





# **XT-1500AC Access Controller**

User manual





www.xontel.com

Kuwait Tel.: 1880005 KSA Tel.: 920011982



**XonTel** 



# 01/ Route Connection:



www.xontel.com





# 02/ Route Settings

## 2.1 Login Device

Connect (Lan) port of device to PC, login in via any internet browser

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

#### Username: admin

#### Password: admin

MULTI-FUNCTION GA	TEWAY Current ope	eration System Stat	us >> Device Info				Refresh   Change	password   Logou				
System Status	Network interface stat	us										
Device Info												
<ul> <li>Interface Status</li> </ul>												
LAN IP Flow	LAN1 LAN2	LAN3 LAN4	WANZ 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	192.168.8.2	94-09-D3-0F-8D-29	218.63 KB/S	115.79 KB/S				
Flow Control Policy	WAN2		WAN port Offline	Disconnect		94-09-D3-0F-8D-28	0.00 KB/S	0.00 KB/S				
	LAN4		LAN port	Disconnect	172.19.0.1	94-09-D3-0F-8D-27	0.00 KB/S	0.00 KB/S				
AC Management	LAN3		LAN port	Disconnect	172.18.0.1	94-09-D3-0F-8D-26	0.00 KB/S	0.00 KB/S				
Auth Internet Access	LAN2		LAN port	Disconnect	172.17.0.1	94-09-D3-0F-8D-25	0.00 KB/S	0.00 KB/S				
Behavior Control	LAN1		LAN port	1000M/Full duplex	192.168.1.1	94-09-D3-0F-8D-24	121.55 KB/S	220.63 KB/S				
Object Management	Device basic informat	▲Device basic information										
Safety Protection	Device ID:	Y23190000388 M	ax Users:512 , Max AP can be managed:512									
Log Record	Uptime:	7:55:35 up 6 days										
VPN	Memory utilization:	12%	233.54MB/1.83GB									
Device Maintenance	CPU utilization:	1%										
	Temperature:	48°C										
	Connection monitoring:	0%	1745/800000									
	Online users:	50 users										
	Device model:	AC950,Firmware ve	ersion:V3.11 B20210109									
Current user:admin[192.168.1.9	07] Device time:2022-03-2	24 11:55:23 Sy	stem alert: 🌍 The device is running normally!									



www.xontel.com





#### 2.2 WAN port settings

Select the network port to configure, and configure the information of the external network, as shown in the following image:

stem Status	WAN configure					
twork Configure	WAN2	WAN2 Interface configure				
Interface Configure	WAN1		Internet access	ADSL/PPPOE Static		
WAN Configure			IP address:	192.168.9.2		
LAN/DHCP			Netmask:	255.255.255.0		
Physical Port Definition			Default gateway:	192.168.9.1		
Subinterface Configure				Please input the IP address	of the specified DNS	
Route Rule			DNS 1:	192.168.9.1	DNS 2:	8.8.8.8
Multi-line Deversion Rules			Line interruption detection:			
Static Route			Please input	two public network server IF	P which ping stable as IP de	ection
		180	Ping detect IP 1:	8.8.8.8	Ping detect IP 2:	8.8.4.4
DDNS		3	Advanced configuration			Save
IAT/Port Forwarding						
w Control Policy						
Management						
h Internet Access						
navior Control						
ject Management						
ety Protection						
lect Management lety Protection ] Record						

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 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 line quality 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.



#### www.xontel.com





#### 2.3 Physical port division:

This feature supports separate and merge port divisions. When the main road is recommended touse 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.





www.xontel.com





### 2.4 Multi-line Deversion Rules

This function is for multiple WAN and Bandwidth superposition; If one WAN only, then no need to configure it.

Such as assign some users to WAN1, some users to WAN2; And these users are divided by some rules, such as IP addess, use time, role and department. Pls kindly to note that multi-line deversion rules is for PPPoE and DHCP, it is auto in static IP, no need to configure it if WAN internet access in static IP.

