

Hashi User Manual
FCC ID:MG3-7010

Ver1.0

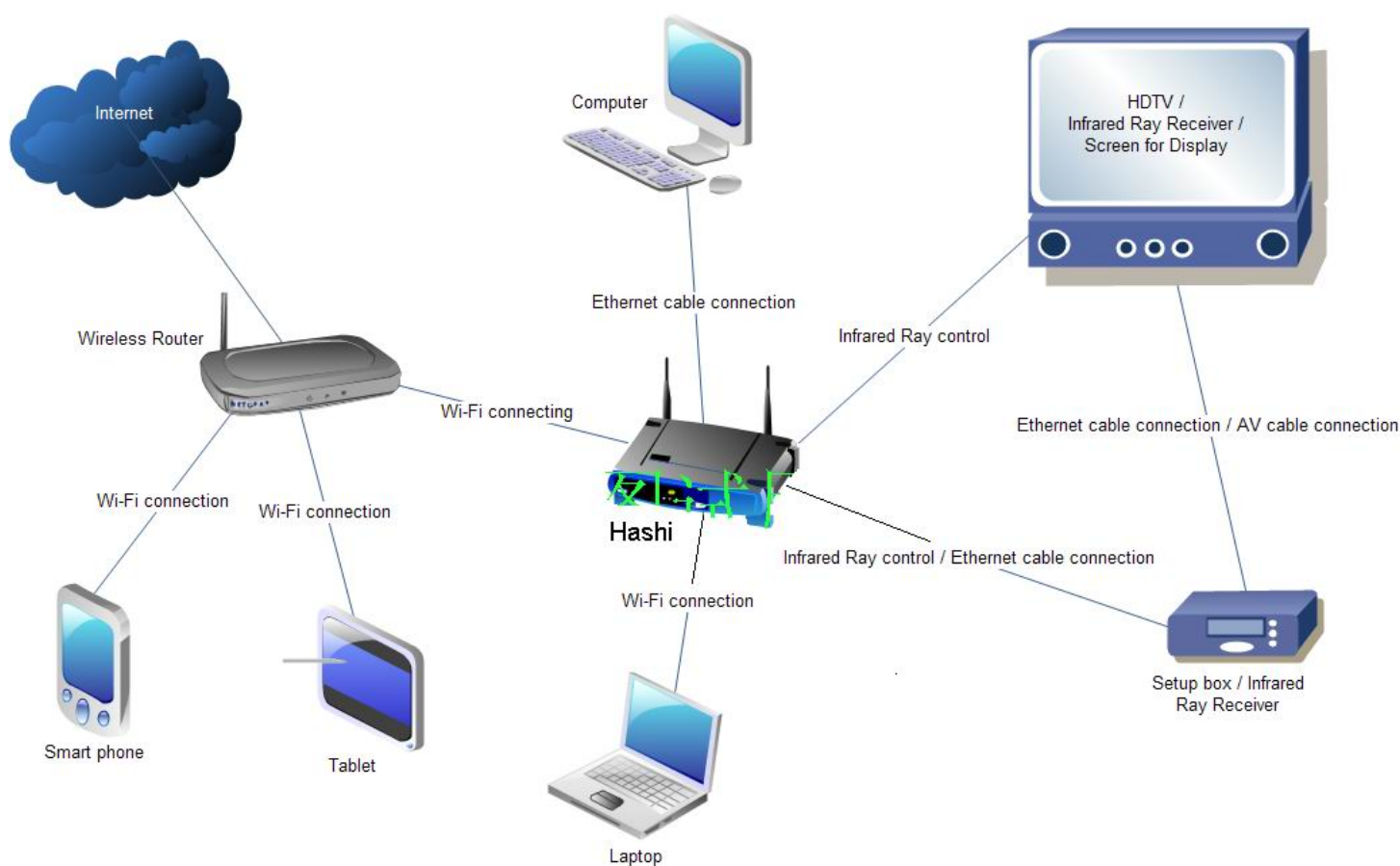
Content

1 Summary	2
2 Key feature	2
3 Using the Configuration Menu	3
3.1 Preparation	3
3.2 Setup Wizard.....	6
3.3 Wireless.....	9
3.4 LAN	15
3.5 QOS.....	16
3.6 Security	16
3.7 Service.....	19
3.8 Management.....	22
3.9 Status.....	25
4 Wireless Basics	27
5 Wireless Modes	28

1 Summary

Hashi wireless bridge collecting with wire, wireless network, specifically for satisfied office and family getting on the Internet, high-speed data tone video transmission need. The Hashi supports Infrared Ray remote control; The Hashi provides 64/128-bit WEP encryption, WPA/WPA2, WPA-PSK/WPA2-PSK data security and AES encryption; The Hashi supports QOS; The Hashi provides the reset button and the Wi-Fi protected setup (WPS) function; The Hashi supports the Bridge pattern the prolong network coverage range.

In general, the best location to place the Hashi is at the center of your wireless coverage area, within all wireless stations. Ensure all stations are within the service range of the Hashi.



2 Key feature

- Comply with IEEE802.11n Draft 2.0, and IEEE 802.11b/g/n
- Supports Infrared Ray remote control
- Supports working mode: Infrastructure mode, Ad-Hoc mode and WDS mode
- Supports Virtual Server, DMZ host, Dynamic DNS, NTP and QOS
- Supports Wi-Fi Protected Setup (WPS) with reset button

- Supports 64/128-bit WEP encryption, WPA/WPA2, WPA-PSK/WPA2-PSK data security
- Supports MAC/IP filtering and URL filtering
- Supports DHCP server
- Supports Web user interface
- Supports System status and security log
- Supports Firmware upgradeable

3 Using the Configuration Menu

Please conclude the steps of installing Hashi as below:

- A. Power on Hashi
- B. Use an Ethernet cable to connect Hashi to your PC with windows OS.
- C. Configure the IP address of your PC so that your PC can be connected with Hashi successfully.
- D. Works on the screen of your PC to configure Hashi and connect your Hashi to the current home
- E. WIFI wireless broadband router.
- F. Use an Ethernet cable to connect one of the Lan ports of Hashi to the Ethernet Port of your Setup box.
- G. Connect your tablet/Smartphone to the same Home WIFI wireless broadband router as Hashi
- H. Install Nevosmart on your tablet/Smartphone

3.1 Preparation

First of all, please connect the cables and power adapters as below before configuring Hashi software interface.

