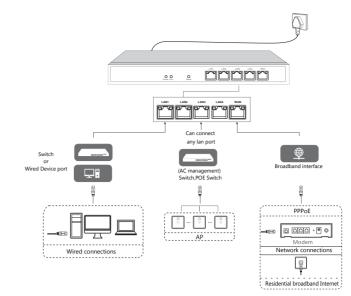


Enterprise Level Multi-Function

flow control Gateway

Quick Install Guide

01/Route Connection



02/Route Settings

2.1 Login Device

Connect Lan port of device to PC, login in via IP:Port <u>172.16.0.1:2011</u>, ID/Password: admin as below:

Multi-functional appliance

Gateway - Router - Load balance - Firewall - Controller - Captive portal

Port	IP Address	Mask
LAN1	172.16.0.1:2011	255.255.0.0
LAN2	172.17.0.1:2011	255.255.0.0
LAN3	172.18.0.1:2011	255.255.0.0
LAN4	172.19.0.1:2011	255.255.0.0

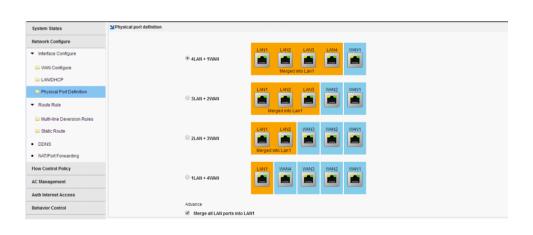
*Note:Please check the IP address of default port above

2.2 WAN port settings

(Network configuration) (Interface Configuration) "External network configuration", select the network port to configure, and configure the information of the external network, as shown in the following image:



MULTI-FUNCTION	GATEWAY Current oper	ition System Status >> Device Info			Refresh Change passw	ord Logout Langua	age English 🗖			
System Status	Network interface status									
 Device Info 										
 Interface Status 										
 LAN IP Flow 	LAN1 LAN2 L	AN3 WAN2 WAN1								
 Application Flow 	Interface	Туре	Link mode	IP address	MAC address	Receive speed	Send speed			
Network Configure	WAN1	WAN port Online	100M/Full duplex	192.168.1.2	10121170-00170-001	2.24 MB/S	83.52 KB/S			
Flow Control Policy	WAN2	WAN port Online	100M/Full duplex	192.168.0.3	10121170-00-70180	6.62 MB/S	239.93 KB/S			
AC Management	LAN3	LAN port	1000M/Full duplex	172.18.0.1	10121170-00-70100	0.26 KB/S	0.30 KB/S			
	LAN2	LAN port	1000M/Full duplex	172.17.0.1	10121170-00-7010-	32.90 KB/S	614.29 KB/S			
Auth Internet Access	LAN1	LAN port	1000M/Full duplex	172.16.0.1	1012110-00-00100	247.19 KB/S	8.35 MB/S			
Behavior Control	Device basic information									
Object Management	Device ID:	Max Users:256 , Max AP can be ma	anaged:256							
Safety Protection	Uptime: :	3:21:57 up 7 days Connectin								
Log Record	Memory utilization:	Memory utilization: 12% 59.89MB/498.17MB								
VPN	CPU utilization:	12%								
Device Maintenance	Connection monitoring:	8% 4237/50000								
	Online users:	55 users								



03/AC Management

3.1 AP Device List

S

The AC controller feature allows centralized management and release configuration of the AP devices connected to it, with parameters including

Line channels, SSIDs, transmit power, encryption modes and keys, AP coverage thresholds, number of access users, and VlAunID, as follows As shown in the figure:

System Status	AP list							Online A	P quantity/ Tota	I AP:6 / 7, AC service status	Conline 3
Network Configure	Restart AP	Reset AP	Delete AP	Apply configuration template	Refresh	All device 🔹	device model filb 🔻	Search conditions:	Device IP 🔻		
	search										