For example: there are three networking in this gateway, they are WAN1, WAN2; Total 10 users will access into this gateway; They can be divided by IP address: such as IP 172.200.0.2~172.200.0.6 to WAN1, IP 172.200.0.7~172.200.0.12 to WAN2;

The steps showed below:

A. Check the LAN/DHCP for users IP address pool for users and AP.

MULTI-FUNCTION GATE	Current opera	tion Network Configure >> Interface Configure >> LAN/DHCP	Refresh   Change password   Logout   Language English 🗸
System Status	LAN/DHCP		
Network Configure	LAN/DHCP configure	DHCP allocation status	
<ul> <li>Interface Configure</li> </ul>	LAN1	LAN1interface configure	
🗀 WAN Configure		IP Address: 172.200.0.1	
LAN/DHCP		Netmask: 255.255.0.0	
Physical Port Definition		Custom MAC:	
▼ Route Rule		Intranet MAC Broadcast: Disable 🗸	
🗀 Multi-line Deversion Rules		DHCP configure	
🗀 Static Route		Fucntion Enabled: Enabled, click to disable	
<ul> <li>DDNS</li> </ul>		Basic parameters	DHCP static allocation
<ul> <li>NAT/Port Forwarding</li> </ul>		Main DNS: 172.200.0.1	Add Delete
Flow Control Policy		Alternate DNS: 114.114.114.114	SN MAC Address IP Address Remarks Operation
AC Management		Address lease time: 3600 sec	No assigned IP address
Auth Internet Access		The default fill in: <u>3600</u>	
Behavior Control		not assigned to AP	
Object Management		Save	



www.xontel.com





System Status	LAN/DHCP					
Network Configure	LAN/DHCP configure	DHCP allocation	status			
<ul> <li>Interface Configure</li> </ul>	All interface	SN	Interface	IP Address	MAC Address	Terminal Name
	LAN1	1	LAN1	172.200.100.2	44-D1-FA-26-91-C0	FIT-3200
WAN Configure		2	LAN1	172.200.100.3	00-22-68-19-40-B8	USER-20190606WJ
🗅 LAN/DHCP		3	LAN1	172.200.100.4	A2-68-B9-14-99-CD	
Physical Port Definition		4	LAN1	172.200.100.5	C0-D0-12-D1-CE-0D	iPhone
▼ Route Rule		5	LAN1	172.200.100.6	FC-D8-48-DA-C6-11	iPhone
🗀 Multi-line Deversion Rules		6	LAN1	172.200.100.7	84-A1-34-22-31-CD	iPhone
Static Route		7	LAN1	172.200.100.8	D6-82-77-F8-10-68	
		8	LAN1	172.200.100.9	7E-F5-EF-89-B1-9D	
NAT/Port Forwarding		9	LAN1	172.200.100.10	44-D1-FA-B2-35-48	AX820
		10	LAN1	172.200.100.11	98-9E-63-E6-76-F5	iPhone
Flow Control Policy		11	LAN1	172.200.100.12	EA-1C-00-BC-B4-A2	
AC Management		12	LAN1	172.200.100.13	1E-B9-1E-D5-74-6C	
Auth Internet Access		13	LAN1	172.200.100.14	12-0D-06-76-D3-BD	
Behavior Control		14	LAN1	172.200.100.15	86-D0-1B-09-49-28	

B. Set the shunt rule as IP address, then add user IP address based on your request.

MULTI-FUNCTION GATE	Current operation Netw	ork Configure >> Route Rule	>> Multi-line Dever	sion Rules	Refresh   Change passw	ord   Logout   Lan	nguage English 🗸
System Status	Multi-line deversion rules						
Network Configure	Add Delete Note: The d	iversion rules are executed in	turns from top to bo	ottom. Can be operated by 🕇 🖣	arrow to adjust the sequence	ce, Top, Botto	om
<ul> <li>Interface Configure</li> </ul>	SN Source address	Time Destina	ation port	Destination IP	Application type	Policy	Operation
🗀 WAN Configure		Policy shunt rule			×		
LAN/DHCP		Source address:	According to Add	ress User Level Depart	ment		
Physical Port Definition		Time:	ANY	✓ ♣ <u>Add</u>			
<ul> <li>Route Rule</li> </ul>		Destination IP:	ANY	✓ ♣ Add			
Multi-line Deversion Rules		Destination Port: Application type:	ANY	✓ ♣ <u>Add</u>			
Static Route		Shunt mode:  Session	shunt O Source +	Destination address shunt O	Source IP shunt		
DDNS		Line selection:					
<ul> <li>NAT/Port Forwarding</li> </ul>		WAN1					
Flow Control Policy							
AC Management							
Auth Internet Access		Session shunt: diversion	on in connection ses	sion unit			
Behavior Control					Canfirm		
Object Management					Confirm Cancel		
Current user:admin[2.2.2.2] Dev	vice time:2021-11-03 07:46:23 Syste	m alert: 🥥 The device is runr	ning normally!				



www.xontel.com

Kuwait

Tel.: 1880005

KSA Tel.: 920011982





C. Input the name as WAN1 users, input the IP address, confirm to add this shunt rule, all users who get this IP address to get the internet from WAN1.

