radio"/> Ja <input type="radio"/> Neen
Internet serviceprovider	L2TP
Gebruikersnaam	<input type="text"/>
Wachtwoord	<input type="text"/>
Service-naam (indien nodig)	<input type="text"/>
Verbindingsmodus	Altijd ingeschakeld
Time-out na inactiviteit (in minuten)	5
Domeinnaam (DNS) server-adres	
<input checked="" type="radio"/> Haal dynamisch van ISP	
<input type="radio"/> Gebruik deze DNS-servers	
Primaire DNS	<input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/>
Secundaire DNS	<input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/>
MTU-instelling	
MTU-grootte (616-1492 bytes)	1450
Router MAC-adres	
<input checked="" type="radio"/> Gebruik standaardadres	
<input type="radio"/> Gebruik MAC-adres van computer	
<input type="radio"/> Gebruik dit MAC-adres	
	00:1E:E3:4B:06:6D
<input type="button" value="Toepassen"/> <input type="button" value="Annuleren"/>	

Verwijs voor meer details over de parameterinstellingen voor deze pagina naar de bovenstaande parameterbeschrijvingen voor **PPTP**.

8.4.3 DHCP-server

Kies **Netwerkinstellingen > DHCP-server** om de pagina van de **DHCP-server** op de display te zien.

DHCP staat voor Dynamische Host Configuratieprotocol. Als **Gebruik apparaat als DHCP-service** is geselecteerd, kent het apparaat automatisch IP-adressen toe aan computers in de LAN. Gebruikers hoeven de parameters van het TCP/IP-protocol niet te configureren, als daar zijn het IP-adres, het subnetmasker, de gateway en de DNS-server informatie voor computers die zijn verbonden met de LAN van de router.

DHCP-server					
<input checked="" type="checkbox"/> Gebruik router als DHCP-server					
Startend IP-adres		<input type="text" value="192"/>	<input type="text" value="168"/>	<input type="text" value="100"/>	<input type="text" value="2"/>
Eindigend IP-adres		<input type="text" value="192"/>	<input type="text" value="168"/>	<input type="text" value="100"/>	<input type="text" value="200"/>
IDHCP-leasetijd (1-160 uur)		<input type="text" value="24"/>			
Adresreservatie					
	#	IP-adres	Apparaat-naam	MAC-adres	
		Toevoegen Bewerken Verwijderen			
		Toepassen Annuleren			

8.4.3.1 De router als een DHCP-server gebruiken

- **De router as DHCP-server gebruiken:** als het vakje naast **De router als DHCP-server gebruiken** is aangevinkt, doet het apparaat dienst als een DHCP-server om IP-adressen toe te kennen aan computers die ermee verbonden zijn.
- **Startend IP-adres/eindigend IP-adres:** stel de startende en eindigende IP-adressen in om een poel van IP-adressen te specificeren die door de DHCP-server zullen worden toegekend. Na het instellen van het **Startend IP-adres/eindigend IP-adres** zullen hosts in de LAN IP-adressen verkrijgen die binnen de reikwijdte van het startend en eindigend IP-adres liggen.
- **DHCP-leasetijd:** de geldigheidsduur van een IP-adres dat automatisch door de DHCP-server aan een host is toegekend. De DHCP-server kent binnen deze geldigheidsduur deze IP-adressen niet toe aan andere hosts.

8.4.3.2 Adresreservatie gebruiken

Wanneer u een gereserveerd IP-adres voor een computer in de LAN specificeert, zal de computer altijd hetzelfde IP-adres ontvangen wanneer hij de DHCP-server van de router binnegaat. Gereserveerde IP-adressen moeten worden toegekend aan computers of servers die permanente IP-instellingen vereisen.

Adresreservatie			
#	IP-adres	Apparaat-naam	MAC-adres

Om een IP-adres te reserveren:

Stap 1 Klik op **Toevoegen** om de pagina van de **Adresreservatie** binnen te gaan.

Adresreservatie

Tabel van de adresreservatie			
#	IP-adres	Apparaat-naam	MAC-adres
<input type="radio"/>	1		
<input type="radio"/>	2	192.168.100.2	Z2oyMjE3ZA== 00:1F:A4:91:F2:0E

IP-adres:
 MAC-adres:
 Apparaat-naam:

Stap 2 Selecteer een item uit de **Tabel van de adresreservatie** of voer in het veld voor het **IP-adres** het IP-adres in dat is toegekend aan de computer of server (kies een IP-adres uit de poel van IP-adressen die u heeft gespecificeerd, bijv. 192.168.100.x). Voer het MAC-adres en de apparaat-naam van de computer of server in.

Stap 3 Klik op **Toevoegen** om een nieuw item toe te voegen aan **adresreservatie**.

Stap 4 Klik op **Toepassen** om de instellingen op te slaan.

8.4.4 NAT ALG

Kies **Netwerkinstellingen > NAT ALG** om de pagina van **NAT ALG** op de display te zien.

NAT ALG

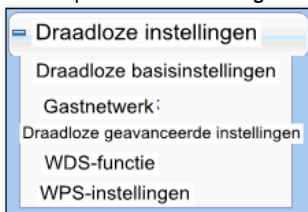
<input checked="" type="checkbox"/> SIP ALG uitschakelen
<input type="checkbox"/> IPSEC pass-through uitschakelen
<input type="checkbox"/> L2TP pass-through uitschakelen
<input type="checkbox"/> PPTP pass-through uitschakelen

- **SIP ALG uitschakelen:** bepaalde SIP-applicaties hebben speciale mechanismen om doorheen de NAT-firewall te passeren en SIP ALG kan met deze mechanismen conflicteren. In de meeste gevallen volstaat het SIP ALG uit te schakelen.
- **IPSEC/L2TP/PPTP pass-through uitschakelen:** IPSEC/PPTP/L2TP pass-through biedt computers een veilige manier van op afstand communiceren in een breed

gebiedsnetwerk (WAN) (bijv. het internet). Activeer de overeenkomstige VPN pass-through functie als een intra-netwerk host een VPN-protocol (zoals de PPTP, L2TP, IPSEC) moet gebruiken om via de router met een VPN-netwerk te verbinden. Klik als u klaar bent met de instellingen op **Toepassen** om de instellingen op te slaan.

8.5 Draadloze instellingen

Klik op **Draadloze instellingen** om het **uitgebreide navigatiemenu** op de display te zien.



8.5.1 Draadloze basisinstellingen

Verwijs voor details naar **7.5.1 Draadloze basisinstellingen**.

8.5.2 Gastnetwerk

Als u niet wil dat bezoekers uw draadloze beveiligingssleutel kennen, kunt u hen via het gastnetwerk op uw internet toelaten zonder dat zij het wachtwoord van uw draadloze verbinding kennen.

Kies **Draadloze instellingen** > **Gastnetwerk** om de pagina van het **Gastnetwerk** op de display te zien.

Gastnetwerk

Netwerkprofielen					
	Schema	SSID	Beveiliging	Toepassen	SSID-uitzending
<input checked="" type="radio"/>	1	ITWORKS-002	Geen	NEEN	JA
<input type="radio"/>	2	ITWORKS-003	Geen	NEEN	JA
<input type="radio"/>	3	ITWORKS-004	Geen	NEEN	JA
<input type="radio"/>	4	ITWORKS-005	Geen	NEEN	JA
Draadloze instellingen – Profiel 1					
<input type="checkbox"/> Activeer Gastnetwerk					
<input checked="" type="checkbox"/> Activeer SSID-uitzending					
<input type="checkbox"/> Sta gasten toegang tot mijn plaatselijk netwerk toe					
<input type="checkbox"/> Activeer draadloze isolatie					
Draadloos gastnetwerk-naam (SSID):				<input type="text" value="ITWORKS-002"/>	
Beveiligingsopties- Profiel 1					
Beveiligingsopties:				<input type="text" value="Geen"/>	

- **Netwerkprofielen:** korte beschrijving van het aangemaakte gastnetwerk. U kunt tot vier gastnetwerken aanmaken. Een netwerkprofiel omvat de SSID en

encryptie-modus, of het gastnetwerk wordt gebruikt of niet en of SSID wordt uitgezonden of niet. U kunt op de radiotoets van een profiel drukken om gedetailleerde informatie te zien of instellingen te wijzigen.

- **Activeer gastnetwerk:** als dit geactiveerd is kunnen zowel u als bezoekers door middel van de SSID van het gastnetwerk met het netwerk verbinden.
- **Activeer SSID-uitzending:** als dit geactiveerd is, stuurt het apparaat zijn SSID naar alle draadloze stations.
- **Sta gasten toe mijn lokale netwerk te gebruiken:** als dit geactiveerd is krijgen bezoekers die de SSID van een gastnetwerk gebruiken niet alleen toegang tot het internet maar ook tot de LAN van het apparaat, zoals gebruikers die de primaire SSID van het netwerk gebruiken. Indien uitgeschakeld, hebben bezoekers die de SSID van een gastnetwerk gebruiken geen toegang tot de LAN van het apparaat.
- **Activeer draadloze isolatie:** als dit is geselecteerd, krijgen draadloze cliënten die met het gastnetwerk van eenzelfde SSID zijn verbonden alleen toegang tot het internet, maar kunnen niet met elkaar communiceren.
- **Gast draadloze netwerk-naam (SSID):** stel de naam in van het gastnetwerk.
- **Beveiligingsopties:** verwijst naar de beschrijvingen van de beveiligingsoptie in de paragraaf **8.5.1 Draadloze basisinstellingen**.

