

XonTel

XT-2500AC Access Controller User Manual





Menu

1.	Product Overview	4
2.	WEB Login	4
3.	Product Features	5
	 3. 1. System Status Device Info Interface Status LAN IP Flow Application Flow 	5 5 6 7 8
	3. 2. Network Configure	9
	WAN Configure	9
	LAN/DHCP Physical Port Definition	10
	Multi-line Diversion Rules	
	Static Route	15
	DDNS	16
	NAT/Port Forwarding	17
	3. 3. Flow Control Policy Smart Flow Control	19 19
	Bandwidth Control	19
	Free Flow Control	20
	3. 4. AC Management	21
	AP List	21
	AP Configure Template	24
	AF Opgrade	24 25
	Auto Channel Select	
	3 5 Auth Internet Access	27
	Auth Configure	27 27
	PPPoE Auth	27
	Portal Auth	28
	Radius Billing	29
	Auth User	29
	Auth User Status	30
	Department/Level Definition	30
	3. 6. Behavior Control	31
	Application Firewall	31
	URL Redirect	32
	Domain Redirect	32

شركــة زونـتـل تـكنـولـوجـي للتجارة العامة ذ.م.م



3.7.	Object Management	33
-	Time Object	33
:	Source IP Object	33
	Port Object	34
	Destination IP Object	34
I	Built-in Application Object	35
	Custom Application Object	35
3.8.	Safety Protection	37
	IP-MAC Banding	37
(Connection Quantity Limit	37
l	LAN Abnormal Detection	38
	LAN Attack Protection	38
,	WAN Ping Forbid/WAN Login	39
3.9.	Log Record	39
ļ	User Auth Log	39
(Online User Log	40
	Interface Flow Log	40
;	System Log	41
3.10	. VPN	41
	PPTP	41
	L2TP	42
,	VTUNS	43
3.11.	Device Maintenance	44
l	Firmware Upgrade	44
I	Modify Password	45
	Authority Management	45
	Ping Detection	46
(Configure File Maintenance	47
l	Restart Device	48
-	Time Task	48
-	Time Synchronization	49
(Cloud Configure	50



1. Product Overview

XonTel XT-2500AC is a multi-functional flow control gateway wireless control AC, which has the function of multi-line shunting and multi-line overlapping load balancing. It provides wireless data control services with large capacity, high performance, high reliability, easy installation and maintenance, and has the advantages of flexible networking, green energy conservation, etc.

2. WEB Login

- 2.1. Power on gateway, when "Run" led blink regularly, connect computer to LAN port by ethernet cable.
- 2. 2. Visit default LAN IP 172.16.0.1:2011 in browser, default username & password are both: admin

Main page after login successfully:

P	System Status	^	Network interface statu	15	
	Device Info				
	Interface Status				
	LAN IP Flow		LAN1 WAN5	WAN4 WAN3 WAN2 WAN1 EXT1 EXT2	
	Application Flow		Interface	Туре	Link mode
	Network Configure	\sim	EXT2	LAN port	Disconnect
Ø	Flow Control Policy	\sim	EXT1	LAN port	Disconnect
0	AC Management		WAN1	WAN port Online	1000M/Full duplex
50	AC management	V	WAN2	WAN port Offline	Disconnect
9	Auth Internet Access	V	WAN3	WAN port Offline	Disconnect
ļ îj	Behavior Control	V	WAN4	WAN port Offline	Disconnect
60	Object Management	V	WAN5	WAN port Offline	Disconnect
Ο	Safety Protection	\sim	LAN1	LAN port	2500M/Full duplex
₽	Log Record	V	Nevice basic information	n	
Ē	VPN	\sim	Device ID:	Y23230000114, Max Users:512 , Max AP can be managed:512	
*	Device Maintenance	\sim	Uptime:	0:56:16 up 42 days	
			Memory utilization:	6% 461.37MB/7.54GB	
			CPU utilization:	2%	
			Connection monitoring:	1% 5371/800000	
			Online users:	82 users	

+965 1880005



3. Product Features

3.1. System Status

Display a comprehensive information of the gateway, including the status of each interface, information of intranet clients, uplink and downlink, real-time uplink and downlink speed and total traffic of each application.