- Step 1

Use the attached power adapter to connect with the power interface of Hashi, plug the other end of the power adapter to the power socket.

- Step 2

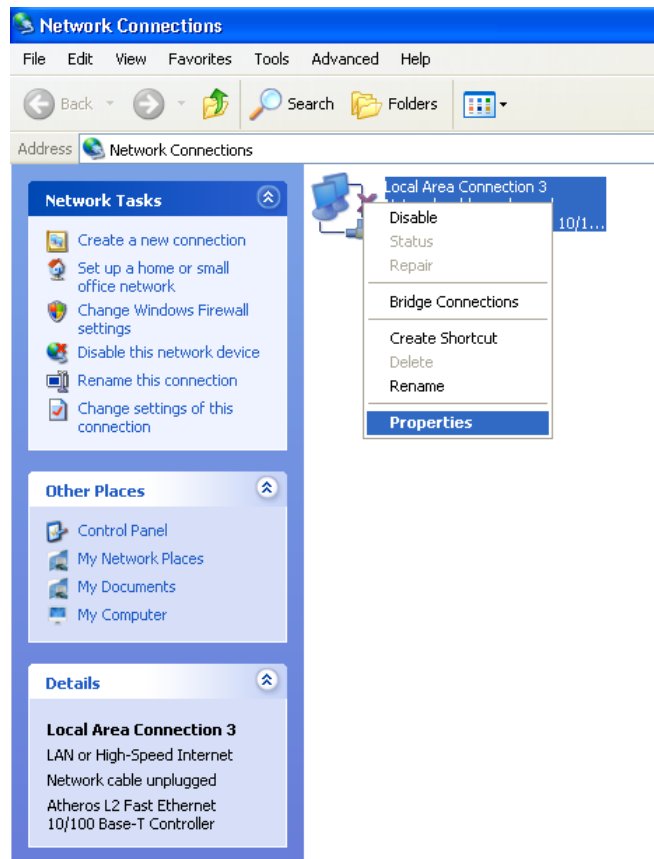
Use an Ethernet cable to connect the one of the LAN ports (Ethernet Ports) of Hashi to the Ethernet port of your PC with Windows OS.

- Step 3

Configure IP addresses for your PC as below: Please click **Start > Settings > Control Panel > Network Connections**. Or if you are in Start menu view, **click Start > Control Panel > Network Connections**.

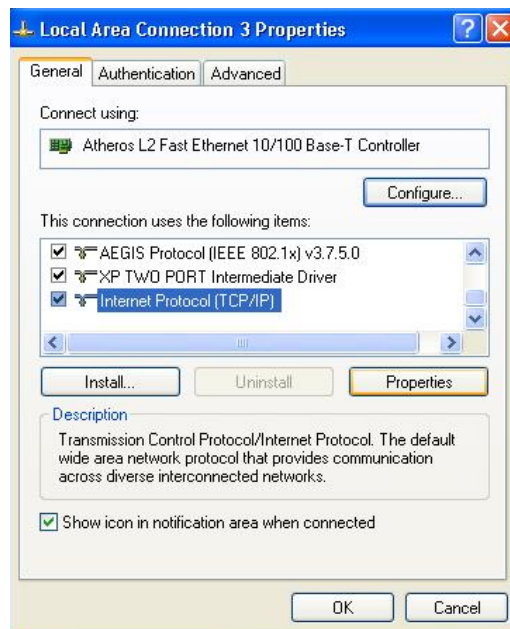
- Step 4

Double click **Local Area Connection**.



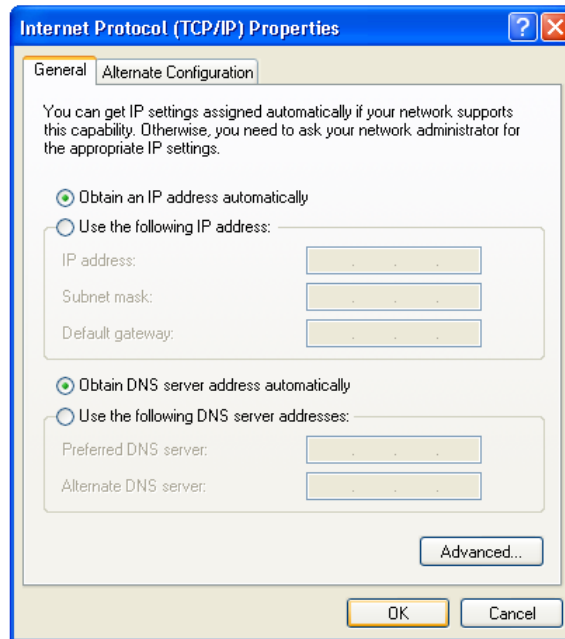
➤ Step 5

Choose **Internet Protocol (TCP/IP)** and click **Properties**.



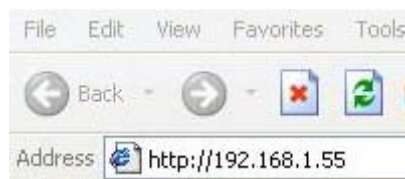
➤ Step 6

Please choose **“Obtain an IP address automatically”** to specify IP addresses automatically. Please click the **OK** button after your configuration.



➤ Step 7

Please access the configuration menu by opening the Internet Explorer and type <http://192.168.1.55> in the Address band. The Hashi's default IP Address is shown below:



➤ Step 8

Please enter the User name and Password. The factory default User name and Password are “**admin**”.



➤ Step 9

Click on a menu item, you can configure it. The menu contains the following sub-menu: Wizard, Wireless, LAN, QOS, Security, Service, Management, Status.

[Home](#) **Status >> Current Status**

This page shows the current status and some basic settings of the device.

System Status	
Uptime	0 day 0 h 8 m 1 s
Firmware Version	v1.2f0.8-20120911
Kernel version	2.6.30.9
Configuration file version	0
Build Time	Fri Jun 29 17:49:48 CST 2012

Wireless Status	
Mode	Infrastructure Client
Band	2.4 GHz (B+G+N)
SSID	Router
Channel Number	4
Encryption	WPA
BSSID	00:27:19:9f:24:c4
State	Connected

LAN Status	
IP Address	192.168.1.100

3.2 Setup Wizard

The wizard setting will guide you to configure the Hashi. Please follow the wizard setting step by step.

➤ Step 1

Please begin by clicking on **Next**.