Klik als u klaar bent op **Toepassen** om de instellingen op te slaan.

8.5.3 Draadloze geavanceerde instellingen

Verwijst voor details naar de paragraaf **7.5.3 Draadloze geavanceerde instellingen**.

8.5.4 WDS-functie

Het draadloze distributiesysteem (WDS) activeert interconnectie tussen AP' s in een IEEE 802.11-draadloos netwerk. Het breidt het draadloze netwerk uit via verschillende AP' s, zonder verbinding van het draadgebonden backbone-netwerk. Activeer WDS als u WDS wilt gebruiken om een draadloze repeating of bridging tot stand te brengen.

Kies **Draadloze instellingen > WDS-functie** om de pagina van de **WDS-functie** op de display te zien.

WDS-functie	
<input type="checkbox"/>	Activeer WDS-functie
<input type="checkbox"/>	Deactiveer draadloze cliëntenassociatie
Draadloze MAC van deze router: 00:1E:E3:4B:06:8C	
Draadloos basisstation	
Repeater MAC-adres 1:	<input type="text"/>
Repeater MAC-adres 2:	<input type="text"/>
Repeater MAC-adres 3:	<input type="text"/>
Repeater MAC-adres 4:	<input type="text"/>
<input type="button" value="Toepassen"/> <input type="button" value="Annuleren"/>	

- **Activeer WDS-functie:** activeer de WDS-functie als u deze functie wenst te gebruiken. Noteer dat de WDS-functie niet kan worden geactiveerd als het kanaal is ingesteld op **Auto**.
- **Deactiveer draadloze cliëntenassociatie:** als dit is geselecteerd, zendt het draadloze basisstation geen signalen naar cliënten die er rechtstreeks mee zijn verbonden.
- **Centraal basisstation:** in deze modus doet de router dienst als een basisstation om met repeaters te communiceren. Het basisstation stuurt de gegevens van communicatie tussen repeaters naar de eindbestemming-repeaters. Repeaters moeten in overeenstemming geconfigureerd worden. Merk op dat een draadloos basisstation voor maximaal 4 repeaters kan worden geconfigureerd.
- **Repeater MAC-adres 1/2/3/4:** voer het MAC-adres van de repeater in.

Klik als u klaar bent met de instellingen op **Toepassen** om de instellingen op te slaan.

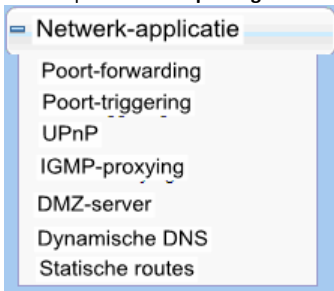
Verwijs voor een beschrijving van de WDS-toepassing naar **6.4.3 WDS-toepassing**.

8.5.5 WPS-instelling

Verwijs voor details naar **7.5.4 WPS-instelling**.

8.6 Netwerktoeepassing

Klik op **Netwerktoeepassing** om het uitgebreide navigatiemenu op de display te zien.



8.6.1 Poort-forwarding

Standaard is uw LAN door de firewall-functie van de router verborgen. Daardoor kunnen andere gebruikers op het internet alleen de router detecteren, zonder dat zij rechtstreeks een bepaalde pc in de LAN kunnen binnengaan. Als u een pc in een LAN wilt binnengaan, moet u poort-forwarding voor de router configureren en de gewenste poort op de overeenkomstige pc in de LAN mappen. De router verstuurt na het ontvangen van een toegangsverzoek van het internet pakketten naar de pc in overeenstemming met de regels van de poort-mapping. Op deze manier wordt communicatie tussen het internet en de pc in de LAN met succes tot stand gebracht.

Kies **Netwerktopassing > Poort-forwarding** om de pagina van de **Poort-forwarding** op de display te zien.

Poort-forwarding

Service-naam
FTP

Service IP-adres
192 168 100 Toevoegen

Service-lijst
Max. aantal regels: 32

#	Server-naam	Start Port	Eindpoort	Server IP-adres
---	-------------	------------	-----------	-----------------

Service bewerken Service verwijderen

Service op maat toevoegen

- **Service-naam:** selecteer een service-type.
- **Service IP-adres:** voer het IP-adres in van de computer die de services aanbiedt.

Klik op de button **Service op maat toevoegen** om de pagina van de **Poorten – Service op maat** op de display te zien:

Poorten – service op maat

Service-naam

Protocol: TCP

Startpoort: (*)-65535

Eindpoort: (*)-65535

Server IP-adres: 192 168 100

Toepassen Annuleren

- **Service-naam:** selecteer een service-type.
- **Protocol:** het protocol gebruikt bij de mapping-poort. U kunt kiezen uit **TCP/UDP**, **TCP** of **UDP**. Het is aanbevolen **TCP/UDP** te gebruiken als u niet zeker bent welk protocol te gebruiken.
- **Startpoort:** nadat de verbinding met de mapping-poort tot stand is gebracht, is de overeenkomstige poort open en kan de toepassing daaropvolgende verbindingsverzoeken aan de open poort initiëren.
- **Eindpoort:** stel de eindpoort van de reikwijdte van de mapping-poort in.
- **Service IP-adres:** voer het IP-adres in van de computer die services aanbiedt.

Klik als u klaar bent op **Toepassen** om de instellingen op te slaan.

8.6.2 Poort-triggering

Bepaalde toepassingen, zoals WAN-netwerk games, videoconferenties en netwerkoproepen vergen meerdere verbindingen. Door de firewall-instelling kunnen deze applicaties niet op een eenvoudige NAT-router werken. Bepaalde speciale

applicaties kunnen deze applicaties echter wel laten werken op een NAT-router. Wanneer een applicatie een verbindingsverzoek naar een trigger-poort stuurt, zijn de overeenkomstige poorten geopend voor latere verbinding en het aanbieden van services. Kies **Netwerktoeassing > Poort-triggering** om de pagina van **Poort-triggering** op de display te zien.

Poort-triggering

Poort-triggering activeren

Poort-triggering time-out (in minuten) (1-9999)

Max aantal regels: 32

#	Server-naam	Service-type	Vereiste binnenkomende verbinding	Service-gebruiker
		Service toevoegen	Service bewerken	Service verwijderen

[Toepassen](#) [Annuleren](#)

- **Activeer poort-triggering:** als het vakje naast Activeer poort-triggering niet is aangevinkt is deze functie uitgeschakeld.
- **Poort-triggering time-out:** de time-out waarde bepaalt de inactiviteitstimer bij de gespecificeerde ingress-poort. Bij time-out van de inactiviteitstimer zal de ingress-poort uitschakelen.

Klik op de button **Service toevoegen** om de pagina van de **Poort-triggering – Services** op de display te zien:

Poort-triggering - Services

Service-naam	<input type="text"/>
Service-gebruiker	Alle <input type="button" value="v"/>
	<input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/>
Service-type	TCP <input type="button" value="v"/>
Triggering-startpunt	<input type="text"/> (1-65535)
Triggering-eindpunt	<input type="text"/> (1-65535)
Vereiste inkomende verbinding	
Verbindingstype	TCP <input type="button" value="v"/>
Startpoort	<input type="text"/> (1-65535)
Eindpoort†	<input type="text"/> (1-65535)

[Toepassen](#) [Annuleren](#)

- **Service-naam:** voer een service-naam in.
- **Service-gebruiker:**
 - **Alle:** sta iedereen in het gebruikersnetwerk toe de service te gebruiken.
 - **Enkel adres:** voer het IP-adres van de netwerkadapter in op de pc. De service is dan alleen toepasselijk op de specifieke netwerkadapter van de pc.

- **Service-type:** het protocol dat wordt gebruikt bij de triggering-poort. U kunt kiezen uit **TCP/UDP**, **TCP** of **UDP**.
- **Triggering-startpoort:** de eerste poort waarheen een applicatie een verbindingsverzoek stuurt. Alle relevante poorten kunnen alleen geopend worden nadat de verbinding bij deze startpoort tot stand is gebracht. Zo niet zijn de andere relevante poorten niet open.
- **Triggering-eindpoort:** stel de eindpoort van de reikwijdte van de triggering-poort in.
- **Startpoort:** de startpoort van de poort-reikwijdte.
- **Eindpoort:** de eindpoort van de poort-reikwijdte.