Device Info

X	System Status	^	Vetwork interface status							
	Device Info Interface Status					1		2		
	LAN IP Flow Application Flow		LAN1 WAN5 WAN4 W	/AN3 WAN2 WAN1 EXT	1 EXT2	Туре	Link mode	IP address	MAC address	Receive sr
@	Network Configure	\sim	EXT2			LAN port	Disconnect	172.23.0.1	7C-27-3C-48-B4-0D	0.00 KB/
	Flow Control Policy	V	EXT1			LAN port	Disconnect	172.22.0.1	7C-27-3C-48-B4-0C	0.00 KB/
0	AC Management		WAN1			WAN port Online	1000M/Full duplex	192.168.8.2	7C-27-3C-48-B4-0B	124.84 KE
÷0	AC management	v	WAN2			WAN port Offline	Disconnect	~	7C-27-3C-48-B4-0A	0.00 KB/
•	Auth Internet Access	\sim	WAN3			WAN port Offline	Disconnect	-	7C-27-3C-48-B4-09	0.00 KB/
414	Behavior Control	V	WAN4			WAN port Offline	Disconnect	-	7C-27-3C-48-B4-08	0.00 KB/
50	Object Management	V	WAN5			WAN port Offline	Disconnect	-	7C-27-3C-48-B4-07	0.00 KB/
Ο	Safety Protection	\sim	LAN1			LAN port	2500M/Full duplex	192.168.1.1	7C-27-3C-48-B4-06	86.20 KB
₽	Log Record	v	Device basic information 3							
Ē	VPN	V	Device ID: Y232300001	114 Max Users:512 , Max AP can be	managed:512					
*	Device Maintenance	\sim	Uptime: 1:0:15 up 42	2 days						
			Memory utilization: 6%	453.34MB/7.54GB						
			CPU utilization: 1%							
			Connection monitoring: 1%	6008/800000						
			Online users: 82 users	4						
			Device model: AC950,Firm	ware version:V5.11 B20231125	5					

SN 1: Display the physical connection of the interface, and the color icon represents connected

- SN 2: Display interface IP address
- SN 3: Device unique ID, used for remote access
- SN 4: User quantity (AP quantity is excluded)
- SN 5: Device model name

Click online users to filter AP and terminals according to three types of users, IP and MAC addresses, and view the corresponding relationship between IP and MAC.



شركة زونـتـل تـكنـولـوجـي للتجارة العامة ذ.م.م

Online	user list											
VIP-N	IP-MAC address table											
	otice: click 膨 to bind the IP	address and MAC address, click 😤 to Unbindg, click	袅 can be quickly add	led as a user ob	ject!							
Use	r 🗸	Search										
User IP	IP	User	MAC	Auth method	Connection time	Operation						
1	<u>192.168.234.3</u>	-	00-21-CC-71-3D-49		11-17 09:08:35	2 4 🔍						
2	<u>192.168.234.4</u> 🕑	-	44-D1-FA-59-2F-ED		11-17 15:12:26	<mark>2</mark> , 🙈						

Interface Status

Check the comprehensive information of current interfaces. SN 1: View interface details and WAN port speed.

쟟	System Status	~	Interface status												
	Device Info		Line detection												
	Interface Status		Interface name1	Interface type	Upstream	Downstream	IP	Status	Connection quantity	Line quality	Upstream speed(KB/S)	Downstream speed(KB/S)	Total upstream flow	Total downstream flow	Operation
	LAN IP Flow				bandwidth(KB)	bandwidth(KB)									
	Application Flow		LAN1	LAN port		-	192.168.1.1	Online		-	57.60	94.31	156.80GB	633.00GB	0
æ	Network Configure		WAN5	DHCP	100000	100000	-	Offline	14 (-	-	-	-	· · L)	0
45	Network Configure	v	WAN4	DHCP	100000	100000		Offline	14 C	2	121				0
Ś	Flow Control Policy	V	WAN3	Static IP	100000	100000	-	Offline						-	0
(;;0	AC Management	V	WAN2	Static IP	100000	100000		Offline	-	-	-	-			0
•	Auth Internet Access	\sim	WAN1	Static IP	100000	100000	192.168.8.2	Online	4955	Excellent	52.55	93.77	141.58GB	632.29GB	0

