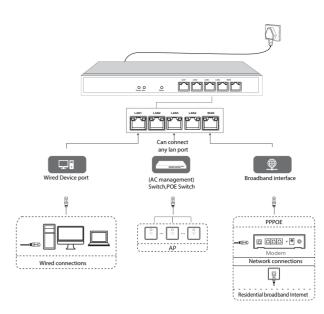
Enterprise Level Multi-Function flow control Gateway

# **Quick Install Guide**



# 02/Route Settings

01/Route Connection

### 2.1 Login Device

Connect Lan port of device to PC,login in via 172.0.1:2011 ,ID/Password: admin ,as below:

System Status	Network interface statu	S					
<ul> <li>Device Info</li> </ul>							
<ul> <li>Interface Status</li> </ul>							
<ul> <li>LAN IP Flow</li> </ul>	LAN1 LAN2	LAN3 LAN4 WAN1					
<ul> <li>Application Flow</li> </ul>	Interface	Туре	Link mode	IP address	MAC address	Receive speed	Send speed
Network Configure	WAN1	WAN port Online	1000M/Full duplex	182.17.0.101	44-D1-FA-45-53-F9	0.40 KB/S	0.39 KB/S
Flow Control Policy	LAN4	LAN port	Disconnect		Merged into D	N1	
	LAN3	LAN port	Disconnect		Merged into L/	N1	
AC Management	LAN2	LAN port	Disconnect		Merged into L/	N1	
Auth Internet Access	LAN1	LAN port	1000M/Full duplex	172.16.0.1	44-D1-FA-45-53-F5	0.04 KB/S	0.04 KB/S
Behavior Control	Device basic informatio	1					
Object Management	Device ID:	Y21180001054, Max Users:80 , Max AP can be r	managed:64				
Safety Protection	Uptime:	1:14:10 up 5 days					
Log Record	Memory utilization:	35% 85.07MB/244.94MB					
VPN	CPU utilization:	0%					
Device Maintenance	Connection monitoring:	0% 116/50000					
	Online users:	Zusers					

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:



System Status	Physical port definition				
Network Configure					_
✓ Interface Configure		# 4LAN + 1WAN		LAN3 LAN4	WAN1
🗀 WAN Configure		- 4LAN + IVIAN	Merged into	Lan1	
LAN/DHCP					
Physical Port Definition		SLAN + 2WAN	LAN1 LAN2	LAN3 WAN2	WAN1
<ul> <li>Route Rule</li> </ul>		SLAN + 2WAN	Merged into Lan1		
🗀 Multi-line Deversion Rules			Merged into carr		
🗀 Static Route		2LAN + 3WAN	LAN1 LAN2	WAN3 WAN2	WAN1
<ul> <li>DDNS</li> </ul>		U ZLAN + SWAN	Merged into Lan1		
<ul> <li>NAT/Port Forwarding</li> </ul>			Merged into Carri		
Flow Control Policy		0	LAN1 WAN4	WAN3 WAN2	WAN1
AC Management		1LAN + 4WAN			
Auth Internet Access					
Behavior Control		Advance  Merge all LAN por	ts into LAN1		

# 03/AC Management

# 3.1 AP Device List

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 VIAunID, as follows As shown in the figure:

System Status																
Network Configure	estart A search		eset AP Del	ete AP Apply o	onfiguration temp	late	Refres	All device	• •	levice mo	del filb	<ul> <li>Search conditions:</li> </ul>	Device IP •			
Flow Control Policy	search	AP						Channel(2.4G/	Channel		AP			Black	AP	
AC Management	SN	name		MAC address	SSID(2.4G/5.8G)	Use	r Status	5.8G)	Analysis	Power	model	AP version	Uptime	white list	remarks	Config
AP List	1	My	172.16.0.102		770A_2.4G 💣			10	2.4G 🤿	100%	FIT-	V5.3-	0:45:25 up	Disable		-
<ul> <li>AP Configure Template</li> </ul>		WTP 1			770A_5.8G 💕	0 ≗ online	36	5.8G 🖈	100%	770A	Build2019041909175	9 5 days				
<ul> <li>AP Upgrade</li> </ul>	 2	My	172.16.0.101	44-D1-FA-72-	MB550-		offline	8	2.4G 🤿	100%	FIT-	V5.3-		Disable	admin	
Auth Internet Access		WTP 1		8E-ED	FITAP_2.4G 💣		onnie	0	2.40 %		MB550	Build2019040810055	6		aumin	
Behavior Control	3	Му	172.16.0.111	44-D1-FA-23-	Wireless_2.4G		online	Auto[3]	2.4G 🔿	100%	PW1200	V3.2-	23:40:29 up	Disable		
Object Management		WTP 1		43-7F	Wireless_5.8G		onine	Auto[44]	5.8G 🖈	100%	PW1200	B20190429100313	4 days			ø
Safety Protection					<b>°</b>											
Log Record	4	Му	172.16.0.112	44-D1-FA-63-	Wireless_2.4G	0.5	online	Auto[11]	2.4G 🔿	100%	FIT-	V5.3-	23:40:5 up	Disable		
VPN		WTP 1		43-98	Wireless_5.8G			Auto[64]	5.8G 🖈	100%	770A	Build2019041909175	9 4 days			
Device Maintenance		Му		44-D1-FA-63-	Wireless_2.4G			Auto[6]	2.4G 🔿	100%	FIT-	V5.3-	23:40:3 up	Disable		-
	5	WTP 1	172.16.0.113	43-E0	Wireless_5.8G		online	Auto[149]	5.86	100%	7704	Build2019041909175		C		ø