Klik als u klaar bent op **Toepassen** om een regel voor poort-triggering toe te voegen.

8.6.3 UPnP

Door het Universele plug-en-play (UPnP) protocol te gebruiken kan een host in de LAN de router verzoeken om specifieke poortconversies uit te voeren, om een externe host toe te staan hulpbronnen op de internet-host binnen te gaan als dat nodig is. Bijvoorbeeld, als MSN Messenger op de besturingssystemen Windows ME en Windows XP is geïnstalleerd, kan UPnP worden gebruikt voor audio- en videoconversaties. Op deze manier werken functies die door NAT beperkt worden behoorlijk.

Kies **Netwerktoepassing > UPnP** om de pagina van **UPnP** op de display te zien.

UPnP

<input type="checkbox"/> UPnP inschakelen					
Advertentieperiode (in minuten)		<input type="text" value="30"/>			
Advertentie tijd te leven (in sprongen)		<input type="text" value="4"/>			
UPnP-draagbaar tabel					
Actief	Protocol	Int. poort	Ext. poort	IP-adres	Beschrijving
<input type="button" value="Toepassen"/> <input type="button" value="Annuleren"/> <input type="button" value="Hernieuwen"/>					

- **UPnP inschakelen:** als dit is geselecteerd is UPnP geactiveerd.
- **Advertentieperiode (in minuten):** stel het uitzend-interval in. Dit staat voor het interval waarmee de router zijn UPnP-informatie uitzendt. De waarde moet tussen 1 en 1440 minuten bedragen en de standaard is 30 minuten.
- **Advertentie tijd te leven (in sprongen):** de duur dat de uitzending levend blijft. Dit is het aantal sprongen nadat elk UPnP-pakket werd verzonden. Het aantal sprongen is het aantal keren dat elk pakket kan worden uitgezonden voordat het verdwijnt. De waarde bevindt zich tussen 1 en 255 sprongen en de standaard is 4 sprongen.
- **UPnP-draagbaar tabel:** deze tabel toont de IP-adressen van UPnP-apparaten die met de router zijn verbonden en de open (interne en externe) poorten op de apparaten. Het toont ook een lijst van de types en status van de open poorten.



Opmerking:

Alleen applicaties die UPnP ondersteunen kunnen gebruik maken van de UPnP-functie. De functionaliteit van UPnP vereist ondersteuning door de applicatie en besturingsystemen zoals Windows ME, Windows XP en Windows Vista.

8.6.4 IGMP-proxying

Klik op **Netwerktoepassing > IGMP-proxying** om de pagina van **IGMP-proxying** op de display te zien.

IGMP-proxying

IGMP-proxying uitschakelen

- **Activeer IGMP-proxying:** IGMP-proxying staat een pc in de LAN toe om gewenst multi-cast verkeer van het internet te ontvangen. Schakel IGMP-proxying uit als u deze functie niet nodig hebt.

Klik als u klaar bent op **Toepassen** om de instelling toe te passen.

8.6.5 DMZ-server

DMZ (gedemilitariseerde zone) is een speciale netwerkzone die anders is dan het externe of interne netwerk. Servers die toegang hebben tot het externe netwerk, zoals het web en e-mail, verbinden met de DMZ. Het interne netwerk is beveiligd achter de Trustzone-interface en geeft geen gebruikers toegang. Daarom zijn de interne en externe netwerken afgezonderd, zodat zij de privacy-vereisten van de gebruiker kunnen voldoen. Gewoonlijk zijn er enkele publieke servers in DMZ, zoals web, mail en FTP. Gebruikers uit het externe netwerk hebben toegang tot services in DMZ, maar kunnen niet bij de geheime informatie van het bedrijf of persoonlijke informatie die op het interne netwerk is opgeslagen. Zelfs wanneer de servers in de DMZ beschadigd zijn, leidt dit niet tot verlies van geheime informatie op het interne netwerk.

Kies **Netwerktoepassing > DMZ-server** om de pagina van de **DMZ-server** op de display te zien.

DMZ-server

Standaard DMZ-server

- **Standaard DMZ-server:** voer het IP-adres van een pc in die dienst doet als de DMZ-server.



Opmerking:

Wanneer een pc op het interne netwerk als de DMZ-host wordt ingesteld, zullen alle interfaces van de pc worden blootgesteld aan het internet en is de pc niet langer beveiligd. Stel de DMZ niet onwillekeurig in tenzij dat nodig is.

Na het instellen van de DMZ-host richten mappings van alle interfaces zich naar de DMZ-host en worden de poort-mappings die naar andere hosts zijn gericht ongeldig.

8.6.6 Dynamische DNS

Dynamische domeinnaam-resolutie (DDNS) wordt voornamelijk gebruikt om een resolutie tussen vaste domeinnamen en dynamische IP-adressen te bekomen. Voor een gebruiker die een dynamisch IP-adres gebruikt, stuurt de dynamische domeinnaam-software die in de host is geïnstalleerd, nadat de gebruiker een nieuw IP-adres in de internettoegang heeft verkregen, het IP-adres naar de DDNS-server geleverd door de DDNS service-provider en werkt de database van de domeinnaam-resolutie bij. Wanneer een andere internetgebruiker toegang tot de domeinnaam probeert te vinden, stuurt de dynamische domeinnaam-resolutie server het correcte IP-adres terug.

Kies **Netwerktoepping > Dynamische DNS** om de pagina van de **Dynamische DNS** op de display te zien.

Dynamische DNS

<input type="checkbox"/> Een dynamische DNS-service gebruiken	
Serviceprovider	<input type="text" value="dyndns.org"/> ▼
Host-naam	<input type="text" value="myhostname"/>
Gebruikersnaam	<input type="text" value="User"/>
Wachtwoord	<input type="password" value="*****"/>

- **Een dynamische DNS-service gebruiken:** als u bij een DDNS-serviceprovider bent geregistreerd, selecteer dan **Een dynamische DNS-service gebruiken**.
- **Serviceprovider:** selecteer uw DDNS-serviceprovider.
- **Host-naam:** voer de host-naam of domeinnaam in van uw DDNS-serviceprovider.
- **Gebruikersnaam:** voer de naam van uw DDNS-account in.
- **Wachtwoord:** voer het wachtwoord van de DDNS-account in.

Klik als u klaar bent op **Toepassen** om de instellingen toe te passen.

8.6.7 Statische routes

Statische routing is een speciaal type van routing dat in een netwerk kan worden toegepast om het probleem van routing-selectie en overbelasting van datastroom te verminderen, welke worden veroorzaakt door de routing-selectie in een poging om de doorstuursnelheid van pakketten te verbeteren. U kunt het bestemmings-IP-adres, subnetmasker en de gateway instellen om een routing-regel te specificeren. Het bestemmings-IP-adres en subnetmasker bepalen een bestemmingsnetwerk of host naar wie de router pakketten via de gateway zal sturen.

Kies **Netwerktoppassing > Statische routes** om de pagina van de **Statische routes** op de display te zien.

Statische routes

Max. aantal regels: 32

#	Actief	Naam	Bestemming	Gateway
Toevoegen Bewerken Verwijderen				

Klik op **Toevoegen** om een regel voor de statische routing toe te voegen.

Statische routes

Actief	<input type="checkbox"/>
Route-naam	<input type="text"/>
Bestemmings-IP-adres	<input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/>
IP-subnetmasker	<input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/>
Gateway IP-adres	<input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/>
Metriek	<input type="text"/>

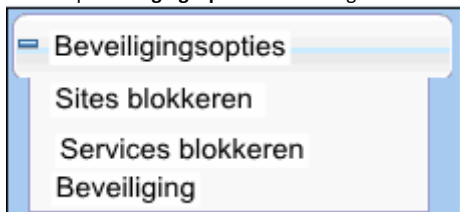
Toepassen Annuleren

- **Actief:** de regel voor statische routing kan alleen van kracht gaan als het vakje **Actief** is aangevinkt.
- **Route-naam:** voer de naam van de statische route in.
- **Bestemmings-IP-adres:** het bestemmingsadres of netwerk dat u wilt binnengaan. Dit IP-adres mag zich niet in hetzelfde netwerksegment bevinden als het IP-adres van de WAN of LAN-interface van het apparaat.
- **IP-subnetmasker:** dit IP-subnetmasker identificeert samen met het bestemmings-IP-adres het doelnetwerk.
- **Gateway IP-adres:** het IP-adres van het volgende knooppunt waarheen pakketten worden verzonden. Het gateway IP-adres moet zich in hetzelfde netwerksegment bevinden als het IP-adres van de WAN of LAN-interface van het apparaat.
- **Metriek:** het aantal andere routers in het gebruikersnetwerk. De waarde ligt tussen 2 en 15. Gewoonlijk leidt de waarde 2 of 3 tot de beste prestaties. Stel **Metriek** in op 2 als de route een rechtstreekse verbinding is.

Klik als u klaar bent met de instellingen op **Toepassen** om de instellingen op te slaan.