LAN1	LAN port	-		192.168.1.1	Online	-	-	45.42	154.11	156.80GI
WAN5	DHCP	100000	100000		Offline		-		-	-
WAN4	DHCP	100000	100000	Interface details					-	
WAN3	Static IP	100000	100000	Interface name	e: LAN1		S	end speed :154.11	-	
				Interface statu	s: Enable		R	eceive speed:45.42		
WAN2	Static IP	100000	100000	Interface type	e: LAN(Intranet po	ort)		82	5	5
WAN1	Static IP	100000	100000	Operation mode	e: 2500M/Full dup	lex			153.48	141.58GF
EVEA	1.441.554			TCPMS	5: 1460					
EXIT	LAN port	-		MTU	J: 1500				0.00	0.00B
EXT2	LAN port	-	-	MAG	C: 7C-27-3C-48-B4	H-06			0.00	0.00B
				IP addres	s: 192.168.1.1					
				Netmas	k: 255.255.255.0					



LAN IP Flow

View the traffic information independently used by each terminal of the intranet, as well as the link tracking table.

			_													
2	System Status	^	S Intr	anet IP flow												
	Device Info			Upstream rat	te — Downstream rate]			Real tim	e total flow chart						
	Interface Status		1	2000												
	LAN IP Flow			1500 -							_					
	Application Flow		(S													
	Network Configure	\sim	it (KB/	1000-												
kő	Flow Control Policy	×	5													
0	AC Management			500 -												
50	AC Management	~														
9	Auth Internet Access	V		0 11:45 35	11:45 35 11:45 3	6 11:45	36 11:45 37	11:45 37	11:45 38	11:45 38	11:45 39	11:45 39	11:45 40	11:45 40 11:45 41	11:45 41	1 11
649	Behavior Control	V	Us Vs	er flow												
50	Object Management	\sim		10					Terminal			TOD		UDD compation available	Downstream rate	Upstream ra
σ	Safety Protection	V	SN	IP.	MAC	USEI			Terminal	type		TCP	connection quantity	ODP connection quantity	(KB/S)	(KB/S)
f≣}	Log Record	\sim	1	<u>192.168.1.42</u>	A2-FC-83-73-2B-B6								30	30	199.00	3.00
	VDN		2	192.168.1.129	0A-25-30-8C-4B-7D	-							12	8	11.00	1.00
	VFN	v	3	192.168.1.67	74-4C-A1-A2-F0-67	-			LAPTOP-IR	/34T2M			29	81	8.00	7.00
\$	Device Maintenance	V	4	<u>192.168.1.53</u>	E4-F8-9C-2B-E1-E3				DESKTOP-B	RL8MA0			21	84	6.00	4.00
			5	192.168.1.113	B0-7D-64-40-D6-48	-			FOUADKA	LLAS			30	47	4.00	2.00
			6	192.168.1.110	6C-02-E0-7F-C3-A7	-			DESKTOP-IN	CMA82			12	50	2.00	12.00
			7	192.168.1.77	00-E0-70-AD-EF-BE	-			-				102	33	2.00	2.00
			8	192.168.1.179	D4-67-61-C7-05-7D	-			-				2	3	1.00	0.00
			9	192.168.1.200	00-0C-29-BC-49-D8				-				2	1	1.00	0.00
			10	192.168.1.167	A0-92-08-37-5B-1C	-			wlant				1	2	0.00	0.00
			11	192.168.1.47	2A-8A-35-0C-6F-0C	-							0	0	0.00	0.00
			12	192.168.1.103	D4-67-61-D4-2C-A5	-			2				0	12	0.00	0.00
			13	192.168.1.74	B8-08-CF-EF-E5-61	-			DESKTOP-6	M6083I			16	81	0.00	0.00

View the traffic type, speed, and number of protocol connections of selected user.

