CreatComm

CForce N100

Wireless CPE

Intelligent Rate Control

ACK Time-out Adjustment

2x2 MiMo

High Throughput

Long Distance Coverage

PTP

TDMA

Hardware Watchdog

Catalog

Purpose

This document is proposed for the users of CFORCE N100 devices, helping them to configure the device and list the troubleshooting, so that the devices can be used successfully quickly.

This document mainly contains the following parts: hardware information, web configuration menu descriptions, network configuration examples, and troubleshooting. It can help the customers quickly be familiar with the devices and use them correctly.

Definitions

No.	Items	Description
1	CFORCE N100	Outdoor, long distance CPE/Bridge devices by CreatComm Technologies Inc.
2	VTrans	VTrans is a series of wireless technologies, developed and patented by Creatcomm, including TDMA, 20M/40MHz bandwidth support, intelligent rate control, Auto ACK Time-out adjust, having the advantage of long transmission range, high date rate and robust transmission.
3	Station(Client)	WIFI station that can be associated to an access point.

1 Product Overview

CFORCE N100 is a powerful wireless broadband access and transmission product. It has built-in VTrans wireless technology, which combines industry-leading core technologies with long transmission distance, high throughput and strong anti-interference.

VTrans technology includes TDMA, 10M/20M/40MHz bandwidth flexible configuration, rate control, ACK timeout automatic adjustment and other technologies. TDMA effectively solves the hidden node problem that is often encountered in large point-to-multipoint WLANs. The 10M/20M/40MHz bandwidth flexible configuration balances between the scarce wireless bandwidth resources and complex work scenarios. Advanced rate control algorithms keep the rate as stable as possible while quickly adapting to channel quality variations. The ACK timeout automatic adjustment technology automatically detects the distance between the access point and the station, and adjusts the wireless parameters to optimize the performance of the device.

The CFORCE N100 has a maximum transmission rate of 300Mbps and has excellent long-distance transmission performance for transmitting multiple HD videos. It can be used as a point-to-point and point-to-multipoint remote access wireless bridge, the last 1 km access to rural wireless broadband.

1. 1 Electrical Specifications

The electrical specifications are shown are the following table:

Table 1-1 Electrical Specifications

Wireless	Items	Specifications
	Standard	IEEE802.11 a/n
	Operation Frequency	5150~5350 MHz, 5470~5875 MHz
	Antenna gain	10dBi
	Beam Width	H: 65°, V:18°
	Max Power	24dBm
	Receive Sensitivity	-85dBm@MCS0，-85dBm@6Mbps

	Max Transmission Rate	300Mbps
Hardware	Power requirement	24V PoE
	Physical Interface	10/100M Base-TX (Cat. 5/5E, RJ-45) ×2
	LED indicator	Power, LAN, WLAN, Signal strength indicator
	Working temperature	-30℃~70℃
	Storage temperature	-40℃~85℃
	Working humidity	5%~95%RH Non-condensing
	Equipment size	45.5x98.8x200 mm
Software	Encryption	WPA-PSK/WPA2-PSK/802.1x
	Network mode	Bridge/ Router
	Operating mode	Station, WDS Access point, WDS Station
	Security	IP/MAC filter, SSID hidden
	Network Protocol	TCP/UDP/ARP/ICMP/DHCP/HTTP/NTP
	TDMA	Supported
	Auto ACK Timing Adjust	Supported
	Management and Logs	NTP, SNMP, Syslog, AC
	Configuration management	Support web page configuration, support AC remote configuration, support SNMP management
	Firmware update	Support web page update, support AC remote upgrade
	Bandwidth Supported	20M/40MHz

1. 2 Features

- High-performance 802.11n 2X2 MIMO chip with a maximum speed of 300Mbps.
- Supports 4 working modes: Access point, Station, WDS Access point, WDS Station.
- The product uses the core VTrans technology, including TDMA, intelligent

rate control, automatic ACK timeout adjustment and other technologies.

- TDMA protocol overcomes the inherent hidden node problem of 802.11, making the product have better long-distance, point-to-multipoint performance.
- Support point-to-point or point-to-multipoint transmission.
- Unique antenna, RF amplifier, low noise receiver design to ensure the reliability of long-distance video, voice and data transmission.
- Customize common scenes and working modes for users to use and assemble for non-professionals.
- Unique TDMA technology can maximize the use of bandwidth resources to better support point-to-multipoint data transmission.
- Supports 802.3af standard PoE power supply.
- Support remote control and management

1. 3 Hardware Overview

The simple hardware information for CFORCE N100 is shown in the following table:

Table 1-2 Hardware Specifications

Hardware Specifications	
CPU/Baseband Radio	AR9344
Memory	64MB DRAM, 8MB Flash
Physical Interface	2×10/100M Base-TX (Cat. 5/5E, RJ-45) Ports
LED indicator	Power, LAN, WLAN, Signal strength indicator
Power supply	24V PoE

2 Installation

In different network modes, the line connection mode of CFORCE N100 is different. Since the device is set to the bridge mode by default, this chapter mainly describes the line connection mode of the bridge mode.

2. 1 Connections and installation

The installation of CFORCE N100 is shown below:

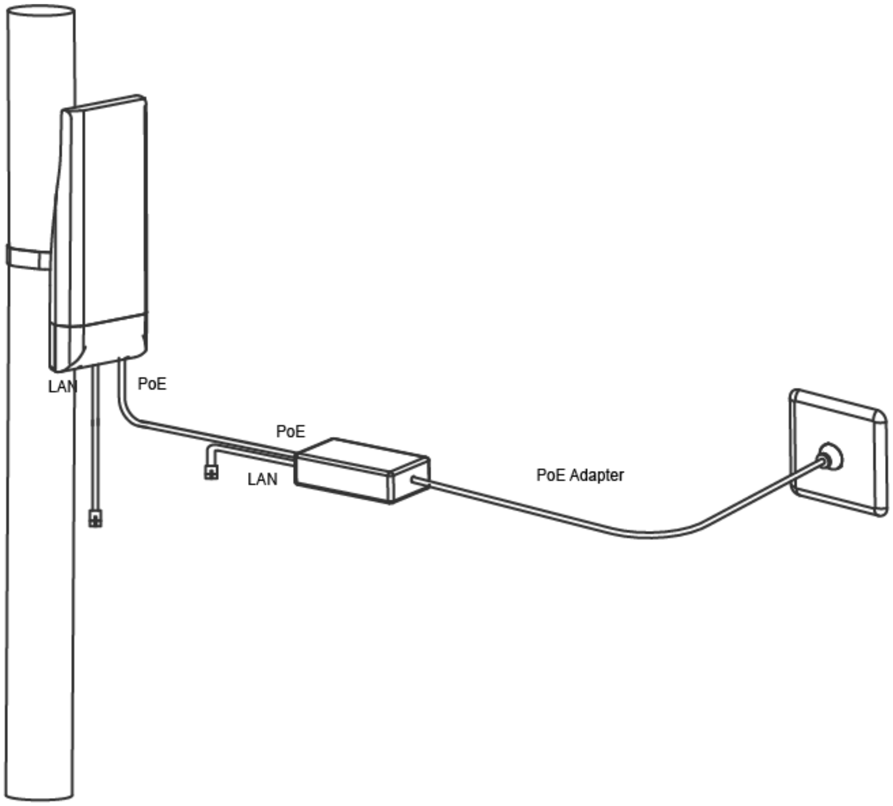


Figure 2-1 Line connection

The CFORCE N100 device has two network ports (RJ45 ports) labeled "PoE" and "LAN" ports. Because the device defaults to the bridge mode, the PoE interface is connected to the PoE power port with the PoE type on the network cable to provide 24V power and data connection to the CFORCE N100 device. The LAN port of the device can be used to connect to the IP camera. Such as video surveillance applications and other equipment. In general data communication applications, the "LAN" port of the device is usually not connected to any device.

2. 2 Restore to the Factory Settings

When the user forgets the IP of CFORCE N100, the webpage of CFORCE N100 cannot be opened again. In this case, we choose manual operation, as shown in the figure below, hold down the Reset button for 5-10 seconds, and wait until all the LED lights are on, you can loose on, the device has been restored to the default factory settings. At the same time, the network port of the host directly connected to CFORCE N100 will display two consecutive connections and disconnections.

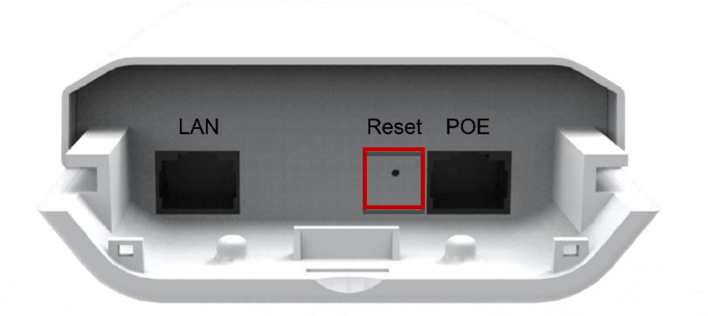


Figure 2-2 Restore to the factory settings

The main parameters of the default factory settings of CFORCE N100 are as follows:

Table 2-1 Main parameters at the factory settings

Items	Default Settings
IP address	192.168.1.36
User name	admin
Password	admin

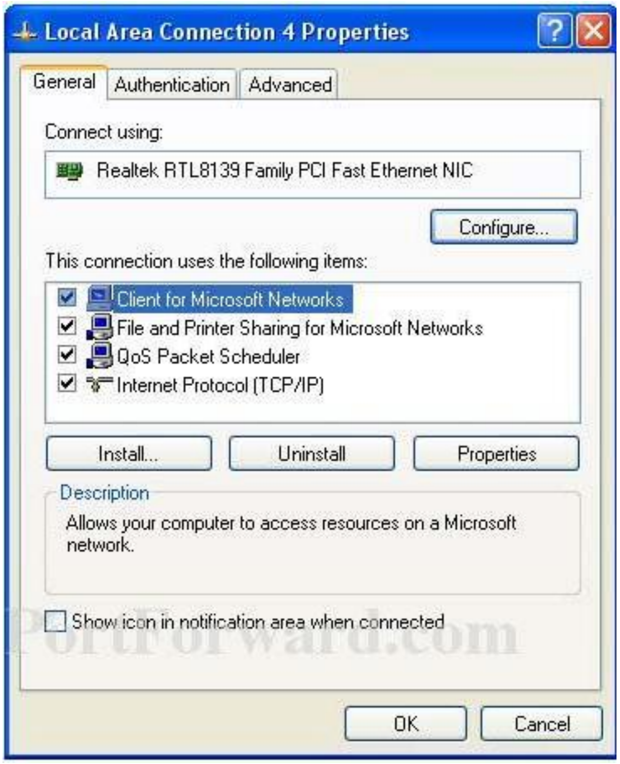
3 Quick Configuration

This chapter describe how to configure the device quickly.

3. 1 Log in

To log in the CFORCE N100 device, user needs to configure the TCP/IP of your computer first as the following steps:

1. Right click Local Area Connection icon of your computer and click properties, then click Continue, the Local Area Connection Properties dialog box appears as Figure 3-1.



Local Area Connection 4 Properties

Connect using:

Realtek RTL8139 Family PCI Fast Ethernet NIC

This connection uses the following items:

☑ Client for Microsoft Networks
☑ File and Printer Sharing for Microsoft Networks
☑ QoS Packet Scheduler
☑ Internet Protocol (TCP/IP)

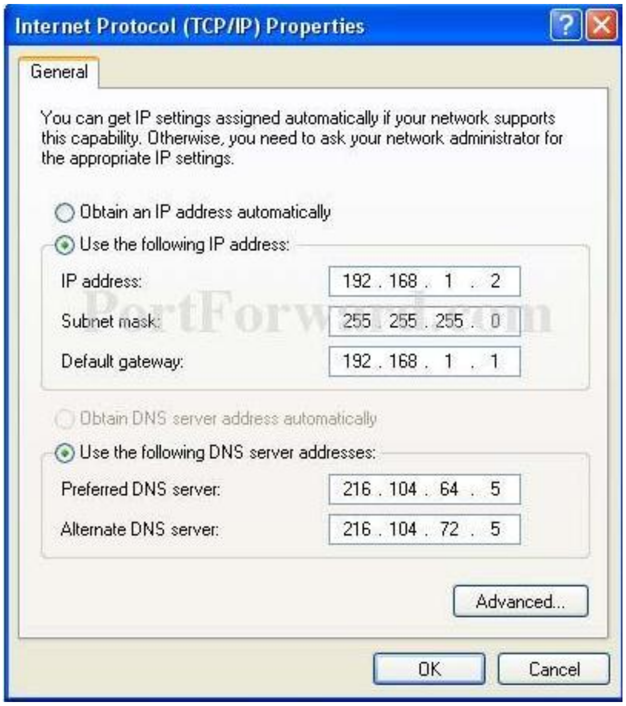
Description

Allows your computer to access resources on a Microsoft network.