8.7 Beveiligingsopties

Klik op **Beveiligingsopties** om het uitgebreide navigatiemenu op de display te zien.



8.7.1 Sites blokkeren

Gebruikers kunnen toegang tot de repeater verhinderen op basis van Webadressen en Webadres sleutelwoorden. Wanneer een gebruiker een beveiligde website probeert binnen te gaan verschijnt een bericht op de display, aangevend dat de firewall toegang tot die website verhindert.

Kies **Beveiligingsopties > Sites blokkeren** om de pagina van **Sites blokkeren** op de display te zien.

Sites blokkeren

Sleutelwoord blokkeren

Nooit

Volgens schema

Altijds

Voer het sleutelwoord of de domeinnaam hier in.

Sleutelwoord toevoegen

Blokkeer sites die deze sleutelwoorden of domeinnamen bevatten (max. aantal termen: 32)

Sleutelwoord verwijderen Lijst verwijderen

Sta vertrouwd IP-adres bezoek toe geblokkeerde sites binnen te gaan

Vertrouwd IP-adres

Volg de onderstaande werkwijze om de toegang tot internetsites te blokkeren.

Stap 1 Selecteer **Volgens schema** of **Altijd** om een sleutelwoordblokkade te activeren. Om volgens tijdschema te kunnen blokkeren moet u een tijdsperiode hebben ingesteld in de pagina **Tijdschema**. Verwijs voor meer informatie over het programmeren van een tijdschema naar paragraaf **8.8.3 Tijdschema's**.

Stap 2 Voer de sleutelwoorden of domeinnamen die u wilt blokkeren in het veld van het sleutelwoord en klik op **Sleutelwoord toevoegen**. Het sleutelwoord of de domeinnaam verschijnt dan in de lijst van **Blokkeer sites die deze sleutelwoorden of domeinnamen bevatten**.

Voorbeelden van sleutelwoord-applicaties:

- Als het sleutelwoord **XXX** is gespecificeerd is de URL `www.aabbcc.com/xxx.html` geblokkeerd.
- Als het sleutelwoord **.com** is gespecificeerd zijn alleen websites met andere domeinsuffixen (zoals `.edu`, `.org` of `.gov`) toegankelijk.

Stap 3 U kunt één vertrouwde gebruiker specificeren, die een computer is zonder restricties in de netwerktoegang. Om een vertrouwde gebruiker aan te duiden voert u het IP-adres van de computer in het veld **Vertrouwd IP-adres** en vinkt u het vakje bij **Sta vertrouwd IP-adres bezoek toe geblokkeerde sites binnen te gaan** aan.

Aangezien de vertrouwde gebruiker wordt geïdentificeerd door middel van zijn IP-adres, moet u deze computer configureren met een vast IP-adres.

Stap 4 Klik op **Toepassen** om de instellingen op te slaan.

8.7.2 Services blokkeren

Gebruikers kunnen met de repeater het gebruik van bepaalde internet-services blokkeren voor computers op uw netwerk.

Kies **Beveiligingsopties > Services blokkeren** om de pagina van **Services blokkeren** op de display te zien.

Services blokkeren

Services blokkeren

Nooit

Black List

Black List

Regeltabel van services blokkeren – zwarte lijst

Max. aantal regels: 32

#	Service-naam	Poort	IP

Regeltabel van services blokkeren – witte lijst

Max. aantal regels: 32

#	Service-naam	Poort	IP

Volg de onderstaande werkwijze om een te blokkeren service te selecteren.

Stap 1 Selecteer **Volgens tijdschema** of **Altijd** om de blokkade van een trefwoord te activeren.

Om per tijdschema te kunnen blokkeren moet u een tijdsduur instellen in de pagina van het **Tijdschema**. Verwijs voor meer informatie over het tijdschema naar de paragraaf

8.8.3 Tijdschema's.

- **Zwarte lijst:** voor het blokkeren van een service die overeenstemt met de regels in het veld **Regeltabel van services blokkeren – zwarte lijst** zodat deze niet kunnen worden gebruikt.
- **White List:** geeft aan dat alleen services zijn toegestaan die overeenstemmen met de regel in het veld **Regeltabel van services blokkeren – witte lijst** zodat deze beschikbaar zijn voor gebruik.

Stap 2 Klik op **Toevoegen** om een service voor blokkade toe te voegen. De **Instellingen van services blokkeren** verschijnt op de display:

Instellingen van services blokkeren

Service-type	Door gebruiker gedefinieerd
Protocol	TCP
Startpoort	(1~65535)
Eindpoort	(1~65535)
Service-type/door gebruiker bepaald	
Filter service voor:	
<input type="radio"/> Alleen dit IP-adres	192 . 168 . 1 .
<input type="radio"/> IP-adres reikwijdte	192 . 168 . 1 .
	to 192 . 168 . 1 .
<input checked="" type="radio"/> Alle IP-adressen	

Stap 3 Stel in deze pagina de parameters in.

- **Service-type:** selecteer een service-type. Als uw gewenste type niet aanwezig is in de lijst selecteert u **Door gebruiker bepaald**. U moet dan het protocol selecteren, de service-naam invoeren en de reikwijdte van de poort definiëren. Voor services die in de neerklappende lijst aanwezig zijn is de overeenkomstige informatie reeds geprogrammeerd.
- **Protocol:** stel het protocol in dat bij de service-poorten wordt gebruikt. Als u niet zeker bent van het protocol dat de applicatie gebruikt, selecteer dan **TCP/UDP**.
- **Startpoort/eindpoort:** de start- en eindpoorten van de poort-reikwijdte waar de gespecificeerde service is geblokkeerd. Als de applicatie gebruik maakt van een enkel poortnummer, voert u dat nummer in beide velden.
- **Service-type/door gebruiker bepaald:** voer de service-naam in.
- **Filter service voor:** u kunt de gespecificeerde service voor een enkele computer, computers binnen een reikwijdte van IP-adressen of voor alle computers blokkeren.

Klik als u klaar bent op **Toevoegen** om een nieuwe regel toe te voegen. Klik daarna op **Toepassen** om de instellingen op te slaan.

8.7.3 Beveiliging

Kies **Beveiligingsopties > Beveiliging** om de pagina van **Beveiliging** op de display te zien.

Beveiliging

Poort-scan en DOS-beveiliging uitschakelen

Reageer op Ping of internet-poort

NAT-filtrage

Beveiligd

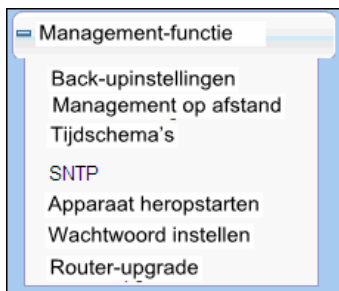
Toepassen Annuleren

- **Poort-scan en DOS-beveiliging uitschakelen:** de beveiliging Ontkennen van service (DoS) beschermt uw LAN tegen DOS-aanvallen. Over het algemeen is het raadzaam de poortscanning en de functie DOS-beveiliging te activeren.
- **Reageer op Ping of internet-poort:** als dit is geactiveerd reageert de router op ping-commando's van het internet. Zoals de DMZ-server, zal het activeren van deze functie echter veiligheidsrisico's met zich meebrengen. Over het algemeen is het raadzaam deze functie uit te schakelen.
- **NAT-filtrage:** NAT-filtrage bepaalt de manier waarop de router met inkomend verkeer omgaat.
 - **Beveiligd:** deze optie biedt een beveiligde firewall om pc's op LAN te beschermen tegen aanvallen van het internet, maar het is mogelijk dat het sommige internet-games, punt-naar-punt applicaties of multimedia-applicaties niet toestaat.
 - **Open:** deze optie biedt een minder veilige firewall waarbij de meeste internetapplicaties werken.

Klik als u klaar bent op **Toepassen** om de instellingen toe te passen.

8.8 Managementfunctie

Klik op **Managementfunctie** om het uitgebreide navigatiemenu op de display te zien.



8.8.1 Back-up-instellingen

Verwijs voor details naar de paragraaf 7.6.1 **Back-up-instellingen**.

8.8.2 Management op afstand

De managementfunctie op afstand staat u toe te router via de webbrowser te configureren vanaf de WAN. Zo kunt u uw router ook op een host op afstand beheren.

Kies **Managementfunctie > Management op afstand** om de pagina van **Management op afstand** op de display te zien.