	融合网关												
P	System Status	^	Intranet IP flow										
	Device Info		- Upstream rate - Downstream rate	e			Real time total	flow chart					
	Interface Status		4000										
	LAN IP Flow		3000 -	٨									٨
	Application Flow		(S) (S)	\wedge		\wedge							\land
۲	Network Configure	\sim	¥ 2000-		\wedge	$\langle \rangle$			\wedge			\wedge	
Ø	Flow Control Policy	\sim	1000			$/ \rangle$		\wedge /			\wedge	$/ \vee$	
(i0	AC Management	\sim		User Link Tracking Table(192	168.1.66:192.168.1.66)				\setminus /		/ *		
۲	Auth Internet Access	\sim	0 11:45 40 11:45 50	SN Application name	Application type	Sond(KB/S)	Pacalya(KP/S)	TCP link quantity	UDP link quantity	00 11:4	7 10 11:47 20	11:47 30	11
Į∳Į.	Behavior Control	\sim	User flow	1 ssl	WehPane	27.00	20.00	16	0				
5	Object Management	\sim			incoroge		20100					Downstream rate	Upstream ra
D	Safety Protection	\sim	SN IP MAC							connection quantity	UDP connection quantity	(KB/S)	(KB/S)
(II)	Log Record	\sim	1 192.168.1.66 50-C2-E8-72-15-CF							12	2	309.00	21.00
	VPN	~	2 <u>192.168.1.74</u> B8-08-CF-EF-E5-61							27	85	291.00	37.00
	Device Maintenance		3 <u>192.168.1.44</u> B0-7D-64-43-1A-93							46	76	213.00	74.00
	Device maintenance	v	4 <u>192.168.1.67</u> 74-4C-A1-A2-F0-67							28	88	8.00	5.00
			5 <u>192.168.1.53</u> E4-F8-9C-2B-E1-E3							26	71	4.00	5.00
			6 <u>192.168.1.83</u> 9C-DA-3E-7C-07-0E							27	32	4.00	3.00
			7 <u>192.168.1.68</u> E6-92-3E-50-47-5E				*			7	21	1.00	8.00



Application Flow



View the proportion of download and upload traffic.

🗲 +965 1880005 🛛 🌐 www.xontel.com 🖉 💌 kuwait@xontel.com



3.2. Network Configure

Used to set the configuration information of the external network and the internal network, and the routing of the internal network.

WAN Configure

1	System Status	V	WAN configure			
	Network Configure	^	WAN5	WAN1 Interface configure		
	WAN Configure		WAN4	Internet access	○ ADSL/PPPOE	
	LAN/DHCP		WAN3	IP address:	192.168.8.2	
	Physical Port Definition		WAN1	Netmask	255.255.255.0	
	Multi-line Diversion Rules	s		Default gateway:	192.168.8.1	
	Static Route			DNS 1:	Please input the IP address of the specified DNS 192.168.8.1	DNS 2: 8.8.8.8
	DDNS			Line interruption detection:		
	NAT/Port Forwarding			Ping detect IP 1:	8.8.8.8 Ping dete	ect IP 2: 8.8.4.4
	Flow Control Policy	\sim		Advanced configuration		Save
()?	AC Management	V				
9	Auth Internet Access	\sim		Smart QoS Ena	able	
∳ Ŷ ↓	Behavior Control	\sim		Bandwidth setting Up: Line Quality/Packet Exc	stream 100000 / Downstream 100000 KBps	
50	Object Management	\sim		Loss Rate/Delay		
	Safety Protection					

Internet access-Select the Internet access mode according to the actual situation

- **ADSL/PPPOE**: Fill account and password supplied by operator
- Static IP: Fill IP, Netmask, Gateway, DNS supplied by operator
- **DHCP**: Directly insert the line provided by the operator to obtain the IP address.

Line interruption detection - Ping detection (Google, Facebook...). If the continuous ping fails, the delay is high, and there is no data interworking, it will be considered as a line exception. When the quality is poor, dial-up attempts to redial, DHCP attempts to retrieve, and fixed IP addresses are processed offline. Offline lines do not participate in the load. Multi line environment, it is recommended to enable line interruption detection, and automatic switching can only be performed when individual lines are offline.

Marks: If the operator prohibits ping, line detection cannot be enabled. PING detection IP: 0.0.0.0 by default, which means the built-in IP (114DNS, Tencent official website, Alibaba DNS, Baidu DNS) is used for detection. If the local DNS can be pinged, or other public IP with lower latency can be pinged, it can be filled in as the detection basis.