□ Show icon in notification area when connected

Figure 3-1 Local Area Connection Properties

2. Select Internet Protocol (TCP/IP) and click Properties button, and the following dialog box appear:



Internet Protocol (TCP/IP) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 1 . 2

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 192 . 168 . 1 . 1

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: 216 . 104 . 64 . 5

Alternate DNS server: 216 . 104 . 72 . 5

Figure 3-2 IP settings

3. In the above Figure 3-2, IP address should be set to 192.168.1.*, here * can be a number between 1-255 (but not 36) since the CFORCE N100 default IP address is 192.168.1.36.

4. Enter the IP address of CFORCE N100 in the browser, and then press the Enter key to jump to the following login interface:

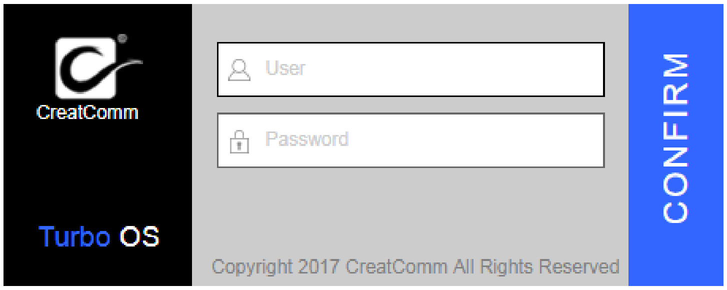


Figure 3-3 CFORCE N100 login interface

5. Enter the user name and password corresponding to CFORCE N100 in the page username and password as shown above, and click Login to log in to CFORCE N100.

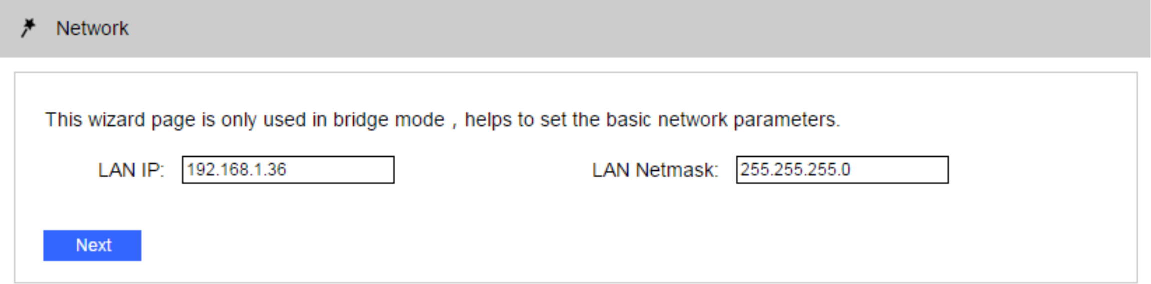
3. 2 Wizard

Users can quickly configure the device through the setup wizard according to the steps in this section.

1. The first page shown after log in is the Status page, which indicates the working status, current setting, software version and other information of the CFORCE N100 device. Users can switch to other pages by clicking the left main menus.

2. Click Wizard menu, the users can configure the device quickly, including Network and Wireless settings and so on. It is Wizard-Network page as shown in Figure 3-4, and this page helps to set the basic network parameters. The default mode is Bridge mode, and the default LAN IP address is 192.168.1.36. If the user wants to configure the device to Router mode, please click Network in the main menu.

Note: If several CFORCE N100 devices are connected in the Point-to-Point or Point-to-Multi-Point topologies, they must be configured to different IP address to avoid collisions.



This wizard page is only used in bridge mode，helps to set the basic network parameters.

LAN IP: 192.168.1.36

LAN Netmask: 255.255.255.0

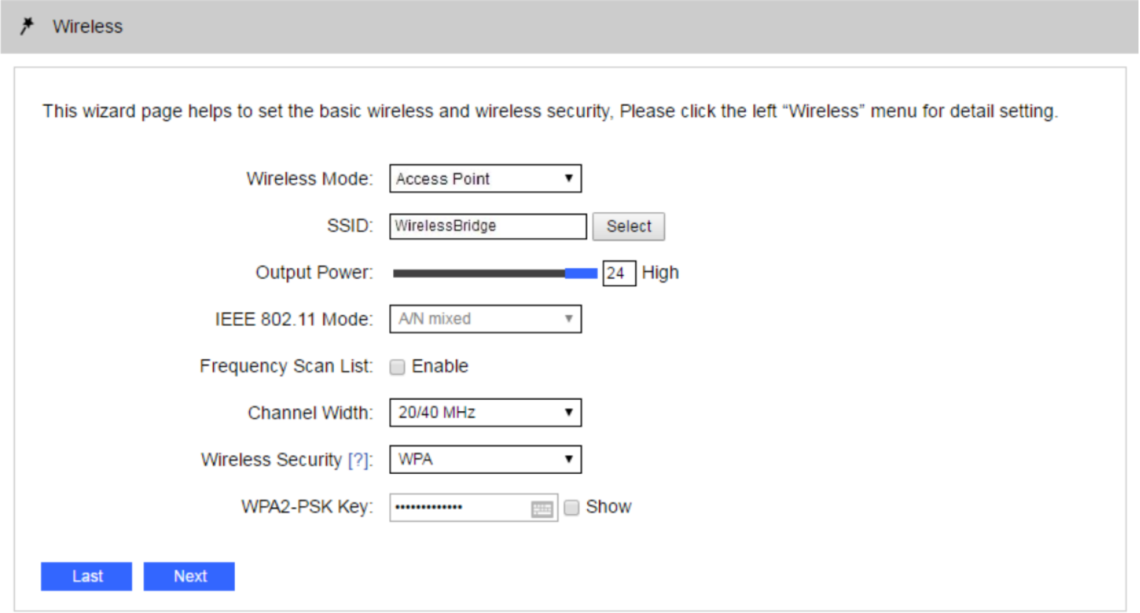
Figure 3-4 Wizard Network

3. Click "Next" to display the basic wireless parameter configuration and wireless encryption options, as shown below. The two most common wireless modes for CFORCE N100 devices are the “Station” and “Access Point."

Station mode: The device acts as a WIFI station, and it can be connected to a normal home access point or CFORCE N100 access point.

Access Point mode: The CFORCE N100 device can be connected to a normal wireless network card or to a CFORCE N100 device in “Station” mode. The premise is that the wireless encryption options and SSID of both sides of the wireless connection are configured consistently. For other detailed wireless configurations, please click on the "Wireless Settings" menu on the left.

Note: If two CFORCE N100 devices need to be connected in point-to-point topology, one of the device need to be configured as Access Point, and the other one need to be configured as Station, and both of them should have the same Encryption method.



This wizard page helps to set the basic wireless and wireless security, Please click the left "Wireless" menu for detail setting.

Wireless Mode: Access Point

SSID: WirelessBridge

Output Power: 24 High

IEEE 802.11 Mode: A/N mixed

Frequency Scan List: □ Enable

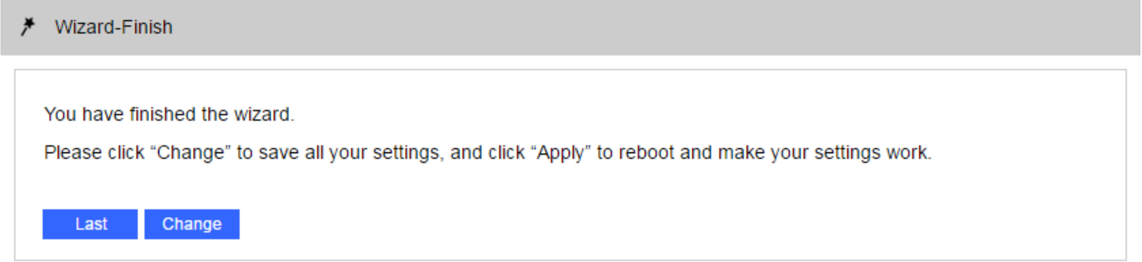
Channel Width: 20/40 MHz

Wireless Security [?]: WPA

WPA2-PSK Key: ••••••••••••• □ Show

Figure 3-5 Wizard - Wireless

4. The last page of Wizard is shown in Figure 3-6. User can click Change to save all the settings, and then click Apply the make the setting effective, or click last to modify the previous settings.



You have finished the wizard.

Please click "Change" to save all your settings, and click "Apply" to reboot and make your settings work.

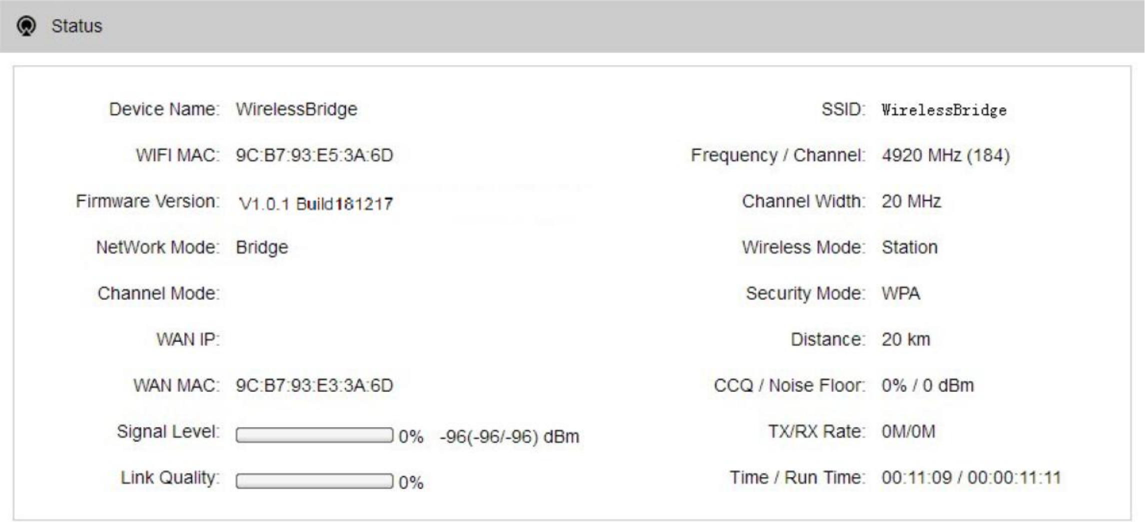
Figure 3-6 Wizard-Finish

4 Status

Status shows the current configuration and real-time monitoring of the device. This page is divided into 2 parts: Status and Monitor.