Management op afstand	
<input type="checkbox"/> Schakel management op afstand in	
Afstand management adres:	<input type="text" value="http://0.0.0.0:8080"/>
Poortnummer:	<input type="text" value="8080"/>
Sta toegang op afstand toe voor:	
<input type="radio"/>	Alleen deze computer <input type="text"/>
<input type="radio"/>	IP-adres reikwijdte <input type="text"/> Van <input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/>
	Naar <input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/>
<input checked="" type="radio"/>	Iedereen
<input type="button" value="Toepassen"/> <input type="button" value="Annuleren"/>	

- **Schakel management op afstand in:** als dit is geselecteerd kunt u web-management van de router op afstand beheren vanaf de WAN.
- **Afstand management adres:** het IP-adres dat wordt gebruikt om de router vanaf het internet binnen te gaan. De standaard is `http://0.0.0.0:8080`. Bij het binnengaan van de router moet u een adres invoeren in de vorm van **“het WAN IP-adres van de router” + “:” + “het poortnummer”** in de IE-adresbalk. Bijvoorbeeld, als uw externe adres **10.0.0.123** is en het gebruikte poortnummer is **8080**, voer dan **10.0.0.123:8080** in uw browser.
- **Poortnummer:** het poortnummer voor toegang tot de router via web-management op afstand.

- **Sta toegang op afstand toe voor:** stel het IP-adres van de computer waarop web-management op afstand wordt uitgevoerd om de router binnen te gaan.
 - **Alleen deze computer:** alleen het gespecificeerde IP-adres krijgt toegang tot de router.
 - **IP-adres reikwijdte:** een reikwijdte van IP-adressen op het internet krijgt toegang tot de router. U moet de startende en eindigende IP-adressen invoeren om een reikwijdte te definiëren.
 - **Iedereen:** iedereen op het internet heeft toegang tot de router.

Klik als u klaar bent met de instellingen op **Toepassen** om de instellingen op te slaan.

8.8.3 Tijdschema's

Kies **Managementfunctie > Tijdschema's** om de pagina van **Tijdschema** op de display te zien.

Tijdschema

Te blokkeren dagen:		
<input checked="" type="checkbox"/>	Elke dag	
<input checked="" type="checkbox"/>	Zondag	
<input checked="" type="checkbox"/>	Maandag	
<input checked="" type="checkbox"/>	Dinsdag	
<input checked="" type="checkbox"/>	Woensdag	
<input checked="" type="checkbox"/>	Donderdag	
<input checked="" type="checkbox"/>	Vrijdag	
<input checked="" type="checkbox"/>	Zaterdag	
Te blokkeren tijd van de dag (gebruik 24-uurklok)		
<input checked="" type="checkbox"/>	De hele dag	
Start blokkeren	00	Uur · 00
		Minuten
Einde blokkeren	23	Uur · 59
		Minuten
<input type="button" value="Toepassen"/> <input type="button" value="Annuleren"/>		

Als u al site-filtrage in de pagina van **Sites blokkeren** of service-filtrage in de pagina van **Services blokkeren** had ingesteld, kunt u een tijdschema instellen om de tijd en modus van geblokkeerde internettoegang te bepalen.

- Te blokkeren dagen: Selecteer de dagen waarop u de blokkade wil uitvoeren door de overeenkomstige vakjes aan te vinken. Selecteer **Elke dag** om de vakjes van alle dagen aan te vinken.
- Te blokkeren tijd van de dag:
 - **De hele dag:** voor een 24-uur durende blokkade.

- **Start blokkeren/einde blokkeren:** om de toegang in een vaste periode op de ingestelde dagen te blokkeren voert u de start- en eindtijd in een 24-uur opmaak.

Klik als u klaar bent met de instellingen op **Toepassen** om de instellingen op te slaan.

8.8.4 SNTP

Kies **Managementfunctie > SNTP** om de pagina van **SNTP** op de display te zien.

SNTP

Instelling van de tijd				
<input type="checkbox"/> Automatisch synchroniseren met tijdservers op internet				
Eerste NTP-tijdserver:	<input type="text" value="210.72.145.44"/>			
Tweede NTP-tijdserver:	<input type="text"/>			
Tijdconfiguratie				
Huidige routertijd:	1971-01-01 14:39:45			
Tijdzone :	(GMT+01:00) Parijs, Brussel, Kopenhagen, Madrid <input type="button" value="v"/>			
<input type="checkbox"/> Zomertijd activeren <input type="button" value="j"/>				
Zomertijd offset: :	<input type="text" value="0:00"/> <input type="button" value="v"/>			
Zomertijd data: (Tijdsinterval moet groter zijn dan de dagen van de startmaand)	Maand	Week	Dag	
	Start	<input type="text" value="Apr"/> <input type="button" value="v"/>	<input type="text" value="2nd"/> <input type="button" value="v"/>	<input type="text" value="Sun"/> <input type="button" value="v"/>
	Einde	<input type="text" value="Sep"/> <input type="button" value="v"/>	<input type="text" value="2nd"/> <input type="button" value="v"/>	<input type="text" value="Sun"/> <input type="button" value="v"/>

SNTP staat voor simpel netwerk tijdprotocol. U kunt in deze pagina tijdinformatie over uw router instellen. Het is absoluut raadzaam eerst de correcte tijd op uw router in te stellen. Zo kunnen de log, het blokkeren van sites en het tijdschema correct werken om dat de tijdinstellingen hiervan gebaseerd zijn op de tijdinformatie van deze pagina.

- **Automatisch synchroniseren met tijdservers op internet:** als dit is geselecteerd gebeurt de synchronisatie automatisch zodra de tijdserver op het netwerk is ingeschakeld.
- **Eerste NTP-tijdserver:** voer het IP-adres van de primaire NTP-server in. De NTP-server is een timerserver op het netwerk die wordt gebruikt voor het synchroniseren van de tijd van computers op het internet. Wanneer u de primaire NTP-server instelt ontvangt de router, na te zijn verbonden met het internet, de GMT-tijd van de gespecificeerde NTP-server met prioriteit.
- **Tweede NTP-tijdserver:** voer het IP-adres van een secundaire NTP-server in als deze beschikbaar is.
- **Huidige routertijd:** om de huidige systeemtijd van de router te tonen.
- **Tijdzone:** selecteer de tijdzone waar u zich bevindt.
- **Zomertijd activeren:** schakel de zomertijd (DST) uit of in.
- **Zomertijd offset:** selecteer de juiste offset. Als dit is ingesteld op +1:00, wordt 10:00 uur in de ochtend in DTS 11:00 uur in de ochtend.

- **Zomertijd data:** stel de start- en eindtijd van DST in.

Klik als u klaar bent met de instellingen op **Toepassen** om de instellingen op te slaan.

8.8.5 Apparaat heropstarten

Verwijs voor details naar de paragraaf **7.6.2 Apparaat heropstarten**.

8.8.6 Wachtwoord instellen

Verwijs voor details naar de paragraaf **7.6.3 Wachtwoord instellen**.

8.8.7 Router-upgrade

Kies **Managementfunctie > Router-upgrade** om de pagina van **Router-upgrade** op de display te zien.

Router-upgrade

Vind en selecteer het upgrade-bestand van uw harde schijf:

<input type="text"/>	Bladeren	Config. verwijderen
----------------------	----------	---------------------

Uploaden Annuleren

Volg de onderstaande werkwijze om de software van de router bij te werken.

- Stap 1** Klik op **Bladeren...** om naar de nieuwste software te navigeren.
- Stap 2** Selecteer het correcte upgrade-bestand. Als u **Config. verwijderen** selecteert, zal de router na het upgraden terugstellen naar de standaardinstellingen. Als u dit niet selecteert, blijft de huidige instelling van kracht.
- Stap 3** Klik op **Uploaden** om het bijwerken te starten.

De router herstart automatisch nadat de upgrade is voltooid.



Opmerking:

Na de software-upgrade keert het apparaat terug naar de standaard fabrieksinstellingen. Als de vroegere configuratie-informatie verloren is gegaan, moet u de instellingen opslaan voordat u de software bijwerkt.

Schakel de router niet uit tijdens de upgrade.

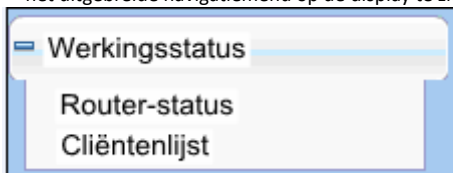
9 Webconfiguratie in de draadloze universele repeater-modus

Opmerking:

Schakel de driewegschakelaar op het zijpaneel naar **Repeater**. Meld aan op de configuratiepagina nadat het apparaat is herstart.

9.1 Werkingsstatus

Schakel de driewegschakelaar op het zijpaneel naar **Repeater**. Klik op **Werkingsstatus** om het uitgebreide navigatiemenu op de display te zien.



9.1.1 Router-status

Kies **Werkingsstatus** > **Router-status** om de pagina van de **Router-status** op de display te zien.

