



**TVWS Backpack Wi-Fi
Operation manual**

목차

1. System Introduction
 - 1.1 Service Configure
 - 1.2 Network Configure
 - 1.3 TVWS Backpack Wi-Fi
 - 1.4 Safety precaution
2. TVWS WEB UI
 - 2.1 PC Setting
 - 2.2 Device WEB UI
 - 2.3 Wi-Fi Setting
3. Maintenance
 - 3.1 Maintenance System
 - 3.2 Failure Check and Action
 - 3.3 How to Verify Equipment Operation

※ Free service users may not be provided with all services in the manual. In addition, the service can be changed without any special mention due to service improvement

FCC COMPLIANCE STATEMENT

CAUTION: Changes or modifications not expressly approved could void your authority to use this equipment

This device complies with Part 15 of the FCC Rules. Operation to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

FCC §15.105 Information to the user.

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.

FCC §15.706 Information to the user.

This equipment has been tested and found to comply with the rules for white space devices, pursuant to part 15 of the FCC rules. These rules are designed to provide reasonable protection against harmful interference. 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. 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:

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

FCC RF Radiation Exposure Statement

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment.

Caution: Exposure to Radio Frequency Radiation

To comply with FCC RF exposure compliance requirements, for fixed configurations, a separation distance of at least 30cm must be maintained between the antenna of this device and all persons. This device must not be co-located or operating in conjunction with any other antenna or transmitter.

1. System Introduction

1.1 Service Configure

The service composition using backpack Wi-Fi is shown below.



1) Advantages of TVWS Internet of Things

With the rapid activation of the Internet of Things recently, services that require high-speed data communication such as video, Wi-Fi, and IP camera services are rapidly increasing.

Although LTE, which is a wireless communication, is used in rural households, islands, livestock farms, and fish farms, which are difficult to establish wired communication, there is a burden of communication charges.

TVWS eliminates the burden of telecommunications charges in unlicensed bands and saves time and money over wired communication.

2) TVWS configuration and utilization

It consists of master equipment and slave equipment for TVWS communication.

Where the master equipment needs to be wired to the TCP/IP network, the slave equipment is installed in an area to supply Internet of Things services, and each device communicates with a wireless TVWS signal.

Using backpack Wi-Fi, you can provide public Wi-Fi services and live streaming services to the venue.

In addition, if your network collapses due to disasters such as earthquakes and fires, and power is difficult, you can use your battery to provide emergency Wi-Fi services.

Precaution

Do not use outdoor, In door use only

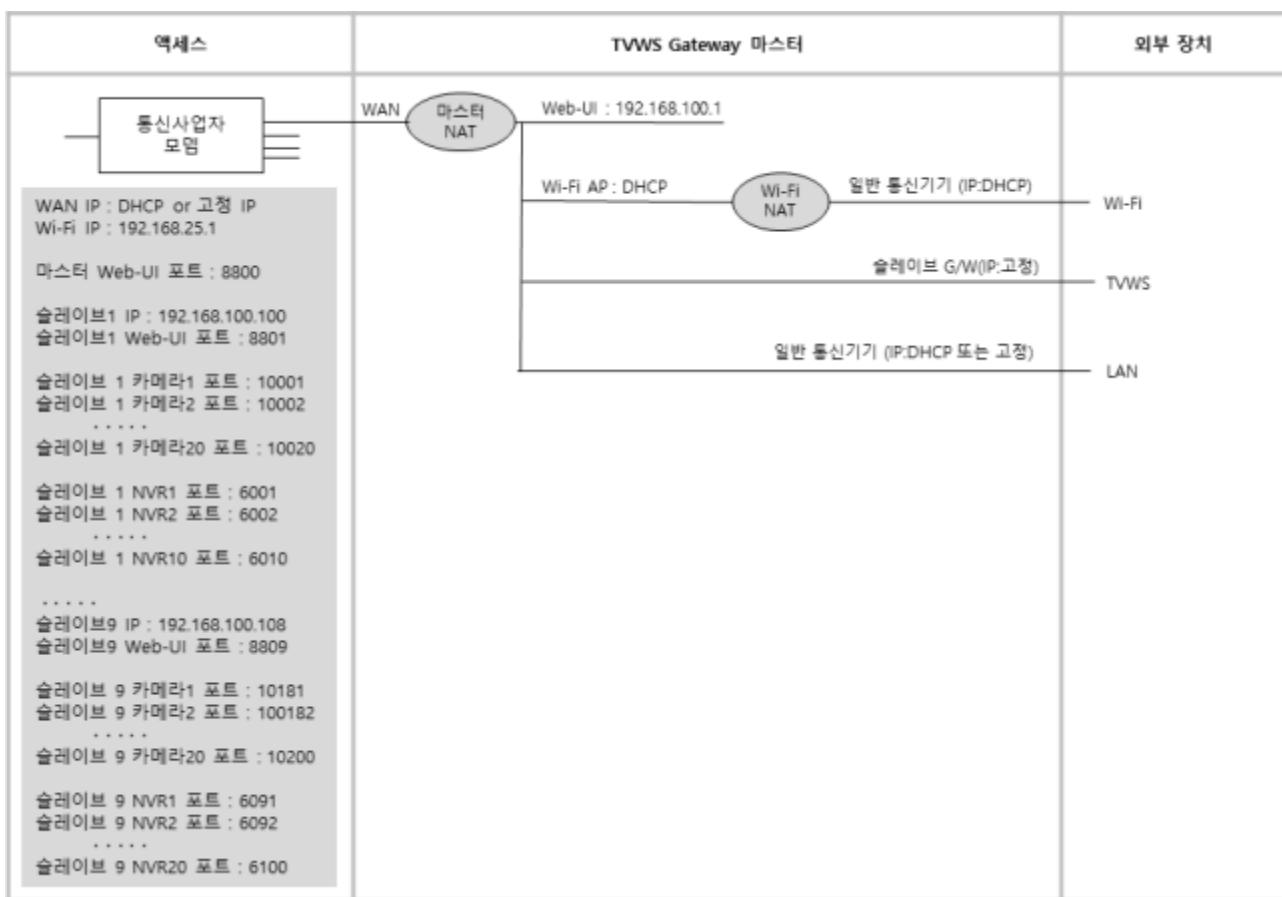
1.2 Network Configure

The TVWS Gateway consists of 1:1 connections between one master equipment and one slave equipment. Depending on the service area, 1:N can be configured to connect up to 9 slave equipment to 1 master equipment.

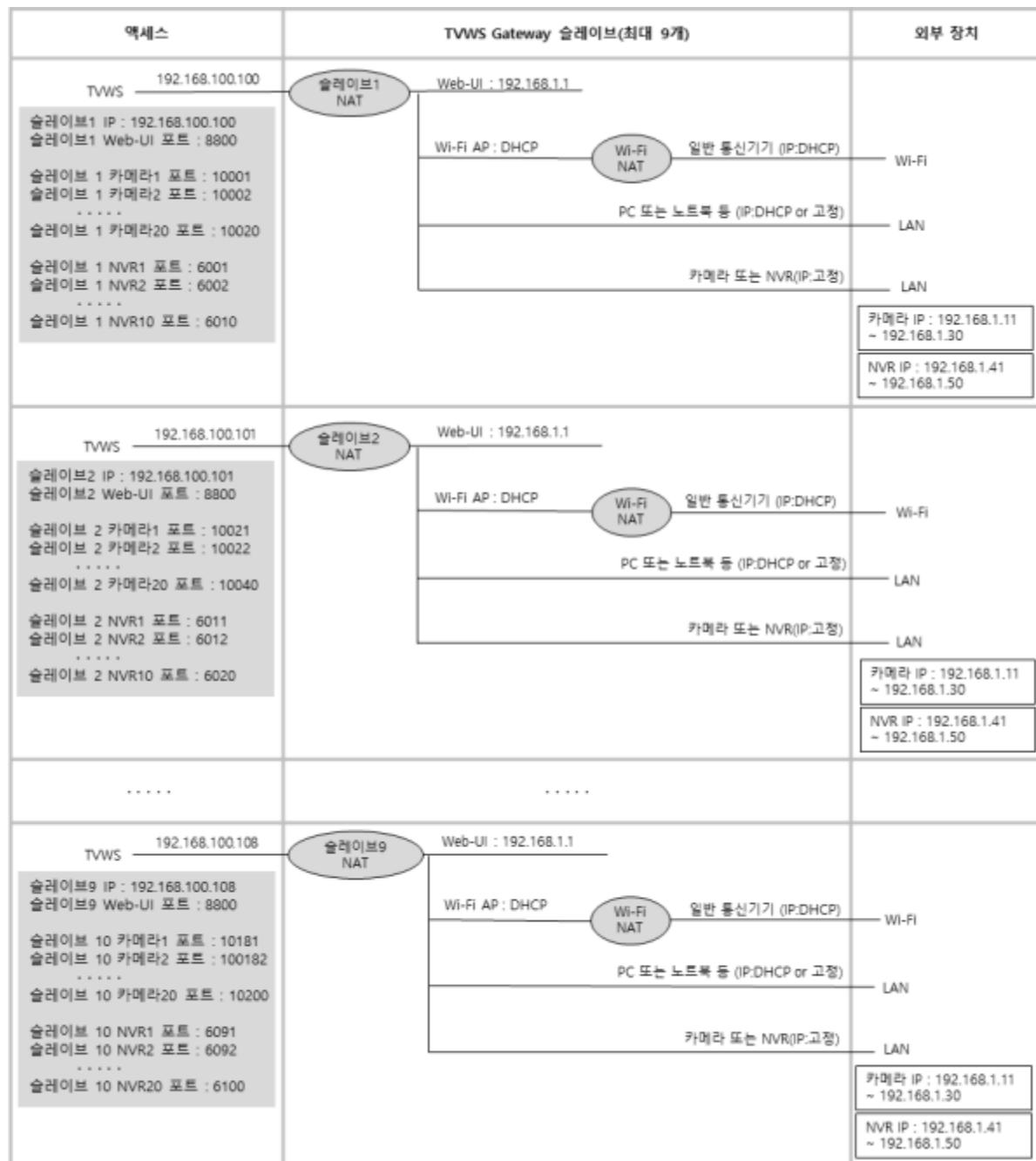
Multiple cameras can be connected to each slave device, and equipment from other companies can be connected using the following ports.



This is the network configuration diagram of the backpack Wi-Fi master equipment.
Please refer to the example below and check the network configuration as needed.
(Each port can be changed.)



This is the network configuration diagram of the backpack Wi-Fi Slave equipment. Please refer to the example below and check the network configuration as needed. To connect equipment other than the equipment provided, refer to the NVR IP and port in the figure below to change the settings of the equipment you want to connect to and connect to the configuration of the slave equipment. (Each port can be changed.)



1.3 TVWS Backpack Wi-Fi

1.3.1 Wi-Fi equipment and support backpack.

- Introduction and function.

- IEEE 802.11af modem support
- Access to the TV White Space database
- WEB UI support
- LOS distance communication greater than 10 km
- Support for bonding of neighboring two channels (6+6MHz)
- Transmit power control function
- Long-range Point-to-Multi Point (PtMP) support
- Wi-Fi(IEEE 802.11n) support.
- remote firmware update for the support.
- **Supports battery operation when power is difficult to use, such as a power outage**

Precautions

This equipment must be installed by professionals and must comply with the regulations of their country and region. In addition, depending on the surrounding wireless environment, communication between equipment may not be possible without a TVWS available channel.

장비 사양

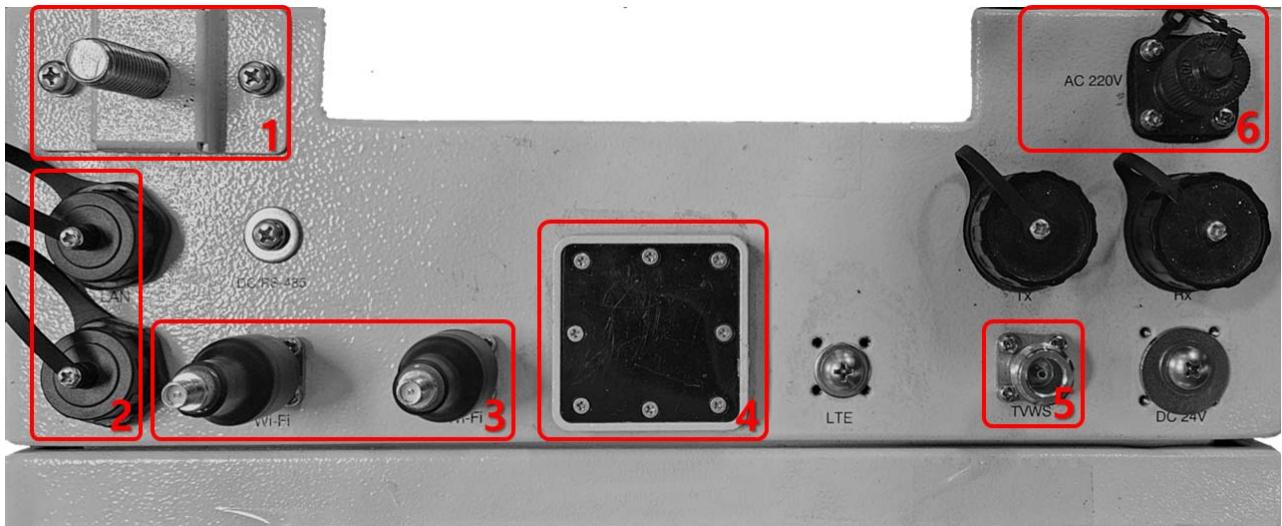
Technical Standards	IEEE 802.11af
Duplex	TDD
Channel bandwidth	6MHz / 12MHz (Support for bonding of neighboring two channels (6+6MHz))
Operating Frequency	470 – 698MHz
Modulation Method	BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM
Maximum Data Rate (TCP)	19Mbps @6MHz BW 26Mbps @12MHz BW
Maximum Output Power	27dBm±2dB @6MHz BW 17dB Gain Control @1dB step
TX/RX Carrier	1x1 SISO
Output Spectrum Mask	55dBc @C.F±3.0MHz, 6MHz BW
Out of band launch.	≤ -42.8dBm @RBW 100kHz
Receipt Sensitivity	-77dBm @MCS8(256-QAM 3/4) -84dBm @MCS5(64-QAM 2/3) -91dBm @MCS3(16-QAM 1/2) -96dBm @MCS1(QPSK 1/2) -98dBm @MCS0(BPSK 1/2)
Maximum Access Devices	9
GPS	built-in type
Operating Temperature	-20°C to 50°C @elevation 0 m
IP Rating	IP65
Electrostatic Discharge	8kV air, 4kV contact
Battery	14.4V / 19.8Ah / 294Wh
AC Power	AC 110 ~ 230 V / 50-60Hz
Power Consumption	35W
Size	500 mm x 500 mm x 300 mm (including backrest)
Weight	12 kg or less
HOUSING	sheet metal aluminum
Antenna Port	TVWS ANT port 1ea (N Type(F) / 50 ohm) Wi-Fi ANT port 2ea (RP-SMA Type(F) / 50 ohm)
Ethernet Ports	RJ45 Connectors 2ea (10/100Base-T) (WAN Port, LAN Port)
Standard / BW (Wi-Fi)	802.11n / 20 MHz
Operating Frequency	2 412 ~ 2 462 MHz (Varies by region/country)
Switch	2 (power switch, battery switch)

1.3.2 TVWS Backpack Wi-Fi Component

TVWS Backpack Wi-Fi	 A rectangular, light-colored metal box with a blue label that reads "TVWS Backpack Wi-Fi". It has several mounting holes and a black cable attached to the top left.
AC Cable	 A coiled white AC power cable with a black connector on one end and a standard three-prong AC plug on the other.
Patch Antenna	 A white rectangular patch antenna mounted on a black vertical pole.
Wi-Fi omni Antenna	 A dark blue, omnidirectional Wi-Fi antenna with a flared, bullet-like shape.