	Bandwidth setting Upstream 100000 / Downstream 100000 KBps	
Auth Internet Access	·····	
Behavior Control		
Current user admini2 2 2 21 Dev	time:0110_06_06_16_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)."

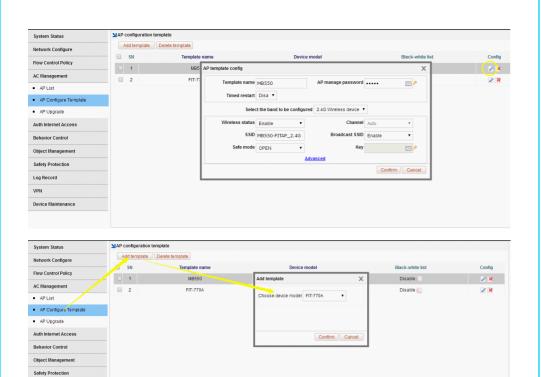
Note: After the definition of the physical port feature is modified, the route needs to be reconfigured. (Note: The version of the X86 platform does not support Ethernet port merge).

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	MAP upgrade				
Network Configure				batch online upgrade to upgrade the firmware Batch Local Upgrade to upgrade the firmware	
Flow Control Policy	v			Refresh Batch online upgrade Batch local i	upgrade Upload mirror
AC Management	SN AP name IP N	AC Status Device model	Current version	Online upgrade	Upload file and Local upgrade
AP List	I My WTP 1 172.16.0.102 44-D1-Fr	-63-43-18 Online FIT-770A	V5.3-Build20190419091759	Already the latest version	-
AP Configure Template	2 My WTP 1 172.16.0.101 44-D1-F/	-72-8E-ED Offline FIT-MB550	-	-	
AP Upgrade	3 My WTP 1 172.16.0.111 44-D1-F	-23-43-7F Online PW1200	V3.2-B20190429100313	V3.3-Build20190621095606 Download file to upgrade	e
Auth Internet Access	My WTP 1 172.16.0.112 44-D1-Fr	-63-43-98 Online FIT-770A	V5.3-Build20190419091759	Already the latest version	
Behavior Control	5 My WTP 1 172.16.0.113 44-D1-Fr	-63-43-F0 Online FIT-770A	V5.3-Build20190419091759	Already the latest version	-
	6 My WTP 1 172.16.0.114 44-D1-F	-63-44-50 Online FIT-770A	V5.3-Build20190419091759	Already the latest version	-
Object Management	7 My WTP 1 172.16.0.115 44-D1-F	-63-43-78 Online FIT-770A	V5.3-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.