Tips: It is suggested that professional technicians should fill in the test IP after evaluation.

LAN/DHCP

SN 1: LAN1 IP address.

SN 2: IP address pool: IP address for users & APs managed by gateway. Can't be same IP segment as obtained WAN IP address.

SN 3: DHCP, can manage banded IP and MAC.

*	System Status	\sim	LAN/DHCP	
	Network Configure	^	LAN/DHCP configure	DHCP allocation status
	WAN Configure		💼 LAN1	LANIInterface configure
	LAN/DHCP		EXT1	IP Address: 192.168.1.1
	Physical Port Definition		EXT2	Netmast: 255.255.0
	Subinterface Configure			
	Multi-line Diversion Rules			Intranet MAC Broadcast Enable
	Static Route			Operation mode: Self-nerotation
	DDNS			
	NAT/Port Forwarding			DHCP configure
Ś	Flow Control Policy	\sim		Fuchtion Enabled; Enabled citick to disable
()?	AC Management	V		Basic parameters DHCP static allocation
۲	Auth Internet Access	v		Main DNS 122 158 1 1 Add Delete
498	Behavior Control	V		SN MAC Address IP Address Remarks Operation
	Object Management	V		Alemate Lines: 192.106.1.1 IP-MAC is not currently defined
	Safety Protection	~		Address lease time: 3600 sec The default fill in 3800
0	Salety Protection	, ,		IP assignment polcy of an AP: UP assigned only to AP UP not assigned to AP
Ð	Log Record	\sim		IP address and
Ē	VPN	V		Start IP End IP
\$	Device Maintenance	V		IP address pool 192.168.1.5 192.168.1.199



View DHCP allocation status

*	System Status		LAN/DHCP				
	Network Configure	•	LAN/DHCP configure	DHCP allocation status			
	WAN Configure		All interface	SN	Interface	IP Address↑	MAC Address
	LAN/DHCP		M LAN1	1	LAN1	192.168.1.7	00-A8-59-FB-A5-74
	Physical Port Definition		EXT1	2	LAN1	192.168.1.9	0C-11-05-07-8B-68
	Subinterface Configure		EXT2	3	LAN1	192.168.1.10	D4-67-61-D4-2E-79
	Multi-line Diversion Rules			4	LAN1	192.168.1.11	00-A8-59-FB-F9-A1
	Static Route			5	LAN1	192.168.1.12	D4-67-61-A9-64-B0
	DDNS			6	LAN1	192.168.1.13	D4-67-61-D4-05-5B
	NAT/Port Forwarding			7	LAN1	192.168.1.14	D4-67-61-C7-09-76
رکيا.	Flow Control Policy V	,		8	LAN1	192.168.1.15	4C-3B-74-03-8E-FD

Markes: If gateway works as by pass mode, need to select "IP assigned only to AP".

	System Status	\sim	LAN/DHCP									
	Network Configure	^	LAN/DHCP configure	DHCP allocation st	atus							
	WAN Configure		🛋 LAN1	LAN1interface config	ure							
	LAN/DHCP		M EXT1					IP Address	192.168.1.1			
	Physical Port Definition		EXT2					Netmask	255,255,255.0			
	Subinterface Configure							Custom MAC	· [].			
	Multi-line Diversion Rule	s						Intranet MAC Broadcast	Enable V			
	Static Route							Operation mode	Colf accetiation			
	DDNS							Operation mode				
	NAT/Port Forwarding			DHCP configure								
$\langle \rangle$	Flow Control Policy	\sim						Fucntion Enabled: Ena	bled,click to disable)		
((;;	AC Management	V		Basic parameters						DHCP s	static allocation	
•	Auth Internet Access	\sim			Main DNS:	192,168,1,	1			A	dd Delete	
41	Behavior Control	\sim		Alte	ernate DNS:	102 168 1	1				SN	MAC Address
궘	Object Management	\sim		Ait	ernate Divo.	192.108.1.	-					
_	Safety Protection	V		Address	s lease time:	3600	S	ec The default fill in:3600				
	Les Breed			IP assignment poli	cy of an AP:	IP assigne	ed only to AP 🗌	IP not assigned to AP				
Ð	Log Record	\sim		ID address as at								
Ē	VPN	\sim		IP address pool	Start IP		End IP					
*	Device Maintenance	\sim		IP address pool	192.168.1	.5	192.168.1.1	99				



Physical Port Definition

Divide multiple WAN ports and LAN ports according to requirements.