1.3.3 TVWS Backpack Wi-Fi component description.

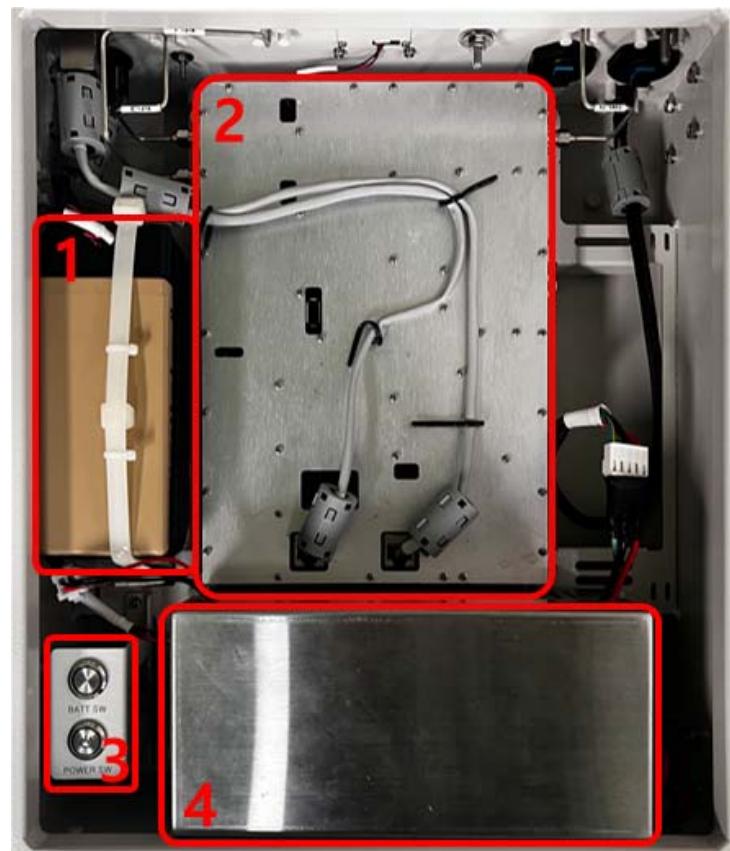
1) TVWS Backpack Wi-Fi Top



1 : Extension pole (GND)
2 : Ethernet port (WAN/LAN)
3 : Wi-Fi Antenna Port

4 : GPS
5 : TVWS Antenna Port
6 : Power

2) TVWS Backpack Wi-Fi Inner



1 : Battery
2 : TVWS Module

3 : Power Switch / Battery Switch
4 : PSU

4) TWSS Patch Antenna



Electrical Specification	
Frequency Range(MHz)	470-698 MHz
Gain(dBi)	8±0.5 dBi
Polarization	Dual Slant V/H
Horizontal Beam width	80±12°
Vertical Beam width	75±12°
Isolation	>25 dB
Front to Back Ratio	>13 dB
VSWR	<2
Maximum Power Per Port	50 W
Impedance	50 Ω
Lighting protection	DC Ground
Mechanical Specification	
Connector	2 x N Female
Height/width/depth	310x310x150 mm
Antenna Weight	2 kg
Radome color	white
Radome material	UV Protection ABS
Operational Temperature	-40°C to +50°C (-32°F to +122°F)
Humidity	ETS 300 019-1-4, EN 302 085 (ANNEX A.1.1)

5) Wi-Fi Omni Antenna



Electrical Specification	
Frequency Range(MHz)	2400 ~ 2483.5 MHz
Band width	83.5 MHz
VSWR	vertical.9 : 1
Gain	5 ± 1 dBi
Impedance	50 Ω
Polarization	Linear
Mechanical Specification	
Antenna Size (Length x Height)	194 x 13 mm
Connector	RP-SMA Male
Radiator Material	Copper
Operation Temperature	-30°C to +70°C
Operation Humidity	10 ~ 90 (%)

1.4 Safety Precautions

1.4.1 General precautions

- 1) Do not use outdoor, In door use only
- 2) Do not use or store in an environment with vibration
- 3) Do not allow foreign objects such as water, liquids, or metal powders to enter the product. This may cause breakage or electric shock
- 4) Do not charge or use the battery in explosive environments with flammable liquids, gased, or dust
- 5) Users cannot replace the internal battery, If there is any problem of battery, replacing or maintenance should be done by manufacturer
- 6) Do not use out of position, such as upside down or sideways

2. TVWS WEB UI

2.1 PC Setting

This procedure changes the TCP/IP settings in Windows to allow access to equipment in its initial state.

- 1) Click the Start Windows button and select Windows System > Control Panel.
- 2) Double-click the Network and Sharing Center icon in the Control Panel window.



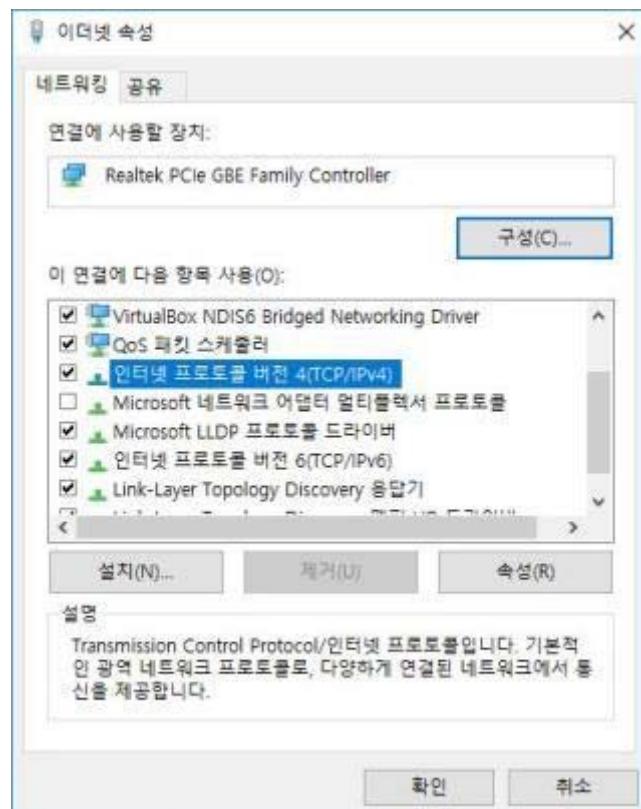
- 3) Click Change Adapter Settings in the left menu bar.



4) Right-click Ethernet, then select Properties.



5), double-click on Internet Protocol version 4 (ip and tcp).

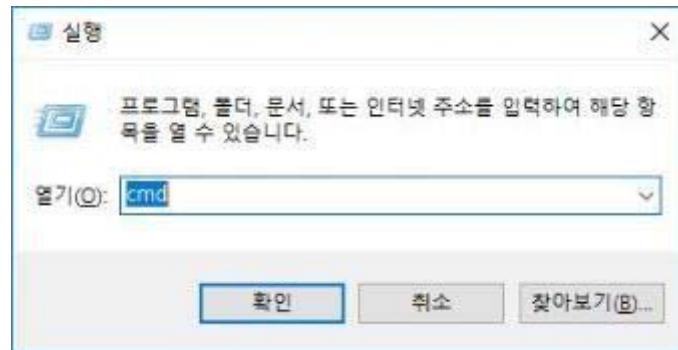


6) Set 'Get IP address automatically' and 'Get DNS server address automatically' as follows, then click the OK button.

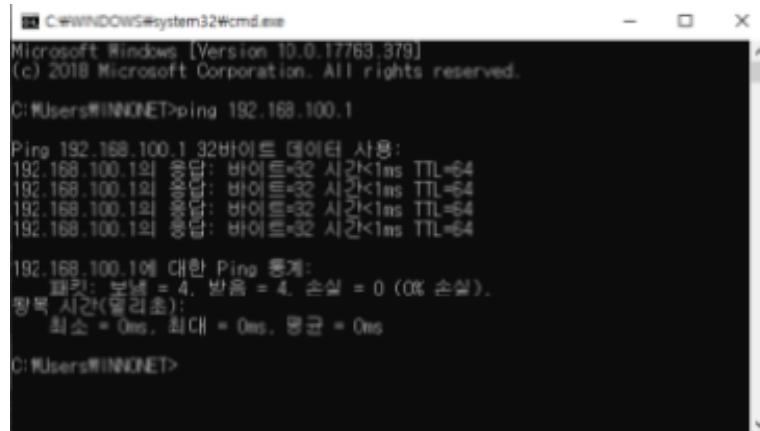


7) In the Ethernet Properties window, also click the OK button.

8) Press the Windows Launcher button, then click the command prompt for the Assistant in all programs to execute it (press the window button and R on the keyboard, enter cmd, and click the OK button).



9) When the PC and master equipment are connected, type 'ping 192.168.100.1', press Enter and check the response message. (Master Equipment LAN Port to Ethernet Cable PC)



```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.17763.379]
(c) 2018 Microsoft Corporation. All rights reserved.

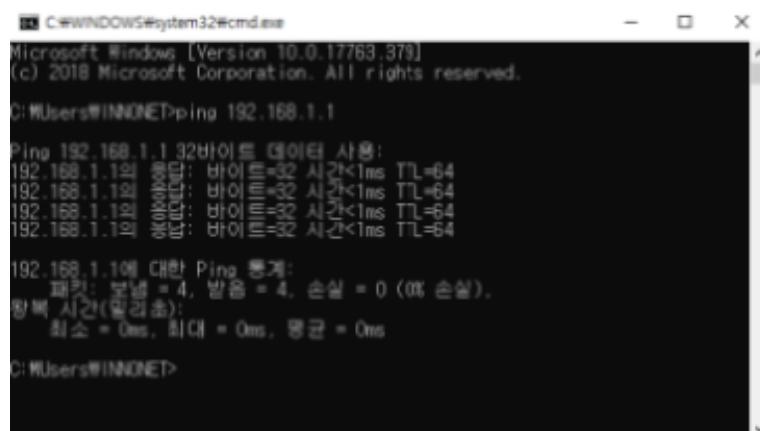
C:\Users\WINNONE>ping 192.168.100.1

Ping 192.168.100.1 32바이트 데이터 사용:
192.168.100.1의 응답: 바이트=32 시간<1ms TTL=64

192.168.100.1에 대한 Ping 통계:
  패킷: 보낸 = 4, 받음 = 4, 손실 = 0 (0% 손실).
 往返 시간(밀리초):
  최소 = 0ms, 최대 = 0ms, 평균 = 0ms

C:\Users\WINNONE>
```

10) When the PC and slave equipment are connected, type 'ping 192.168.1.1', press Enter and check the response message. (LAN port of slave equipment or PoE LAN port to Ethernet cable PC)



```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.17763.379]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\WINNONE>ping 192.168.1.1

Ping 192.168.1.1 32바이트 데이터 사용:
192.168.1.1의 응답: 바이트=32 시간<1ms TTL=64

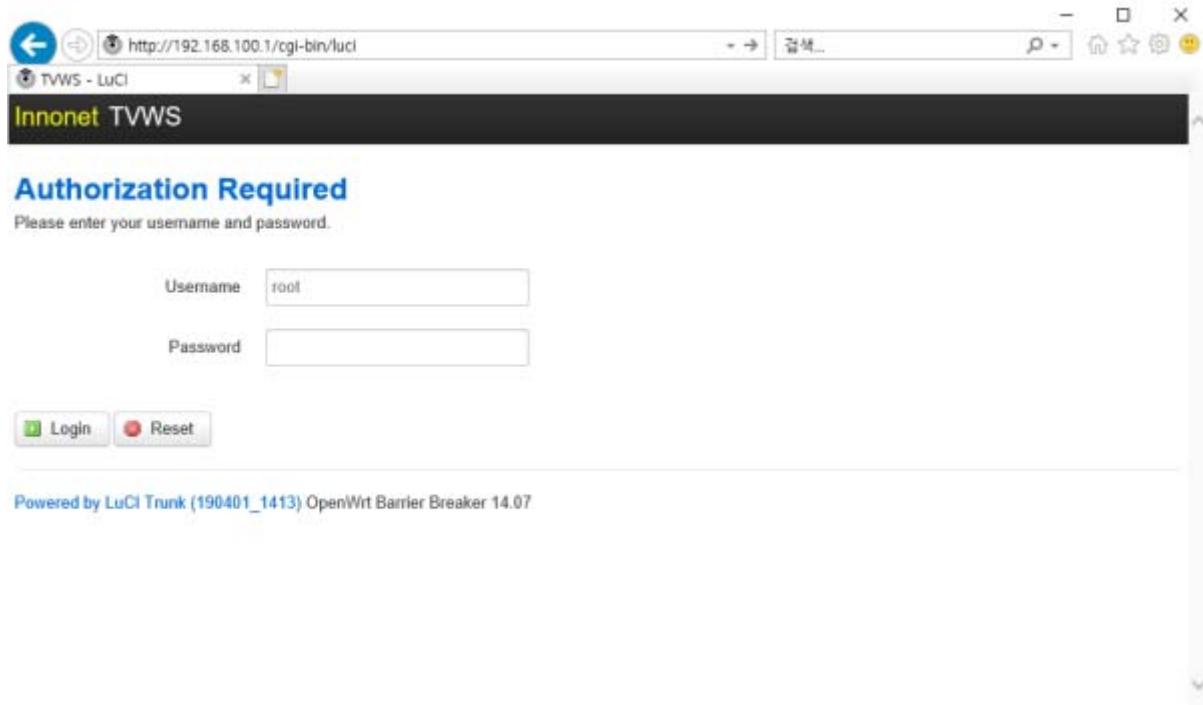
192.168.1.1에 대한 Ping 통계:
  패킷: 보낸 = 4, 받음 = 4, 손실 = 0 (0% 손실).
 往返 시간(밀리초):
  최소 = 0ms, 최대 = 0ms, 평균 = 0ms

C:\Users\WINNONE>
```

2.2 TVWS WEB UI

2.2.1 Connection Method

- 1) After confirming that there is no problem with the ping test, enter '192.168.100.1:8800' in the Internet address window to access the WEB page of the master device.
- 2) After confirming that there is no problem with the ping test, enter '192.168.1.1:8800' in the Internet address window to access the WEB page of the slave device.