4. 1 Status

The status page is shown in the following Figure：

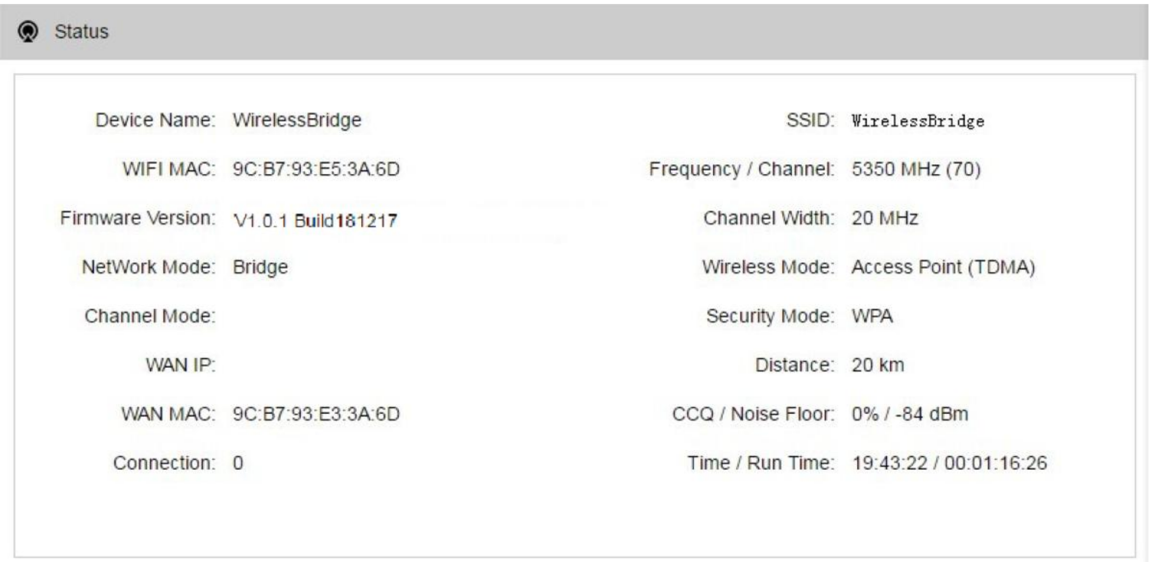


Status

Device Name: WirelessBridge
WIFI MAC: 9C:B7:93:E5:3A:6D
Firmware Version: V1.0.1 Build181217
NetWork Mode: Bridge
Channel Mode:
WAN IP:
WAN MAC: 9C:B7:93:E3:3A:6D
Signal Level: 0% -96(-96/-96) dBm
Link Quality: 0%

SSID: WirelessBridge
Frequency / Channel: 4920 MHz (184)
Channel Width: 20 MHz
Wireless Mode: Station
Security Mode: WPA
Distance: 20 km
CCQ / Noise Floor: 0% / 0 dBm
TX/RX Rate: 0M/0M
Time / Run Time: 00:11:09 / 00:00:11:11

Figure 4-1 Status-Station



Status

Device Name: WirelessBridge
WIFI MAC: 9C:B7:93:E5:3A:6D
Firmware Version: V1.0.1 Build181217
NetWork Mode: Bridge
Channel Mode:
WAN IP:
WAN MAC: 9C:B7:93:E3:3A:6D
Connection: 0

SSID: WirelessBridge
Frequency / Channel: 5350 MHz (70)
Channel Width: 20 MHz
Wireless Mode: Access Point (TDMA)
Security Mode: WPA
Distance: 20 km
CCQ / Noise Floor: 0% / -84 dBm
Time / Run Time: 19:43:22 / 00:01:16:26

Figure 4-2 Status-AP

All the configurations in Status page is shown in Table 4-1.

Table 4-1 Configurations shown in Status

Items	Description	Items	Description
Device Name	Name of the device , for example:	SSID	The name of the wireless network

	WirelessBridge		
WIFI MAC	MAC of the wireless port	Frequency/Channel	Wireless channel chosen
Firmware Version	Software version number	Channel Width	10MHz/20MHz/40MHz
Network Mode	Network mode: Router or Bridge	Wireless Mode	Access Point, Station, WDS Access Point, WDS Station, WDS repeater
Channel Mode	Wireless communication protocol, for example, 11 a/n	Security Mode	Wireless encryption method
WAN IP	WAN IP address	Distance	The distance between two associated devices
WAN MAC	MAC of the WAN port	CCQ/Noise Floor	CCQ: Station link quality, the general recommended value of 90% or more, when the CCQ shows less than 90%, the user may consider to take the appropriate method to improve the link quality (Such as changing the environment, channel, etc.) Noise Floor: Noise Floor value, in order to achieve the best equipment, it is generally recommended at least less than -95dBm noise in the use of the environment.

Signal Level(Only the station page is displayed)	It indicates the signal strength of the device, recommended signal strength of 60% or more (or -30dBm ~ -60dBm), when the signal strength is less than 25%, the display bar turns red	TX/RX Rate(Only the station page is displayed)	The date rate of current device during sending and receiving data
Link Quality(Only the station page is displayed)	Quality of the connection link, the recommended value is more than 60%, when the display is less than 25%, the display turns red	Time/Run Time	Time: The real-time. Run Time: Equipment running time.
Connection(Only the AP page is displayed)	The number of station devices that the device is connected to		

4. 2 Monitor

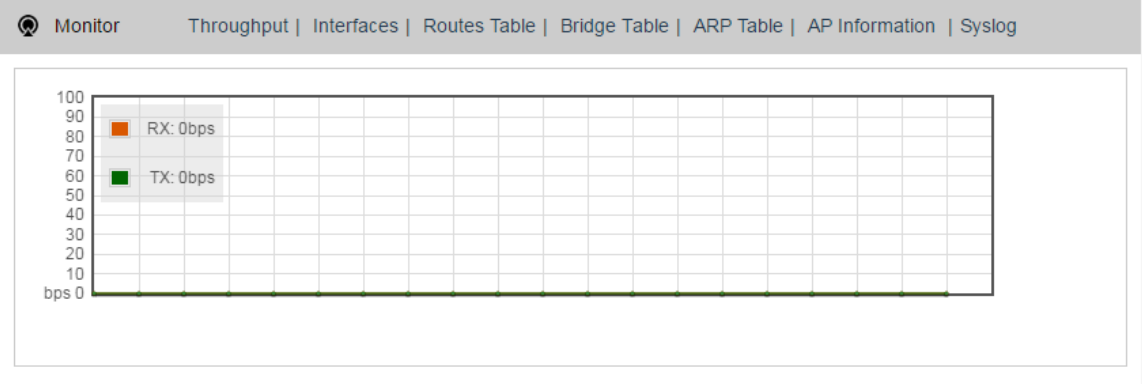

Monitor
Throughput | Interfaces | Routes Table | Bridge Table | ARP Table | AP Information | Syslog
100
90
80
70
60
50
40
30
20
10
bps 0
🟥 RX: 0bps
🟩 TX: 0bps

Figure 4-3 Monitor

Throughput: Refers to the amount of data passing through each section per unit time. The throughput rate of the status display page is used to refer to the amount of data transmitted over the network per unit time. It is the main indicator for measuring network performance. Through it, users can monitor the speed of data transmission by the device in real time.

Interfaces: Device interface MAC address, MTU, IP, RX Bytes, RX Errors, TX Bytes, and TX Errors.

Routes Table: It is stored in a router that lists the routes to particular network destinations, and in some cases, metrics (distances) associated with those routes. The route table contains information about the topology of the network immediately around it.

Bridge Table: It lists all the devices that communicate through the CFORCE N100 device.

ARP Table: It lists the IP address and MAC address of the devices that communicate through the LAN port of the CFORCE N100 device.

AP/Station Information: Showing the status information of the associated devices. For example, if the CFORCE N100 device is an AP, and the associated device is a Station, and this Station Information shows the related information of the Station device. If the CFORCE N100 is a Station, and AP Information shows the associated AP device's information.

Syslog: Display the log information of CFORCE N100.

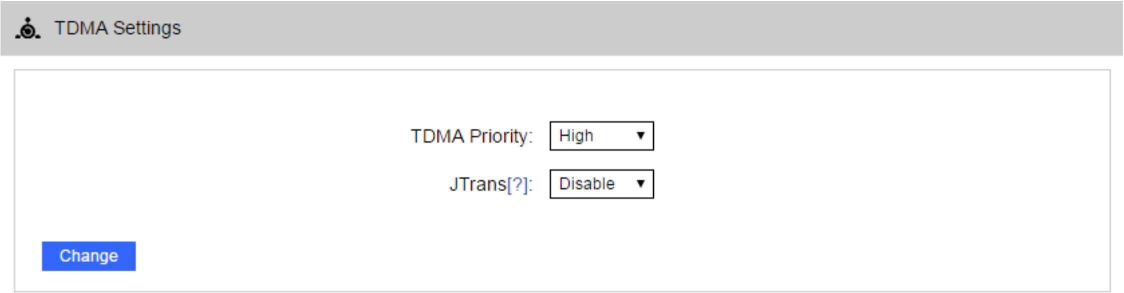
5 TDMA

Currently, most of the outdoor bridge products are developed based on 802.11 protocols, however, it has the limitations of short-distance, hidden node problems, and poor point-to-multi-point performance.

VTrans technology is developed and patented by CreatComm, utilizing a series of advanced technologies such as TDMA, 10M/20M/40MHz bandwidth support, intelligent rate control, Auto ACK Time-out Adjust, having the advantage of long transmission range, high date rate and robust transmission.

TDMA technology solves the problems of hidden-node problem in the 802.11 network infra-structure. 10M/20M/40MHz bandwidth can be flexibly configured by the uses in different working scenario to achieve the best link quality. Intelligent rate control algorithm can be adapted to quick channel quality variations, while stabilize the wireless throughput, thus suitable for long-distance transmission. ACK Time-out Auto Adjust can automatically detect the distances of the CFORCE N100 devices, and adjust the wireless parameters to achieve the best link quality.

The TDMA setting is shown in the following figure.



TDMA Settings

TDMA Priority: High

JTrans[?]: Disable

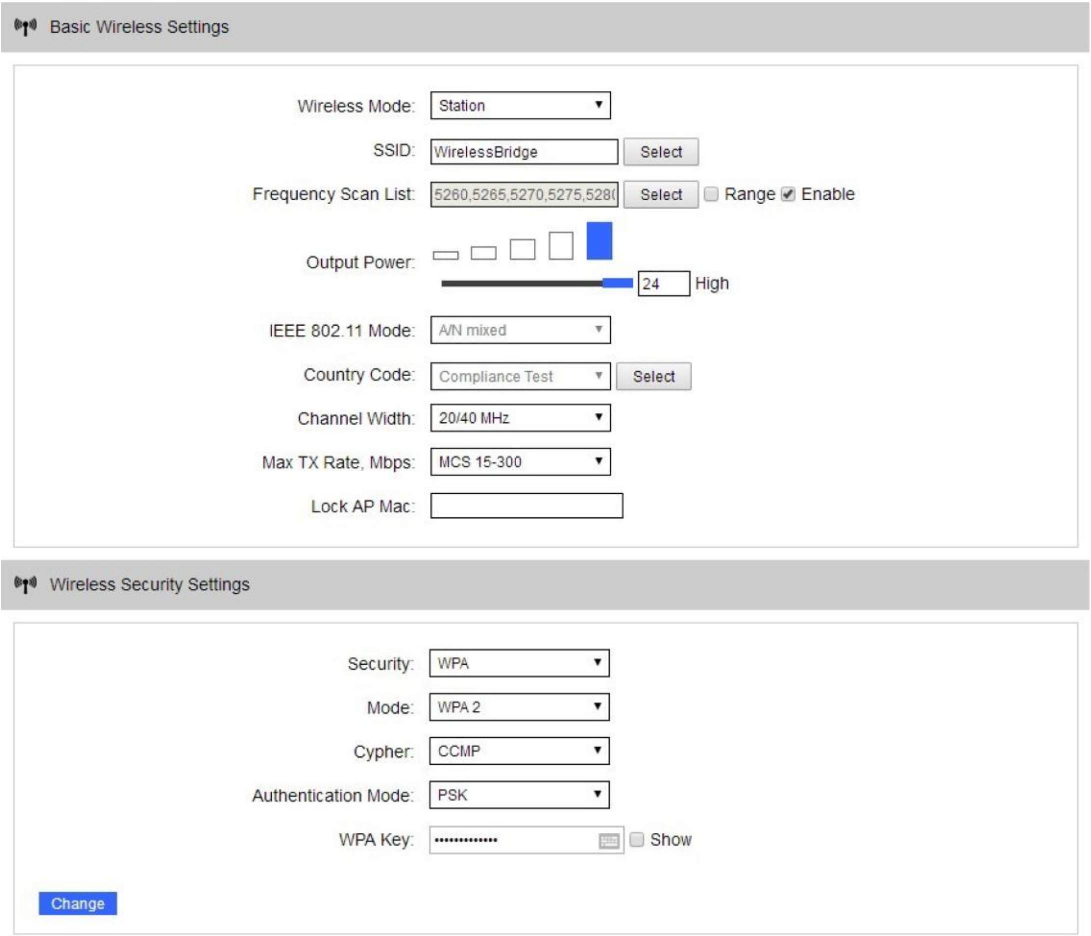
Figure 5-1 TDMA

To use the TDMA, the user needs to enable TDMA mode in the AP device, and set a priority level in the station device. When several stations are connected to one AP, different stations demand different throughput. If the station demands higher throughput, its priority level can be set to High, otherwise set to Low. When the stations demand the same throughput, their priority level can be set to the same level.