[Home](#) **Wizard >> Wizard Settings**

Wizard Setting

The setup wizard will guide you to configure access point for first time. Please follow the setup wizard step by step. Welcome to Setup Wizard. The Wizard will guide you the through following steps. Begin by clicking on Next.

Exit wizard Next

➤ Step 2

Please click **Scan**, and select the wireless router which you want to connect.

Wizard >> Wizard Settings

Wizard Setting						
SSID	BSSID	Channel	Type	Encrypt	Signal	Select
Router	00:e0:4c:31:96:c1	2 (B+G+N)	AP	WPA2-PSK	56	<input type="radio"/>
QHCMCC	00:0a:eb:11:f3:a8	9 (B+G+N)	AP	WPA2-PSK	32	<input type="radio"/>
T01	00:0a:eb:37:32:03	1 (B+G+N)	AP	no	26	<input type="radio"/>
test555	08:10:74:be:08:ea	1 (B+G+N)	AP	WPA2-PSK	12	<input type="radio"/>
DSLWR_356456	00:0a:eb:35:64:56	1 (B+G+N)	AP	WPA2-PSK	10	<input type="radio"/>
BR895WL	00:0c:43:30:52:88	6 (B+G+N)	AP	no	6	<input type="radio"/>
KN-004	00:0a:eb:09:08:bd	9 (B+G+N)	AP	WPA-PSK	2	<input type="radio"/>
Kingnet1111	00:0a:eb:35:6e:03	11 (B+G+N)	AP	WPA-PSK	2	<input type="radio"/>

➤ Step 3

Please enter the password of your wireless router, and click **Next**.

Wizard >> Wizard Settings

Wizard Setting	
SSID:	<input type="text" value="Router"/>
Authentication:	<input type="radio"/> Enterprise (RADIUS) <input checked="" type="radio"/> Personal (Pre-Shared Key)
WPA2 Cipher Suite:	<input type="checkbox"/> TKIP <input checked="" type="checkbox"/> AES
Pre-Shared Key Format:	<input type="text" value="Passphrase"/>
WPA Key:	<input type="text" value="••••••••"/>

➤ Step 4

Please select **Client** as your DHCP mode, and click **Finished**.

Wizard >> Wizard Settings

Wizard Setting

This IP is the equipment's management IP. Please keep this IP in mind. You need this IP to enter the web to scan the SSID. Please avoid IP that your accessed SSID's network segment already in using. For example: your accessed SSID's network segment is 192.168.1.x, you can use a 192.168.1.188 (not in using IP) as the management IP.

DHCP:

IP Address:

Subnet mask:

➤ Step 5

When it show “Connect successfully!”, click “Reboot Now”

Wizard >> Wizard Settings

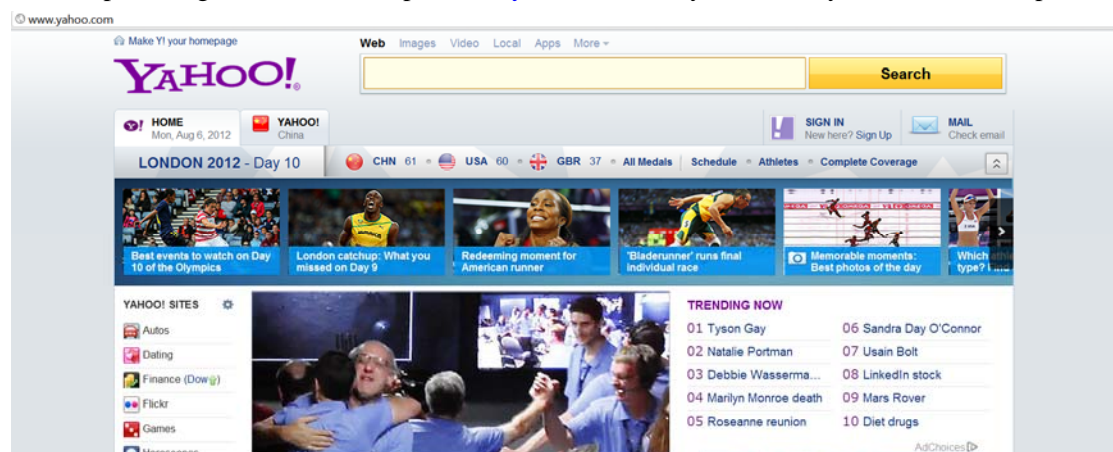
Wizard Setting

Connect successfully!

Now you have connected Hashi to your Wireless broadband router, your PC can visit wireless WIFI broadband network via Hashi now.

➤ Step 6

Please open IE again to test this, input www.yahoo.com and you can see yahoo website is opened:

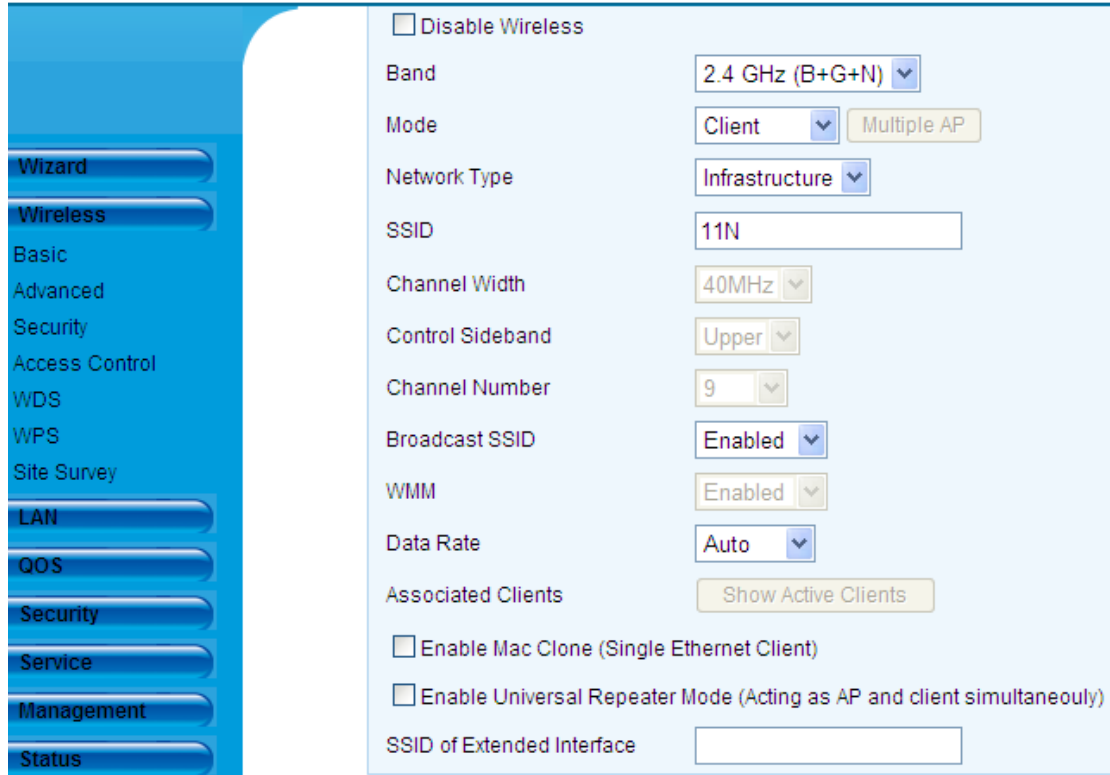


Now, Hashi is correctly configured and you can unplug the Ethernet cable between Hashi and your PC. You can also power off Hashi now. All the configuration you have done just now has already be stored inside Hashi.

3.3 Wireless

➤ Basic

This page provides the basis wireless settings, which keep the default configuration when you access it the first time.



1. Band:

- 2.4 GHz (B) Select it if your wireless router is configured in 802.11b.
- 2.4 GHz (G) Select it if your wireless router is configured in 802.11g.
- 2.4 GHz (N) Select it if your wireless router is configured in 802.11n.
- 2.4 GHz (B + G) Select it if your wireless router is configured in mix mode of 802.11b and 802.11g.
- 2.4 GHz (G + N) Select it if your wireless router is configured in mix mode of 802.11g and 802.11n.
- 2.4 GHz (B + G + N) Select it if your wireless router is configured in mix mode of 802.11b, 802.11g and 802.11n.

2. Mode:

- AP you can use Hashi as access point in this mode.
- Client you can configure Hashi connect to the wireless router, it is default mode.
- WDS you can configure Hashi connect to the wireless router in WDS mode, the wireless router should configure WDS mode too.
- AP+WDS you can configure wireless router connect to Hashi in AP+WDS mode.

3. Network Type:

- Infrastructure All wireless clients will connect to an access point or wireless router.
- Ad-hoc Directly connecting to another computer, for peer-to-peer communication, using wireless network adapters on each computer.

4. SSID:

Service Set Identifier (SSID) is the name of your Hashi, the SSID is case-sensitive.

5. Channel Width:

40MHz This is default setting, Select it if you are using both 802.11n and non-802.11n wireless devices.

20MHz Select it if you are not using any 802.11n wireless clients.

6. Control Sideband:

Upper Select it so you can change the channel number from 5 to 11.

Lower Select it so you can change the channel number from 1 to 9.

7. Channel Number:

The channel can be changed to fit the channel setting for an existing wireless network or to customize the wireless network.

8. Broadcast SSID:

Enabled Choose Enabled to broadcast the SSID across the network.

Disabled Choose Disabled if you do not wish to broadcast the SSID over the network.

9. WMM:

The default setting of Wi-Fi MultiMedia is enabled

10. Data Rate:

Select the data rate, the default setting is Auto.

11. Associated Clients:

Show Active Clients It shows the information for each associated wireless client.

➤ Advanced

These settings are only for more technically advanced users who have a sufficient knowledge about wireless LAN. These settings should not be changed unless you know what effect the changes will have on your Access Point.

Advanced Settings	
Fragment Threshold	<input type="text" value="2346"/> (256-2346)
RTS Threshold	<input type="text" value="2347"/> (0-2347)
Beacon Interval	<input type="text" value="100"/> (20-1024 ms)
Preamble Type	<input checked="" type="radio"/> Long Preamble <input type="radio"/> Short Preamble
IAPP	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Protection	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Aggregation	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Short GI	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
WLAN Partition	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
STBC	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
20/40MHz Coexist	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
RF Output Power	<input checked="" type="radio"/> 100% <input type="radio"/> 70% <input type="radio"/> 50% <input type="radio"/> 35% <input type="radio"/> 15%

1. Fragment Threshold:

It is specified in bytes, determines whether packets will be fragmented. Packets exceeding the 2346 byte setting will be fragmented before transmission.

2. RTS Threshold:

This value should remain at its default setting of 2347. If inconsistent data flow is a problem, only a minor modification should be made.

3. Beacon Interval:

Beacons are packets sent by an Access Point to synchronize a wireless network. Specify a value. 100 is default setting and is recommended.

4. Preamble Type:

The long preamble can reduce the guard interval packet therefore increasing the data capacity. However, it's less reliable and may create higher data loss.

5. IAPP:

The default setting of Inter-Access Point Protocol is enabled.

6. Protection:

The default setting of BG protection is disabled.

7. Aggregation:

If it is enabled, the packets will be aggregated before they are forwarded. The default setting of Aggregation is enabled.

8. Short GI:

Enabled it can reduce the guard interval time therefore increasing the data capacity. However, it's less reliable and may create higher data loss.

9. WLAN Partition:

The default setting of WLAN partition is disabled.

10. STBC:

The default setting of Space Time Block Code is disabled.

11. 20/40MHz Coexist:

The default setting of 20/40MHz Coexist is disabled.

12. RF Output Power:

The default setting of RF Output Power is 100%.

➤ Security

It is recommended to enable encryption on Hashi. Please establish connectivity before enabling encryption.

🏠 Wireless >> Security Settings

This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.

Security Settings

Select SSID

Encryption Settings

Encryption

- Disable
- WEP**
- WPA
- WPA2

1. Select SSID: Select the SSID which you want to set as Encryption mode.
2. Encryption: Set the encryption mode at the SSID which you select.

➤ Access Control

🏠 Wireless >> Access Control Settings

If you choose 'Allowed Listed', only those clients whose wireless MAC addresses are in the access control list will be able to connect to your Access Point. When 'Deny Listed' is selected, these wireless clients on the list will not be able to connect the Access Point.

Access Control Settings

Wireless Access Control Mode

MAC Address

Comment

- Disable
- Allow Listed**
- Deny Listed

Current Access Control List

MAC Address	Comment	Select
-------------	---------	--------

1. Wireless Access Control Mode:
You can choose one of the strategies.
2. MAC Address:
Type the MAC Address. For example: 00e1a2b3c456

➤ WDS

WDS is commonly used in areas requiring multiple APs, where wiring is not possible or costly and for providing back-up paths between APs. You must set Hashi and AP in the same channel,

and set MAC Address of other AP which you want to communicate with in the table.