Router-status	
Systeeminfo	
Hardware-versie	V1.0.0
Firmware-versie	V1.0.0
Productnaam	Draadloze router
Werkmodus	Repeater-modus
Tijd en datum	1971-01-01 08:03:07
LAN-poort	
MAC-adres	00:1E:E3:4B:05:6C
IP-adres	192.168.100.253
IP-subnetmasker	255.255.255.0
Draadloze cliënt	
Draadloos netwerk geselecteerde naam (SSID)	TW-2B08
Draadloos kanaal	2.457GHz-CH10
Wi-Fi-beveiligd kanaal (WPS)	AAN
Draadloze beveiligingsmodus	Geen
Verbindingsstatus	Niet verbonden
Draadloze universele repeater	
SSID van uitgebreide interface	TW-2B08
Draadloze beveiligingsmodus	Geen

U kunt in deze pagina informatie over de huidige werkingsstatus van het apparaat zien, met onder meer systeeminformatie, de status van de LAN-poort, informatie over de draadloze cliënt en de status van de draadloze universele repeater.

9.1.2 Cliëntenlijst

Kies **Werkingsstatus** > **Cliëntenlijst** om de pagina van de **Cliëntenlijst** op de display te zien.

Clëntenlijst

Draadverbonden apparaten			
#	IP-adres ^s	MAC-adres	Apparaat-naam
1	192.168.100.10	48:02:2A:D1:A9:60	Onbekend

Draadloze apparaten (draadloze indringers worden hier ook aangegeven)			
#	IP-adres ^s	MAC-adres	Apparaat-naam

[Hernieuw](#)

Deze pagina toont informatie over apparaten die met de repeater zijn verbonden, met onder meer de IP-adressen, de apparaat-naam en het MAC-adres van elk apparaat.

9.2 Installatie-wizard

Verwijs voor de instellingen naar de paragraaf **6.3 Configuratie van de repeater-modus**.

9.3 Instelling van de repeater-modus

Klik op **Instellingen van de repeater-modus** om de pagina van **Instelling van de repeater-modi** op de display te zien. Selecteer **Draadloze universele repeater-modus**.
Instellingen van de repeater-modus

Er zijn twee manieren voor het uitbereiden van uw draadloze netwerk van de Repeater-modus. U kunt kiezen tussen de WDS-modus en de UR-modus.

Geef uw repeater-modus als volgt te kiezen:

- WDS-modus
- Draadloze universele repeater-modus

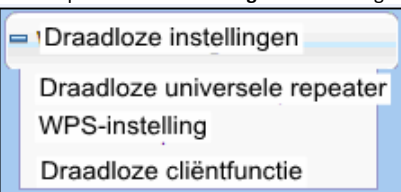
[Toepassen](#) [Annuleren](#)

9.4 Netwerkinstellingen

Verwijs voor details naar de paragraaf **7.4 Netwerkinstellingen**.

9.5 Draadloze instellingen

Klik op **Draadloze instellingen** om het uitgebreide navigatiemenu op de display te zien.



9.5.1 Draadloze universele repeater

In de universele repeater-modus doet het apparaat tegelijkertijd dienst als AP en als cliënt.

Kies **Draadloze instellingen** > **Draadloze universele repeater** om de pagina van **Draadloze universele repeater** op de display te zien.

Draadloze universele repeater

SSID van uitgebreide interface	<input type="text" value="TW-2808"/>
Beveiligingsopties	
Beveiligingsopties:	<input type="text" value="geen"/>

- **SSID van uitgebreide Interface:** stel de SSID van de repeater in.
- **Beveiligingsopties:** stel de beveiligingsencryptie-modus voor de repeater in. Het is raadzaam de repeater met dezelfde encryptie-modus als die van zijn uplink-AP te configureren.

Klik als u klaar bent met de instellingen op **Toepassen** om de instellingen op te slaan.

9.5.2 WPS-instelling

Kies **Draadloze instellingen** > **WPS-instelling** om de onderstaande pagina op de display te zien.

WPS-instelling
Nieuwe en gemakkelijke manier om met de draadloze router te verbinden via WiFi-beveiligde instelling (WPS)
Een draadloze cliënt moet de WPS-functie ondersteunen om deze wizard te kunnen gebruiken voor het toevoegen van de cliënt aan uw WPS-geactiveerde draadloze router.
Kijk de handleiding en verpakking van uw draadloze cliënt na om te zien of hij de WPS-functie ondersteunt.
Als uw draadloze cliënt de WPS-functie niet ondersteunt moet u uw draadloze client handmatig configureren zodat hij dezelfde SSID en draadloze beveiligingsinstellingen heeft als deze router.
<input type="button" value="Volgende"/>

WPS staat voor WiFi-beveiligde instelling.

U kunt WPS gebruiken om snel en veilig een draadloze verbinding tot stand te brengen als de uplink-AP of terminal (bijvoorbeeld de netwerkadapter) is uitgerust met de WPS-functie. Wij suggereren dat u eerst de draadloze encryptie voor de uplink-AP configureert. Als u, na het tot stand brengen van de draadloze verbinding via WPS, de draadloze encryptie-modus wijzigt moet u WPS gebruiken om opnieuw een draadloze verbinding tot stand te brengen. Merk op dat, als de draadloze cliënt WPS niet ondersteunt, u de draadloze cliënt handmatig moet configureren (zoals SSID, beveiligingsmodus en wachtwoord) met dezelfde SSID en draadloze beveiligingsinstellingen als de router.

In de Repeater-modus, met WDS uitgeschakeld, voert het apparaat een WPS-geëncrypteerde verbinding uit met zowel de uplink-AP als het downlink-cliëntapparaat.

Klik op **Volgende** om de pagina van de **WPS-instelling** binnen te gaan. Volg de onderstaande beschrijving om WPS voor de Repeater-modus te configureren.

9.5.2.1 Via de WPS-toets

- WPS-verbinding met de uplink-AP

Druk in de Repeater-modus met WDS uitgeschakeld binnen de 3 seconden op de **WPS-toets** op het zijpaneel van het apparaat en laat los. Druk dan op de **WPS-toets** van de uplink-AP. Beide kunnen dan de WPS-sessie starten.

- WPS-verbinding naar het downlink-cliëntapparaat

Houd in de Repeater-modus met WDS uitgeschakeld de **WPS-toets** op het zijpaneel van het apparaat gedurende 3-10 seconden ingedrukt en laat los. Druk dan op de **WPS-toets** van het cliëntapparaat. Beide kunnen dan de WPS-sessie starten.



Opmerking:

Nadat het apparaat erin is geslaagd met de uplink-AP te verbinden via de methode van de WPS-toets, zullen de SSID, authenticatie en vooraf-gedeelde sleutel van het apparaat automatisch veranderen naar dezelfde als die van haar uplink-AP.

9.5.2.2 Via de webpagina

U kunt de WPS-instellingen maken via de webpagina voor configuratie.

Kies **Draadloze instellingen > WPS-instelling** om de pagina van de **WPS-instelling** te zien.

WPS-instelling

Als een AP, selecteer een instelmethode:	
<input checked="" type="radio"/> Druktoets (aanbevolen))	
U kunt ofwel fysiek op de druktoets van de router drukken of op de onderstaande (soft)button klikken.	<input type="button" value="Start PBC"/>
<input type="radio"/> IPIN (persoonlijk identificatienummer)	
Als een cliënt, selecteer een instelmethode:	
<input checked="" type="radio"/> Druktoets (aanbevolen)	
U kunt ofwel fysiek op de druktoets van de router drukken of op de onderstaande (soft)button klikken.	<input type="button" value="Start PBC"/>
<input type="radio"/> PIN (persoonlijk identificatienummer)	

– Als een AP

U kunt de WPS-instellingen ook doen via de webpagina voor configuratie.

Kies **Draadloze instellingen > WPS-instelling** om de pagina van WPS op de display te zien.

- PBC-modus

Stap 1 Selecteer **Druktoets** en klik op **Start PBC**. De WPS-geëncrypteerde verbinding start op.

WPS-instelling

Als een AP, selecteer een instelmethode:

Druktoets (aanbevolen))

U kunt ofwel fysiek op de druktoets van de router drukken of op de onderstaande (soft)button klikken.

IPIN (persoonlijk identificatienummer)

Als een cliënt, selecteer een instelmethode:

Druktoets (aanbevolen))

U kunt ofwel fysiek op de druktoets van de router drukken of op de onderstaande (soft)button klikken.

PIN (persoonlijk identificatienummer)

- Stap 2** Druk binnen de 2 minuten op de **WPS**-toets van de netwerkadapter of klik op de **PBC**-button in het hulpmiddel van de netwerkadapter-configuratie om de WPS-verbinding te starten. Nadat de WPS-verbinding tot stand is gebracht verschijnt de onderstaande pagina op de display, aangevend dat de WPS-verbinding is voltooid.

Success

De draadloze cliënt is met succes toegevoegd aan het netwerk.
Klik op OK om terug te keren naar de WiFi-beveiligde instelpagina...OK

- PIN-modus

- Stap 1** Selecteer **PIN**, voer de PIN-code van de netwerkadapter in (verwijs naar de cliënt van de netwerkadapter) en klik op **Start PIN** om de WPS-verbinding te starten.