Note: When using TDMA mode, the TDMA button need to be enabled at both AP and station devices in the web-based configuration menu. The devices from other vendors cannot be connected to CFORCE N100 in the TDMA mode.

6 Wireless

The wireless settings pages are shown below:



Basic Wireless Settings

Wireless Mode: Station

SSID: WirelessBridge Select

Frequency Scan List: 5260,5265,5270,5275,528(Select □ Range ☑ Enable

Output Power: 24 High

IEEE 802.11 Mode: A/N mixed

Country Code: Compliance Test Select

Channel Width: 20/40 MHz

Max TX Rate, Mbps: MCS 15-300

Lock AP Mac:

Wireless Security Settings

Security: WPA

Mode: WPA 2

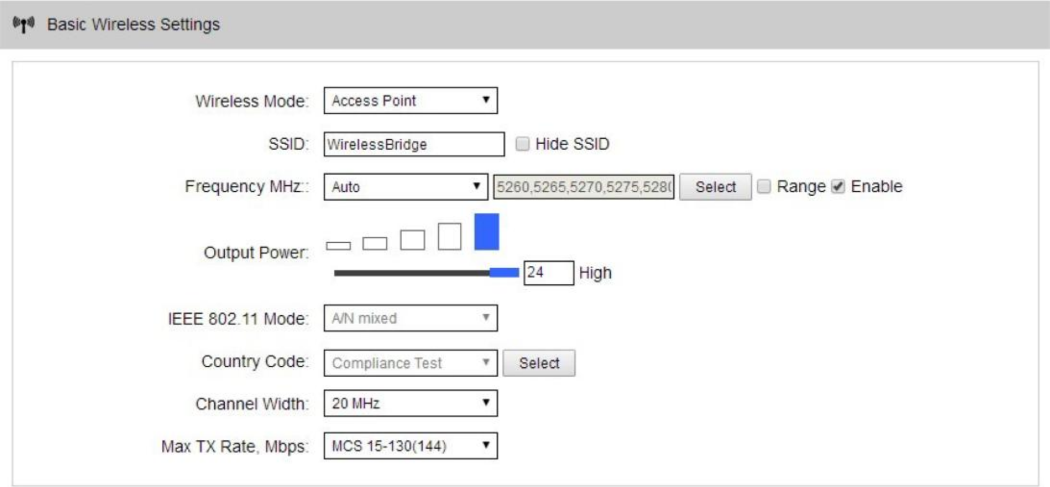
Cypher: CCMP

Authentication Mode: PSK

WPA Key: ••••••••••••• □ Show

Change

Figure 6-1 Wireless-Station



Basic Wireless Settings

Wireless Mode: Access Point

SSID: WirelessBridge □ Hide SSID

Frequency MHz:: Auto 5260,5265,5270,5275,528(Select □ Range ☑ Enable

Output Power: 24 High

IEEE 802.11 Mode: A/N mixed

Country Code: Compliance Test Select

Channel Width: 20 MHz

Max TX Rate, Mbps: MCS 15-130(144)

Figure 6-2 Wireless-AP

Wireless Mode: There are totally 4 wireless modes, including: Station, Access Point, WDS Station, and WDS Access Point.

Access point: The wireless access node, the station device connects to it, the station device can be a computer, a mobile phone, a wireless bridge, etc., and an AP can connect to multiple stations.

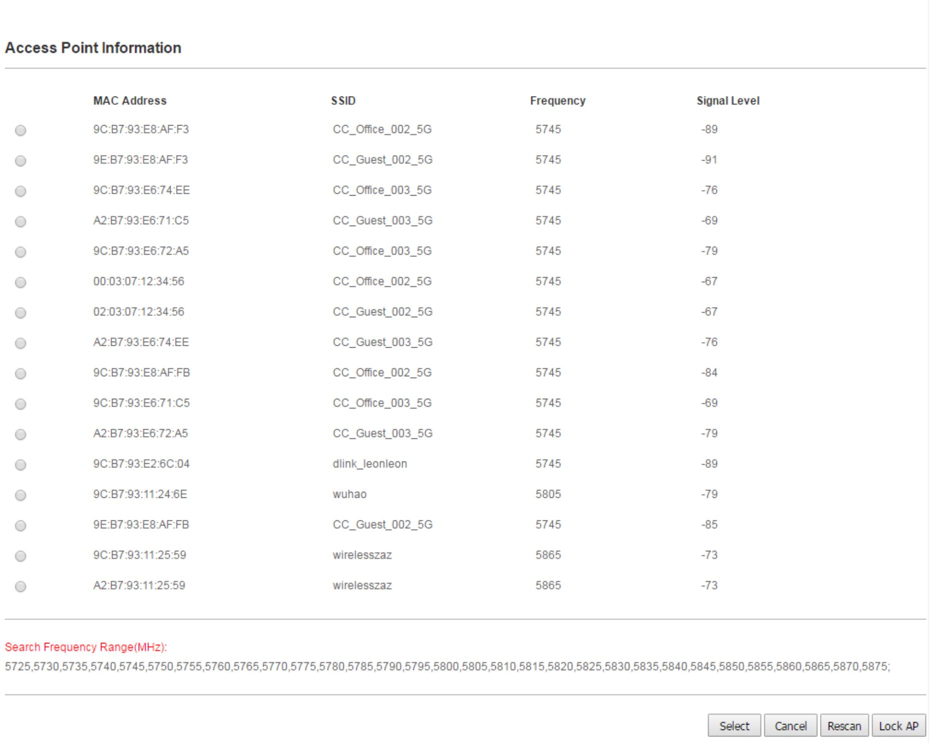
Station: It needs to be used with the AP. It connects to the AP. A station can only connect to one AP.

WDS Station: Use WDS feature to link multiple APs in a network, all associated stations from any AP can communicate with each other like in ad-hoc mode. WDS station means this device is a station in WDS mode.

WDS Access Point: Use WDS feature to link multiple APs in a network, all associated stations from any AP can communicate with each other like in ad-hoc mode. WDS AP means this device is an AP in WDS mode.

SSID: The value used to control access to the wireless network. When other devices connect to the device, only the set SSIDs are the same to communicate with each other to establish a local area network.

Click the selection button on the right side of the network name to jump to the access point information interface. As shown in the following figure, the device can search for the network name of the surrounding wireless network, and then the user can connect to the corresponding wireless network according to his own needs.



Access Point Information

	MAC Address	SSID	Frequency	Signal Level
○	9C:B7:93:E8:AF:F3	CC_Office_002_5G	5745	-89
○	9E:B7:93:E8:AF:F3	CC_Guest_002_5G	5745	-91
○	9C:B7:93:E6:74:EE	CC_Office_003_5G	5745	-76
○	A2:B7:93:E6:71:C5	CC_Guest_003_5G	5745	-69
○	9C:B7:93:E6:72:A5	CC_Office_003_5G	5745	-79
○	00:03:07:12:34:56	CC_Office_002_5G	5745	-67
○	02:03:07:12:34:56	CC_Guest_002_5G	5745	-67
○	A2:B7:93:E6:74:EE	CC_Guest_003_5G	5745	-76
○	9C:B7:93:E8:AF:FB	CC_Office_002_5G	5745	-84
○	9C:B7:93:E6:71:C5	CC_Office_003_5G	5745	-69
○	A2:B7:93:E6:72:A5	CC_Guest_003_5G	5745	-79
○	9C:B7:93:E2:6C:04	dlink_leonleon	5745	-89
○	9C:B7:93:11:24:6E	wuhao	5805	-79
○	9E:B7:93:E8:AF:FB	CC_Guest_002_5G	5745	-85
○	9C:B7:93:11:25:59	wirelesszaz	5865	-73
○	A2:B7:93:11:25:59	wirelesszaz	5865	-73

Search Frequency Range(MHz):
5725,5730,5735,5740,5745,5750,5755,5760,5765,5770,5775,5780,5785,5790,5795,5800,5805,5810,5815,5820,5825,5830,5835,5840,5845,5850,5855,5860,5865,5870,5875;

Figure 6-3 Access Point Information

Frequency Scan List: When the device is in station mode, check “Enable”, click “Select”, the user can enter “Frequency Scan List” to select the frequency by himself, and check “Scope”. Users can set the frequency range by themselves. When the frequency of the AP is not the frequency selected by the station, the station cannot connect to the AP. Only when the frequency of the AP is one of the station selections can be connected to each other (only the station page is displayed).

Frequency MHz: This parameter needs to be set as the access point mode. The default is "automatic selection". Check "Enable". Click "Select". Users can enter the "Frequency Scan List" to select the frequency by themselves, and check the "Range". You can set the frequency range yourself (only the access point page is displayed).

Output Power: The output power of the wireless signal transmitted by the device. The user adjusts according to the distance between the devices. When the output power is increased, the transmitted signal distance and signal strength will be improved.

IEEE 802.11 Mode: The wireless LAN standard, which defaults to A/N mixed to ensure optimal transmission rate.

Country Code: Different countries or regions have different standard channels, which are distinguished by country codes.

Channel Width: The channel width refers to the maximum data transmission rate of the channel.

Max TX Rate, Mbps: The maximum transmission and reception rate of the device. It is set to limit the maximum transmission and reception rate of the device to maintain the stability of the device performance.

Lock AP Mac: The station or WDS station sets the object to which the device is connected by setting it (only the station page is displayed).

Security: Encrypts the wireless connection, and users can choose the appropriate encryption method according to their security requirements. The wireless encryption of the devices to be associated with each other must be set to the same, otherwise, the association is not.

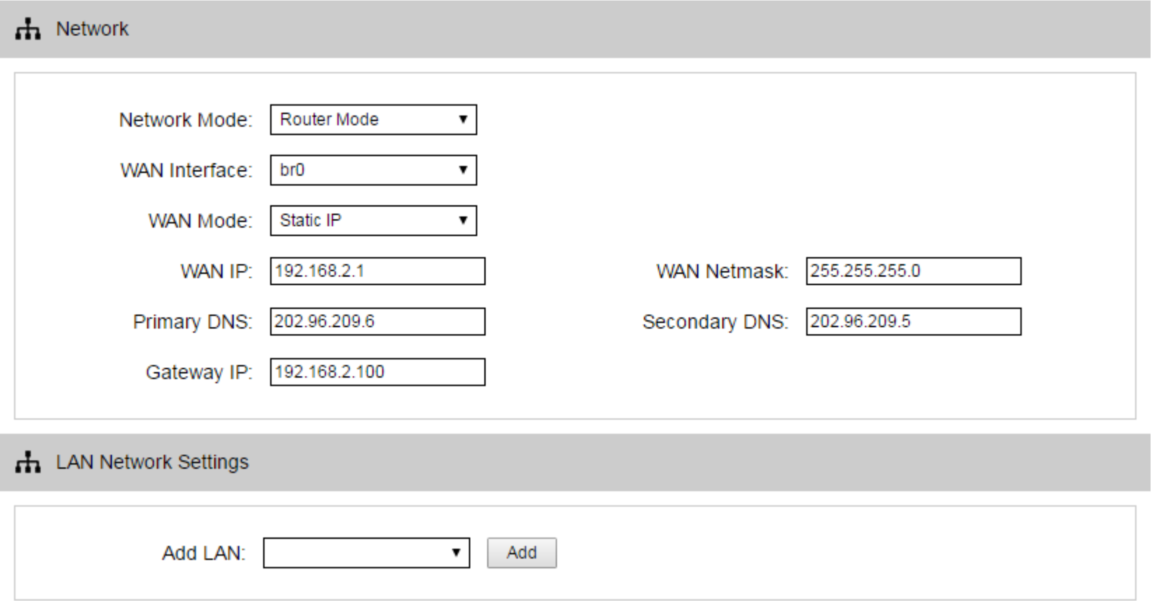
WPA: WPA is a standards-based specification that enhances interoperable security and greatly improves data protection and access control in existing and future wireless LAN systems. Designed as a software upgrade to run on existing hardware, Wi-Fi Protected Access is derived and will be compatible with future IEEE 802.11i standards. When properly installed, it provides a high level of protection to users of the wireless network so that their data is always protected and only authorized network users can access the network. WPA compensates for all the defects of Wired Equivalent Privacy (WEP).