e deversion rules						
Delete Note: The diversion rul	es are executed in turns fror	n top to bottom. Can be o	perated by 🕇	arrow to adjust th	ne sequence, 🌁 To	p, 🛣 Bottom
Source address	Time Destina	tion port	Destination	1 IP	Application type	Policy Operation
	Policy shunt rule				×	
	Source address:	According to Address	Liner Lev	n Department		
	ource address.	ANY				
	Time:	ANY				
	Destination IP:	ANY	•	Add		
	Destination Port:	ANY	•	Add		
	Application type:	ANY	•			
	Shunt mode: @ Seesis	e abuet - Course + Deal	Engling address	aa ahuat 🔿 Sauraa	Shunt policy	
	Line selection:	in and it is bounded in Deal	anauon acore		in anom	
	Line					
	U WANT					
	🕈 Session shunt diversi	ion in connection session	n unit			
				Confirm	n Cancel	
	Delete Note: The diversion rul	Detet Note: The diversion rules are executed in turns from Source address Time Destina Policy shunt rule Source address Time Destination Port Application Port Application Port Application type: Une setection: Line Section:	Detete         Note: The diversion rules are executed in sums from top to bottom. Can be on the second of the	Delete         Note: The diversion rules are executed in turns from top to bottom. Can be operated by the source address         Time         Destination port         Destination           Source address         Time         Destination port         Destination port         Destination port         Destination port           Policy shunt rule         Source address.         Correling to the Address.         User: Lee           Destination right         ANY         •           Destination right         ANY         •           Opsimation rule         ANY         •           Destination rule         ANY         •           Shurt mode & Session shurt © Source + Destination address         Line election:	Detete       Note: The diversion rules are executed in turns from top to bottom. Can be operated by the arrow to adjust it         Source address       Time       Destination port       Destination IP         Policy shunt rule       Source address       Address       User       Level       Destination IP         NN <ul> <li>Add</li> <li>Destination IP</li> <li>NN</li> <li>Add</li> <li>Destination IP</li> <li>NN</li> <li>Add</li> <li>Application IP</li> <li>NN</li> <li>Add</li> <li>Application IP</li> <li>NN</li> <li>Add</li> <li>Application IP</li> <li>NN</li> <li>Add</li> <li>Shurt mode:</li></ul>	Detete       Note: The diversion rules are executed in turns from top to bottom. Can be operated by the arrow to adjust the sequence. The sequence of

#### 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 WeChat authentication, 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, scertified 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 so needs to be used in conjunctio	on, that is, if an interface opens n with Portal authentication.	the PPPoE authentication switch, the PPP	oE 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						
<ul> <li>PPPoE Auth</li> </ul>						
<ul> <li>Portal Auth</li> </ul>						
<ul> <li>Radius Billing</li> </ul>						
<ul> <li>Notify Page</li> </ul>						
▼ 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	NPPpoE 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, dick 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
<ul> <li>Auth Configure</li> </ul>	Password-free auth: 9 Enable the password-free authentication function, any account and password can be dialed
<ul> <li>PPPoE Auth</li> </ul>	Passwordniee autor
Portal Auth	Assign DNS according to 'departmentlevel' (in order to assign different DNS to different users, when the 'departmentlevel' where the user belongs is configured DNS, PPPoE service will directly use the DNS configured here and assign DNS to users).
<ul> <li>Radius Billing</li> </ul>	Add Delete
<ul> <li>Notify Page</li> </ul>	🕏 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. 🗷 Bottom
<ul> <li>User Management</li> </ul>	SN Type Name Main DNS Alternate DNS Operation
	PPPoE advance configuration is not added yet, please Add
🗀 Auth User	
🗀 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 contentford for loops (for intranet fault positioning).

System Status	Intranet anomaly detection	1
Network Configure	DHCP detection:	Disabled, click to enable 9 detect whether there are other DHCP servers in the intranet.
Flow Control Policy	Loop detection:	Disabled,click to enable 9 Check whether there are some loops on the intranet (for intranet fault location)
AC Management		
Auth Internet Access	Clear status	
Behavior Control	💡 Intranet DHCP service de	tection result: Please enable "Intranet DHCP detection" first.
Object Management	💡 Intranet loop detection r	sult Please enable "intranet loop detection" first
Safety Protection		
IP-MAC Binding		
Connection Quantity Limit		
LAN Abnormal Detection		
<ul> <li>LAN Attack Protection</li> </ul>		
<ul> <li>WAN Ping Forbid/WAN Login</li> </ul>		
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 I 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			
Network Configure	Add Delete			
	SN Source address	Time	Bandwidth limited	Operatio
low Control Policy		Bandwidth control rule	×	
Smart Flow Control		● ✓ Enable ○ 🗶 Disable		
Bandwidth Control				
Free Flow Control		Source address: According to  Address ANY	User Level Department	
AC Management		Time: ANY	• Add	
		Upstream limit: WUNUMITED		
Auth Internet Access		Downstream limit: WUNLIMITED		
Behavior Control		Downstream mill, is stand		
Object Management				
Safety Protection				
Log Record		Tips: Click icon to edite ba	andwidth Confirm Cancel	
/PN				
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)