MULTI-FUNCTION GATI	EWAY	Current ope	ration Network Co	onfigure >> Route Rule >> Multi-line Deversion Rule:	s Refre	sh   Change password   Logout   Lang
System Status	Multi-lin	Address object	management			23
Network Configure	Add	Add	Delete			st the sequence, Top, Bottor
<ul> <li>Interface Configure</li> </ul>	SN	SN SN	Name	Address object	×	on type Policy
<ul> <li>WAN Configure</li> <li>LAN/DHCP</li> </ul>		- 1	ANY	Any addr Name: IP Start IP End IP		×
Physical Port Definition						
<ul> <li>Route Rule</li> </ul>						
Deversion Rules						
Static Route						Shunt policy
DDNS						r.
<ul> <li>NAT/Port Forwarding</li> </ul>						
Flow Control Policy						
AC Management						
Auth Internet Access						
Behavior Control					Confirm Cancel	Cancel
Object Management						Y Caricer

For the other shunt rules, such as you can set all users can get the Internet from WAN1 on the morning, or set finance people to get the internet from WAN1, sales people get the internet from WAN2.

And in the shunt mode, there are session shunt, source+destination address shunt, source IP shunt, what's the different for that?

Session shunt: divide the network connections generated by users to WAN ports; For example, you PC connected to LAN port, and get the Ethernet from WAN1 and WAN2, then make your PC to download and generated many concurrent links, your PC's downlink speed should be total bandwidth of WAN1 and WAN2.

Source+Destination address shunt: according to destination address, we can divide the networking connections to different WAN; For examples: I need to visit google and facebook at the same time but they are different address, we can use Source+Destination address shunt, divide google to WAN1, facebooke to WAN2.

And for some special application will verify the IP address, such as online bank, will visit it based on SSL(TCP433 port), suggest to select source+destination address shunt.



www.xontel.com





Policy shunt rule		X
Source address:	According to Address User Le	evelO Department
Time:	working day	+ Add
Destination IP:	ANY 🗸	🕈 Add
Destination Port:	SSL 🗸	• <u>Add</u>
Application type:	Custom 🗸	+ Custom
Selected application: Shunt mode: O Session Line selection: Line WAN1	shunt  Source + Destination addr	Shunt policy
- Gource - Destination a		
		Confirm Cancel

## **Object Management**

We can set the multi-line deversion rules from Object management also.

For example, I want to divide game to WAN1 internet, we can configure it from Object management in below steps:

MULTI-FUNCTION GAT	EWA	Y	Current operation Object	t Management >> Application Obj	ct >> Custom Application Object Refresh   Change password
System Status	NC	ustomiz	re app object		
Network Configure	C	ustomize	e app object Define app	by domain Define app by obje	ctive IP + port
Flow Control Policy		Add	]		•
AC Management		1	App name	App type	Description
Auth Internet Access		1	110003	Online game	Customize app
Behavior Control		Ľ	175pt	Online game	
		3	300 mero	Undel	App Name: GameI
Object Management	Ч	*	260cafe	Refluere Lindate	Description DDD
<ul> <li>Basic Object</li> </ul>	17	0	Sousaie	Opline copulate	
🖿 Time Object	Ľ	•	3guonero	Online game	
🗀 Source IP Object	E	,	Score	Uliab Video	Confirm Cancel
Dort Object		0	Zfamo	Opline appe	
Destination IP Object		10	name	Web Wriep	
Application Object		10	actum	Opline apme	
		12	android ann dl	Pottware Lindate	
Build-in Application Object		12	android_app_ur	Opline arms	
Custom Application Object		14	annia etora di	Contine game	
Safety Protection		15	appre_store_or	Webcome	
Log Record		18	hattlenst apport	Opling game	
VPN		17	bduede	Web Downloade	
Device Maintenance		18	bilbili	Web Video	
		19	bitiorregt	P7P	
		20	caitonadao	Online name	
		21	caa	Online game	
	5		- 34	Online game	
		_			
					www.xontel.com









## 2.5 DDNS

For the DDNS, the service is from DDNS provider.