Current user admin[2:2:2:2] Device time:2010.06.26 18:20:07 System start: The device is running normality

Internet access: (choose how to access the Internet according to the actual situation)

ADSL/PPPOE: Fill in bandwidth account numbers and passwords (this type of Internet access is recommended)

Fixed IP: Fill in IP, mask, gateway and DNS provided by the operator

DHCP: Direct access to lines provided by the operator to obtain IP

Line interruption check: detect whether the line is connected to the network, if the line is not accessible or the linequality is poor, the packet is serious, the route is automatically processed, does not load to the Line. It is recommended to enable line interrupt detection.

Bandwidth configuration: configure the bandwidth of the line, such as the dial-up fiber of the upstream 4M downlink 100M, can be configured with behavior 500KB, downside 10000KB.Configure the line Bandwidth is important, and intelligent streaming is automatically streamed based on the bandwidth that is matched. (The "Enable Smart Streaming" option needs to be checked to configure bandwidth values for effective)

2.3 Physical port division

This feature supports separate and merge port divisions. When the main road is recommended to use the merge port division, that is, open All LAN ports are one LAN1 port function. If it is bypass mode, it is recommended to turn this feature off. Select the corresponding according to the actual situation Physical port division type, check "Merge all LAN ports as one intranet port (LAN1)."

Note: After the definition of the physical port feature is modified, the route needs to be reconfigured. (Note: The version of the <u>X86 platform</u> does not support Ethernet port merge).

<u>X86 Platform</u> include model: *GAC9500, GAC9600, GAC9800 These models will use separate LAN ports and integrated VLAN function on LAN*

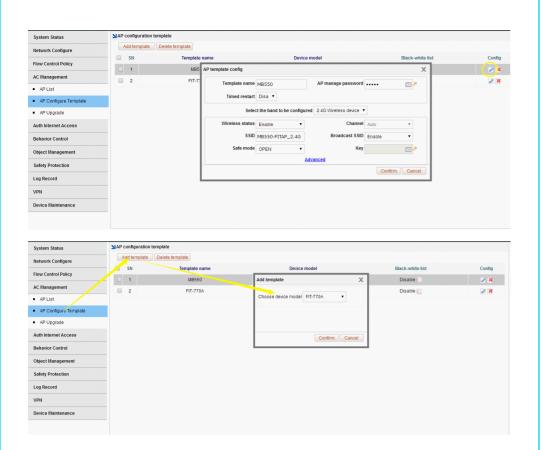


Note: The default configuration issued by AP is achieved by establishing the template, with one template for each model.

Only in the AC list should The template of the corresponding model will be released normally. Note: An AP model can also create multiple templates.Apply to the same floor or geography of the same model A scene with a different location.

3.2 AP Device Configuration

AP device configuration, is a single AP or multiple APs in the list of parameter modifications, including the wireless state on or off, The modification of the channel, the modification of the wireless bandwidth mode, the modification of the AP coverage threshold, the modification of the transmit power, and the marking of the device location.



3.3 AP Upgrade Management

AP Upgrade Management allows you to upload the AP version that needs to be upgraded to the device, and then select the AP list in full or selected to upgrade, while also supporting the AP remote upgrade.