Wireless >> WDS Settings

Wireless Distribution System uses wireless media to communicate with other APs, like the Ethernet does. To do this, you must set these APs in the same channel and set MAC address of other APs which you want to communicate with in the table and then enable the WDS.

WDS Settings	
<input checked="" type="checkbox"/> Enable WDS	
MAC Address	<input type="text"/>
Data Rate	Auto <input type="button" value="v"/>
Comment	<input type="text"/>
<input type="button" value="Apply"/> <input type="button" value="Reset"/> <input type="button" value="Show Statistics"/>	

Current WDS AP List			
MAC Address	Tx Rate (Mbps)	Comment	Select

1. **MAC Address:**
Specify the MAC address of the destination access point.
 2. **Data Rate:**
The default setting is Auto.
- **WPS**
The WPS settings are valid when Hashi works in AP mode.

Wireless >> WPS (Wi-Fi Protected) Settings

This page allows you to change the setting for WPS (Wi-Fi Protected Setup). Using this feature could let your wireless client automatically synchronize its setting and connect to the Access Point in a minute without any hassle.

WPS (Wi-Fi Protected) Settings

Disable WPS

WPS Status Configured UnConfigured

Self-PIN Number 99956042

Push Button Configuration (PBC)

Current Key Info

Authentication	Encryption	Key
Open	None	N/A

Client PIN

Client PIN Number

1. WPS(Wi-Fi Protected) Settings:

There are two ways to start PBC(Push Button Configuration) mode: you can click “Start PBC” button on the configuration menu or press “WPS” button on Hashi. After started PBC mode, press PCB button on Wireless Network card.

2. Client PIN:

You can type the PIN Number of Wireless Network card at Client PIN Number blank, and click “Start PIN” button. After started PIN mode, configure PIN mode on Wireless Network card.

➤ Site Survey

🏠 Wireless >> Wireless Site Survey

This page provides tool to scan the wireless network. If any Access Point or IBSS is found, you could choose to connect it manually when client mode is enabled.

Site Survey						
SSID	BSSID	Channel	Type	Encrypt	Signal	Select
QHCMCC	00:0a:eb:11:f3:a8	9 (B+G+N)	AP	WPA2-PSK	34	<input type="radio"/>
BR895WL	00:0c:43:30:52:53	6 (B+G+N)	AP	no	18	<input type="radio"/>
Topway_147151	00:0a:eb:40:0b:cd	1 (B+G)	AP	WPA-PSK	10	<input type="radio"/>
DSLWR_356456	00:0a:eb:35:64:56	1 (B+G+N)	AP	WPA2-PSK	10	<input type="radio"/>
coship_444444	00:0a:eb:40:0c:be	1 (B+G+N)	AP	WPA-PSK	6	<input type="radio"/>
BR918WL	00:0c:43:30:52:88	6 (B+G+N)	AP	no	0	<input type="radio"/>

This page shows the equipment information of AP which Hashi can connected to, it displays BSSID, Channel etc, you can select the wireless router which you want to connect.

3.4 LAN

🏠 LAN >> LAN Settings

This page is used to configure the parameters for local area network which connects to the LAN port of your Access Point. Here you may change the setting for IP address, subnet mask, DHCP, etc..

LAN Settings	
IP Address	<input type="text" value="192.168.1.55"/>
Subnet Mask	<input type="text" value="255.255.255.0"/>
Default Gateway	<input type="text" value="0.0.0.0"/>
DHCP	<input type="button" value="Disabled"/> ▾
DHCP Client Range	<input type="text" value="192.168.1.100"/> - <input type="text" value="192.168.1.200"/>
Domain Name	<input type="text" value="net11n"/>
802.1d Spanning Tree	<input type="button" value="Disabled"/> ▾
Clone MAC Address	<input type="text" value="000000000000"/>

1. IP Address: The IP address of LAN.
2. Subnet Mask: The subnet mask of LAN.

3. Default Gateway: You can enter the Gateway IP address here.
4. DHCP:

Enabled – select it if you want to use Hashi as a DHCP server, and enter the starting IP address and ending IP address for the DHCP server's IP assignment.

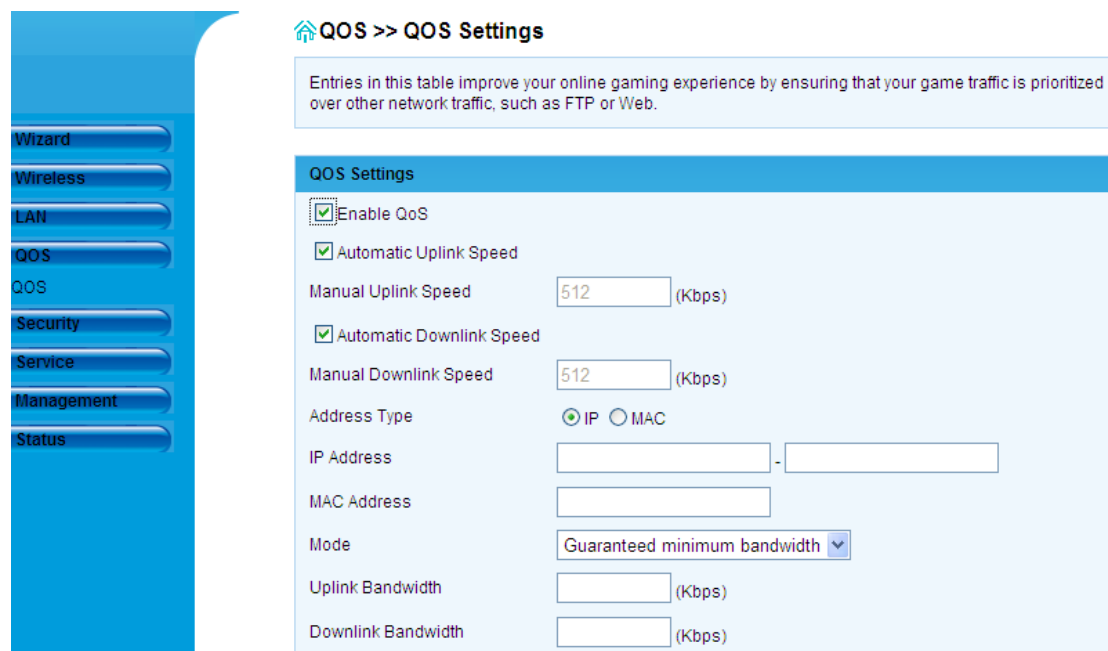
5. DHCP Client Range: Enter the starting IP address and ending IP address here.
6. Domain Name: Enter the domain name here.
7. 802.1d Spanning Tree:

The 802.1d Spanning Tree is designed at a time when the recovery of connectivity after an outage within a minute or so is considered adequate performance.