2.2.2 VWS WEB UI Tab

The WEB UI of the TVWS equipment consists of Status, System, Network, Logout.



2.2.3. Status

- Status consists of four tabs.



1) Overview

- The Status Overview of the Equipment is divided into System, Memory, Network, and DHCP Leases.

Status : Displays information about the name of the equipment, model, firmware version, Linux kernel version, synchronized time, equipment running time, and average load amount of equipment.

Status	
System	
Hostname	TWIS
Model	mtb-apsoc-demo
Firmware Version	OpenWrt Barrier Breaker 14.07 / LuCI Trunk (210108_1025)
Kernel Version	3.10.14
Local Time	Wed Feb 10 13:38:15 2021
Uptime	3d 10h 36m 35s
Load Average	1.62, 0.76, 0.68

- Memory : Information about the total available memory, free memory, cache, and buffer of the equipment is displayed.

Memory	
Total Available	485912 kB / 514568 kB (94%)
Free	471788 kB / 514568 kB (91%)
Cached	10924 kB / 514568 kB (2%)
Buffered	3200 kB / 514568 kB (0%)

- Network : Network information of the equipment is displayed.

Network

IPv4 WAN Status	 Type: static wlan0 Address: 192.168.100.100 Netmask: 255.255.255.0 Gateway: 192.168.100.1 DNS 1: 8.8.8.8 Connected: 3d 10h 39m 14s
IPv6 WAN Status	 <i>Not connected</i> 
Active Connections	10 / 16384 (0%)

- DHCP Leases : The DHCP information assigned by the equipment is displayed.

DHCP Leases

Hostname	IPv4-Address	MAC-Address	Leasetime remaining
?	192.168.1.127	bc:0f:2b:00:00:8b	7h 20m 19s

DHCPv6 Leases

Hostname	IPv6-Address	DUID	Leasetime remaining
<i>There are no active leases.</i>			

2) System Log

- You can monitor system logs, which disappear when you reboot the equipment with volatile logs.

System Log

```
Wed Feb 10 12:52:29 2021 user:warn:kernel [294648.372000] TWWSLINK: TEMPERATURE Normal
Wed Feb 10 12:52:29 2021 user:warn:kernel [294648.494000] TWWSLINK: BATTERY READ ( 0xFFFF )
Wed Feb 10 12:52:30 2021 user:warn:kernel [294648.560000] TWWSLINK: BATTERY 2nd READ ( 0xFFFF )
Wed Feb 10 12:52:30 2021 user:warn:kernel [294648.532000] TWWSLINK: WLAN8 TX:POWER ( Offset CH:1, Temp:0 ) Changed ( To 16 )
Wed Feb 10 12:52:30 2021 user:warn:kernel [294648.560000] TWWSLINK: RSSI READ (00) ( 255 )
Wed Feb 10 12:52:30 2021 kernel:warn:kernel [294648.604000] Set_TxPower_Proc: KR Bandwidth = 0 MHz / Channel = 31 / Tx power = 16 dBm / CH Offset = 2.0
Wed Feb 10 12:52:30 2021 user:warn:kernel [294648.640000] TWWSLINK: STA PROCESS MAIN (PATH=0)
Wed Feb 10 12:52:30 2021 user:warn:kernel [294648.676000] TWWSLINK: STA PROCESS : CONNECTED
Wed Feb 10 12:52:30 2021 user:warn:kernel [294648.740000] TWWSLINK: RSSI Normal
Wed Feb 10 12:52:30 2021 user:warn:kernel [294648.824000] TWWSLINK: HPA(0) : RD 0x0f 0x0a 0x50 0x00 0x00 0x20 0x30 0x32 0x32 0x0c 0x0f 0x0f
Wed Feb 10 12:52:31 2021 user:warn:kernel [294648.912000] TWWSWD: UDP Received From TWWSLINK (16) 5a 0b 8c ffffff 0e 0f 10 11 ( - 61 )
Wed Feb 10 12:52:31 2021 user:warn:kernel [294650.644000] TWWSLINK: WLAN8 TX:POWER ( Offset CH:1, Temp:0 ) Changed ( To 16 )
Wed Feb 10 12:52:31 2021 kernel:warn:kernel [294650.888000] Set_TxPower_Proc: KR Bandwidth = 0 MHz / Channel = 31 / Tx power = 16 dBm / CH Offset = 2.0
Wed Feb 10 12:52:31 2021 user:warn:kernel [294650.116000] TWWSLINK: STA PROCESS MAIN (PATH=0)
Wed Feb 10 12:52:31 2021 user:warn:kernel [294650.164000] TWWSLINK: STA PROCESS : CONNECTED
Wed Feb 10 12:52:32 2021 user:warn:kernel [294651.116000] TWWSLINK: GPS Error in Opening thyUSB0
Wed Feb 10 12:52:33 2021 user:warn:kernel [294651.476000] TWWSLINK: WLAN8 TX:POWER ( Offset CH:1, Temp:0 ) Changed ( To 16 )
Wed Feb 10 12:52:33 2021 kernel:warn:kernel [294651.520000] Set_TxPower_Proc: KR Bandwidth = 0 MHz / Channel = 31 / Tx power = 16 dBm / CH Offset = 2.0
Wed Feb 10 12:52:33 2021 user:warn:kernel [294651.548000] TWWSLINK: STA PROCESS MAIN (PATH=0)
Wed Feb 10 12:52:33 2021 user:warn:kernel [294651.592000] TWWSLINK: STA PROCESS : CONNECTED
Wed Feb 10 12:52:34 2021 user:warn:kernel [294652.520000] TWWSLINK: HPA(0) : RD 0x61 0x61 0x61 0x61 0x20 0x00 0xa1 0x0a 0x00 0x13 0x00 0x0f 0x0f 0x0f
Wed Feb 10 12:52:34 2021 kernel:warn:kernel [294652.524000] Set_TxPower_Proc: KR Bandwidth = 0 MHz / Channel = 31 / Tx power = 16 dBm / CH Offset = 2.0
Wed Feb 10 12:52:34 2021 user:warn:kernel [294652.562000] TWWSLINK: STA PROCESS MAIN (PATH=0)
Wed Feb 10 12:52:34 2021 user:warn:kernel [294652.604000] TWWSLINK: STA PROCESS : CONNECTED
Wed Feb 10 12:52:34 2021 user:warn:kernel [294653.192000] TWWSLINK: BLE Error in Opening thyUSB2
Wed Feb 10 12:52:35 2021 user:warn:kernel [294654.172000] GPS Upload at 210218-12:52:35
Wed Feb 10 12:52:35 2021 user:warn:kernel [294654.360000] TWWSLINK: WLAN8 TX:POWER ( Offset CH:1, Temp:0 ) Changed ( To 16 )
Wed Feb 10 12:52:35 2021 kernel:warn:kernel [294654.404000] Set_TxPower_Proc: KR Bandwidth = 0 MHz / Channel = 31 / Tx power = 16 dBm / CH Offset = 2.0
Wed Feb 10 12:52:35 2021 user:warn:kernel [294654.432000] TWWSLINK: STA PROCESS MAIN (PATH=0)
Wed Feb 10 12:52:36 2021 user:warn:kernel [294654.468000] TWWSLINK: STA PROCESS : CONNECTED
Wed Feb 10 12:52:36 2021 user:warn:kernel [294654.584000] TWWSLINK: HPA(0) : Send Request TSST (12)
Wed Feb 10 12:52:37 2021 user:warn:kernel [294655.764000] TWWSLINK: WLAN8 TX:POWER ( Offset CH:1, Temp:0 ) Changed ( To 16 )
Wed Feb 10 12:52:37 2021 kernel:warn:kernel [294655.808000] Set_TxPower_Proc: KR Bandwidth = 0 MHz / Channel = 31 / Tx power = 16 dBm / CH Offset = 2.0
Wed Feb 10 12:52:37 2021 user:warn:kernel [294655.836000] TWWSLINK: STA PROCESS MAIN (PATH=0)
Wed Feb 10 12:52:37 2021 user:warn:kernel [294655.876000] TWWSLINK: STA PROCESS : CONNECTED
Wed Feb 10 12:52:37 2021 user:warn:kernel [294656.112000] TWWSLINK: RSCHECK Error in Opening thyUSB1
Wed Feb 10 12:52:38 2021 user:warn:kernel [294656.832000] TWWSLINK: HPA(0) : RD 0x0f 0x0a 0x50 0x00 0x00 0x31 0x32 0x30 0x34 0x17 0x0f 0x0f
Wed Feb 10 12:52:38 2021 user:warn:kernel [294657.192000] TWWSLINK: WLAN8 TX:POWER ( Offset CH:1, Temp:0 ) Changed ( To 16 )
Wed Feb 10 12:52:38 2021 kernel:warn:kernel [294657.236000] Set_TxPower_Proc: KR Bandwidth = 0 MHz / Channel = 31 / Tx power = 16 dBm / CH Offset = 2.0
Wed Feb 10 12:52:38 2021 user:warn:kernel [294657.264000] TWWSLINK: STA PROCESS MAIN (PATH=0)
Wed Feb 10 12:52:38 2021 user:warn:kernel [294657.304000] TWWSLINK: STA PROCESS : CONNECTED
Wed Feb 10 12:52:40 2021 user:warn:kernel [294658.644000] TWWSLINK: UDP [- M to S -] IP 192.168.100.1 (40990) Response received (54) 5a 0b 0c 0d
Wed Feb 10 12:52:40 2021 user:warn:kernel [294658.760000] TWWSLINK: STA PROCESS MAIN (PATH=0)
Wed Feb 10 12:52:40 2021 user:warn:kernel [294659.016000] TWWSLINK: STA PROCESS : CONNECTED
Wed Feb 10 12:52:41 2021 user:warn:kernel [294660.048000] TWWSWD: UDP received From FM10 (307) 30 01 01 01 00 00 00 00 ( - 11 )
Wed Feb 10 12:52:41 2021 user:warn:kernel [294660.088000] TWWSWD: FM10 Ping Enabled(2) FailCount 0, 0, 0, 0
Wed Feb 10 12:52:41 2021 user:warn:kernel [294660.340000] TWWSLINK: WLAN8 TX:POWER ( Offset CH:1, Temp:0 ) Changed ( To 16 )
Wed Feb 10 12:52:41 2021 kernel:warn:kernel [294660.384000] Set_TxPower_Proc: KR Bandwidth = 0 MHz / Channel = 31 / Tx power = 16 dBm / CH Offset = 2.0
Wed Feb 10 12:52:41 2021 user:warn:kernel [294660.412000] TWWSLINK: STA PROCESS MAIN (PATH=0)
```

3) Kernel Log

- The logs distributed to the console allow you to monitor the debugging logs in the kernel, which disappear when you reboot the equipment with a volatile log.

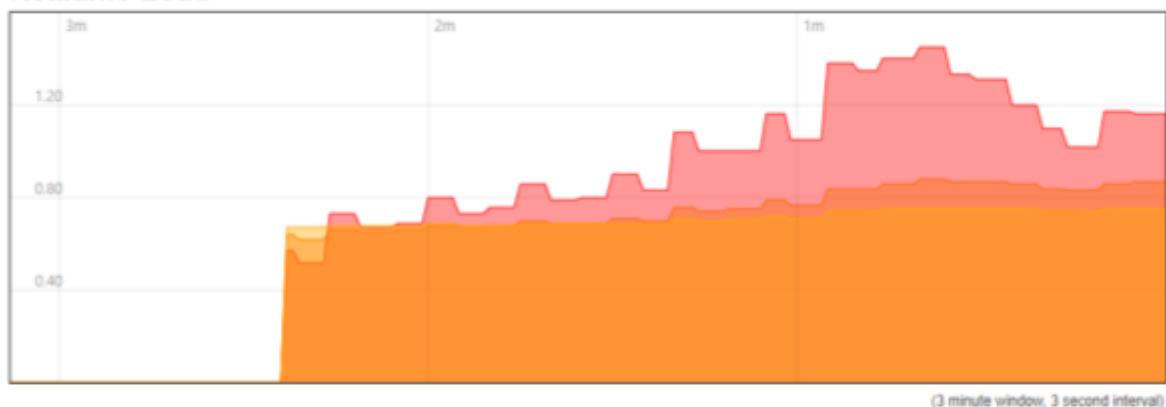
Kernel Log

```
[300302.484000] TVWSLINK: WLAN0 TX POWER ( Offset CH:1, Temp:0 ) Changed ( To: 16 )
[300302.520000] Set_TxPower_Proc: KR Bandwidth = 0 MHz / Channel = 31 / Tx power = 16 dBm / CH Offset = 2 ./ (8) = 2
[300302.548000] TVWSLINK: STA PROCESS MAIN (PATH=0)
[300302.588000] TVWSLINK: STA PROCESS: CONNECTED
[300302.916000] TVWSLINK: GPS Error in Opening myUSB0
[300303.880000] TVWSLINK: HPA(0): Send Request TSSI (12)
[300303.928000] TVWSLINK: WLAN0 TX POWER ( Offset CH:1, Temp:0 ) Changed ( To: 16 )
[300303.964000] Set_TxPower_Proc: KR Bandwidth = 0 MHz / Channel = 31 / Tx power = 16 dBm / CH Offset = 2 ./ (8) = 2
[300303.992000] TVWSLINK: STA PROCESS MAIN (PATH=0)
[300304.032000] TVWSLINK: STA PROCESS: CONNECTED
[300304.268000] TVWSLINK: BLE Error in Opening myUSB2
[300304.924000] TVWSLINK: HPA(0): RD 0x61 0x61 0x20 0x00 0x20 0x30 0x31 0x37 0x10 0xff 0x8f
[300305.356000] TVWSLINK: WLAN0 TX POWER ( Offset CH:1, Temp:0 ) Changed ( To: 16 )
[300305.400000] Set_TxPower_Proc: KR Bandwidth = 0 MHz / Channel = 31 / Tx power = 16 dBm / CH Offset = 2 ./ (8) = 2
[300305.428000] TVWSLINK: STA PROCESS MAIN (PATH=0)
[300305.468000] TVWSLINK: STA PROCESS: CONNECTED
[300307.100000] TVWSLINK: UDP [- M to S -] IP:192.168.100.1 (4090) Response received (54) 0a 0b 0c 0d
[300307.408000] TVWSLINK: WLAN0 TX POWER ( Offset CH:1, Temp:0 ) Changed ( To: 16 )
[300307.452000] Set_TxPower_Proc: KR Bandwidth = 0 MHz / Channel = 31 / Tx power = 16 dBm / CH Offset = 2 ./ (8) = 2
[300307.486000] TVWSLINK: STA PROCESS MAIN (PATH=0)
[300307.520000] TVWSLINK: STA PROCESS: CONNECTED
[300308.004000] TVWSLINK: HPA(0): RD 0x61 0x61 0x61 0x20 0x00 0xa1 0xa0 0x00 0x13 0x00 0xff 0xff 0x74 0x00 0x03 0x01 0x7c 0x8a
[300308.732000] GPS Upload at 210210-14:26:50
[300308.932000] TVWSLINK: WLAN0 TX POWER ( Offset CH:1, Temp:0 ) Changed ( To: 16 )
[300308.972000] Set_TxPower_Proc: KR Bandwidth = 0 MHz / Channel = 31 / Tx power = 16 dBm / CH Offset = 2 ./ (8) = 2
[300309.000000] TVWSLINK: STA PROCESS MAIN (PATH=0)
[300309.040000] TVWSLINK: STA PROCESS: CONNECTED
[300310.080000] TVWSLINK: HPA(0): Send Request TSSI (12)
[300310.356000] TVWSLINK: WLAN0 TX POWER ( Offset CH:1, Temp:0 ) Changed ( To: 16 )
[300310.380000] Set_TxPower_Proc: KR Bandwidth = 0 MHz / Channel = 31 / Tx power = 16 dBm / CH Offset = 2 ./ (8) = 2
[300310.408000] TVWSLINK: STA PROCESS MAIN (PATH=0)
[300310.448000] TVWSLINK: STA PROCESS: CONNECTED
[300310.492000] TVWSLINK: RSCHECK Error in Opening myUSB1
[300311.132000] TVWSLINK: HPA(0): RD 0x61 0xa0 0x50 0x00 0x00 0x31 0x31 0x39 0x36 0x21 0xff 0x8f
[300311.776000] TVWSLINK: WLAN0 TX POWER ( Offset CH:1, Temp:0 ) Changed ( To: 16 )
[300311.820000] Set_TxPower_Proc: KR Bandwidth = 0 MHz / Channel = 31 / Tx power = 16 dBm / CH Offset = 2 ./ (8) = 2
[300311.848000] TVWSLINK: STA PROCESS MAIN (PATH=0)
[300311.888000] TVWSLINK: STA PROCESS: CONNECTED
[300312.944000] TVWSLINK: GPS Error in Opening myUSB0
[300313.212000] TVWSLINK: WLAN0 TX POWER ( Offset CH:1, Temp:0 ) Changed ( To: 16 )
[300313.252000] Set_TxPower_Proc: KR Bandwidth = 0 MHz / Channel = 31 / Tx power = 16 dBm / CH Offset = 2 ./ (8) = 2
[300313.280000] TVWSLINK: STA PROCESS MAIN (PATH=0)
[300313.320000] TVWSLINK: STA PROCESS: CONNECTED
[300314.240000] TVWSLINK: HPA(0): RD 0x61 0x61 0x61 0x20 0x00 0xa1 0xa0 0x00 0x13 0x00 0xff 0xff 0x72 0x00 0x7f 0x00 0x10 0x80
[300314.296000] TVWSLINK: BLE Error in Opening myUSB2
[300314.644000] TVWSLINK: WLAN0 TX POWER ( Offset CH:1, Temp:0 ) Changed ( To: 16 )
[300314.684000] Set_TxPower_Proc: KR Bandwidth = 0 MHz / Channel = 31 / Tx power = 16 dBm / CH Offset = 2 ./ (8) = 2
[300314.712000] TVWSLINK: STA PROCESS MAIN (PATH=0)
[300314.752000] TVWSLINK: STA PROCESS: CONNECTED
[300316.084000] TVWSLINK: WLAN0 TX POWER ( Offset CH:1, Temp:0 ) Changed ( To: 16 )
[300316.128000] Set_TxPower_Proc: KR Bandwidth = 0 MHz / Channel = 31 / Tx power = 16 dBm / CH Offset = 2 ./ (8) = 2
[300316.156000] TVWSLINK: STA PROCESS MAIN (PATH=0)
[300316.196000] TVWSLINK: STA PROCESS: CONNECTED
```