802.1x: The 802.1x protocol is based on the Client/Server access control and authentication protocol. It can restrict unauthorized users/devices from accessing LAN/WLAN through an access port. 802.1x authenticates users/devices connected to the switch port before obtaining the various services provided by the switch or LAN. Before the authentication is passed, 802.1x only allows EAPoL (LAN-based Extended Authentication Protocol) data to pass through the switch port to which the device is connected; after authentication is passed, normal data can successfully pass through the Ethernet port.

7 Network

7. 1 Router mode

In the router mode, CFORCE N100 is equivalent to a router, which has a WAN port and a LAN port. At this time, the LAN port on the CFORCE N100 is equivalent to the LAN port of the router, and the LAN port on the PoE power supply is equivalent to the WAN port of the router. The route mode page is shown below:



Network

Network Mode: Router Mode

WAN Interface: br0

WAN Mode: Static IP

WAN IP: 192.168.2.1

WAN Netmask: 255.255.255.0

Primary DNS: 202.96.209.6

Secondary DNS: 202.96.209.5

Gateway IP: 192.168.2.100

LAN Network Settings

Add LAN:

Figure 7-1 Router mode

WAN Mode: The WAN mode item is an option for the WAN port to obtain an IP address. It is classified into static IP, DHCP (dynamic acquisition), and PPPoE. When set to static IP, the user needs to manually set the IP, subnet mask, etc. When set to DHCP, the device can automatically obtain an IP address from the DHCP server; when set to PPPoE, the user needs to fill in the PPPoE server name, Internet account number, and Internet access password. The device uses the dial-up authentication method to obtain an IP address through the PPPoE server.

WAN IP: Only exists under static IP. It can be set to the IP address of the same network segment as the network to be connected.

WAN Netmask: The subnet mask of the WAN port, which exists only under static IP and is used with the WAN IP.

Note: WAN IP address should not be the same as the IP devices of the internet to avoid collision.

Primary DNS and Secondary DNS: DNS server, set to the value of the local DNS server.

Gateway IP: Generally, the gateway address and the WAN IP address are on the same network segment, and are generally set to the LAN port address of the upper-level router.

LAN Network Settings: The LAN network settings are settings that exist in the routing mode. You can add and manage LAN ports. The IP address of the LAN port is generally the gateway address of the device in the lower LAN, and the LAN port IP address and WAN IP address are not on the same network segment.

7. 2 Bridge mode

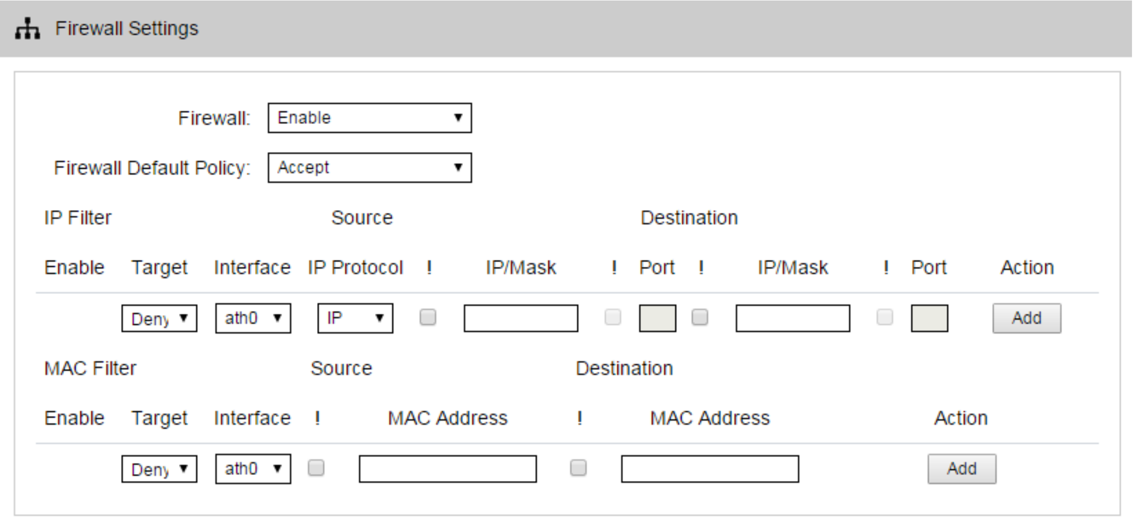
In Bridge mode, there is no WAN port. The LAN port of the PoE adaptor, and the LAN port of the CFORCE N100 device can all be the LAN port, and the user can choose one of them to use as LAN port, and the IP address/Netmask information setting is the same as Router mode.

7. 3 Management Network Settings

The IP address of the device can be modified, and the management of the device can be performed by setting the specified management interface.

7. 4 Firewall Settings

When the user wants to shield some devices from CFORCE N100, a firewall can be used to implement this function. The firewall is as shown in the following figure:



Firewall Settings

Firewall: Enable

Firewall Default Policy: Accept

IP Filter			Source					Destination				
Enable	Target	Interface	IP Protocol	!	IP/Mask	!	Port	!	IP/Mask	!	Port	Action
	Deny	ath0	IP	□		□		□		□		Add

MAC Filter			Source			Destination	
Enable	Target	Interface	!	MAC Address	!	MAC Address	Action
	Deny	ath0	□		□		Add

Figure 7-2 Firewall

1. Filter the device whose LAN port IP address is 192.168.1.100.

The firewall is enabled, the firewall default policy is Accept, the target of the IP address filtering is Deny, the interface eth0, the IP protocol is IP, the source IP/mask 192.168.1.100/32, and other values are null.

2. Filter the device whose MAC address is 00:00:00:00:00:01.

The firewall is enabled. The firewall default policy is Accept. The target of the MAC filtering mode is Deny, the interface is eth0, the source MAC address is 00:00:00:00:00:01, and the other values are empty.

7. 5 IP Aliases Settings

This function can add multiple IP addresses of the same network segment or different network segments to a network interface. The IP aliases of different interfaces cannot be the same.

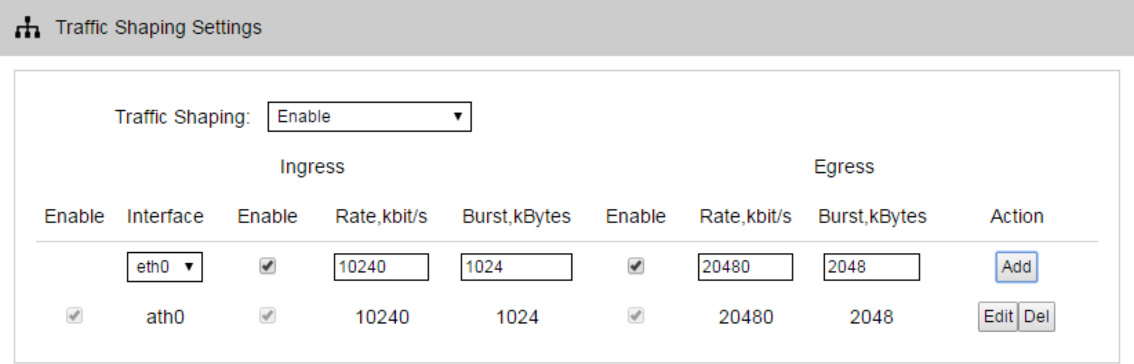
7. 6 Static Routes Settings

This feature allows you to set up a static route.

7. 7 Traffic Shaping Settings

Traffic shaping is used to control the traffic of ingress/egress based on each network port. As show below, the ingress of ath0 is limited to 10240Kbps, and the egress is limited to 20480Kbps. That means the receiving rate of the wireless link is limited within 10Mbps, the sending rate is limited to less than 20Mbps. But usually, the input limited effect is not obviously, that's because we could not control how quickly the traffic arrives. However, when a port sends out egress traffic, it can control how quickly the traffic exits.

Burst defines the how many bytes allowed for downloading/uploading during a quick time. That leads to momentary throughput can greater than the limit value.



Traffic Shaping Settings

Traffic Shaping: Enable

		Ingress			Egress			
Enable	Interface	Enable	Rate,kbit/s	Burst,kBytes	Enable	Rate,kbit/s	Burst,kBytes	Action
	eth0	☑	10240	1024	☑	20480	2048	Add
☑	ath0	☑	10240	1024	☑	20480	2048	Edit Del

Figure 7-3 Traffic Shaping

- Ingress traffic entering ath0, control the input rate
- Egress traffic exiting ath0, control the output rate

The relationship of rate and burst for ingress:

- Set burst to 0, the rate of ingress is unlimited
- Set burst to about 1/10 of rate limit, the rate curve is stable
- Set burst larger than rate limit, the rate curve will hold a high value for a while then down to stable

Below is the table that reflects the relationship between ingress rate limit and burst.

Ingress		Throughput when reach stable	
Rate Limit(kbps)	Burst(Kbytes)	(Mbps)	Description
10000	0	29.587	Unlimited
10000	10	4.286	Stable
10000	100	8.037	Oblique up to stable
10000	1000	8.825	From 9.5 down to stable
10000	10000	8.6	From 28.5 down to stable
10000	40000	8.6	Hold on 10 seconds at 29.6, then suddenly down to stable

The relationship of rate and burst for egress:

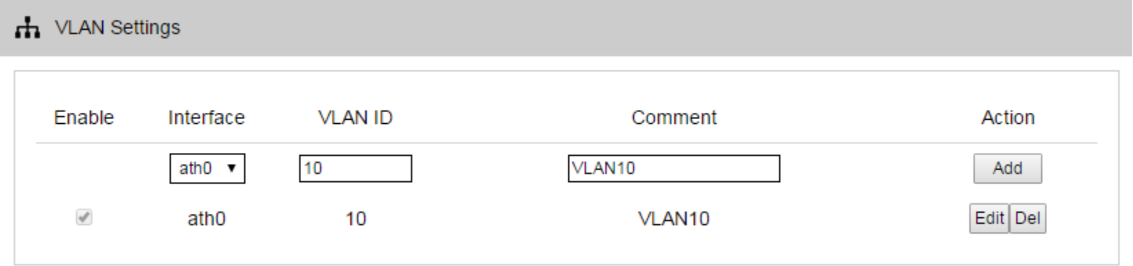
- Set burst less than 1/10 of rate limit, the rate curve is stable totally
- Set burst larger than rate limit, the rate curve will hold a while at a higher value then down to stable

Below is the table that reflects the relationship between egress rate limit and burst.

Egress		Throughput when reach stable	
Rate Limit(kbps)	Burst(Kbytes)	（Mbps）	Description
20000	0	18.853	Stable
20000	20	19.021	Stable
20000	200	19.205	Stable
20000	2000	19.437	From 23.5 down to stable
20000	20000	19.2	Hold on 20 seconds at 24.5, then suddenly down to stable
20000	80000	19.2	Hold on several minutes at 24.5, then suddenly down to stable

7. 8 VLAN Settings

The VLAN function allows user to create multiple virtual local area network. As show below, we add a VLAN on port ath0. The VLAN ID is 10. The range of VLAN ID is 2~4094. Each VLAN ID represents a different VLAN.