System Status	AP upgrade								
Network Configure	Online Upgrade. First, click download file, download the upgrade file to route, then click upgrade or batch online upgrade to upgrade the firmware Uscal Upgrade. First, click the Upload Mirror button to upload the upgrade file, then click Upgrade or Batch Local Upgrade to upgrade the firmware								
Flow Control Policy	v	Device model filt Refresh Batch online upgrade Batch local up	grade Upload mirror						
AC Management	SN AP name IP MAC Status Device model	Current version Online upgrade	Upload file and Local upgrade						
AP List	I My WTP 1 172.16.0.102 44-D1-FA-63-43-18 Online FIT-770A V5	5.3-Build20190419091759 Already the latest version	-						
AP Configure Template	2 My WTP 1 172.16.0.101 44-D1-FA-72-8E-ED Offline FIT-MB550		-						
AP Upgrade	3 My WTP 1 172.16.0.111 44-D1-FA-23-43-7F Online PW1200	V3.2-B20190429100313 V3.3-Build20190621095606 Download file to upgrade	-						
Auth Internet Access	4 My WTP 1 172.16.0.112 44-D1-FA-63-43-98 Online FIT-770A V5	5.3-Build20190419091759 Already the latest version	-						
Behavior Control	5 My WTP 1 172.16.0.113 44-D1-FA-63-43-F0 Online FIT-770A V5	5.3-Build20190419091759 Already the latest version	-						
	6 My WTP 1 172.16.0.114 44-D1-FA-63-44-50 Online FIT-770A V5	5.3-Build20190419091759 Already the latest version	-						
Object Management	0 7 My WTP 1 172.16.0.115 44-D1-FA-63-43-78 Online FIT-770A V5	5.3-Build20190419091759 Already the latest version	-						
Safety Protection									
Log Record									
VPN									
Device Maintenance									

05/Configure shunt rules

5.1 Configuring shunt rules

A single line can not configure a shunt rule; (Network configuration)

Multi-line shunt rule, point Hit Add creates a policy shunt rule, selects the shunt mode, selects which apps the line hosts, and click OK after checking.

System Status	Multi-line deversion rules							
Network Configure		n rules are executed in turns from						
 Interface Configure 	SN Source address	Time Destina	tion port	Destinatio	on IP	Application type	Policy	Operation
		Policy shunt rule				×		
WAN Configure		Course address	According to Add	lana la la constante		-		
LAN/DHCP		Source address.	ACCOLUNG TO ACC		Add Add			
Physical Port Definition		Time	ANY		+ Add			
		Destination IP:	ANY		+ Add			
 Route Rule 		Destination Port			+ Add			
🖿 Multi-line Deversion Rules		Application type:						
Static Route		Shunt mode: Sessie		- Deallasting add		Shunt policy		
 DDNS 		Line selection:	on shunt U Source	+ Destination add	ress shunt U Si	burce in shunt		
 NAT/Port Forwarding 		Line						
-		WAN1						
Flow Control Policy								
AC Management								
Auth Internet Access		🕈 Session shunt divers	ion in connection s	ession unit				
Behavior Control						onfirm Cancel		
					C	ouncer		

Note: Multi-line load balancing is achieved by shunt rules.

5.2 Configure bandwidth speed limit policy

04/Authentications

4.1 Enable authentication to the Internet

Enable authentication Online, means that only PPPOE dial-up authentication, WEB password authentication, IP authentication, MAC authentication.

Users can only access the Internet, for example, allow the user PPPOE dial-up Internet access under LAN1, certified Internet access, "Certification switch", select LAN1, enable the authentication network switch, check the type of "PPPOE dial" that allows Internet access, click Save.

System Status	Auth switch Free auth	IP				
Network Configure	One key auth config: Ena	ble all Disable all				
Flow Control Policy	Notes: PPPoE authenticat interface must be configured	ion switch needs to be used in co ed; Portal authentication switch al	njunction with PPPOE authenticati Iso needs to be used in conjunctio	ion, that is, if an interface opens on with Portal authentication.	the PPPoE authentication switch, the PPPoE	E authentication of this
AC Management	Interface name	PPPoE auth switch	Portal auth switch	IP auth switch	MAC auth switch	
Auth Internet Access	LAN1	Disable	Disable	Disable	Disable	
Auth Configure						
 PPPoE Auth 						
 Portal Auth 						
 Radius Billing 						
 Notify Page 						
 User Management 						
🗀 Auth User						
🗀 Auth User Status						
😑 Department/Level Definition						
Behavior Control						
Object Management						

4.2 PPPOE Authentications

Users who use PPPOE dial-up Internet access need to enable PPPOE services at the intranet, such as PPPOE services on LAN1. (Certified Internet Access) (PPPOE Certification) (PPPOE Advanced Options) and select the app.