4) Realtime Graphs

- Realtime Graphs displays real-time graphs such as equipment load and traffic. You can select each tab to see the corresponding graph.

Realtime Load



1 Minute Load: 1.16

Average: 1.16

Peak: 1.45

5 Minute Load: 0.87

Average: 0.87

Peak: 0.88

15 Minute Load: 0.75

Average: 0.75

Peak: 0.75

Realtime Connections

This page gives an overview over currently active network connections.

Active Connections



UDP: 7

Average: 7

Peak: 17

TCP: 11

Average: 11

Peak: 17

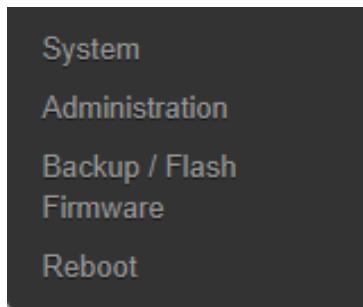
Other: 4

Average: 3

Peak: 4

2.2.4. System

- Divided into System, Administration, Backup/Flash Firmware, Reboot



1) System

- System Properties: You can change the time information and log settings of the equipment.
 - Local Time : Check the current equipment setting time. The Sync with browser button allows synchronization with the browser you are connected to.
 - Hostname : You can set the name of the equipment.
 - Timezone : You can set the time zone for the equipment. The initial value is Asia/Seoul.

System Properties

General Settings **Logging** Language and Style

Local Time: Wed Feb 10 15:00:45 2021 Sync with browser

Hostname: TVWS

Timezone: Asia/Seoul

- Time Synchronization
- Enable NTP Client : Activate the NTP client of the equipment.
- Provide NTP server : Activates the NTP server through the current equipment vision.
- NTP server candidates : Set the list of NTP servers to connect to.

Time Synchronization

Enable NTP client

Provide NTP server

NTP server candidates

0 openwrt.pool.ntp.org	
1 openwrt.pool.ntp.org	
2 openwrt.pool.ntp.org	
3 openwrt.pool.ntp.org	

2) Administration

- change the password and remote SSH settings of the Router Password device.
- Password : Enter the password you want to change.
- Confirmation : Enter the password you want to change once more.

Router Password

Changes the administrator password for accessing the device

Password

Confirmation

- SSH Access

- Interface : Set up an interface to allow SSH connections.
- Port : Set the port to use for SSH connections.
- Password authentication : Use the password when accessing SSH.
- Allow root logins with password : Allow root account access when SSH is accessed.
- Gateway ports : Set a port that allows SSH access on the external network.
- SSH-Keys : Set the public key to use for SSH.

SSH Access
Dropbear offers [SSH](#) network shell access and an integrated [SCP](#) server

Dropbear Instance

Interface [lan](#) [wan](#) [unspecified](#)
 [Listen only on the given interface or, if unspecified, on all](#)

Port [Specifies the listening port of this Dropbear instance](#)

Password authentication [Allow SSH password authentication](#)

Allow root logins with password [Allow the root user to login with password](#)

Gateway ports [Allow remote hosts to connect to local SSH forwarded ports](#)

SSH-Keys
Here you can paste public SSH-Keys (one per line) for SSH public-key authentication.

3) Backup / Flash Firmware

- **Backup/ Restore** You can back up, restore, or update new firmware settings for the equipment.

- **Download backup** : Download the current settings as a backup file.
- **Reset to defaults** : Change all settings to preferences.
- **Restore backup** : Restore settings using the backup file you downloaded.

Backup / Restore
Click "Generate archive" to download a tar archive of the current configuration files. To reset the firmware to its initial state, click "Perform reset" (only possible with squashfs images).

Download backup:

Reset to defaults:

To restore configuration files, you can upload a previously generated backup archive here.

Restore backup: 선택된 파일 있음

- Flash new firmware image
- Keep settings : Maintain existing settings after firmware update.
- Image : Select the firmware update file, then click the Flash image button to proceed with the firmware update. Be careful not to lose power during firmware updates. After the firmware update is complete, the equipment will reboot.

Flash new firmware image

Upload a sysupgrade-compatible image here to replace the running firmware. Check "Keep settings" to retain the current configuration (requires an OpenWrt compatible firmware image).

Keep settings:

Image: 선택된 파일 없음

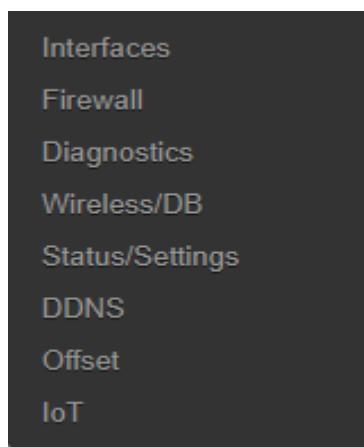
4) Reboot

- You can reboot the equipment remotely. Pressing Perform reboot will reboot the equipment immediately, and will take you to the login page after the operation is complete.

The screenshot shows a web-based management interface for a MediaTek TVWS device. The top navigation bar includes links for Status, System, Network, and Logout. The main content area is titled 'System' and contains a 'Reboot' section. The 'Reboot' section is described as 'Reboots the operating system of your device' and includes a blue 'Perform reboot' button. The overall layout is clean and functional, typical of a network configuration tool.

2.2.5. Network

- Interfaces, Firewall, Diagnostics, Wireless/DB, Status/Settings, DDNS, Offset, IoT로 나눠져 있습니다.



1) Interfaces

- You can set up a network of equipment and assign IPs. The default network is divided into WAN and LAN. The WAN assigns the interface from which the equipment supplies the Internet, and the LAN assigns the interface from which the equipment supplies the Internet. You can set Protocol, IPv4 address, etc. through the LAN and WAN Edit, and you can add any user interface by clicking the Add new interface button.

Interface Overview

Network	Status	Actions
LAN	Uptime: 3d 12h 34m 17s MAC-Address: 00:0C:43:00:04:98 RX: 10.03 MB (66968 Pkts.) TX: 11.17 MB (68677 Pkts.) IPv4: 192.168.1.1/24	Connect Stop Edit Delete
WAN	MAC-Address: 00:00:00:00:00:00 RX: 0.00 B (0 Pkts.) TX: 0.00 B (0 Pkts.)	Connect Stop Edit Delete

Add new interface...

Global network options

IPv6 ULA-Prefix: fd54:57e2:1d06::/48

- Common Configuration – General Setup
- Status : You can check the interface status of the WAN network.
- Protocol : You can apply the protocol to the WAN interface. Use DHCP client for flexible IP assignments and Static address for static IPs.
- When setting the protocol to Static address, you can enter the setting value below.
- IPv4 address : Set the static IP.
- IPv4 netmask : Set up Netmask.
- IPv4 gateway : Set the Gateway IP.

Common Configuration

General Setup	Advanced Settings	Physical Settings	Firewall Settings
Status	br-lan	Uptime: 3d 12h 43m 27s MAC-Address: 00:0C:43:00:04:98 RX: 10.04 MB (67076 Pkts.) TX: 11.19 MB (68787 Pkts.) IPv4: 192.168.1.1/24	
Protocol	Static address		
IPv4 address	192.168.1.1		
IPv4 netmask	255.255.255.0		
IPv4 gateway			

- IPv4 broadcast : Set the Broadcast IP.
- Use custom DNS servers : Set up a DNS server.
- IPv6 assignment length : Sets the length of Prefix for IPv6.
- IPv6 address : Set an IPv6 address.
- IPv6 gateway : Set the IPv6 gateway address.
- IPv6 routed prefix : Set the IPv6 routed prefix address.

IPv4 broadcast	<input type="text"/>
Use custom DNS servers	<input type="text"/> 8.8.8.8 
IPv6 assignment length	<input type="text"/> disabled 
<small>Assign a part of given length of every public IPv6-prefix to this interface</small>	
IPv6 address	<input type="text"/>
IPv6 gateway	<input type="text"/>
IPv6 routed prefix	<input type="text"/>
<small>Public prefix routed to this device for distribution to clients.</small>	

- Common Configuration – Advanced Settings

- Bring up on boot : Set the network to turn on at boot time.
- Use builtin IPv6-management : Enables built-in IPv6 management.
- Override MAC address : Overwrite the MAC address of the network.
- Override MTU : Use the User Settings MTU.
- Use gateway metric : Establish metrics gateway.

Common Configuration

General Setup	Advanced Settings	Physical Settings	Firewall Settings
<hr/>			
Bring up on boot	<input checked="" type="checkbox"/>		
Use builtin IPv6-management	<input checked="" type="checkbox"/>		
Override MAC address	<input type="text"/> 00:0C:43:00:04:98		
Override MTU	<input type="text"/> 1500		
Use gateway metric	<input type="text"/> 0		

- Common Configuration – Physical Settings
- Bridge Interface : Set the network to a bridge.
- Interface : Assign an interface to the network. For bridge networks, you can select multiple interfaces.

Common Configuration

General Setup Advanced Settings **Physical Settings** Firewall Settings

Bridge Interfaces  creates a bridge over specified interface(s)

Enable STP  Enables the Spanning Tree Protocol on this bridge

Interface  Ethernet Adapter: "bond0"
  Ethernet Adapter: "eth0" (lan)
  Ethernet Adapter: "eth1" (lan)
  VLAN Interface: "mt7790u_sta.network1" (wan)
  VLAN Interface: "mt7790u_ap.network1"
  Wireless Network: Master "OpenWrt" (lan)
  Custom Interface:

- Common Configuration – Firewall Settings
- Create/Assign firewall-zone : Select firewall rules to apply to your network.

Common Configuration

General Setup Advanced Settings Physical Settings **Firewall Settings**

Create / Assign firewall-zone  lan:   
  wan: 
  unspecified -or- create:

 Choose the firewall zone you want to assign to this interface. Select unspecified to remove the interface from the associated zone or fill out the create field to define a new zone and attach the interface to it.

-DHCP Server – General Setup

- Ignore interface : Disable DHCP for the network.
- Start : Sets the starting range of floating IPs allocated by the DHCP server.
- Limit : Set the end range of floating IPs allocated by the DHCP server.
- Leasetime : Set the expiration date of the floating allocation IP.

DHCP Server

General Setup Advanced Settings IPv6 Settings

Ignore interface [Disable DHCP for this interface.](#)

Start [Lowest leased address as offset from the network address.](#)

Limit [Maximum number of leased addresses.](#)

Leasetime [Expiry time of leased addresses, minimum is 2 minutes \(2m\).](#)

- DHCP Server – Advanced Settings

- The menu is displayed only when DHCP Server is enabled.
- Dynamic DHCP : Ensure that unregistered clients are also assigned flexible IP.
- Force : Service persists even if another DHCP server is found on the network.
- IPv4-Netmask : Overwrite the Netmask passed to the client.
- DHCP-Option : Sets DHCP-related options.

DHCP Server

General Setup Advanced Settings IPv6 Settings

Dynamic DHCP [Dynamically allocate DHCP addresses for clients. If disabled, only clients having static leases will be served.](#)

Force [Force DHCP on this network even if another server is detected.](#)

IPv4-Netmask [Override the netmask sent to clients. Normally it is calculated from the subnet that is served.](#)

DHCP-Options [Define additional DHCP options, for example "6,192.168.2.1,192.168.2.2" which advertises different DNS servers to clients.](#)

- DHCP Server – IPv6 Settings

- Router Advertisement-Service : Set RA Service related options.
- DHCPv6-Service : Set DHCPv6-Service related options.
- NDP-Proxy : Sets NDP-Proxy related options.
- DHCPv6-Mode : Sets DHCPv6-Mode related options.
- Always default router : This setting always notifies you that it is the default router.
- Announced DNS servers : Set up a DNS server.
- Announced DNS domains : Set the DNS domain.