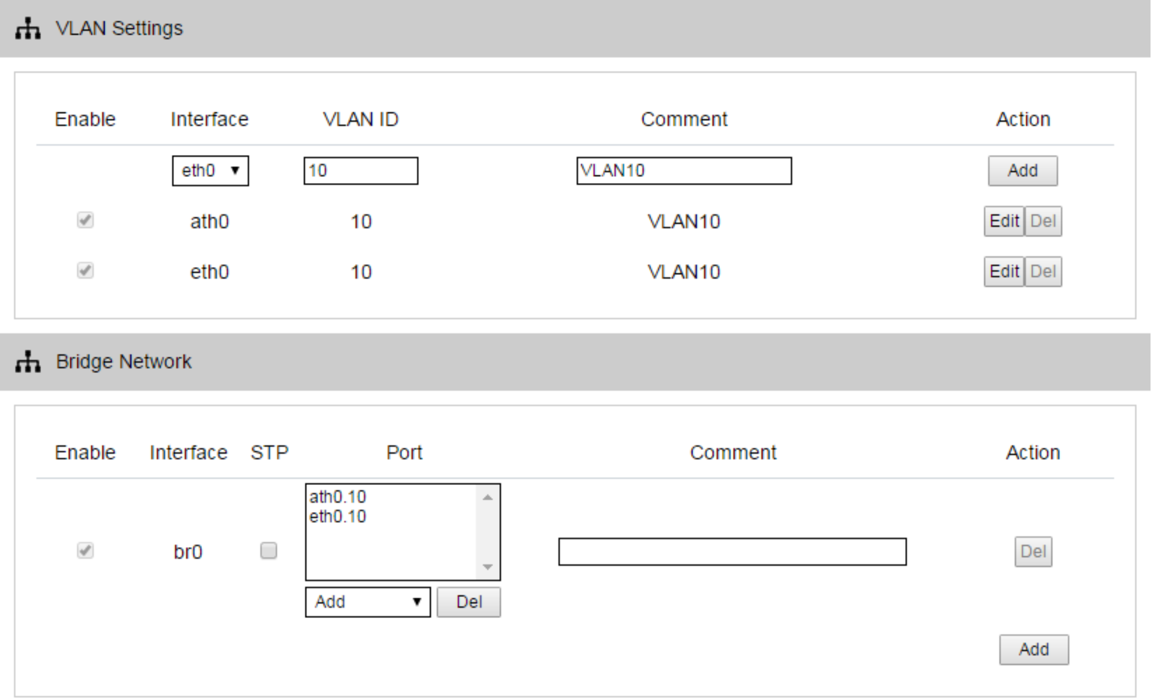
VLAN Settings

Enable	Interface	VLAN ID	Comment	Action
	ath0 ▾	10	VLAN10	Add
☑	ath0	10	VLAN10	Edit Del

Figure 7-4 VLAN

The VLAN function needs to be used in conjunction with the bridge settings. As shown in the following figure, virtual interfaces are added to both eth0 and ath0 with an ID of 10 and placed in a bridge so that they are in a VLAN. Packets coming out of and coming from ath0.10 or eth0.10 will be tagged with a VLAN tag of ID 10. This requires: for wireless connection, the other party also supports

VLAN 10 (that is, ath0 adds a virtual interface with ID 10); wired eth0 interface needs to connect to devices that support VLAN 10 (such as VLAN switches, and supports VLANs with ID 10).



VLAN Settings

Enable	Interface	VLAN ID	Comment	Action
	eth0 ▾	10	VLAN10	Add
☑	ath0	10	VLAN10	Edit Del
☑	eth0	10	VLAN10	Edit Del

Bridge Network

Enable	Interface	STP	Port	Comment	Action
☑	br0	□	ath0.10 eth0.10 Add ▾ Del		Del
					Add

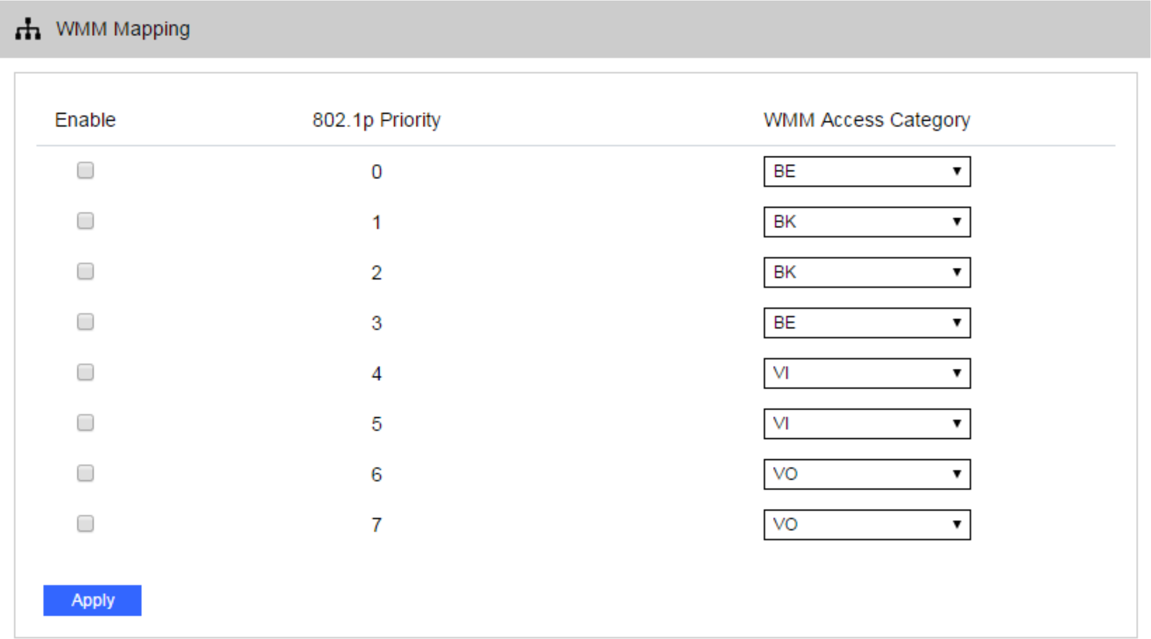
Figure 7-5 Bridge Network

7. 9 WMM Mapping

Enable WMM mapping to perform QoS on the device data stream and match the specified data stream and adjust the priority of the specified data stream. Different network service quality is provided for various application scenarios. It provides better quality of service for data packets with high real-time and high reliability requirements, and prioritizes them. For ordinary data packets with low real-time performance, it provides lower processing priority.

WMM (Wi-Fi Multimedia): WMM is a wireless QoS protocol that is a subset of the 802.11e protocol. It is used to ensure that packets with high priority have priority to send, so that voice, video and other applications have better quality in the wireless network.

AC (Access Category): WMM is divided into four priority queues: Voice, Video, Best-effort, and Back-ground according to the order of priority. It is used to ensure that packets with high priority classification preferentially preempt the wireless channel and transmit.



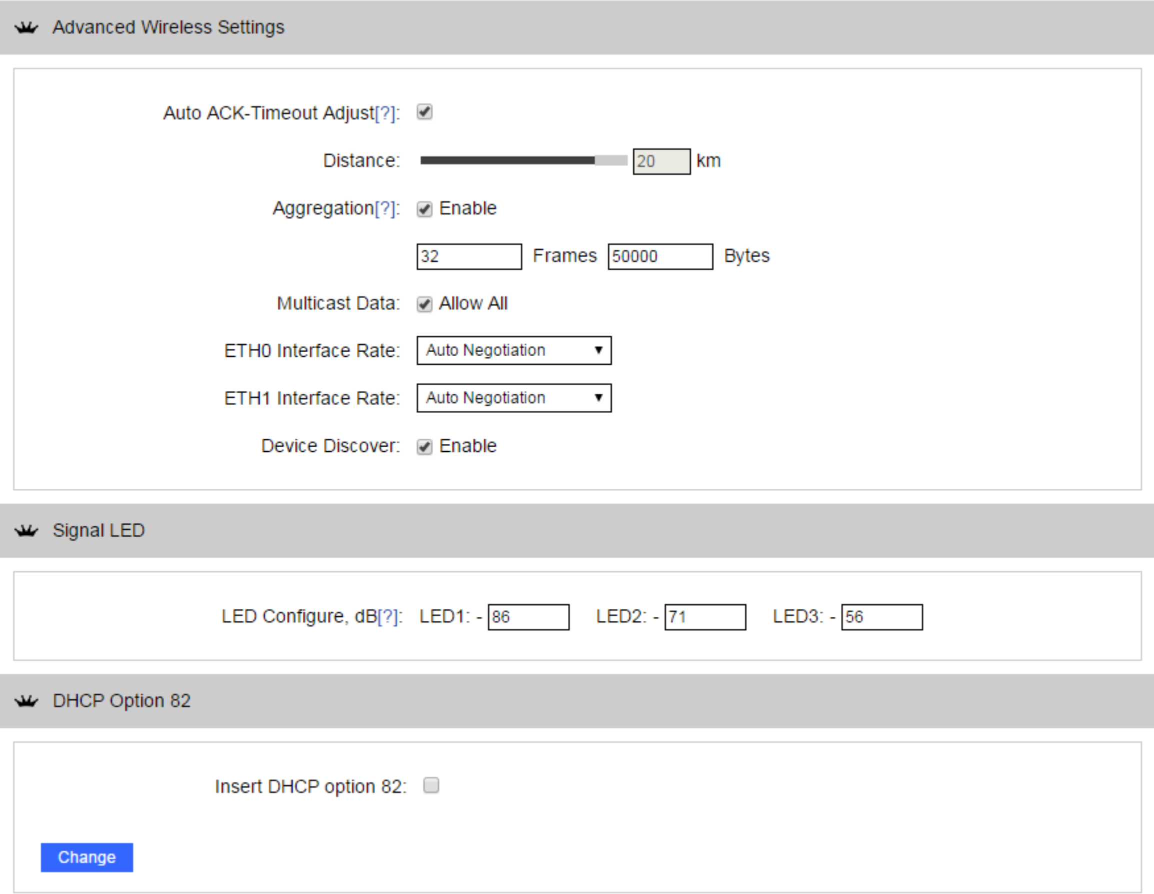
WMM Mapping

Enable	802.1p Priority	WMM Access Category
□	0	BE
□	1	BK
□	2	BK
□	3	BE
□	4	VI
□	5	VI
□	6	VO
□	7	VO

Figure 7-6 WMM Mapping

8 Advanced

The advanced settings page is shown below:



Advanced Wireless Settings

Auto ACK-Timeout Adjust[?]: ☑

Distance: 20 km

Aggregation[?]: ☑ Enable

32 Frames 50000 Bytes

Multicast Data: ☑ Allow All

ETH0 Interface Rate: Auto Negotiation

ETH1 Interface Rate: Auto Negotiation

Device Discover: ☑ Enable

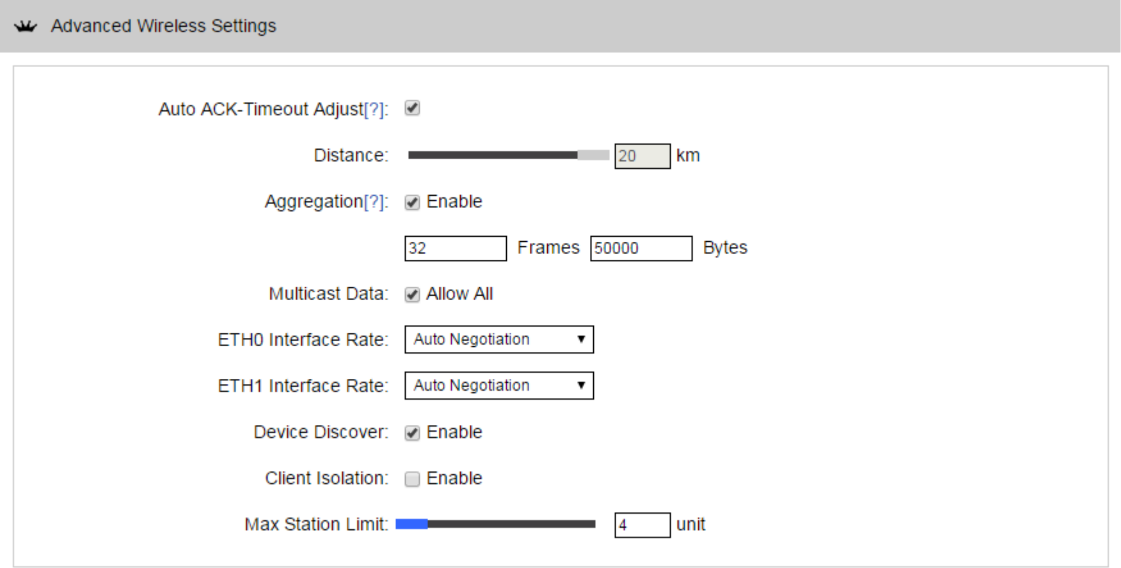
Signal LED

LED Configure, dB[?]: LED1: - 86 LED2: - 71 LED3: - 56

DHCP Option 82

Insert DHCP option 82: □

Figure 8-1 Advanced-station



Advanced Wireless Settings

Auto ACK-Timeout Adjust[?]: ☑

Distance: 20 km

Aggregation[?]: ☑ Enable

32 Frames 50000 Bytes

Multicast Data: ☑ Allow All

ETH0 Interface Rate: Auto Negotiation

ETH1 Interface Rate: Auto Negotiation

Device Discover: ☑ Enable

Client Isolation: □ Enable

Max Station Limit: 4 unit

Figure 8-2 Advanced-AP

Auto ACK-Timeout Adjust: The user turns on “ACK-Timeout Auto Adjustment”. This option automatically tests the distance between two devices and sets the parameters according to this distance to optimize the quality of the wireless connection.