System Status	PPPoE Service
Network Configure	PPPoE Service PPPoE Advance option Access status
Flow Control Policy	Isolate intranet dial-up users: Disabled Click to enable
AC Management	Expired Users cannot dial. Enabled, click to disable
Auth Internet Access	Disable the same MAC address dialing: Disabled,Click to enable 🖓 When Enabled, the intranet PPPoE dialing request for the same MAC address will be rejected
 Auth Configure 	Password-free auth: Disabled Click to enable 9 Enable the password-free authentication function, any account and password can be dialed
PPPoE Auth	Размицитее авлетности и правле у споле ин развиотитее авлетности и правлетности и правлетности и развиотитее авлетности и правлетности и правле
 Portal Auth 	Assign DNS according to 'department/level' (in order to assign different DNS to different users, when the 'department/level' where the user belongs is configured DNS, PPPoE service will directly use the DNS configured here and assign DNS to users).
 Radius Billing 	Add Delete
 Notify Page 	🕏 Note: The rules are executed in turns from top to bottom. So, top side with high priority in DNS assignments. Can be moved by 🕈 arrow to adjust the sequence, Top 2000000000000000000000000000000000000
 User Management 	SN Type Name Main DNS Atternate DNS Operation
🗀 Auth User	PPPoE advance configuration is not added yet, please Add
🗀 Auth User Status	
Department/Level Definition	
Behavior Control	
Object Management	

06/Safety

6.1 End-network anomaly detection

Turn on DHCP detection to detect the presence of other DHCP servers in the intranet; Turn on Loop Detection to check the content for loops (for intranet fault positioning).

System Status	Vintranet anomaly detection
Network Configure	DHCP detection: Disabled,click to enable 🛛 😌 detect whether there are other DHCP servers in the intranet.
Flow Control Policy	Loop detection: Disabled.clickto enable 🖓 Check whether there are some loops on the intranet (for intranet fault location)
AC Management	
Auth Internet Access	Clear status
Behavior Control	Original Provided Anticipation Provided Anticipatio Provided Anticipation Provided Anticipation Provided
Object Management	♀ Intranet loop detection result: Please enable 'intranet loop detection' first
Safety Protection	
 IP-MAC Binding 	
Connection Quantity Limit	
LAN Abnormal Detection	
 LAN Attack Protection 	
 WAN Ping Forbid/WAN Login 	
Log Record	
VPN	

Description: Routing has intelligent flow control function, configuration speed limit strategy, the purpose is to prevent the endonet machine poisoning, or advertising uncontrolled Upload, usually the speed limit up to 100-300KB, the downlink speed limit can be properly l iberalized, such as the speed limit of 1000-3000, usually recommended The speed limit does not exceed one-third of the total bandwidth.

System Status	Bandwidth control				
letwork Configure	Add Delete				
low Control Policy	SN Source address	т	ime	Bandwidth limited	Operation
		Bandwidth control	rule	×	
Smart Flow Control		🔍 🖌 Enable 🔍 🛪	Disable		
Bandwidth Control					
Free Flow Control		Source address:	According to Address User Lev ANY	el Oppartment	
AC Management		Time		Add	
with Internet Access		Upstream limit:			
Behavior Control		Downstream limit:	WUNLIMITED		
bject Management					
Safety Protection					
.og Record		- n	ps: Click icon to edite bandwidth Cor	firm Cancel	
VPN					
Device Maintenance					

For example: a 50M peer fiber, then each machine speed limit up 100-300KB, down1000-3000 KB can be, advanced recommendation configuration P2P The limit allows 70% of the allowed for the upstream and 70% allowed for the downstream. As shown above (ANY means arbitrary, that is, anyone, any time)