WPS-instelling

Als een AP, selecteer een instelmethode:

Druktoets (aanbevolen))

PIN (persoonlijk identificatienummer)

Als uw adapter WPS ondersteunt, klikt u op "Genereer een cliënt-beveiligingspin voor input in de AP/router/gateway" en voer het gegenereerde PIN-nummer hier in.

Als een cliënt, selecteer een instelmethode:

Druktoets (aanbevolen))

U kunt ofwel fysiek op de Druktoets van de router drukken of op de onderstaande (soft)button klikken.

PIN (persoonlijk identificatienummer)

- Stap 2** Klik binnen de 2 minuten op de PIN-toets van de netwerkadapter om de WPS-verbinding te starten. Nadat de WPS-verbinding tot stand is gebracht verschijnt de onderstaande pagina op de display, aangevend dat de WPS-verbinding is voltooid.

Success

De draadloze cliënt is met succes toegevoegd aan het netwerk.
Klik op OK om terug te keren naar de WiFi-beveiligde instelpagina...OK

Als een cliënt

U kunt de WPS-instellingen uitvoeren via de webpagina voor configuratie.

Kies **Draadloze instellingen > WPS** om de pagina van WPS op de display te zien.

- PBC-modus

Stap 1 Selecteer **Druktoets** en klik op **Start PBC**. De WPS-geëncrypteerde verbinding start op.

WPS-instelling

Als een AP, selecteer een instelmethode:

- Druktoets (aanbevolen) 1)

U kunt ofwel fysiek op de druktoets van de router drukken of op de onderstaande (soft)button klikken.

Start PBC

- PIN (persoonlijk identificatienummer)

Als een cliënt, selecteer een instelmethode:

- Druktoets (aanbevolen) 1)

U kunt ofwel fysiek op de druktoets van de router drukken of op de onderstaande (soft)button klikken.

Start PBC

- PIN (persoonlijk identificatienummer)

Stap 2 Start de WPS PBC-procedure. Nadat de WPS-verbinding tot stand is gebracht verschijnt de onderstaande pagina op de display, aangevend dat de WPS-verbinding is voltooid.

Success

De draadloze cliënt is met success toegevoegd aan het netwerk.
Klik op OK om terug te keren naar de WiFi-beveiligde instelpagina...OK

OK

- PIN-modus

Stap 1 Selecteer **PIN**, klik op **Nieuwe PIN genereren** en klik op **Start PIN** om de WPS-verbinding te starten.

WPS-instelling

Als een AP, selecteer een instelmethode:

- Druktoets (aanbevolen) 1)

U kunt ofwel fysiek op de druktoets van de router drukken of op de onderstaande (soft)button klikken.

Start PBC

- PIN (persoonlijk identificatienummer)

Als een cliënt, selecteer een instelmethode:

- Druktoets (aanbevolen) 1)

- PIN (persoonlijk identificatienummer)

Als uw adapter WPS ondersteunt, klikt u op "Genereer een cliëntbeveiligings-PIN voor input in de AP/router/gateway" en voer het gegenereerde cliënt PIN-nummer hier in.

Genereer nieuwe PIN

PIN van cliënt: 12345670

Start PIN

Stap 2 Start binnen de 2 minuten de WPS PBC-procedure om de WPS-verbinding te starten. Nadat de WPS-verbinding tot stand is gebracht verschijnt de

onderstaande pagina op de display, aangevend dat de WPS-verbinding is voltooid.

Success

De draadloze cliënt is met success toegevoegd aan het netwerk.
Klik op OK om terug te keren naar de WiFi-beveiligde instelpagina...OK

OK

9.5.3 Draadloze cliëntfunctie

Kies **Draadloze instellingen > Draadloze cliëntfunctie** om de pagina van **Draadloze cliëntfunctie** op de display te zien.

Draadloze cliëntfunctie

Deze pagina helpt u met het configureren van de draadloze cliënt.

Stap 1: klik op de button "Site-onderzoek" om draadloze sites te onderzoeken terwijl de cliënt-modus is ingeschakeld. Zodra een Access-point of IBSS wordt gevonden, worden de resultaten drie seconden later in de lijst van het site-onderzoek aangegeven. U kunt er dan een uit kiezen om handmatig mee te verbinden. Klik daarna op "Volgende".

Site-onderzoek

Aantal sites onderzocht: 32

Site Survey List

#	SSID	BSSID	Kanaal	Signaal	Encryptie	Selecteer
1	Zoltrix_ZW919	00:28:12:34:56:78	1	100%	None	<input checked="" type="radio"/>
2	www24	00:1E:E3:C0:5F:6B	6	100%	None	<input type="radio"/>
3	TW-2B08	00:1F:A4:91:2A:60	10	100%	WPA-PSK(AES/TKIP) WPA2-PSK(AES/TKIP)	<input type="radio"/>

Volgende

Stap 1 Klik op **Site-onderzoek** om te zoeken naar het draadloze netwerk waarmee u verbinding wilt.

Stap 2 Voer de encryptie-informatie over het geselecteerde draadloze netwerk in. Configureer de cliënt met dezelfde beveiligingsinstellingen als het geselecteerde netwerk. Klik op **Volgende**.

Draadloze cliëntfunctie

Stap2: u moet uw draadloze cliënt handmatig configureren met dezelfde draadloze beveiligingsinstellingen als het netwerk dat u heeft geselecteerd. Klik dan op "Volgende"

Beveiligingsopties

Beveiligingsopties

Geen

Terug Volgende

Stap 3 Het apparaat biedt de draadloze roaming-functie als u **Synchroniseer SSID's en beveiligingsopties van de draadloze universele repeater en Uplink AP** selecteert. Klik op **Voltoeien**. De cliënt kan dan met het geselecteerde netwerk communiceren.

Draadloze cliëntfunctie

Stap3: deze pagina biedt een gemakkelijke manier om de draadloze universele repeater te configureren. Als u deze functie inschakelt, gebruikt uw draadloze universele repeater dezelfde SSID en beveiligingsopties als de uplink-AP. Klik tenslotte op "Voltoeien".

Synchroniseer de SSID en beveiligingsopties van de draadloze repeater en uplink-AP.

Opmerking: als u de instellingen van de draadloze universele repeater heeft gewijzigd, zullen de draadloze cliënten die met uw draadloze universele repeater verbinden dit moeten doen met de nieuwe SSID en beveiligingsopties.

Terug Voltoeien

9.6 Managementfunctie

Verwijs voor details naar de paragraaf **7.6 Managementfunctie**.

10 Webconfiguratie voor de WDS-modus

10.1 Werkingsstatus

Verwijs voor details naar de paragraaf **9.1 Werkingsstatus**.

10.2 Installatie-wizard

Verwijs voor de instellingen naar de paragraaf **6.4 WDS-modus**.

10.3 Modusinstelling

Klik op **Modusinstellingen** om de pagina van **Modusinstellingen** op de display te zien. Instellingen van de repeater-modus

Er zijn 2 manieren voor het uitbreiden van uw draadloze netwerk van de repeater-modus. U kunt kiezen uit de WDS-modus of de UR-modus.

Kies uw repeater-modus als volgt: :

WDS-modus

Draadloze universele repeater-modus

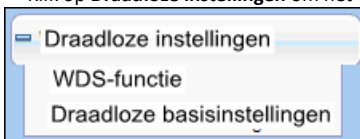
Selecteer **WDS-modus**. Let erop dat de WDS-functie niet kan worden gebruikt als het kanaal niet op **Auto** is ingesteld.

10.4 Netwerkinstellingen

Verwijs voor details naar de paragraaf **7.4 Netwerkinstellingen**.

10.5 Draadloze instellingen

Klik op **Draadloze instellingen** om het uitgebreide navigatiemenu op de display te zien.



10.5.1 WDS-functie

Het draadloze distributiesysteem (WDS) activeert onderlinge verbindingen tussen AP's in een IEEE 802.11-draadloos netwerk. Het breidt het draadloze netwerk uit via

verschillende AP' s zonder verbinding van een draadgebonden backbone-netwerk. Activeer WDS als u WDS wilt gebruiken om een draadloze repeating of overbrugging tot stand te brengen.

Kies **Draadloze instellingen** > **WDS-functie** om de pagina van **WDS-functie** op de display te zien.

WDS-functie

<input type="checkbox"/> Schakel draadloze cliëntassociatie uit	
Draadloze MAC van deze router: 00:1E:E3:4B:06:6C	
Draadloze repeater	
IP-adres van repeater:	<input type="text" value="192"/> <input type="text" value="168"/> <input type="text" value="100"/> <input type="text" value="253"/>
MAC-adres van basisstation:	<input type="text" value="00:1E:E3:4B:06:6C"/>

- **Schakel draadloze cliëntassociatie uit:** als dit is geselecteerd stuurt de repeater geen signalen naar cliënten die ermee zijn verbonden. Over het algemeen is dit vakje uitgevinkt. Over het algemeen moet dit vakje aangevinkt worden.
- **IP-adres van repeater:** stel een ander IP-adres voor de repeater in dan voor het draadloze basisstation en andere repeaters, om conflict van IP-adressen te voorkomen. Wij raden het instellen van IP-adressen van hetzelfde netwerksegment voor het draadloze basisstation en de repeaters aan.
- **MAC-adres van basisstation:** voer het MAC-adres van het draadloze basisstation in.