Distance: If the "ACK-Timeout Auto Adjustment" option is turned on, this distance setting is disabled and the system will automatically test the distance of the device and optimize the connection quality. If the user wants to set the distance set by himself, you need to turn off the "ACK-Timeout Auto Adjustment" option.

Aggregation: The same frames are combined and sent out. Enabling this function has a certain increase in throughput, and the device is enabled by default.

Multicast Data: With this feature, CFORCE N100 allows multicast packets to pass through CFORCE N100.

ETH0 Interface Rate: Set the connection speed and duplex mode of the ETH0 port.

ETH1 Interface Rate: Set the connection speed and duplex mode of the ETH1 port.

Device Discover: When using this function, please use it with the dedicated tool set. The tool set window will display the MAC address, IP address, product name, and firmware name information of the discovered device. Note: When discovering devices wirelessly, keep the multicast support enabled.

Client Isolation: Enable this feature to prevent devices connected to the same access point, WDS access point, and WDS repeater from communicating with each other. Even if the IP of each station is duplicated, it will not affect the communication. This feature only exists in access point mode.

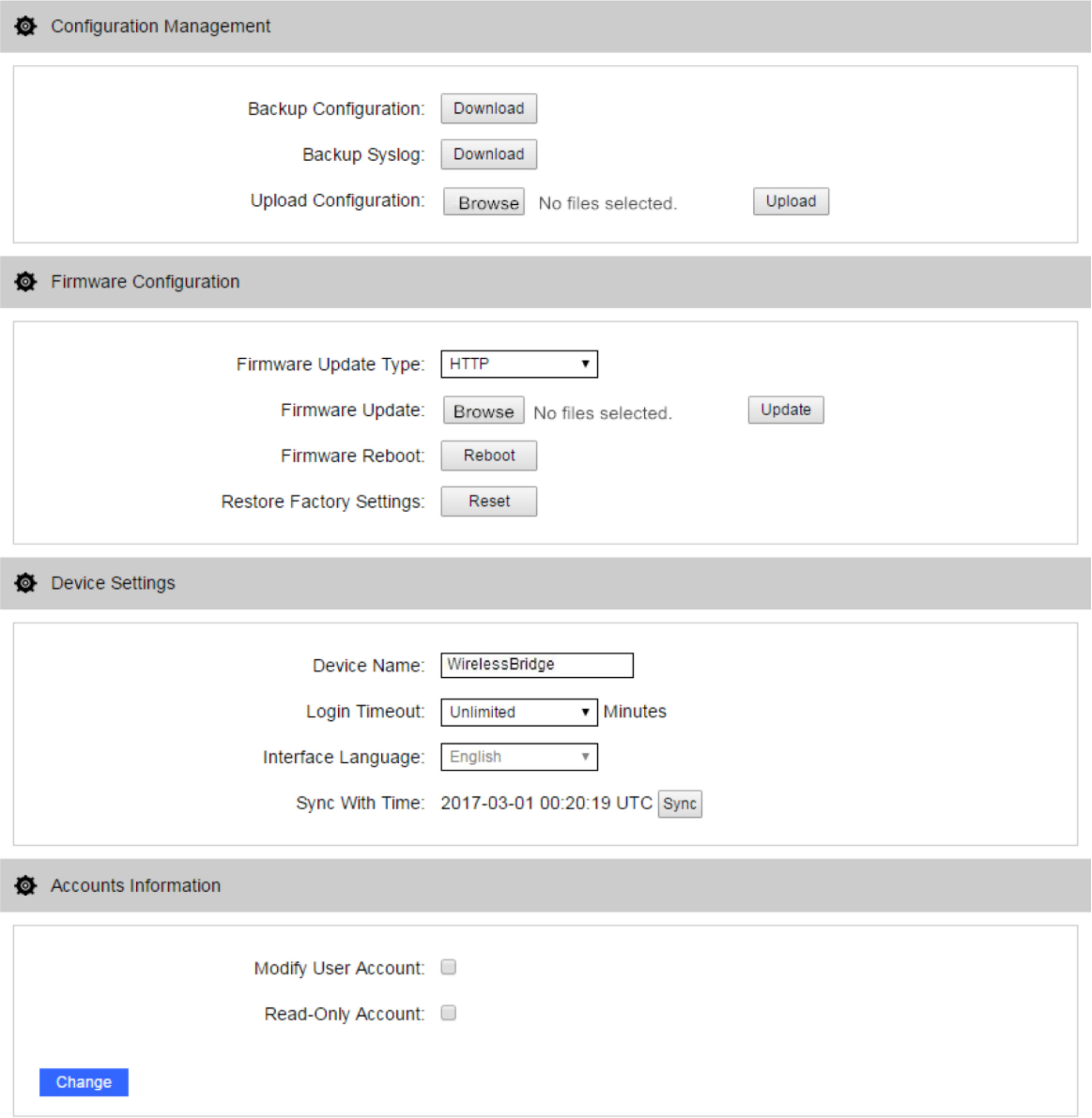
Max Station Limit: Set it to limit the number of stations and WDS stations connected to the access point, WDS access point.

Signal LED: LED1, LED2 and LED3 are set to illuminate the signal intensity value required by the device's 3 LED lights, and LED3 has the highest signal strength value (LED3>LED2>LED1). The default settings are LED1: -86dB, LED2: -71dB and LED3: -56dB. When the signal strength is higher than LED1 is lower than LED2, LED1 is bright. When the signal strength is higher than LED2, lower than LED3, LED1 and LED2 are bright. When the signal strength is higher than LED3, LED1, LED2 and LED3 are both on.

DHCP Option 82: The relay agent information option in the DHCP message.

9 System

The system setting interface is divided into four parts: configuration management, firmware configuration, device settings, and account information, as shown in the following figure:



Configuration Management

Backup Configuration: Download

Backup Syslog: Download

Upload Configuration: Browse No files selected. Upload

Firmware Configuration

Firmware Update Type: HTTP

Firmware Update: Browse No files selected. Update

Firmware Reboot: Reboot

Restore Factory Settings: Reset

Device Settings

Device Name: WirelessBridge

Login Timeout: Unlimited Minutes

Interface Language: English

Sync With Time: 2017-03-01 00:20:19 UTC Sync

Accounts Information

Modify User Account: ☐

Read-Only Account: ☐

Change

Figure 9-1 System

Backup Configuration: Click Download to back up the configuration on the current web page. Note that the contents of the configuration file cannot be modified manually.

Backup Syslog: Click Download to back up the system log on the current web page.

Upload Configuration: Click Browse, select the previously downloaded configuration file, and click Upload to restore the device configuration to the configuration of the device when the configuration file is backed up.

Firmware Update Type: Users can choose to upgrade through HTTP, TFTP, and FTP.

Firmware Update: Click Browse, select the version to be upgraded, click Upgrade, and the device starts to upgrade.

Firmware Reboot: Click to restart and the device starts to restart.

Restore Factory Settings: Click Restore on the web page. After a period of time, the device configuration is restored to the factory settings.

Device Name: The user can set the setting name to the name he needs according to his own needs.

Login Timeout: When the user has not operated the device for a timeout value of the login timeout setting, the page will be automatically redirected to the login interface when the page is operated again.

Interface Language: Users can choose the language of the web page they want according to their needs.

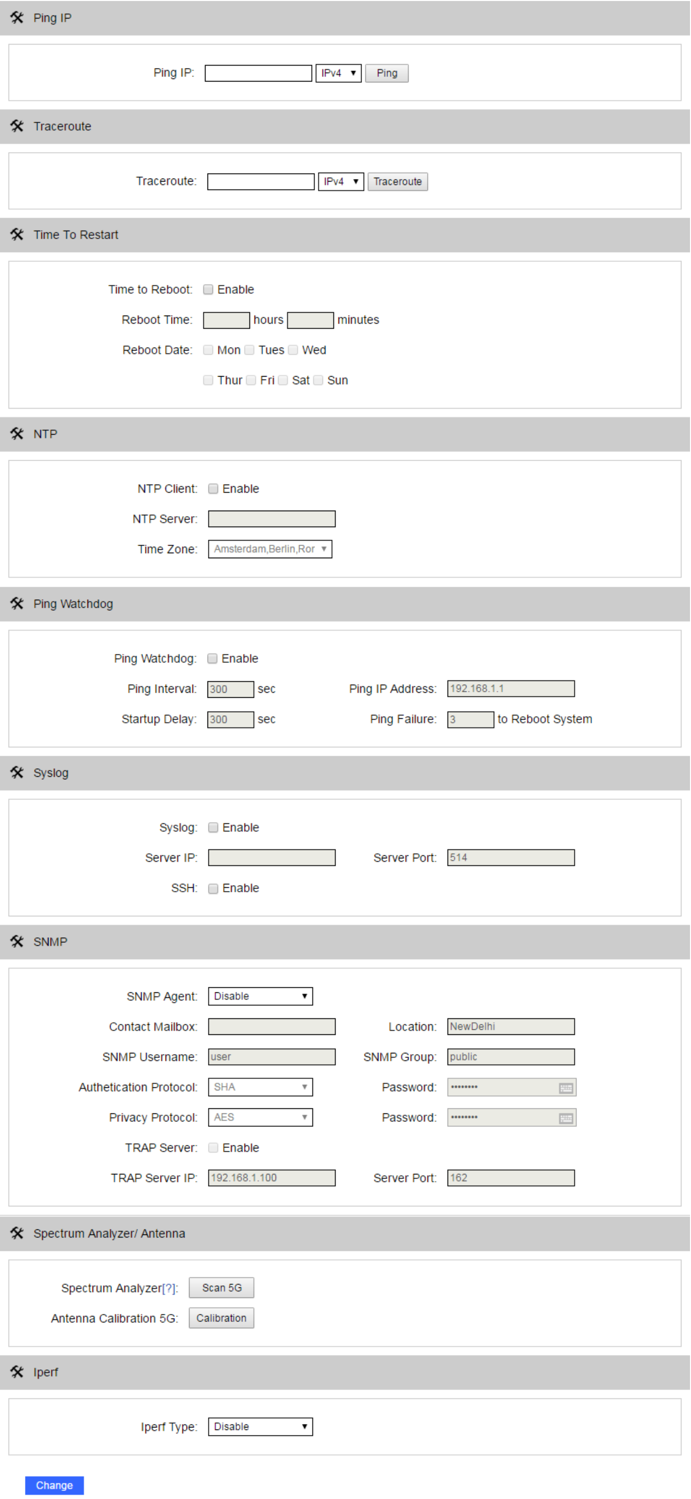
Sync With Time: Click to sync, the device will automatically calibrate the time, synchronize with the system's unified standard clock, and display it on the status display page.

Modify User Account: When the modify user password is enabled, the user can modify the user name and password of the login device management webpage according to his own needs.

Read-Only Account: After logging in to the device, this account can only read the value of the status display page.

10 Tools

The tool application page is shown below:



Ping IP

Ping IP: IPv4 Ping

Traceroute

Traceroute: IPv4 Traceroute

Time To Restart

Time to Reboot: □ Enable

Reboot Time: hours minutes

Reboot Date: □ Mon □ Tues □ Wed

□ Thur □ Fri □ Sat □ Sun

NTP

NTP Client: □ Enable

NTP Server:

Time Zone: Amsterdam,Berlin,Ror

Ping Watchdog

Ping Watchdog: □ Enable

Ping Interval: 300 sec Ping IP Address: 192.168.1.1

Startup Delay: 300 sec Ping Failure: 3 to Reboot System

Syslog

Syslog: □ Enable

Server IP: Server Port: 514

SSH: □ Enable

SNMP

SNMP Agent: Disable

Contact Mailbox: Location: NewDelhi

SNMP Username: user SNMP Group: public

Authecication Protocol: SHA Password: ••••••••

Privacy Protocol: AES Password: ••••••••

TRAP Server: □ Enable

TRAP Server IP: 192.168.1.100 Server Port: 162

Spectrum Analyzer/ Antenna

Spectrum Analyzer[?]: Scan 5G

Antenna Calibration 5G: Calibration

Iperf

Iperf Type: Disable

Change

Figure 10-1 Tools

Ping IP: User can input the destination IP address of another device, and click Ping button. If that destination device is successfully connected to the CFORCE N100 device, the result shows Alive, otherwise shows Not Alive.