DHCP Server

General Setup Advanced Settings **IPv6 Settings**

Router Advertisement-Service	server mode
DHCPv6-Service	server mode
NDP-Proxy	disabled
DHCPv6-Mode	stateless + stateful
Always announce default router	<input type="checkbox"/> <small>Announce as default router even if no public prefix is available.</small>
Announced DNS servers	<input type="text"/> 
Announced DNS domains	<input type="text"/> 

2) Firewall

장비의 방화벽 설정 및 포트 포워딩, 규칙 설정을 할 수 있습니다.

- General Settings

- Enable SYN-flood protection : Enable the firewall against SYN-Flood attacks.
- Drop invalid packets : No invalid packets are received.
- Input : Set the rules for packets that have the equipment as the destination.
- Output : Set rules for packets sent from the equipment.
- Forward : Set rules for packets passing through the equipment.
- Zones : Set the rules for the preset zone.

General Settings Port Forwards Traffic Rules Custom Rules

Firewall - Zone Settings

The firewall creates zones over your network interfaces to control network traffic flow.

General Settings

Enable SYN-flood protection

Drop invalid packets

Input: accept

Output: accept

Forward: accept

Zones

Zone ⇒ Forwardings	Input	Output	Forward	Masquerading	MSS clamping	
lan: lan: ⇒ wan	accept	accept	accept	<input type="checkbox"/>	<input type="checkbox"/>	
wan: wan: ⇒ ACCEPT	accept	accept	accept	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	

Add

- Port Forwards

- Allows the user to set up port forwarding for the desired port.
- Name : Rule name
- Protocol : The protocol type to be applied.
- External zone : Zone to be set to the outside (typically wan)
- External port : External Port
- Internal zone : Zone to be set inside (typically lan)
- Internal IP address : Internal IP Address
- Internal port : Internal Port

Firewall - Port Forwards

Port forwarding allows remote computers on the Internet to connect to a specific computer or service within the private LAN.

Port Forwards

Name	Match	Forward to	Enable	Sort			
This section contains no values yet							
New port forward:							
Name	Protocol	External zone	External port	Internal zone	Internal IP address	Internal port	
<input type="text" value="New port forward"/>	<input type="button" value="TCP+UDP"/>	<input type="button" value="wan"/>	<input type="text"/>	<input type="button" value="lan"/>	<input type="text"/>	<input type="text"/>	<input type="button" value="Add"/>

3) Diagnostics

- Option to self-diagnose network health.
- Ping : Ping can be sent to the entered address to check the network connection with the equipment.
- Traceroute : You can check the path to the entered address and the transfer delay.
- Nslookup : You can check the Name Server information associated with the entered domain.

Diagnostics

Network Utilities

The screenshot shows a network utility interface with three tabs: Ping, Traceroute, and Nslookup. The Ping tab is active, showing the command output for pinging the address openwrt.org. The output is as follows:

```
PING openwrt.org (139.59.209.225): 56 data bytes
64 bytes from 139.59.209.225: seq=0 ttl=48 time=266.593 ms
64 bytes from 139.59.209.225: seq=1 ttl=48 time=263.853 ms
64 bytes from 139.59.209.225: seq=2 ttl=48 time=263.211 ms
64 bytes from 139.59.209.225: seq=3 ttl=48 time=263.240 ms
64 bytes from 139.59.209.225: seq=4 ttl=48 time=263.498 ms

--- openwrt.org ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 263.211/264.539/268.593 ms
```

4) Wireless/DB

- Set information necessary for operation such as Mode, MCS, Bandwidth of TVWS.
- General Setup
- Mode : You can set the master and slave modes.
- MCS : You can set a configuration that combines spatial streams, modulation methods, coding rates, etc.
- Bandwidth : You can set the bandwidth.
- Channel Manual Select : You can set the way in which available channels are assigned.
- SSID : You can set the SSID of the equipment.
- TxPower : You can set the output strength of fixed 1W equipment.
- Portable 100mW TxPower : You can set the output strength of mobile 100mW equipment.
- Portable 40mW TxPower : You can set the output strength of mobile 40mW equipment.
- Channel : Channel Manual Select is activated and the channel can be set.

General Setup

Hardware Type	HIGH_POWER_UHF
Mode	SLAVE
MCS	AUTO
Bandwidth	6MHz
Channel Manual Select	ON
SSID	TVWS
TxPower	25 dBm
Portable 100mW TxPower	14 dBm
Portable 40mW TxPower	14 dBm
Channel	31 (575 MHz)

- NMS Server : You can set the address of the NMS server to which you want to send information about the equipment.
- NMS Report Interval : You can set how often to report to the NMS server.
- Channel Server : You can set whether to use the available channel optimization channel optimization server.
- Channel Server Domain : You can set the domain of the available channel optimization server.
- Channel Server Polling Period : You can set the available channel optimization server registration message transmission frequency.
- Channel Reallocation Polling Period : You can set the available channel optimization server channel reallocation check message sending frequency.
- Slave Location Report Period : (BIS) You can set the slave location information transmission frequency.
- Roaming Table Polling Period : (BIS) You can set how often roaming table request messages are sent.
- Roaming Table Clear : (BIS) You can set roaming table initialization.
- Roaming ID (Bus Line) : (BIS) You can set roaming table route information.

NMS Server	<input type="text" value="https://220.118.0.113:8443/nms_ct"/>
NMS Report Interval	<input type="text" value="1 Min"/>
Channel Server	<input type="text" value="Disable"/>
Channel Server Domain	<input type="text" value="www.tvws.co.kr"/>
Channel Server Polling Period[min]	<input type="text" value="1"/>
Channel Reallocation Polling Period[min]	<input type="text" value="0"/>
Slave Location Report Period[sec]	<input type="text" value="0"/>
Roaming Table Polling Period[min]	<input type="text" value="0"/>
Roaming Table Clear	<input type="text" value="Normal"/>
Roaming ID (Bus Line)	<input type="text" value="seocho01"/>

- Database stores information to identify users in the RRA prior to being assigned available channels, which should not be modified by users should not be modified by users.

Database

TVWS DB	
Domain	tvws.kr
Mobile Slave	Present
Fixed Slave Number	None
DB Access Time	23:55
Tx Power Type	Fixed
Device Type	Fixed
Device Scheme	Manual
Use Device Type Ext	NOT USE
Owner - Full Name	Innonet
Owner - Kind	co
Operator - Full Name	Innonet
Operator - Street	Beobwon-ro 11-gil 7
Operator - Locality	Songpa-gu
Operator - Region	Seoul
Operator - Post Code	05836
Operator - Country	KR
Operator - Tel	02-406-8849
Operator - Email	cs@innonet.net

5) Status/Settings

- TVWS Status

- View the available channels, reception, and output strength of the TVWS.
- TVWS Status : You can check the available channels assigned to the current equipment and the sensitivity of the equipment.
- RSSI Alarm Threshold(Min, Max) : You can set the lowest and highest values of the sensitivity of the alarm (T.D.B.).
- TVWS TSSI : You can check the output value of the equipment.
- TSSI Alarm Threshold(Min, Max) : You can set the lowest and highest values of the output to be alarmed (T.D.B.).
- WiFi#1,2 TSSI : The Wi-Fi output of the machine can be checked (T.D.B.).
- IP Address : You can set the internal IP of the equipment.
- WAN Network Config : Check whether WAN IP has been changed and set.
- TVWS Sleep Mode : You can set the sleep mode of the equipment (T.D.B.).

TVWS STATUS/SETTINGS

Status/Settings

TVWS Status	TVWS Settings	HPA Update
<hr/>		
TVWS Status	CH:31 AP:TVWS RSSI:-57	
RSSI Alarm Threshold (Min,Max)	<input type="text" value="-90,-40"/>	
TVWS TSSI	23.3	
TSSI Alarm Threshold (Min,Max)	<input type="text" value="5,30"/>	
WiFi#1 TSSI	----	
WiFi#2 TSSI	----	
IP Address	<input type="text" value="192.168.100.1"/>	
WAN Network Config	<input type="text" value="NOT CHANGED"/>	

Sleep Mode Control

TVWS Sleep Mode	<input type="text" value="OFF"/>
-----------------	----------------------------------

- TVWS Settings

- TVWS TX : You can control the output of the equipment.
- WIFI : You can control the WIFI output of the equipment.
- LNA Bypass Control : Depending on TVWS reception, you can control the amplifier that amplifies the signal.
- LNA Bypass Mode : Control the amplifier that amplifies the TVWS signal.
- Slave Location Recheck : Check the location of the cruise ship can be set (T.B.D.).
- Slave Notification Interval : Set the positioning cycle for cruise ships (T.B.D.).
- Ext USB Port : You can control whether or not to use the USB output.

TVWS STATUS/SETTINGS

Status/Settings

	TVWS Status	TVWS Settings	HPA Update
TVWS TX	ON		
WIFI	ON		
LNA Bypass Control	Manual		
LNA Bypass Mode	OFF		
Slave Location Recheck	OFF		
Slave Notification Interval	OFF		
Ext 12V Enable	OFF		
Ext USB Port	OFF		

- HPA Update
 - Download File Path : You can set the file path for the HPA firmware.
 - HPA1 Status : View firmware information for the HPA.
 - HPA1 F/W : firmware updates can be made by setting it up.

TVWS STATUS/SETTINGS

Status/Settings

TVWS Status	TVWS Settings	HPA Update
<div style="border: 1px solid #ccc; padding: 5px; display: inline-block;"> Download file path <input type="text" value="http://server/hpamcu303_booxx.bin"/> </div>		
HPA1 Status Ver_1.3.00		
HPA1 F/W <input style="border: 1px solid #ccc; padding: 2px 10px;" type="button" value="NORMAL"/>		

6) DDNS

- You can set up a domain to access the equipment.

TVWS DDNS

DDNS

<input style="border: 1px solid #ccc; padding: 2px 10px;" type="button" value="TVWS DDNS"/>	
DDNS Domain	<input type="text" value="1.tvws.co.kr"/>
Update Enable	<input style="border: 1px solid #ccc; padding: 2px 10px;" type="button" value="OFF"/>
DDNS Server	<input type="text" value="www.tvws.co.kr"/>
Current WAN IP Address	0.0.0.0
DDNS Command Status	--
Connection Status	--

7) Offset

- Adjust the output value by channel by changing the offset of the equipment.

Offset

Offset for Channel & Temperature

ch0x - 6MHz

ch02	ch03	ch04	ch05	ch06	ch07	ch08	ch09
0	0	0	0	0	0	0	0

ch1x - 6MHz

ch10	ch11	ch12	ch13	ch14	ch15	ch16	ch17	ch18	ch19
0	0	0	0	-2	-2	-2	-2	-2	-2

ch2x - 6MHz

ch20	ch21	ch22	ch23	ch24	ch25	ch26	ch27	ch28	ch29
-1	-1	0	-1	0	0	1	2	2	1

ch3x - 6MHz

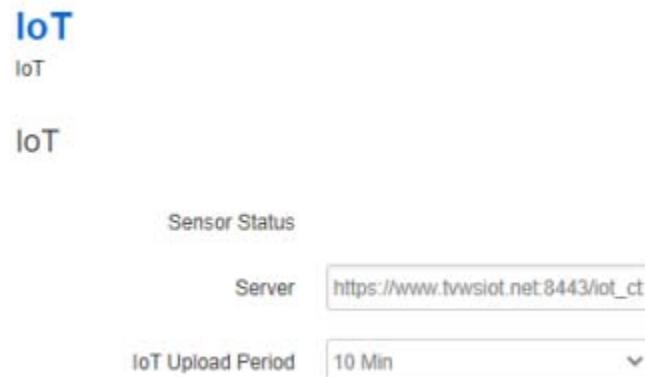
ch30	ch31	ch32	ch33	ch34	ch35	ch36	ch37	ch38	ch39
1	1	-1	-1	-2	-2	-2	-1	0	1

ch4x - 6MHz

ch40	ch41	ch42	ch43	ch44	ch45	ch46	ch47	ch48	ch49
1	1	0	-1	-2	-2	-2	-1	0	0

8) IoT

- You can set the server to monitor the status of IoT equipment and the frequency to upload.



2.2.6. Logout

- Log out the WEB page of the equipment.



2.3 Wi-Fi Setting

You can access the Wi-Fi WEB page to change your password settings. The Wi-Fi WEB setting screen requires wireless connection with the Wi-Fi, laptop, and mobile phone of the TVWS equipment to use the WEB page.

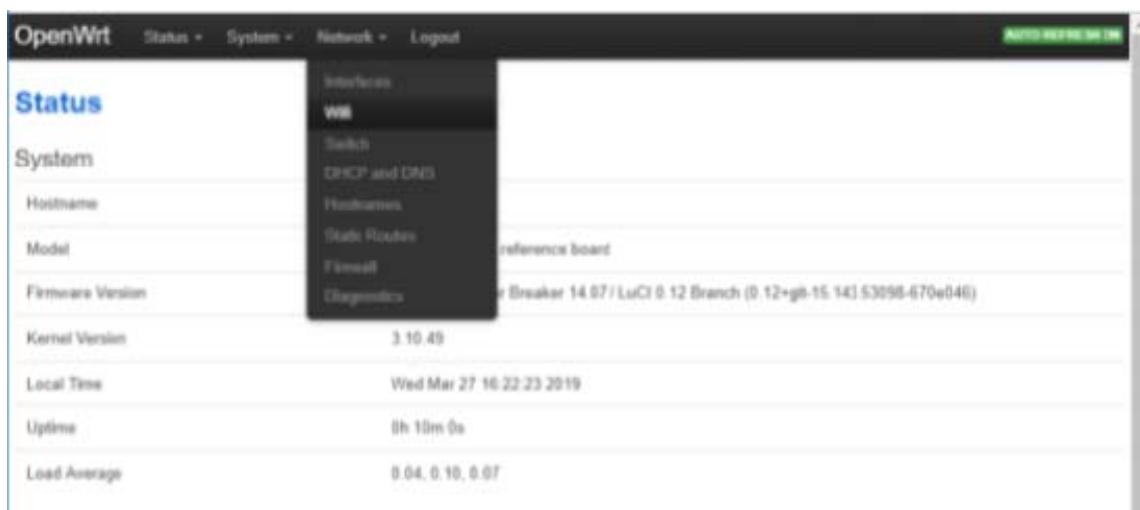
- 1) Use your laptop or mobile phone to find and connect Wi-Fi of your backpack Wi-Fi.