Take DDNS server 3322.org for example:

Pls register an account and password from <u>www.3322.org</u>, such as the account is yunlink, password 123456, the dynamic domain name is yunlink.3322.org.

Login in this gateway, enable DDNS, input Dynamic domain name, account, password.

After this configuration, this gateway will get a new IP when dial up the network. Such as this IP is 113.106.99.99. Banding this IP to the dynamic domain name(yunlink.3322.org) under the DDNS provider, then when you visit yunlink.3322.org, it will be resolving as 113.106.99.99, which can visit this gateway through DDNS.



www.xontel.com





MULTI-FUNCTION GATEWAY Current operation Network Configure >> DDNS											
System Status	DDNS										
Network Configure	WAN1	Dynamic domain name configure									
Interface Configure	_	Function enable: Enabled, click to disable									
🗀 WAN Configure		Soprice provider: PubVIIII E Formel name 3322, registration LIPI : www.pub/uin.com									
LAN/DHCP		Dynamic domain name:									
🗀 Physical Port Definition		Account:									
▼ Route Rule		Password:									
🗀 Multi-line Deversion Rules											
Static Route											
DDNS											
<ul> <li>NAT/Port Forwarding</li> </ul>											

Please kindly to note that some DDNS provider can provide the LAN IP only, which can't visit WAN, We can't set this DDNS in this gateway.

## 2.6 NAT/Port Forwarding:

For the port forwarding, let's take an example as below:

IP 192.168.1.100 is IP address for your PC;

LAN port is 3389, WAN port is 7747, which is porting for remote PC's window.

After confirm, can remote visit PC's window through Internet IP:7747.

MULTI-FUNCTION GATE	WAY Current operation Network Cor	nfigure >> NAT/Port Forward	ng					Refresh
System Status	NAT/Port forwarding							
Network Configure	Port forwarding DMZ host Src NAT	Dst NAT						
Interface Configure	Add Delete							
WAN Configure	SN Protocol LAN IP	LAN port WAN	port	WAN			Remark	
LAN/DHCP		3369 11	47	W201				
Physical Port Definition								
🗎 Multi-line Deversion Rules				Dest fermination		×		
Static Route				Port forwarding		^		
- DDNS				Protocol: TCP 🗸				
NAT/Port Forwarding				LAN IP: 192.158.1.100	- 2280			
Flow Control Policy				WAN port range: 7747	~ 7747			
AC Management				-WAN interface selection				
Auth Internet Access				WAN1				
Behavior Control				Remark				
Object Management								
Safety Protection					Confirm	ancel		
Log Record								
VPN								
Device Maintenance								
					www.xonte	I.com		
Zon				Kuwa	ait	KSA		
				<b>T</b> -1-4	000005		000011000	

Tel.: 1880005

Tel.: 920011982





# 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 VLAN ID, as follows as shown in the figure:

MULTI-FUNCTION GA	TEWA	Y	Current ope	eration AC M	anagement >> AP	List									Refresh   Cha
System Status	MAK	P list											Online Al	P quantity/ Total AP:2	/ <mark>3</mark> , AC servio
Network Configure	B	lestart A	P Reset AP	Delete AP	Country Code A	Apply configuration template	Refresh	All	device v device	e model filti 🗸 Searc	n condition	s: Device IF	1 v	search	
Flow Control Policy	0	SN	AP name	Device IP	MAC address	SSID(2.4G/5.8G)	User	Status	Channel(2.4G/ 5.8	G) Channel Analys	is Power	AP model	AP version	Uptime	AP remarks
AC Management	- 0	1	corridor POE	192.168.1.6	44-D1-FA-AC-2F-2	XonTel2G 🔒	0 8	offline	Auto	2.4G 🔿	100%	XT-1800AX			
AP List						XonTel5G 🔷 / XT-17W	<u>۵</u>		Auto	5.8G 🗇	100%				
AP Configure Template	0	2	corridor new	<u>192.168.1.7</u>	D4-67-61-18-20-D	XonTel2G 🙆 9 XonTel5G 🙆 / XT-17W	5 🙎	online	Auto[6] Auto[149]	2.4G <	100%	AX840-P2	V1.0-Build20220211154321	23:53:29 up 2 days	
<ul> <li>AP Upgrade</li> </ul>						XonTel2G 角			Auto[2]	2.4G 🤿	100%				
Wireless Roaming     Auto Channel Select	0	3	Office	192.168.1.6	44-D1-FA-AC-2F-5	XonTel5G 🚔 / XT-17W	23 🤱	online	Auto[124]	5.8G 🖈	100%	AX840-P2	V1.0-Build20220211154321	11:12:25 up 15 days	
Auth Internet Access															
Behavior Control															
Object Management															
Safety Protection						Ν									
Log Record						13									
VPN															
Device Maintenance															
Current user:admin[192.168.1.	97] [	Device	ime:2022-03-2	24 12:37:41	System alert:	The device is running no	rmally!								