8. Clone MAC Address:

Some service providers require you to register a MAC address in order to access the Internet. The Clone MAC Address screen lets you use the MAC address of a device that has already been registered with your service provider, by copying that MAC address to the device.

3.5 QOS



QOS >> QOS Settings

Entries in this table improve your online gaming experience by ensuring that your game traffic is prioritized over other network traffic, such as FTP or Web.

QOS Settings

Enable QoS

Automatic Uplink Speed

Manual Uplink Speed (Kbps)

Automatic Downlink Speed

Manual Downlink Speed (Kbps)

Address Type IP MAC

IP Address -

MAC Address

Mode ▼

Uplink Bandwidth (Kbps)

Downlink Bandwidth (Kbps)

The QOS screen allows you to specify priorities for different types of traffic. Lower priority traffic will be slowed down to allow greater throughput or less delay for high priority traffic.

3.6 Security

- Port Filtering

Wizard

Wireless

LAN

QOS

Security

Port Filtering

MAC Filtering

IP Filtering

URL Filtering

Firewall

Service

Management

Status

Security >> Port Filtering Settings

Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.

Port Filtering Settings

Enable Port Filtering

Port Range -

Protocol TCP+UDP

Comment

Current Port Filter List

Port Range	Protocol	Comment	Select
<input type="button" value="Delete Selected"/> <input type="button" value="Delete All"/>			

1. Enable Port Filtering: Select it to apply the port filtering policy.
2. Port Range:

Enter in the port range of the TCP/UDP ports that you want the policy to apply to. If it is only a single port that you want the policy applied to, then enter the same port number in the Port Range blank.
3. Protocol: Select the protocol type to allow or deny certain ports.

➤ MAC Filtering

Security >> MAC Filtering Settings

Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.

MAC Filtering Settings

Enable MAC Filtering

MAC Address

Comment

Current MAC Filter List

MAC Address	Comment	Select
<input type="button" value="Delete Selected"/> <input type="button" value="Delete All"/>		

1. Enable MAC Filtering: Select it to apply the MAC filtering policy.
2. MAC Address: Enter the MAC address which you want to set. For example: 00e2a3b34c156

➤ IP Filtering

[Security](#) >> IP Filtering Settings

Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.

IP Filtering Settings

Enable IP Filtering

IP Address

Protocol TCP+UDP ▼
TCP+UDP
TCP
UDP

Comment

Current IP Filter List

IP Address	Protocol	Comment	Select

1. Enable IP Filtering: Select it to apply the IP filtering policy.
2. IP Address: Enter the IP address which you want to set.
3. Protocol: Select the protocol type to allow or deny certain types of IP address.

➤ URL Filtering

[Security](#) >> URL Filtering Settings

URL filter is used to deny LAN users from accessing the internet. Block those URLs which contain keywords listed below.

URL Filtering Settings

Enable URL Filtering

URL Address


Current URL Filter List

URL Address	Select

1. Enable URL Filtering: Select it to apply the URL filtering policy.

2. URL Address: Enter the URI address which you want to set. For example: www.sina.com

➤ Firewall

 **Security >> Firewall Settings**

A denial-of-service (DoS) attack is characterized by an explicit attempt by hackers to prevent legitimate users of a service from using that service.

Firewall (DoS) Settings

<input checked="" type="checkbox"/> Enable DoS Prevention	
<input type="checkbox"/> Whole System Flood(SYN)	<input type="text" value="0"/> Packets/second
<input type="checkbox"/> Whole System Flood(FIN)	<input type="text" value="0"/> Packets/second
<input type="checkbox"/> Whole System Flood(UDP)	<input type="text" value="0"/> Packets/second
<input type="checkbox"/> Whole System Flood(ICMP)	<input type="text" value="0"/> Whole System Flood(ICMP)
<input type="checkbox"/> Per-Source IP Flood(SYN)	<input type="text" value="0"/> Packets/second
<input type="checkbox"/> Per-Source IP Flood(FIN)	<input type="text" value="0"/> Packets/second
<input type="checkbox"/> Per-Source IP Flood(UDP)	<input type="text" value="0"/> Packets/second
<input type="checkbox"/> Per-Source IP Flood(ICMP)	<input type="text" value="0"/> Packets/second
<input type="checkbox"/> TCP/UDP PortScan	<input type="text" value="Low"/> Sensitivity
<input type="checkbox"/> ICMP Smurf	

Enable DoS Prevention: Select it to apply the DoS(denial of service) prevention.

3.7 Service

➤ DMZ

The DMZ (Demilitarized Zone) screen allows you to expose one network user to the Internet for use of a special-purpose service such as Internet gaming or video conferencing. DMZ hosting forwards all the ports at the same time to one computer. You should assign IP address to the destination computer before you use this feature.

Service >> DMZ Settings

A Demilitarized Zone is used to provide Internet services without sacrificing unauthorized access to its local private network. Typically, the DMZ host contains devices accessible to Internet traffic, such as Web (HTTP) servers, FTP servers, SMTP (e-mail) servers and DNS servers.

DMZ Settings	
<input checked="" type="checkbox"/> Enable DMZ	
DMZ IP Address	<input type="text"/>

1. Enable DMZ:

Select it to enable the DMZ. If an application has trouble working from behind the router, you can expose one computer to the Internet and run the application on that computer.

Note: Placing a computer in the DMZ may expose that computer to a variety of security risks. The option is only recommended as a last resort.

2. DMZ IP Address:

Specify the IP address of the computer on the LAN that you want to have unrestricted Internet communication.

➤ Virtual Server

The Hashi can be configured as a virtual server when it work in Gateway mode, so that remote users accessing Web or FTP services via the public IP address can be automatically redirected to local servers in the LAN(Local Area Network).

Service >> Virtual Server Settings

Entries in this table allow you to automatically redirect common network services to a specific machine behind the NAT firewall. These settings are only necessary if you wish to host some sort of server like a web server or mail server on the private local network behind your Gateway's NAT firewall.