- 2) Open the WEB browser, type the IP (192.168.25.1) of the Wi-Fi WEB page in the address bar, type Password, and press Enter to access the WEB page.
(ID= root / Password= fts)



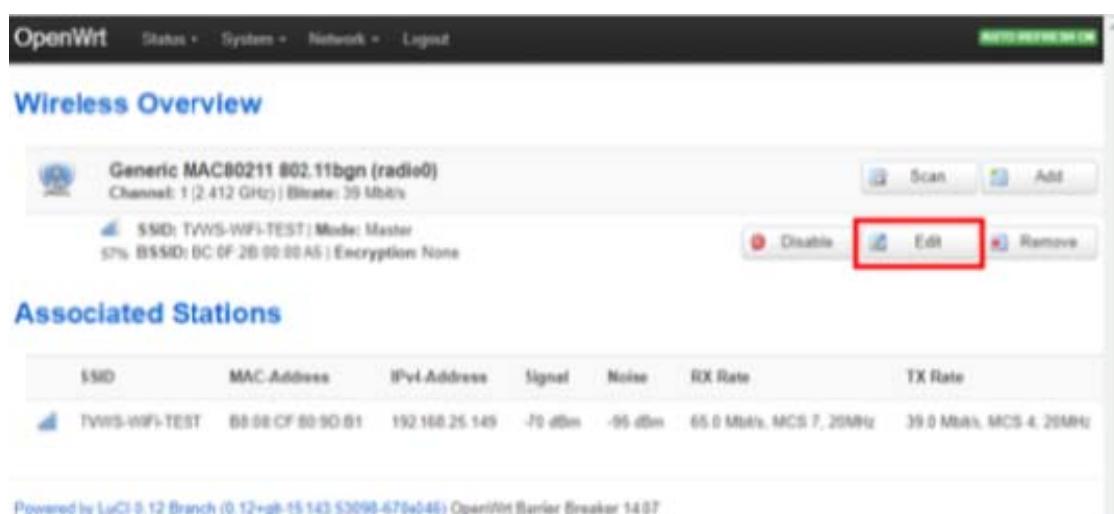
3) On the Network tab at the top of the Wi-Fi WEB UI, select Wifi.



The screenshot shows the OpenWrt Status page. The Network menu is open, with 'Wifi' selected. The main table displays system status information:

Status	
System	
Hostname	
Model	
Firmware Version	Barrier Breaker 14.07 / LuCI 0.12 Branch (0.12+gb-15.143.53098-670e046)
Kernel Version	3.10.49
Local Time	Wed Mar 27 16:22:23 2019
Uptime	8h 18m 0s
Load Average	0.04, 0.10, 0.07

4) In the Wireless Overview, view the SSID, verify that the Wi-Fi signal you connected to is correct, and click the edit you marked.



The screenshot shows the OpenWrt Wireless Overview page. It displays a list of wireless interfaces and associated stations:

Interface	SSID	Mode	Encryption	Disable	Edit	Remove
radio0	TWIS-WIFI-TEST	Master	None	<input type="button" value="Disable"/>	<input style="border: 2px solid red;" type="button" value="Edit"/>	<input type="button" value="Remove"/>

Associated Stations

SSID	MAC Address	IPv4 Address	Signal	Noise	RX Rate	TX Rate
TWIS-WIFI-TEST	B8:08:CF:80:90:81	192.168.25.149	-70 dBm	-95 dBm	65.0 Mbps, MCS 7, 20MHz	39.0 Mbps, MCS 4, 20MHz

Powered by LuCI 0.12 Branch (0.12+gb-15.143.53098-670e046) OpenWrt Barrier Breaker 14.07

5) Select the Wireless Security tab in the Interface Configuration at the bottom to select the WPA2-PSK and set the desired password for the key. Click the green arrow on the right side of the key to see the password you are typing. Click the Save & Apply button to apply the settings.

The screenshot shows the OpenWrt web interface. At the top, there is a navigation bar with links for Status, System, Network, and Logout. The main content area is titled "Wireless Network: Master 'TVWS-WIFI-TEST' (wlan0)". Below this, a note states: "This Device Configuration section covers physical settings of the radio hardware such as channel, transmit power or antenna selection which are shared among all defined wireless networks (if the radio hardware is multi-BSSID capable). Per network settings like encryption or operation mode are grouped in the Interface Configuration." The "Device Configuration" section has tabs for General Setup and Advanced Settings, with General Setup selected. It shows the following status information:

Status	Mode: Master SSID: TVWS-WIFI-TEST BSSID: BC:0F:2B:00:00:A5 Encryption: None Channel: 1 (2.412 GHz) Tx Power: 0 dBm Signal: -71 dBm Noise: -95 dBm Bitrate: 21.7 Mbit/s Country: KR
--------	--

Below this, there are fields for "Wireless network is enabled" (disabled), "Channel" (1 (2.412 GHz)), and "Transmit Power" (0 dBm). The "Interface Configuration" section has tabs for General Setup, Wireless Security (which is selected and highlighted with a red box), and MAC Filter. It shows the following configuration:

Encryption	WPA2-PSK
Cipher	auto
Key	— (with a green arrow icon to its right)

At the bottom right of the interface configuration section, there are buttons for "Save & Apply", "Save", and "Reset".

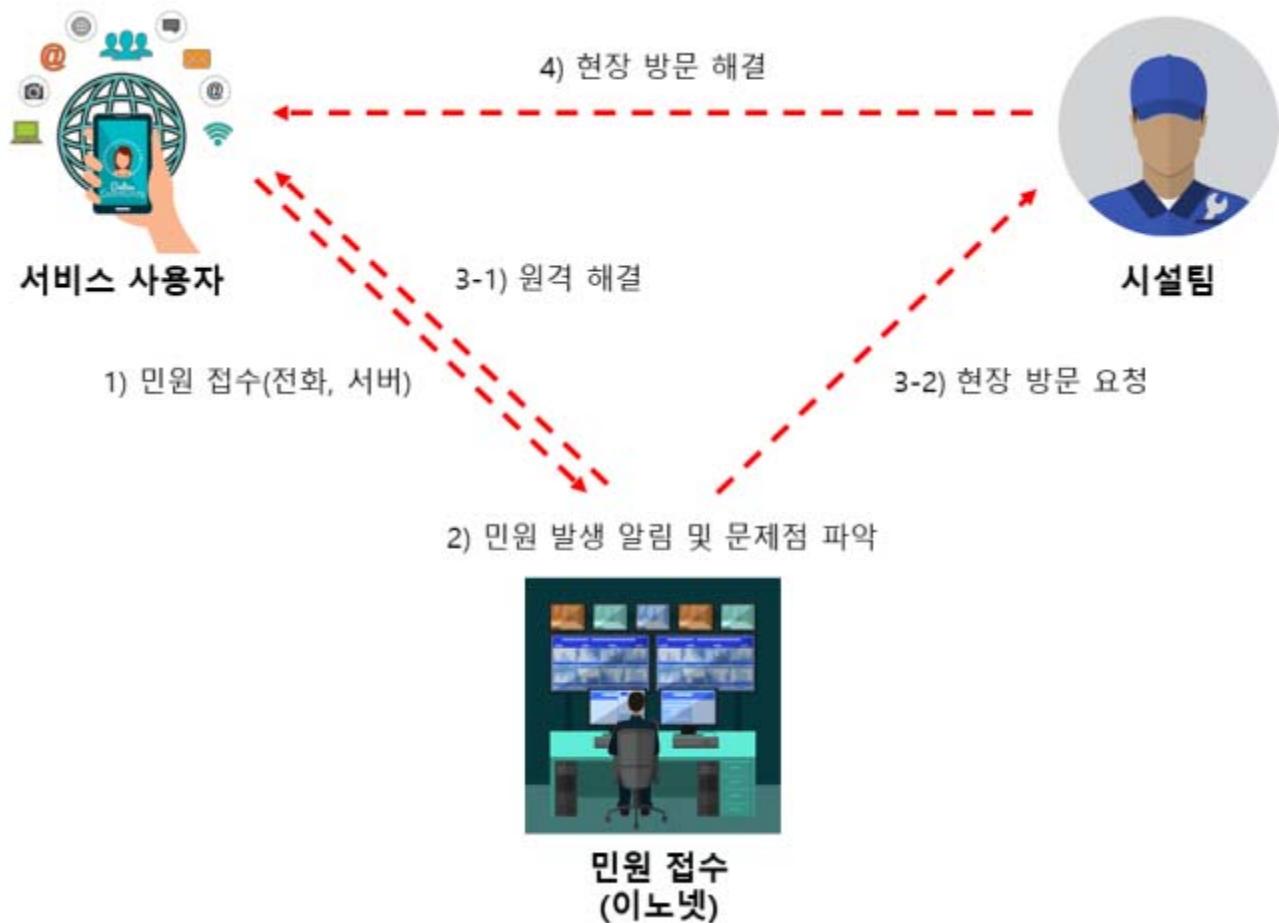
6) If you try to connect the Wi-Fi of your backpack Wi-Fi using your laptop or mobile phone again, and you are prompted for a password, enter the password you set to connect.



3. Maintenance

3.1 Maintenance System

Maintenance is carried out with the following system.



- 1) A service user reports a complaint due to an inconvenience while using the service.
- 2) When a complaint is received, it notifies the occurrence of a complaint and identifies the problem.
- 3) If it can be resolved remotely, support it remotely to resolve complaints.
- 4) If you need to visit the site, ask the facility team to visit the site.
- 5) The facility team visits the site to resolve the complaint.

3.2 Failure Check and Action

If you experience any inconvenience while using the service, please check the following situations first.

If you are not aware of any inconvenience after checking the following clarification and confirmation, please contact A/S at 070-7734-9970.

1) In case the master equipment does not have Wi-Fi

- Verify that your Internet modem is functioning normally.
- Ensure that the Power and WAN LEDs of the master equipment are illuminated.
- Under Master Equipment, check for Wi-Fi signals. (The Wi-Fi signal may be weak or not catchable indoors.)

2) In the case that the Wi-Fi of the slave equipment

- Ensure that the power and link LEDs of the slave equipment are illuminated.
- Under Slave Equipment, check for Wi-Fi signals. (The Wi-Fi signal may be weak or not catchable indoors.)

3) If the camera connected to the slave equipment does not come out

- Ensure that the camera power (12V or 24V) is supplied to the power box.
- Ensure that the LAN port of the slave equipment and the LAN port of the camera are connected.
- Make sure that the camera's connection ports are intact.
- Connect to the slave equipment and ping test with the camera to check for abnormalities.

3.3 How to Verify Equipment Operation

Before installing the Equipment, you should check and follow the instructions below.

(1) Height above average terrain (HAAT). Below 602 MHz, antenna shall not exceed 250 meters or 500 meters in less congested areas.

All other bands not to exceeds 250 meters.

The HAAT is calculated by the White Space database (§73.684(d)).

For HAAT greater than 250 meters the following A-F procedures below are required:

(2) The installing party must contact a White Space database, identify all TV broadcast station contours that would be potentially affected by operation at the planned HAAT and EIRP.

(3) Notification -The installing party must notify each of these licensees and provide geographic coordinates, relevant technical parameters and contact information.

(4) Start operations, No earlier than four calendar days after the notification in paragraph (g)(1)(ii)(B) above

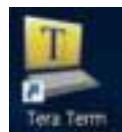
(5) Upon request, the installing party must provide affected licensee the time periods of operations.

(6) Conduct a new notification if increasing its power level, moving more than 100 meters horizontally from its location, or making an increase in the HAAT or EIRP that results in an increase in the minimum required separation distances from co-channel or adjacent channel TV station contours.

(7) All notifications required by this section must be in written form (including email).

To be kept by the White Space device operator for its records and supplied to the Commission upon request.

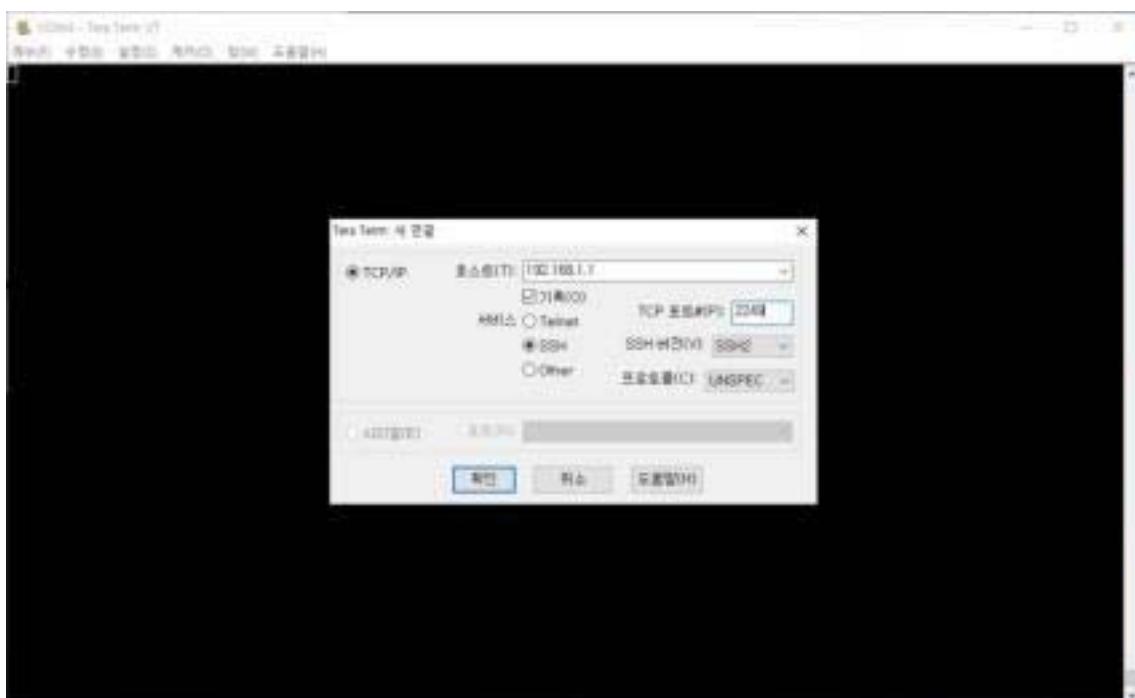
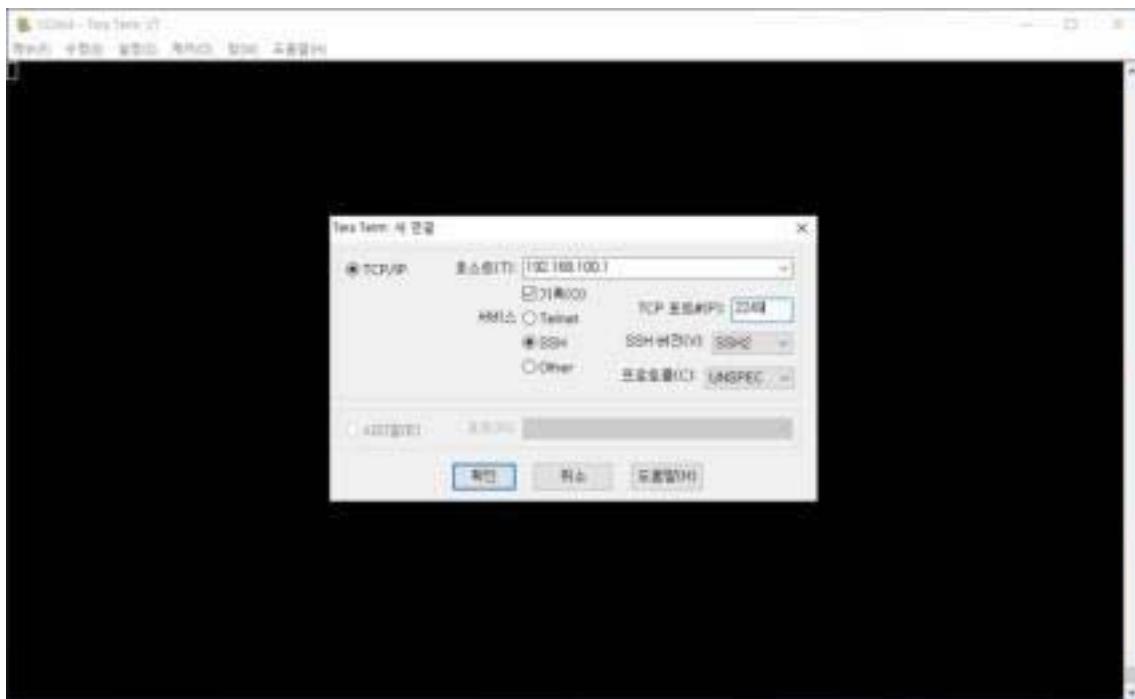
You can check the operation of the equipment using the Terra Term program.