#### 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.

2- An AP model can also create multiple templates. Apply to the same floor or geography of the samemodel A scene with a different location.



#### www.xontel.com





## 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 bandwidthmode, the modification of the AP coverage threshold, the modification of the transmit power, and the marking of the device location.

MULTI-FUNCTION GATE	Current operation AC Ma	insgement >> AP Configure Template			Refresh   Change password   Log
System Status	AP configuration template				
Network Configure	Add template Delete template				
Flow Control Policy	SN SN	Template name		Device model	Config
AC Management		Config template	Add template	XT-1800AX	× 1
AP List					
<ul> <li>AP Configure Template</li> </ul>			Choose device model XT-1800AX V		
<ul> <li>AP Upgrade</li> </ul>					
<ul> <li>Wireless Roaming</li> </ul>					
<ul> <li>Auto Channel Select</li> </ul>			Confirm Cancel		
Auth Internet Access			contra contra		
Behavior Control					/
Object Management					
Safety Protection					
Log Record					
VPN					
Device Maintenance					
Current user:admin[192.168.1.97]	Device time:2022-03-24 12:47:34	System alert: 🥥 The device is running normally!			

MULTI-FUNCTION GAT	EWAY	at as AD Configure Templete		Defrech I Change papaward Llage
System Status	AP configuration template	it >> AP configure remplate	11	Kenesini Cinange password   Lugo
Network Configure	Add template Delete template			
Flow Control Policy	SN SN	Template name	Device model	Config
	- 1	Config template	XT-1800AX	/ X
AC management			AP template config	×
AP LIST     AB Configure Template			Template name Config template	
AP Configure remplate			Timed restart Disabl V	
<ul> <li>Wireless Roaming</li> </ul>			Select the band to be configured 2.4G Wireless device v	
<ul> <li>Auto Channel Select</li> </ul>			Wireless status Enable V Channel Auto V	
Auth Internet Access			SSID XonTel2G Broadcast SSID Enable	
Behavior Control			Safe mode WPAPSK/WPA2PSK v Key	
Object Management			Advanced	×
Safety Protection			Contrin	Cancel
Log Record			AP template config	
VPN				
Device Maintenance				
Current user:admin[192.168.1.97]	Device time:2022-03-24 12:48:14 System a	lert: 🌖 The device is running	ormally!	
			www.xontel.co	om y
VonTe			Kuwait	KSA
			T   1000005	

Tel.: 1880005

Tel.: 920011982





### 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 remoteupgrade.

MULTI-FUNCTION GAT	EWAY		Current operatio	n AC Management	>> AP Upgrade						Refresh	Change password   Lo
System Status	MAP	upgra	de									
Network Configure	9	Online	Upgrade: First, clic	k download file, do	wnload the upgrade file to ro	ute, then clic	k upgrade or batch on	line upgrade to upgrade t	he firmware			
Flow Control Policy	- 7	Locall	Upgrade: First, click	the Upload Mirror t	button to upload the upgrade	file, then click	CUpgrade or Batch Lo	Device model filte V	he firmware Refresh	Batch online upgrade	Batch local upgrade	Upload mirror
AC Management		SN	AP name	IP	MAC	Status	Device model	Current ve	rsion	Online upgrade	Upload file and Lo	ocal upgrade
AP List		1	corridor POE	192.168.1.6	44-D1-FA-AC-2F-25	Offline	XT-1800AX	-		-	-	
<ul> <li>AP Configure Template</li> </ul>		2	corridor new	192.168.1.7	D4-67-61-18-20-D9	Online	AX840-P2	V1.0-Build20220	211154321	12	-	
<ul> <li>AP Upgrade</li> </ul>		3	Office	192.168.1.6	44-D1-FA-AC-2F-51	Online	AX840-P2	V1.0-Build20220	211154321	8 <del>55</del>		
<ul> <li>Wireless Roaming</li> <li>Auto Channel Select</li> <li>Auth Internet Access</li> <li>Behavior Control</li> <li>Object Management</li> <li>Safety Protection</li> <li>Log Record</li> <li>VPN</li> <li>Device Maintenance</li> </ul>												
Current user:admin[192.168.1.97]	Devic	e time:2	2022-03-24 12:54:4	18 System ale	rt: 🌖 The device is running r	normally!						