Klik als u klaar bent met de instellingen op **Toepassen** om de instellingen op te slaan.

Verwijs voor een beschrijving van de WDS-toepassing naar **6.4.3 WDS-toepassing**.

10.5.2 Draadloze basisinstellingen

Verwijs voor details naar **7.5.1 Draadloze basisinstellingen**.

10.6 Managementfunctie

Verwijs voor details naar de paragraaf **7.6 Managementfunctie**.

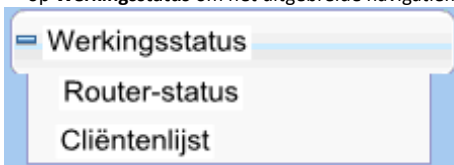
11 Webconfiguratie in de cliëntmodus

Opmerking:

schakel de drierichtingschakelaar op het zijpaneel naar de **Cliënt** modus.

11.1 Werkingsstatus

Schakel de driewegschakelaar op de behuizing van het apparaat naar de Cliëntmodus. Klik op **Werkingsstatus** om het uitgebreide navigatiemenu op de display te zien.



11.1.1 Router-status

Kies **Werkingsstatus** > **Router-status** om de pagina van de **Router-status** op de display te zien.

Router-status ;

:Systeeminfo	
Hardware-versie	V1.0.0
Software-versie	V1.0.0
Productnaam	Draadloze router
Werkmodus	Cliëntmodus
Tijd en datum	1971-01-01 08:14:54
LAN-poort	
MAC-adres	00:1E:E3:4B:06:6C
IP-adres:	192.168.100.253
IP-subnetmasker	255.255.255.0
Draadloze cliënt	
Draadloos netwerk geselecteerde naam (SSID)	
Draadloos kanaal	2.412GHz- CH1
Wi-Fi-beveiligde instellingen (WPS)	AAN
Draadloze beveiligingsmodus	Geen
Status van de verbinding	Niet verbonden

U kunt in deze pagina informatie over de huidige werkingsstatus van het apparaat zien, met onder meer de systeeminformatie, de status van de LAN-poort en de status van de draadloze cliënt.

11.1.2 Cliëntenlijst

Kies **Werkingsstatus** > **Cliëntenlijst** om de pagina van **Cliëntenlijst** op de display te zien.

Cliëntenlijst

Draadgebonden apparatuur			
#	IP-adres	MAC-adres	Apparaat-naam
1	192.168.100.10	48:02:2A:D1:A9:60	onbekend

[Hernieuwen](#)

Deze pagina toont informatie over draadloze apparaten die met apparaat zijn verbonden, met onder meer de IP-adressen en het MAC-adres van elk apparaat.

11.2 Installatie-wizard

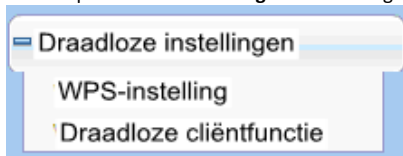
Verwijs voor details naar [6.5 Configuratie van de cliëntmodus](#).

11.3 Netwerkinstellingen

Verwijs voor details naar de paragraaf [7.4 Netwerkinstellingen](#).

11.4 Draadloze instellingen

Klik op **Draadloze instellingen** om het uitgebreide navigatiemenu op de display te zien.



11.4.1 WPS-instelling

Verwijs voor details naar [7.5.4 WPS-instelling](#).

11.4.2 Draadloze cliëntfunctie

Verwijs voor details naar [9.5.3 Draadloze cliëntfunctie](#).

11.5 Managementfunctie

Verwijs voor details naar de paragraaf [7.6 Managementfunctie](#).

Appendix A VAAK GESTELDE VRAGEN

1	Het apparaat wordt niet door de draadloze netwerkadapter gedetecteerd.
	Wanneer het apparaat in de Cliënt- of Repeater-modus is geschakeld maar niet verbonden is met de uplink-AP en geen toegang voor draadloze cliënten toestaat, kan het alleen via een ethernetkabel worden verbonden. Als dit het probleem niet oplost bevindt het apparaat zich wellicht te ver van het terminal-apparaat of belemmert een obstakel dat het draadloze signaal. U kunt het apparaat dichterbij het terminal-apparaat brengen of een draadloze repeater toevoegen. Zorg er bovendien voor dat magnetrons, Bluetooth-apparaten en mobiele telefoons die WLAN-signalen onderbreken uit de buurt van WLAN-apparaten worden gehouden.
2	De draadloze netwerkadapter maakt geen verbinding met het apparaat.
	Sommige oudere draadloze netwerkadapters ondersteunen de WPA2-authenticatie nog niet. U kunt de authenticatie en encryptie instellen op WPA-AES, WPA-TKIP of WEP.
3	Het apparaat in de repeater- of cliëntmodus maakt geen verbinding met de uplink-AP, bijvoorbeeld de domestic gateway, voor toegang tot het internet of de verbinding met het internet wordt regelmatig onderbroken.
	Controleer of het apparaat zich in de draadloze signaaldekking van zijn uplink-apparaat bevindt. Klik op Site-onderzoek in de pagina van de Draadloze cliëntfunctie en controleer of het apparaat sterke draadloze signalen van de uplink-AP kan vinden of niet.
4	De draadgebonden verbinding met het apparaat is abnormaal.
	Controleer de status van de ethernet-indicator op het apparaat. Als de ethernet-indicator uitschakelt, kunt u controleren of de ethernetkabel goed is aangesloten. Als dit het probleem niet oplost kunt u de ethernetkabel vervangen.
5	Geen toegang tot het internet.
	Controleer of de netwerkadapter die met het apparaat is verbonden automatisch een IP-adres verkrijgt. Zo niet moet u DHCP voor de domestic gateway instellen of het IP-adres van de netwerkadapter en DNS handmatig instellen.
6	Het apparaat kan niet via de webpagina worden geconfigureerd.
	Controleer of het IP-adres van de netwerkadapter en dat van het apparaat zich in eenzelfde netwerksegment bevinden. Stel het IP-adres van netwerkadapter handmatig in het netwerksegment van 192.168.100.2/253 in overeenstemming met de werkwijze beschreven in Hoofdstuk 5 "Pc-configuratie en configuratie van de draadloze verbinding". Kies Netwerkinstellingen > Instellingen van de LAN-interface en stel het IP-adres of het apparaat in op hetzelfde netwerkadres als dat van de domestic netwerk-gateway.
7	De WPS-verbinding mislukt.
	Zorg ervoor dat slechts één WPS-apparaat dat is verbonden met het apparaat de WPS-sessie binnen de 2 minuten opstart. Merk een WPS-verschil op tussen het apparaat dat dienst doet als uplink-AP en als downlink-cliënt apparaat in de repeater-modus (zie paragraaf 9.5.2 WPS-instelling). Verwijs naar Tabel 4.1 voor een beschrijving van de WPS-indicatorstatus.

VERWIJDERING



Als een verantwoordelijke verkoper geven wij om het milieu.

Daarom sporen wij u aan de correcte verwijderingsprocedure te volgen voor dit product, de verpakkingsmaterialen en –voor zover van toepassing- de accessoires. Dit zal helpen natuurlijke grondstoffen te besparen en ervoor zorgen dat de materialen worden gerecycled op een manier die de gezondheid en het milieu beschermt.

U dient de wetten en reglementering betreffende verwijdering te volgen. Afgedankte elektrische producten horen aan het eind van hun gebruiksduur in geen geval bij het huisvuil.

Neem contact op met de winkel waar u dit product aankocht en uw plaatselijke overheid voor meer informatie over verwijdering en recycling.

Onze verontschuldiging voor eventueel ongemak door kleine onnauwkeurigheden, die in deze handleiding kunnen voorkomen omdat wij onze producten voortdurend ontwikkelen en verbeteren.

Darty Plc © UK: EC1N 6TE 21 / 11/ 2013

Declaration of Conformity

The following product has been deemed to comply with the requirements of the listed European Directives:-

R&TTE Directive (1999 / 5 / EC)

Electromagnetic Compatibility Directive (2004/108/EC)

Low Voltage Directive (2006/95/EC)

RoHS2 (2011/65/EU)

Product Description: 300 Mbps wireless repeater

Brand: I.T.Works

Model number: REPW300

The above listed products conform to the following EU Standards:

EN 62311: 2008

EN 301 489-17 V2.2.1

EN 300 328 V1.7.1

EN 301 489-1 V1.9.2

EN60950-1:2006 + A11:2009 + A1:2010+A12:2011

The person responsible for this declaration is:

Name: François Lemauf

Position: General Manager of Direct Sourcing

Signature:

Date: 6th January, 2014