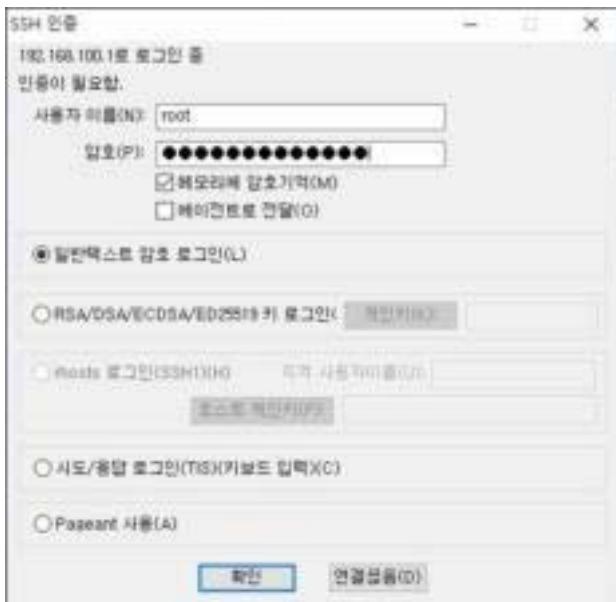
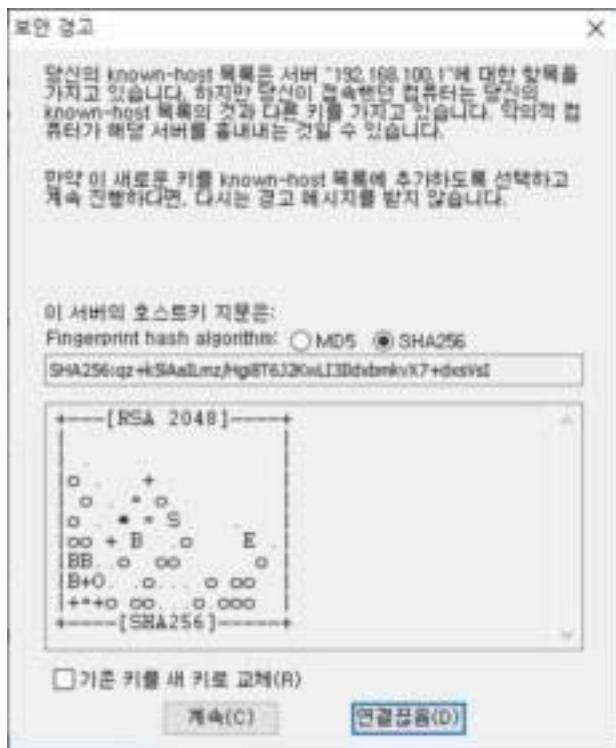
From the menu bar at the top, select Menu, and select New Link.

The master enters IP 192.168.100.1, service SSH, TCP port 2249.

The Slave enters IP 192.168.1.1, service SSH, TCP port 2249.



If you select OK, a security warning window appears, and select Continue.
Then enter your username and password (user name root, password: innonet160905)



3.3.1 IP Verification of Equipment

Type 'ifconfig'

The master displays 192.168.100.1 in br-lan, and the slave displays 192.168.1.1. When DHCP is assigned to the WAN port of the master, eth1 displays the IP. (ex: 192.168.1.155)

```
root@IVWS:~# 
root@IVWS:~# ifconfig
br-lan    Link encap:Ethernet  HWaddr 00:0C:43:06:1A:8A
          inet  addr:192.168.100.1  Broadcast:192.168.100.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:43ff:fe06:1a8a/64  Scope:Link
             UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
             RX packets:22744  errors:0  dropped:0  overruns:0  frame:0
             TX packets:21926  errors:0  dropped:0  overruns:0  carrier:0
             collisions:0  txqueuelen:0
             RX bytes:1670132 (1.5 MiB)  TX bytes:1788445 (1.7 MiB)

eth0      Link encap:Ethernet  HWaddr 00:0C:43:06:1A:8A
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:23274  errors:0  dropped:21  overruns:0  frame:0
          TX packets:22060  errors:0  dropped:0  overruns:0  carrier:0
          collisions:0  txqueuelen:1000
          RX bytes:2077226 (1.9 MiB)  TX bytes:1802366 (1.7 MiB)
          Interrupt:3

eth1      Link encap:Ethernet  HWaddr 00:0C:43:06:1A:89
          inet  addr:192.168.1.155  Broadcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:43ff:fe06:1a89/64  Scope:Link
             UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
             RX packets:44810  errors:0  dropped:0  overruns:0  frame:0
             TX packets:128560  errors:0  dropped:0  overruns:0  carrier:0
             collisions:0  txqueuelen:1000
             RX bytes:3723856 (3.5 MiB)  TX bytes:18531096 (18.0 MiB)

lo        Link encap:Local Loopback
          inet  addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128  Scope:Host
             UP LOOPBACK RUNNING  MTU:65536  Metric:1
             RX packets:42817  errors:0  dropped:0  overruns:0  frame:0
             TX packets:42817  errors:0  dropped:0  overruns:0  carrier:0
             collisions:0  txqueuelen:0
             RX bytes:2908800 (2.7 MiB)  TX bytes:2908800 (2.7 MiB)

wlan0     Link encap:Ethernet  HWaddr 00:0C:43:D0:CB:03
          inet6 addr: fe80::20c:43ff:fed0:cb03/64  Scope:Link
             UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
             RX packets:0  errors:0  dropped:0  overruns:0  frame:0
             TX packets:0  errors:0  dropped:0  overruns:0  carrier:0
             collisions:0  txqueuelen:1000
             RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

root@IVWS:~#
```

```
root@IVWS:~#  
root@IVWS:~# ifconfig  
br-lan  Link encap:Ethernet  HWaddr 00:0C:43:06:10:88  
        inet addr:192.168.1.1  Bcast:192.168.1.255  Mask:255.255.255.0  
        inet6 addr: fe80::20c:43ff:fe06:1a88/64 Scope:Link  
              UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1  
              RX packets:154959 errors:0 dropped:0 overruns:0 frame:0  
              TX packets:68469 errors:0 dropped:0 overruns:0 carrier:0  
              collisions:0 txqueuelen:0  
              RX bytes:10559130 (10.0 MiB)  TX bytes:5652525 (5.3 MiB)  
  
eth0    Link encap:Ethernet  HWaddr 00:0C:43:06:10:88  
        inet6 addr: fe80::20c:43ff:fe06:1a88/64 Scope:Link  
              UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1  
              RX packets:155301 errors:0 dropped:0 overruns:0 frame:0  
              TX packets:68836 errors:0 dropped:0 overruns:0 carrier:0  
              collisions:0 txqueuelen:1000  
              RX bytes:12721044 (12.1 MiB)  TX bytes:5715098 (5.4 MiB)  
              Interrupt:3  
  
eth1    Link encap:Ethernet  HWaddr 00:0C:43:06:10:87  
        inet6 addr: fe80::20c:43ff:fe06:1a87/64 Scope:Link  
              UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1  
              RX packets:355 errors:0 dropped:4 overruns:0 frame:0  
              TX packets:281 errors:0 dropped:0 overruns:0 carrier:0  
              collisions:0 txqueuelen:1000  
              RX bytes:65725 (64.1 KiB)  TX bytes:24974 (24.3 KiB)  
  
lo     Link encap:Local Loopback  
        inet addr:127.0.0.1  Mask:255.0.0.0  
        inet6 addr: ::1/128 Scope:Host  
              UP LOOPBACK RUNNING  MTU:65536  Metric:1  
              RX packets:44595 errors:0 dropped:0 overruns:0 frame:0  
              TX packets:44595 errors:0 dropped:0 overruns:0 carrier:0  
              collisions:0 txqueuelen:0  
              RX bytes:3029624 (2.8 MiB)  TX bytes:3029624 (2.8 MiB)  
  
wlan0   Link encap:Ethernet  HWaddr 00:0C:43:00:99:E4  
        inet6 addr: fe80::20c:43ff:fea9:99e4/64 Scope:Link  
              UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1  
              RX packets:0 errors:0 dropped:0 overruns:0 frame:0  
              TX packets:0 errors:0 dropped:0 overruns:0 carrier:0  
              collisions:0 txqueuelen:1000  
              RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
```

root@IVWS:~#

3.3.2 Checking the mode of the equipment and TVWS SSID

Type 'iwconfig'

```
root@IVWS:~# iwconfig
root@IVWS:~# iwconfig
lo      no wireless extensions.

eth0    no wireless extensions.

wlan0   RTWIFI SoftAP  ESSID:"IVWS-M1"
        Mode:Managed  Channel=14  Access Point: 00:0C:43:D8:CB:03
        Bit Rate=26 Mb/s
        Link Quality=10/100  Signal level:0 dBm  Noise level:0 dBm
        Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
        Tx excessive retries:0  Invalid misc:0  Missed beacon:0

eth0    no wireless extensions.

br-lan   no wireless extensions.

bond0   no wireless extensions.

root@IVWS:~#
```

```
root@IVWS:~# iwconfig
root@IVWS:~# iwconfig
lo      no wireless extensions.

eth0    no wireless extensions.

wlan0   Ralink STA  ESSID:"TVWS"
        Mode:Auto  Frequency=2.484 GHz  Access Point: Not-Associated
        Bit Rate:1 Mb/s
        RTS thr:off  Fragment thr:off
        Encryption key:off
        Link Quality=10/100  Signal level:0 dBm  Noise level:0 dBm
        Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
        Tx excessive retries:0  Invalid misc:0  Missed beacon:0

eth0    no wireless extensions.

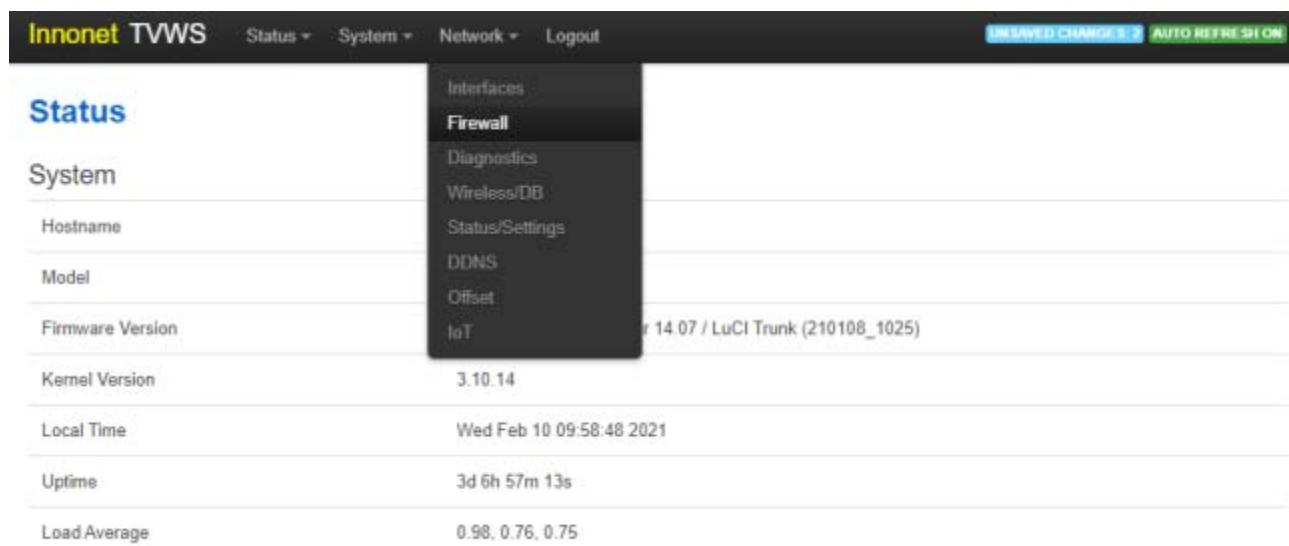
br-lan   no wireless extensions.

bond0   no wireless extensions.

root@IVWS:~#
```

3.3.3 Verify and Modify Port Forwarding Table (Master Equipment)

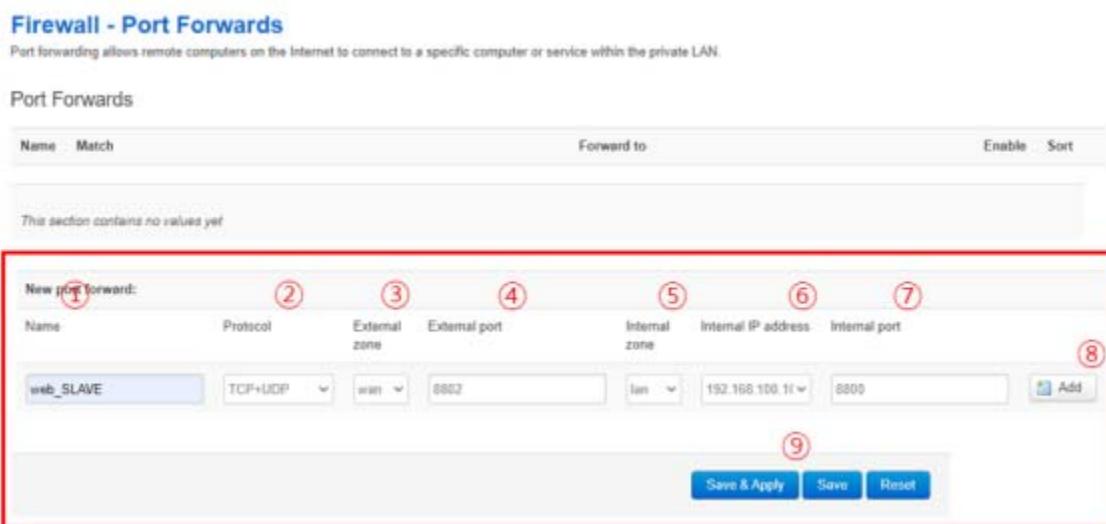
In the WEB UI of the master appliance, select from the Parent Network tab -> Firewall -> Port Forward.