Traceroute: Use the ICMP protocol to locate all routers between your computer and the target computer.

Time to Reboot: This function allows you to periodically reboot the device.

NTP: If this NTP server is set, and the CFORCE N100 device can access to this NTP server. CFORCE N100 device automatically calibrate the time and date information with the NTP server and show the time information in the Status page.

Ping Watchdog: The ping watchdog sets the CFORCE N100 Device to continuously ping a user-defined IP address (for example, it can be the IP address of the AP the station is connecting to). If it is unable to ping under the user defined constraints, the CFORCE N100 device will automatically reboot. It is highly recommended that users enable this feature at the side of “Station” and disable this feature at the side of “Access Point”.

Ping Interval: Specify time interval (in seconds) between the ping requests are sent by the Ping Watchdog.

Ping IP Address: Specify an IP address of the target which will be monitored by Ping Watchdog. If this feature is enabled at the side of “Station”, Ping IP Address should be the IP address of the AP the Station is connecting to.

Startup Delay: Specify initial time delay (in seconds) until first ping request is sent by the Ping Watchdog.

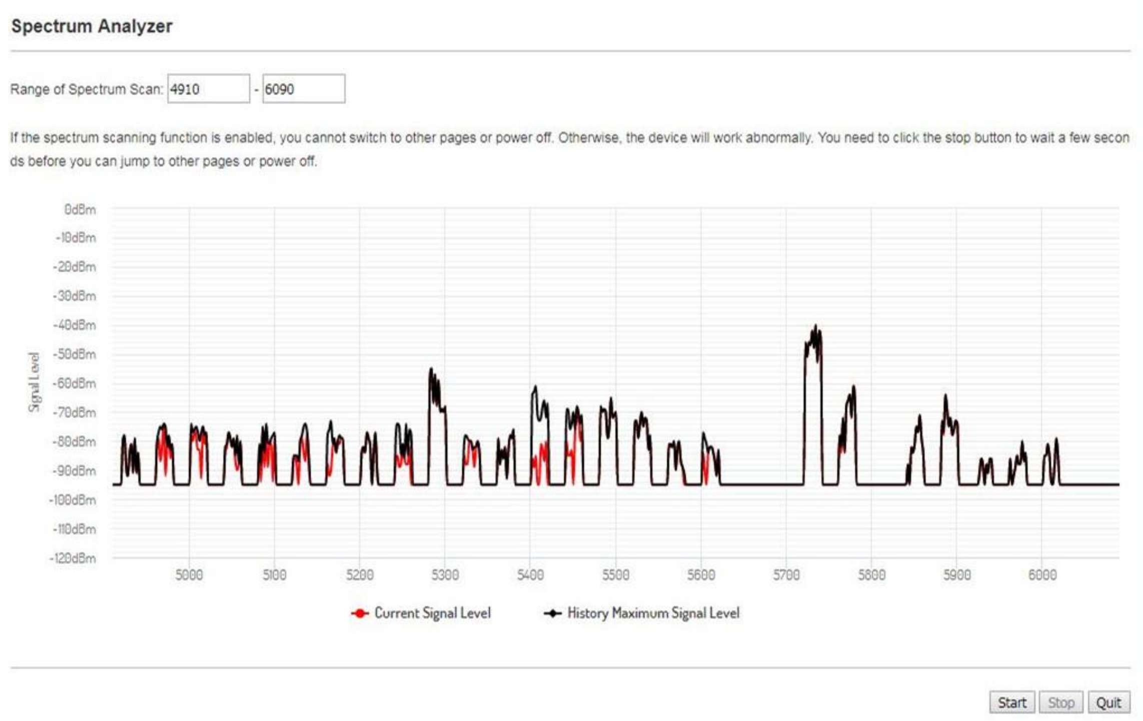
Ping Failure: Specify the number of ping replies. If the specified number of ping replies is not received continuously, the Ping Watchdog will reboot the device.

Note: If users want to modify the parameters of Ping Watchdog, please disable it first and then apply. When the web page shows that Ping Watchdog is really disabled, users can now re-enable it with modified parameters.

Syslog: Enable the Syslog function and set the IP address of the PC where the Syslog server is located. The server port is set to 514. After saving/applying, the related log information can be seen on the system log interface of the status display page and on the Syslog server.

SNMP: The SNMP agent allows network administrators to monitor network performance and find and resolve network problems. Such as: SNMP agent is selected to enable, SNMP community fill in a user's name, such as: user, contact the mailbox to fill the user's corresponding mailbox such as: jerry@user.com, location information fill user. Then save and apply. Install mrtg on the host, open the mrtg web page, and you can observe the traffic through CFORCE N100.

Spectrum Analyzer: View the usage of each frequency band in the 20MHz bandwidth of the peripheral frequency, which can help you configure the device to avoid busy frequency bands. If you perform a spectrum scan, you will not be able to perform any configuration operations on the device page at this time. If you want to reconfigure your device, simply click the Exit button on the Spectrum Scan page to exit this feature.



Spectrum Analyzer

Range of Spectrum Scan: 4910 - 6090

If the spectrum scanning function is enabled, you cannot switch to other pages or power off. Otherwise, the device will work abnormally. You need to click the stop button to wait a few seconds before you can jump to other pages or power off.

Figure 10-2 Spectrum Analyzer

Antenna Calibration 5G: Outdoor remote adjustment of the antenna angle used, every few seconds to refresh the current 5G associated signal strength histogram, the user can judge the current two devices according to the two antenna is at the best angle.

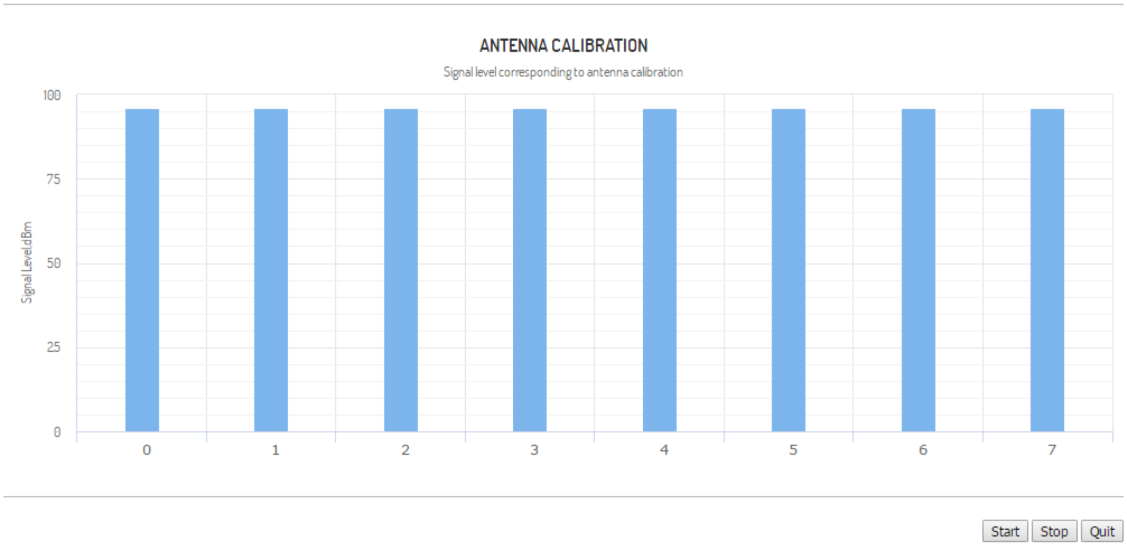


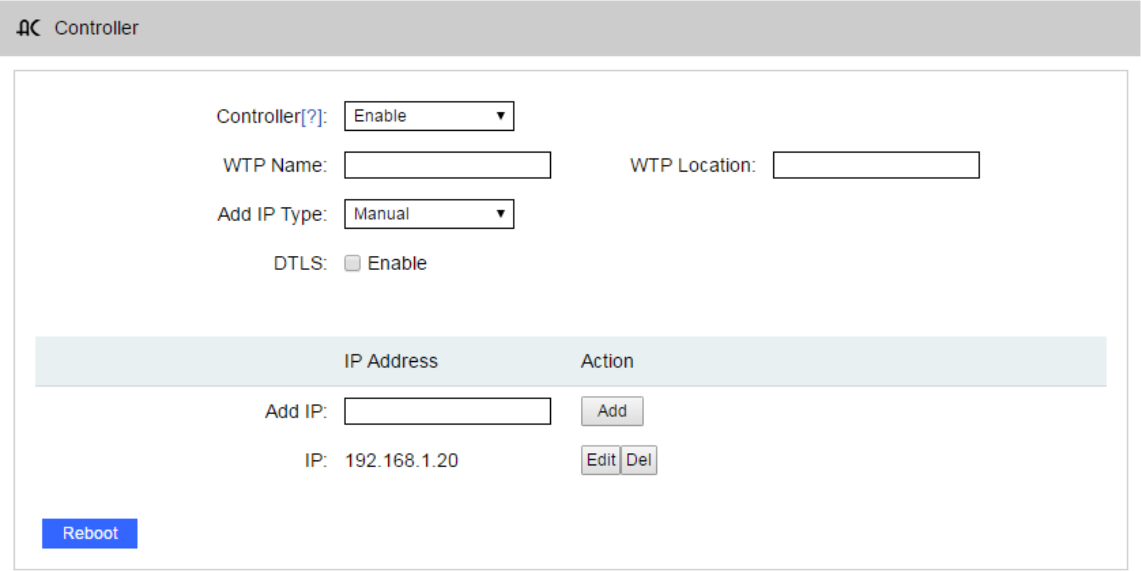
Figure 10-3 Antenna Calibration 5G

Note: When the bar graph shows the signal strength is higher than 60, said the signal strength is poor, it is recommended that users adjust the equipment to ensure that the two devices antenna angle is the best.

Iperf: Divided into servers and clients, used to test the throughput of the wireless side between devices. Device 1 selects "Server", Device 2 selects "Client", and Iperf Server fills in the IP address of Device 1. Iperf Thread is recommended to set the number of threads running simultaneously when testing throughput. Iperf Time is the number of seconds to run Iperf. Iperf Interval is the interval at which throughput is displayed on the web page. Click the "Test" button when testing.

11 AC Management

The AC management page is shown below. After enabling this function, it needs to be used with the AC management system.



AC Controller

Controller[?]: Enable

WTP Name: WTP Location:

Add IP Type: Manual

DTLS: □ Enable

	IP Address	Action
Add IP:		Add
IP:	192.168.1.20	Edit Del

Figure 11-1 AC Management

WTP Name: It’s the name of the device that is displayed on the AC.

WTP Location: It’s the location information that is displayed on the AC.

Add IP Type: Configure the IP address of the AC server. You can use the manual addition method to specify the AC IP address to be connected, or you can use the automatic acquisition method to automatically discover the IP address of the AC server.

DTLS: Datagram Transport Layer Security, used for capwap message encryption.

AC IP: This IP address can add up to eight, add the IP address is AC management interface’s IP and equipment is the same segment. After the AC control function is enabled, click save, application, this time the device will take effect on the AC configuration and restart, the device will join AC. After the AC control function is enabled, the user is able to display the current state of the page on the device page. After the AC control function is disabled, the user is able to modify the device's page.

Note: The station must be able to join the AC after it is connected to an access point that has been joined to the AC.

12 Logout

Logout is used to log out of the product page. When the user clicks Logout in the upper right corner of the page, the product page will jump to the login page.

FCC WARNING

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 received, including interference that may cause undesired operation.

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

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.

To maintain compliance with FCC’s RF Exposure guidelines, This equipment should be installed and operated with minimum distance between 20cm the radiator your body: Use only the supplied antenna.

Contact Us

Creatcomm Technologies Co. Ltd.
Room 311, Y1 Building, No. 112, Liangxiu Road, Pudong Software Park, Shanghai, China
Tel: +86-021-58351681
Email: sales@creatcomm.com
Website: www.creatcomm.com