www.xontel.com





# 04/ AC 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, certified Internet access, "Certification switch", select LAN1, enable

the authentication network switch, check the type of "PPPOE dial" that allows Internet access, click Save.

MULTI-FUNCTION GAT	Current opera	ation Auth Internet Access >> Au	th Configure				Refrest					
System Status	Auth switch Free auth	h IP										
Network Configure	One key auth config: Er	One key auth config: Enable all Disable all										
Flow Control Policy	Solution switch here to be used in conjunction with PPPOE authentication, that is, if an interface opens the PPPoE authentication switch, the PPPoE authentication of this interface must be authentication switch also needs to be used in conjunction with Portal authentication.											
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	LAN2	Disable	Disable	Disable	Disable							
PPPoE Auth			- Handle	Diddeid								
<ul> <li>Portal Auth</li> </ul>	LAN3	Disable	Disable	Disable	Disable							
<ul> <li>Radius Billing</li> </ul>	LAN4	Disable	Disable	Disable	Disable							
<ul> <li>Notify Page</li> </ul>												
▼ User Management												
🗀 Auth User												
📮 Auth User Status												
🗀 Department/Level Definition												
Behavior Control												
Object Management												
Safety Protection												
Log Record												
Current user:admin[192.168.1.97]	Device time:2022-03-24 12:5	59:41 System alert: 🥥 The d	evice is running normally!									



www.xontel.com





#### 4.2 PPPOE Authentications:

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

MULTIEUNCTION GAT	EW/AV					
MULTIFONCTION GAT	Cur	rent operation Auth Interne	t Access >> PPPoE Auth			Refresh   Change password   Logo
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 san	ne MAC address dialing:	Disabled,Click to enable	💡 When Enabled, the intranet PPPoE dia	aling request for the same MAC address will be rejected	
Auth Configure	Paseword free	auth:	Disabled Click to enable	P Enable the password, free authentic:	ation function, any account and password can be dialed	
PPPoE Auth	Fassword-nee	auti.	Disabled, Click to citable	Tradic no passivora-neo danenao	and renerion, any account and passivora can be dated	
Portal Auth	Assign DNS a DNS configur	according to 'departmen red here and assign DNS	nt/level' (in order to assign diffe 5 to users).	erent DNS to different users, when	the 'department/level' where the user belongs is co	onfigured DNS, PPPoE service will directly use the
<ul> <li>Radius Billing</li> </ul>	Add	Delete 💡 Note: The ru	lles are executed in turns from top	to bottom.So, top side with high priority i	in DNS assignments. Can be moved by ${f T} iglacksquare$ arrow to adjus	t the sequence, Top, Bottom
<ul> <li>Notify Page</li> </ul>	□ s	SN Type	Name	Main DNS	Alternate DNS	Operation
▼ User Management				PPPoE advance configuration i	is not added yet, please <u>Add</u>	
🗀 Auth User	-					
🗎 Auth User Status						
Department/Level Definition						
Behavior Control						
Object Management	1			R .		
Safety Protection	-					
Log Record	-					
Current user admin[192 168 1 97]	Device time 2022-0	03-24 13:04:40 System	malert 🌖 The device is running no	irmallvi		