The screenshot shows the Innonet TVWS WEB UI. The top navigation bar includes 'Status', 'System', 'Network', and 'Logout'. A 'UNSAVED CHANGES' button and an 'AUTO REFRESH ON' button are also present. The main content area is titled 'Status' and contains a table with system information. The 'Firewall' tab is selected, and a sub-menu is displayed on the right side of the screen, listing: Interfaces, Firewall, Diagnostics, Wireless/DB, Status/Settings, DDNS, Offset, and IoT. The 'Firewall' option is highlighted with a dark background.

System	
Hostname	innonet-1407
Model	TVWS
Firmware Version	14.07 / LuCI Trunk (210108_1025)
Kernel Version	3.10.14
Local Time	Wed Feb 10 09:58:48 2021
Uptime	3d 6h 57m 13s
Load Average	0.98, 0.76, 0.75

Write the information you want to add sequentially in the Newport forward column, add it, and reboot the equipment.



The screenshot shows the 'Firewall - Port Forwards' page. The table header includes columns for 'Name', 'Match', 'Forward to', 'Enable', and 'Sort'. A message at the top states 'This section contains no values yet'. Below the table, a 'New port forward' form is displayed. The form fields are numbered: 1. Name (web_SLAVE), 2. protocol (TCP+UDP), 3. External zone (wan), 4. External port (8002), 5. Internal zone (lan), 6. Internal IP address (192.168.100.11), 7. Internal port (8000), 8. Add button, and 9. Save & Apply button. A red box highlights the 'New port forward' form and the 'Save & Apply' button.

- ① Name of device and settings to be port forward
- ② Protocol method
- ③ External network
- ④ External Port Settings
- ⑤ Internal network
- ⑥ Address of Internal IP
- ⑦ Internal Port Settings
- ⑧ Added
- ⑨ Save & Apply

3.3.4 Verify and modify port forwarding tables (slave equipment)

Because TVWS G/W does not support NAT features, slave equipment also requires port forwarding.

On the slave appliance, type 'ls' to verify that portconfig exists and enter 'vi /etc/config/portconfig'

You can see that 80 ports of Camera 1 IP 192.168.1.108 are port-forwarded to 10001. 554 port is 20001 port and you can see that it is port forwarding.

To modify port forwarding, press the 'i' key to convert to the input state of the vi editor, press the 'esc' key to release the input state, and type ':wq' to save and exit the editor. If you have nothing to modify or want to leave the editor, type 'q!' and it will leave without saving it.



```
root@TVWS:~# ls
blecheck      ioted      rebootCount      setble_nco      twscheck
bonding       linkcheck  rebootInterval   setfw18      twscheck
conFig_tws.bak  modules    reboot_system    setfw188888    twscheck
dbaccess.lua   mydb      rewatchdog      setfw188888    ver
ops           nms.lua   runningTable.csv  setwatchdog    wldlogfile
ops.sh        notify.lua  rscheck          showpro
hpa          pingcheck   sensor          status
iot.lua      portconfig  setble          tempcheck
root@TVWS:~# vi portconfig
root@TVWS:~#
```

```
SLAVE SYSTEM
# USER NAT PORT FORWARD CONFIGURATION

# IP CAN 1
iptables -t nat -A PREROUTING -i wlan0 -p tcp --dport 10001 -j DNAT --to 192.168.1.108:80
iptables -t nat -A PREROUTING -i wlan0 -p tcp --dport 20001 -j DNAT --to 192.168.1.108:554

# IP CAN 2
iptables -t nat -A PREROUTING -i wlan0 -p tcp --dport 10002 -j DNAT --to 192.168.1.109:80
iptables -t nat -A PREROUTING -i wlan0 -p tcp --dport 20002 -j DNAT --to 192.168.1.109:554

# IP CAN 3
iptables -t nat -A PREROUTING -i wlan0 -p tcp --dport 10003 -j DNAT --to 192.168.1.110:80
iptables -t nat -A PREROUTING -i wlan0 -p tcp --dport 20003 -j DNAT --to 192.168.1.110:554

# IP CAN 4
iptables -t nat -A PREROUTING -i wlan0 -p tcp --dport 10004 -j DNAT --to 192.168.1.111:80
iptables -t nat -A PREROUTING -i wlan0 -p tcp --dport 20004 -j DNAT --to 192.168.1.111:554

# IP CAN 5
iptables -t nat -A PREROUTING -i wlan0 -p tcp --dport 10005 -j DNAT --to 192.168.1.112:80
iptables -t nat -A PREROUTING -i wlan0 -p tcp --dport 20005 -j DNAT --to 192.168.1.112:554

# IP CAN 6
iptables -t nat -A PREROUTING -i wlan0 -p tcp --dport 10006 -j DNAT --to 192.168.1.113:80
iptables -t nat -A PREROUTING -i wlan0 -p tcp --dport 20006 -j DNAT --to 192.168.1.113:554

# IP CAN 7
iptables -t nat -A PREROUTING -i wlan0 -p tcp --dport 10007 -j DNAT --to 192.168.1.114:80
iptables -t nat -A PREROUTING -i wlan0 -p tcp --dport 20007 -j DNAT --to 192.168.1.114:554

# IP CAN 8
iptables -t nat -A PREROUTING -i wlan0 -p tcp --dport 10008 -j DNAT --to 192.168.1.115:80
iptables -t nat -A PREROUTING -i wlan0 -p tcp --dport 20008 -j DNAT --to 192.168.1.115:554

# WiFi Web
iptables -t nat -A PREROUTING -i wlan0 -p tcp --dport 9000 -j DNAT --to 192.168.1.127:80
~  
~  
~  
~  
- /etc/config/portconfig 1/37 2%
```

3.3.5 Check equipment rssi – iwpriv wlan. entering zero British stat

To check the RSSI and MCS of the equipment, enter 'iwpriv wlan0 stat'.

```
root@IVWS: ~
root@IVWS: ~
root@IVWS: ~ iwpriv wlan0 stat
wlan0  stat:
Tx success          = 1824
Tx fail count      = 3431, PER=77.0%
Rx success          = 17827
Rx with CRC         = 77704, PER=82.0%
Rx with PhyErr       = 0
Rx with PileErr      = 0
Rx drop due to out of resource = 0
Rx duplicate frame   = 0
False CCA           = 0
RSSI                 = -60 0 0
Last TX Rate         = MCS9, 20M, SGI, CCK
Last RX Rate         = MCS9, 40M, SGI, CCK
TX AGG Range 1 (1)   = 4126
TX AGG Range 2 (2~5) = 221
TX AGG Range 3 (6~15) = 1
TX AGG Range 4 (>15) = 0
HMPDU Tx success    = 1018
HMPDU Tx fail count = 3697, PER=78.1%
```

```
root@IVWS: ~ iwpriv wlan0 stat
wlan0  stat:
Tx success          = 1327
Tx fail count      = 11326, PER=89.5%
Rx success          = 7761
Rx with CRC         = 24979, PER=76.3%
Rx drop due to out of resource = 0
Rx duplicate frame   = 0
False CCA           = 0
RSSI                 = -45 -99 -99
Last TX Rate         = MCS8, 20M, SGI, CCK
Last RX Rate         = MCS7, 40M, SGI, CCK
TX AGG Range 1 (1)   = 9542
TX AGG Range 2 (2~5) = 2525
TX AGG Range 3 (6~15) = 52
TX AGG Range 4 (>15) = 0
HMPDU Tx success    = 1338
HMPDU Tx fail count = 14590, PER=91.6%
SNR-A                = 0
SNR-B (if available) = 0
IpaSupplicantUP       = 1
```

3.3.6 Verify Equipment Throughput

iperf requires a server and a client. Entering 'iperf -s -i1' means that the equipment entered will become the iperf server and display the value every second. By typing 'iperf -c 192.168.100.1 -i1', it means that the equipment entered will become an iperf client and display what was sent to the server IP 192.168.100.1 every second. By default, the appliance is supposed to run the iperf server process, so you only need to enter the client. You can enter 'ps' to verify that the 'iperf -s' process is working.

```
152 root 0 S/R (kmod)
153 root 0 S/R (inet/igp_neigh)
254 root 0 S/R (cryptof)
257 root 0 S/R (defnames)
258 root 0 S/R (kuerken/2:1)
259 root 0 S/R (kuerken/3:1)
260 root 0 S/R (kuerken/1:1)
270 root 0 S/R (kuerken/2:10)
289 root 0 S/R (jffn2_gcd_mtd61)
324 root 0 S/R (kuerken/2:2)
325 root 0 S/R (kuerken/3:2)
476 root 0 S /sbin/dkmsd
479 root 768 S /sbin/akfd inst 11491 /bin/ash --login
600 root 0 S/R (bcm0)
675 root 3004 S /sbin/led -d 2048
836 root 3245 S /usr/sbin/dhcpd
941 root 0 S/R (kuerken/0:2)
945 root 0 S/R (kuerken/1:2)
1000 root 1348 S /usr/sbin/dropbear -F -p /var/run/dropbear.l.pid -p 2249 -K 300
1052 root 1532 S /usr/sbin/udhtpd -t -b /var -r TMS -w /opt-bin -s /dbs -d 60 -T 10 -k 20 -d 1 -w 3 -s 100 -F -p 6.6.6.6:8000 -g 1:1:00
1120 root 2492 S /usr/sbin/ntpd -n -p 3.openmt.pool.ntp.org -p 1.openmt.pool.ntp.org -p 2.openmt.pool.ntp.org -p 3.openmt.pool.ntp.org
1231 root 0 S/R (kuerken/0:2)
1257 root 12908 S /bin/twink
1258 root 3268 S /bin/tunnel
1259 root 3204 S iperf -s
1271 root 768 S uschedog
1279 root 0 S/R (kuerken/0:10)
1293 root 0 S/R (kuerken/1:10)
1329 root 9608 S /sbin/netfilter
1390 root 0 S/R (RtmpLiverTask)
1393 root 0 S/R (RtmpCloudTask)
1394 root 0 S/R (RtmpRliveTask)
2236 root 1492 S udhcpc -g /var/run/udhcpc/wh1.gid -s /lib/netifd/dhcpc.script -t -t 0 -i eth0 -f
2271 nobody 900 S /usr/sbin/dnsmasq -C /var/etc/dnsmasq.conf -k
2900 root 3560 S curl -s -o /dev/null -X POST -d https://230.111.0.11:9443/ntp.ctx.net -H Content-Type: application/json -H Accept: */*
3044 root 3216 S /usr/sbin/dropbear -F -p /var/run/dropbear.l.pid -p 2249 -K 300
3026 root 2496 S -ash
3219 root 1492 S ps
```

```

Rx duplicate frame          = 0
False CCA                  = 0
RSSI                       = -60 0 0
Last TX Rate                = MCS9, 20M, SGI, CCK
Last RX Rate                = MCS9, 40M, SGI, CCK
TK AGG Range 1 (1)          = 4126
TK AGG Range 2 (2-5)         = 221
TK AGG Range 3 (6-15)        = 1
TK AGG Range 4 (>15)         = 0
AMPDU Tx success           = 1818
AMPDU Tx fail count         = 3637, PER=78.1%
root@TVWS:~#
root@TVWS:~#
root@TVWS:~#
root@TVWS:~#
root@TVWS:~# iperf -c 192.168.100.100 -i1
-----
Client connecting to 192.168.100.100, TCP port 5001
TCP window size: 28.7 KByte (default)
[  3] local 192.168.100.1 port 48448 connected with 192.168.100.100 port 5001
[ ID] Interval           Transfer     Bandwidth
[  3]  0.0- 1.0 sec   256 KBytes   2.10 Mbits/sec
[  3]  1.0- 2.0 sec   768 KBytes   6.29 Mbits/sec
[  3]  2.0- 3.0 sec   1.63 MBytes  13.6 Mbits/sec
[  3]  3.0- 4.0 sec   1.25 MBytes  10.5 Mbits/sec
[  3]  4.0- 5.0 sec   1.13 MBytes  9.44 Mbits/sec
[  3]  5.0- 6.0 sec   1.50 MBytes  12.6 Mbits/sec
[  3]  6.0- 7.0 sec   1.75 MBytes  14.7 Mbits/sec
[  3]  7.0- 8.0 sec   768 KBytes   6.29 Mbits/sec
[  3]  8.0- 9.0 sec   2.00 MBytes  16.8 Mbits/sec
[  3]  9.0-10.0 sec  1.13 MBytes  9.44 Mbits/sec
[  3]  0.0-10.2 sec  12.3 MBytes  10.1 Mbits/sec
root@TVWS:~# 

```

```

[  3] local 192.168.100.1 port 48448 connected with 192.168.100.100 port 5001
[ ID] Interval           Transfer     Bandwidth
[  3]  0.0- 1.0 sec   512 KBytes   4.19 Mbits/sec
[  3]  1.0- 2.0 sec   1.00 MBytes  9.39 Mbits/sec
[  3]  2.0- 3.0 sec   1.13 MBytes  9.44 Mbits/sec
[  3]  3.0- 4.0 sec   1.13 MBytes  9.44 Mbits/sec
[  3]  4.0- 5.0 sec   1.00 MBytes  9.39 Mbits/sec
[  3]  5.0- 6.0 sec   1.25 MBytes  10.5 Mbits/sec
[  3]  6.0- 7.0 sec   1.13 MBytes  9.44 Mbits/sec
[  3]  7.0- 8.0 sec   1.38 MBytes  11.5 Mbits/sec
[  3]  8.0- 9.0 sec   1.13 MBytes  9.44 Mbits/sec
[  3]  9.0-10.0 sec  1.38 MBytes  11.5 Mbits/sec
[  3]  0.0-10.1 sec  11.1 MBytes  9.21 Mbits/sec
root@TVWS:~#
root@TVWS:~#
root@TVWS:~#
root@TVWS:~#
root@TVWS:~# iperf -c 192.168.100.1 -i1
-----
Client connecting to 192.168.100.1, TCP port 5001
TCP window size: 28.7 KByte (default)
[  3] local 192.168.100.100 port 41169 connected with 192.168.100.1 port 5001
[ ID] Interval           Transfer     Bandwidth
[  3]  0.0- 1.0 sec   512 KBytes   4.19 Mbits/sec
[  3]  1.0- 2.0 sec   1.00 MBytes  9.39 Mbits/sec
[  3]  2.0- 3.0 sec   1.13 MBytes  9.44 Mbits/sec
[  3]  3.0- 4.0 sec   1.13 MBytes  9.44 Mbits/sec
[  3]  4.0- 5.0 sec   1.00 MBytes  9.39 Mbits/sec
[  3]  5.0- 6.0 sec   1.25 MBytes  10.5 Mbits/sec
[  3]  6.0- 7.0 sec   1.13 MBytes  9.44 Mbits/sec
[  3]  7.0- 8.0 sec   1.38 MBytes  11.5 Mbits/sec
[  3]  8.0- 9.0 sec   1.13 MBytes  9.44 Mbits/sec
[  3]  9.0-10.0 sec  1.38 MBytes  11.5 Mbits/sec
[  3]  0.0-10.1 sec  11.1 MBytes  9.21 Mbits/sec
root@TVWS:~# 

```