Virtual Server Settings	
<input checked="" type="checkbox"/> Enable Virtual Server	
IP Address	<input type="text"/>
Protocol	TCP+UDP ▾
Port Range	<input type="text"/> - <input type="text"/>
Comment	<input type="text"/>

Current Virtual Server List

IP Address	Protocol	Port Range	Comment	Select
------------	----------	------------	---------	--------

1. Enable Virtual Server: Select it to apply the virtual Server.

2. IP Address:

Enter the IP address of the computer on your local network that you want to allow the incoming service to.

3. Protocol: Select TCP, UDP or TCP+UDP, if you are not sure, select TCP+UDP.


4. Port Range:

Enter the port range of the computer on your local network that you want to allow the incoming service to.

5. Comment: Enter a name for your virtual server entry.

➤ DDNS

The DDNS (Dynamic Domain Name System) screen allows you to assign a fixed host and domain name to a network computer that has been assigned a dynamic Internet IP address. This is useful when you are hosting your own website, FTP server, or other server behind the device.

 **Service >> DDNS Settings**

Dynamic DNS is a service, that provides you with a valid, unchanging, internet domain name (an URL) to go with that (possibly everchanging) IP-address.

DDNS Settings

DDNS Status

Enable DDNS

Service Provider 3322 ▼

Domain Name host.dyndns.org

User Name

Password

Apply
Reset

1. Enable DDNS:

Select it to enable DDNS. When an IP address is automatically assigned by a DHCP server, DDNS automatically updates the DNS server.

2. Service Provider: Choose your DDNS provider from the drop down menu.

3. Domain Name: Enter the Host name that you registered with your DDNS service provider.

4. User Name: Enter the User name for your DDNS account.

5. Password: Enter the Password for your DDNS account.

➤ NTP

The NTP setting allows you to configure, update and maintain the correct time on the internal system clock. From this section you can set the time zone that you are in and set the Time Server. Daylight Saving can also be configured to automatically adjust the time when needed.

Service >> NTP Settings

You can maintain the system time by synchronizing with a public time server over the Internet.

NTP Settings	
Current Time	2012 YY 9 MM 11 DD 17 H 29 M 10 S
Time Zone	(GMT-05:00)Eastern Time (US & Canada) ▼
<input type="checkbox"/> Enable NTP client update	
<input type="checkbox"/> Automatically Adjust Daylight Saving	
NTP Server	<input checked="" type="radio"/> 192.5.41.41 - North America ▼ <input type="radio"/> (Manual)
<input type="button" value="Apply"/> <input type="button" value="Reset"/>	

1. Current Time: You can change the current time here.
2. Time Zone: Select the Time Zone from the drop down menu.
3. Enable NTP client update: Select it to enable updating NTP client.
4. NTP Server:

NTP is short for Network Time Protocol. NTP synchronizes computer clock times in a network of computers. You can select it or enter a NTP server manually. This will only connect to a server on the Internet.

3.8 Management

- Operation Mode

Management >> Operation Mode

You can setup different modes to LAN and WLAN interface for NAT and bridging function.

Operation Mode	
<input type="radio"/> Gateway	In this mode, the device is supposed to connect to internet via ADSL/Cable Modem. The NAT is enabled and PCs in LAN ports share the same IP to ISP through WAN port. The connection type can be setup in WAN page by using PPPOE, DHCP client, PPTP client, L2TP client or static IP.
<input checked="" type="radio"/> Bridge	In this mode, all ethernet ports and wireless interface are bridged together and NAT function is disabled. All the WAN related function and firewall are not supported.
<input type="radio"/> Wireless ISP	In this mode, all ethernet ports are bridged together and the wireless client will connect to ISP access point. The NAT is enabled and PCs in ethernet ports share the same IP to ISP through wireless LAN. You must set the wireless to client mode first and connect to the ISP AP in Site-Survey page. The connection type can be setup in WAN page by using PPPOE, DHCP client, PPTP client, L2TP client or static IP.

1. Gateway: If you select Gateway, The NAT is enabled.
2. Bridge: If you select Bridge, all LAN ports and wireless interfaces are bridged together, firewall is not supported.
3. Wireless ISP: In this mode, all LAN ports are bridged together and the wireless client will connect to ISP access point. The NAT is enabled. You can set the wireless to client mode and connect to the ISP AP in Site-survey page.

➤ System Settings

1. Save Configuration:

The current system settings can be saved as a file onto the local hard drive only clicking Save button. The saved file or any other saved setting file created by the Hashi can be uploaded into the unit.

2. Upload Configuration:

The saved file or any other saved setting file created by the Hashi can be uploaded into the unit. To reload a system settings file, click on browse to search the local hard drive for the file to be used, then click Upload button when finished.

3. Factory Default:

The device can also be reset back to factory default setting by clicking Default button. Use the restore feature only if necessary. This will erase previously saved setting for the unit. Save your system settings before doing a factory restore.

Management >> System Settings

This page allows you save current settings to a file or reload the settings from the file which was saved previously. Besides, you could reset the current configuration to factory default.

Save Configuration

Save Settings to File

Upload Configuration

Load Settings from File

Factory Default

Reset Settings to Default

➤ Reboot

Click **Reboot** button to restart the Hashi.

🏠 Management >> Reboot System

This page allows you could reboot the system.It takes about 1 minute to reboot,please wait patiently.

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

➤ Upgrade Firmware

You can upgrade the firmware or bootloader of the device using this tool. Make sure that the firmware you want to use is saved on the local hard drive of the computer. Click on **Browse** to search the local hard drive for the firmware to be used for the update. Upgrading the firmware or bootloader will not change any of your system settings but it is recommended that you save your system settings before doing a firmware upgrade.

🏠 Management >> Upgrade Firmware

This page allows you upgrade the Access Point firmware to new version. Please note, do not power off the device during the upload because it may crash the system.

Upgrade Firmware	
Current Firmware Version	v1.2f0.8-20120911
Select File	<input type="text"/> <input type="button" value="浏览..."/>
<input type="button" value="Upload"/> <input type="button" value="Reset"/>	

➤ Password

🏠 Management >> Password Settings

This page is used to set the account to access the web server of Access Point. Empty user name and password will disable the protection.

Password Settings	
User Name	<input type="text" value="admin"/>
New Password	<input type="password" value="•••••"/>
Confirmed Password	<input type="password" value="•••••"/>
<input type="button" value="Apply"/> <input type="button" value="Reset"/>	

The Password screen allows you to change the factory default user name and password of Hashi. It is strongly recommended that you change the factory default username and password of the Hashi. All users who try to access the Hashi's web-based utility will be prompted for the Hashi's

user name and password.