www.xontel.com





# 05/ Configure shunt rules

#### 5.1 Configuring shunt rules:

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

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

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

MULTI-FUNCTION GA	TEWAY	Current operation Netw	ork Configure	>> Poute Pule :	>> Multi-line Deversion Rule	-c					Refresh I Change password I I on
System Status	Multi-lin	e deversion rules	ork corrigate -	-> Noute Nule >							nemeen fondinge pasen ere frog
Network Configure	Add	Delete Note: The div	version rules ar	re executed in t	turns from top to bottom. Ci	an be operated	by 🎓 🥾 arrow to adju	ust the sequence, 🏧 Top, 🗟	Bottom		
<ul> <li>Interface Configure</li> </ul>	SN SN	Source address	Time	Destinati	ion port Desti	ination IP	Application t	уре		Policy	Operation
WAN Configure LAN/DHCP		Address:ANY	ANY	A	Policy shunt rule Source address:	According to	Address) User) Li	evelO Department	×	Session shunt WAN2 WAN1	4 🕸 🗷 💌
<ul> <li>Physical Port Definition</li> <li>Subinterface Configure</li> <li>Route Rule</li> </ul>	□ 2	Address:ANY	ANY	۵	Time: Destination IP: Destination Port:	ANY ANY ANY ANY	~			Destination address shunt WAN2 WAN1	<b>春</b> 會 🗷 🗷
<ul> <li>Multi-line Deversion Rules</li> <li>Static Route</li> <li>DDNS</li> <li>NAT/Port Forwarding</li> </ul>					Application type: Shunt policy Shunt mode:  Session Line selection: Line WAN2	ANY shunt O Sourc	<ul> <li>+ Destination addre</li> <li>WAN1</li> </ul>	ess shunt 🔿 Source IP shur	nt		
Flow Control Policy					Pe	olicy shunt rule					
AC Management					Session shunt: diversion	on in connection	session unit				
Auth Internet Access	-1										
Behavior Control	-							Confirm	Cancel		
Object Management				L							
Safety Protection	Device tim	e-2022_03_24 14-50-45	System alert	The device is	s running normally						



www.xontel.com

Kuwait Tel.: 1880005 KSA Tel.: 920011982





#### 5.2 Configure bandwidth speed limit policy:

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

**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).

MULTI-FUNCTION GAT	EWAY Current	operation Flow Control Policy >> Bandwid	th Control				Refresh   Ch
System Status	Bandwidth control						
Network Configure	Add Delet						
Flow Control Policy	- O SN	Source address	Tim	e		Bandwidth limited	
Smart Flow Control			Bandwidth contro	l rule		×	
Bandwidth Control			. Sector	Disable			
Free Flow Control			Source address:	According to  Addres	s O User O Level O De	partment	
AC Management			Terry	ANY	✓ <del>♦</del> <u>Ad</u>	d	
Auth Internet Access			Upstream limit:		V <u>V</u>	<u> </u>	
Behavior Control			Downstream limit:				
Object Management	-		ł				
Safety Protection	-						
Log Record	-						
VPN	-		Т	ips: Click icon to edite t	bandwidth Confirm	Cancel	
Device Maintenance					4		
	1.1						
Current user:admin[192.168.1.97]	Device time:2022-03-24	4 14:58:18 System alert: 🔮 The devic	ce is running normally!				







## 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 ford for loops (for intranet fault positioning).

MULTI-FUNCTION GAT	EWAY	eties Cafeb Destantion v. I AN A	Los and Data data			Dafrach I Change pa	eeword			
System Status	Intranet anomaly detect	ation Safety Protection >> LAN A	onormai Delection			Refreshi j unange pas	ssword			
Network Configure	DHCP detection:	Enabled, click to disable	💡 detect whether there are other D	HCP servers in the intranet.						
Flow Control Policy										
AC Management	Loop detection:	Enabled, click to disable	V Check whether there are some lo	ops on the intranet (for intranet fault lo	cation)					
Auth Internet Access	PPPoE detection:	Enabled, click to disable	g detect whether there are other Pl	PPoE services in the intranet.						
Behavior Control	Clear status									
Object Management	O Intranet DHCP service	e detection result: No other DH	CP service have been found on the intra	net						
Safety Protection	O Intranet loop detection	Intranet loop detection result: No found any intranet port with loops!								
IP-MAC Binding	O Intranet PPPoE service	C Intranet PPPoE service detection result:No other PPPoE services have been found on the intranet								
<ul> <li>Connection Quantity Limit</li> </ul>										
LAN Abnormal Detection										
LAN Attack Protection			23							
WAN Ping Forbid/WAN Login										
Log Record										
VPN										
Device Maintenance										
Current user:admin[192.168.1.97]	Device time:2022-03-24 15:	34:28 System alert: 🔵 The o	device is running normally!							



www.xontel.com