Note: The new user name and password must not exceed 14 characters in length and must not include any spaces. Enter the new password twice to confirm it. And click **Apply** button when finished.

➤ System Log

The Hashi automatically logs (records) events of possible interest in its memory. If there isn't enough space in the memory for all events, logs of older events are deleted but logs of the latest events are retained. The System log allows you to view the Hashi logs. You can also click **Clear** button to the current log.

Management >> System Log

This page can be used to set remote log server and show the system log.

System Log	
Enable Log	<input checked="" type="checkbox"/>
System all	<input type="checkbox"/>
Wireless	<input type="checkbox"/>
DoS	<input type="checkbox"/>
Enable Remote Log	<input type="checkbox"/> <input type="text"/>
Log Server IP Address	<input type="text"/>

3.9 Status

➤ Status

This Status page displays the Hashi's current status and configuration. All information is read-only.

1. System Status:

It displays the current system information for the Uptime, Firmware Version, Kernel version, Configuration file version, Build Time.

2. Wireless Status:

It displays the wireless information for the Mode, Band, SSID, Channel Number, Encryption, BSSID, State.

3. LAN Status:

It displays the Local Network information for the Local IP Address, Local Subnet Mask, Default Gateway, DHCP server, MAC Address.

Status >> Current Status

This page shows the current status and some basic settings of the device.

System Status

Uptime	0 day 0 h 5 m 27 s
Firmware Version	v1.2f0.8-20120911
Kernel version	2.6.30.9
Configuration file version	0
Build Time	Fri Jun 29 17:49:48 CST 2012

Wireless Status

Mode	Infrastructure Client
Band	2.4 GHz (B+G+N)
SSID	11N
Channel Number	1
Encryption	Disabled
BSSID	00:00:00:00:00:00
State	Scanning

LAN Status

IP Address	192.168.1.55
Subnet Mask	255.255.255.0
Default Gateway	0.0.0.0
DHCP Server	Disabled
MAC Address	00:00:01:02:03:01

WAN Status

Attain IP Protocol	Getting IP from DHCP server...
IP Address	0.0.0.0
Subnet Mask	0.0.0.0
Default Gateway	0.0.0.0
MAC Address	00:e0:4c:81:96:c9

➤ Statistics

It displays the current Wireless LAN interface and LAN port packet message for the Wireless LAN Sent Packets, Wireless LAN Received Packets, Ethernet LAN Sent Packets, Ethernet LAN received Packets.

[Home](#) **Status >> Statistics**

This page shows the packet counters for transmission and reception regarding to wireless and Ethernet networks.

Wireless LAN	
Sent Packets	6772
Received Packets	7307
Ethernet LAN	
Sent Packets	750
Received Packets	660

4 Wireless Basics

The Hashi is based on industry standards to provide easy-to-use and compatible high-speed wireless connectivity within your home or public access wireless networks. Strictly adhering to the IEEE standard, the wireless family of products will allow you to securely access the data you want, remote control the Infrared Ray devices, when and where you want it. You will be able to enjoy the freedom that Hashi delivers.

A Wireless Local Area Network (WLAN) is a cellular computer network that transmits and receives data with radio signals instead of wires. Wireless LANs are used increasingly in both home and office environments, and public areas such as airports, coffee shops and universities. Innovative ways to utilize WLAN technology are helping people to work and communicate more efficiently. Increased mobility and the absence of cabling and other fixed infrastructure have proven to be beneficial for many users.

Wireless users can use the same applications they use on a wired network. Wireless adapters and desktop systems support the same protocols as Ethernet adapter cards. Under many circumstances, it may be desirable for mobile network devices to link to a conventional Ethernet LAN in order to use setup box, TV/DVD, servers, printers or an Internet connection supplied through the wired LAN. A Hashi is a device used to provide this link.

➤ What is Wireless?

Wireless or Wi-Fi technology is another way of connecting your computer to the network without using wires. Wi-Fi uses radio frequency to connect wirelessly, so you have the freedom to connect computers anywhere in your home or office network.

➤ How does wireless work?

Wireless works similar to how cordless phone work, through radio signals to transmit data from point A to point B. But wireless technology has restrictions as to how you can access the network. You must be within the wireless network range area to be able to connect your computer. There are two different types of wireless networks Wireless Local Area Network (WLAN), and Wireless Personal Area Network (WPAN).

➤ Wireless Local Area Network

In a wireless local area network, a device called an Access Point (AP) connects computers to the network. The access point has a small antenna attached to it, which allows it to transmit data back and forth over radio signals. With an indoor access point, the signal can travel up to 300 feet. With an outdoor access point the signal can reach out up to 30 miles to serve places like manufacturing plants, college and high school campuses, airports, golf courses, and many other outdoor venues.

➤ Who uses wireless?

Wireless technology has become so popular in recent years that almost everyone is using it, whether it's for home, office, Hashi is a good solution for it.

➤ Where is Hashi used?

Home

- Gives everyone at home broadband access
- Remote control the Infrared Ray devices (TV/setup box/DVD) through your tablet, Smartphone
- Gets rid of the cables around the house
- Simple and easy to use

Small Office and Home Office

- Stay on top of everything at home as you would at office
- Remote control the Infrared Ray devices
- Share Internet connection and printer with multiple computers
- No need to dedicate office space

5 Wireless Modes

There are basically two modes of networking:

- **Infrastructure** — All wireless clients will connect to an access point or wireless router.
- **Ad-hoc** — Directly connecting to another computer, for peer-to-peer communication, using wireless network adapters on each computer.

An Infrastructure network contains an Access Point or wireless router. All the wireless devices or clients, will connect to the wireless router or access point.

An Ad-hoc network contains only clients, such as wireless adapters. All the adapters must be in Ad-hoc mode to communicate.

User Manual Statement:

IMPORTANT REGULATORY INFORMATION

This device complies with Part 15 of the FCC Rules: Operation is subject to the following two conditions:

1. This device may not cause harmful interference and
2. This device must accept any interference that is received, including any interference that may cause undesired operation.

NOTE: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help

WARNING:

Ad Hoc function is supported but not able to operate on non-US frequencies.---WIFI

Do not use the device with the environment which below minimum -10°C or maximum over50, the device may not work.

Changes or modifications to this unit not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

In order to comply with RF exposure requirements, a minimum distance of 20cm must be maintained between the antenna and all persons