P	System Status	\sim	Physical port definition
	Network Configure	^	
	WAN Configure		LAN1 LAN2 LAN3 LAN4 LAN5 WAN1
	LAN/DHCP		
	Physical Port Definition		
	Subinterface Configure		LAN1 LAN2 LAN3 LAN4 WAN2 WAN1
	Multi-line Diversion Rules	5	○ 4LAN + 2WAN
	Static Route		
	DDNS		LAN1 LAN2 LAN3 WAN3 WAN1
	NAT/Port Forwarding		O 3LAN + 3WAN
Ś	Flow Control Policy	V	الحها لهها لهها لعها لعها العبا
((;0	AC Management	V	
•	Auth Internet Access	v	
ψţ	Behavior Control	V	
50	Object Management	V	
Ο	Safety Protection	v	ILAN + 5WAN IN
₽	Log Record	V	
Ē	VPN	V	
*	Device Maintenance	v	
			Save Note: After the physical port feature definition is modified, the router needs to be reconfigured.



Multi-line Diversion Rules

-	System Status	\sim	🔰 Multi	-line deversion	ules					
@	Network Configure	^	Ad	ld Delete	Note: The diversion rules an	re executed in turns	from top to bottom. Can	be operated by 🏦 🦊 arrow to adjust	the sequence, Top, Bottom	
	WAN Configure		SI	4	Source address		Time	Destination port		Destination IP
	LAN/DHCP							0	There is no diversion rule defined yet,	please <mark>Add</mark>
	Physical Port Definition							Policy shunt rule		x
	Subinterface Configure									0.0
	Multi-line Diversion Rule	s	1					Source address:	According to Address User Le	Add
	Static Route							Time:	ANY 🗸	4 Add
	DDNS							Destination IP:	ANY 🗸	Add
	NAT/Port Forwarding							Destination Port:	ANY 🗸	+ Add
Ø	Flow Control Policy	\sim						Application type:	ANY	Shunt policy
6	AC Management	\sim						Shunt mode: O Session	n shunt () Source + Destination addre	ess shunt () Source IP shunt
 (a)	Auth Internet Access							Line		
9	Auth Internet Access	v						WAN5	WAN4	
ŶŶŶ	Behavior Control	V						WAN3	WAN2	
60	Object Management	V						WAN1		
Ο	Safety Protection	\sim						Session shunt: diversion	on in connection session unit	
₽	Log Record	\sim								
Ē	VPN	V								Confirm Cancel
*	Device Maintenance	\sim								

Single line cannot be configured with shunting rules; When two or more WAN ports are connected to the external network, different source addresses and diversion modes can be selected for setting. There are three modes:

- Session shunt: Distribute all Internet connections to each line. For example, Jason started IDM downloading. Many concurrent links of IDM were distributed to three lines, and each line was connected to generate traffic, which was summarized to IDM, achieving the effect of bandwidth superposition.
- Source+Destination address shunt: On the basis of session shunting, determine that the source address and destination address are loaded onto each line. For example, Zhang San opened three websites at the same time, namely ICBC, Jingdong Mall and Taobao (for the purpose of explanation, it is considered that the IP addresses of these three websites are only A, B and C). Use source+destination address diffluence to divert all users to three external networks. The final effect is: Zhang San's ICBC fixed line 1; Jingdong Mall fixed line 2, Taobao fixed line 3.

+965 1880005 🛛 🌐 www.xontel.com 💿 kuwait@xontel.com



 Source IP shunt: It is always shunted on one line according to the source address. Taking the environment of 3 extranets and 9 people online as an example, IP shunts all people to 3 extranets. The result is: Zhang San fixed line 1; Li Si fixed route 2; Wang Wu fixed route 3; Zhao Liu fixed the first route, apportioning the 9 people on 3 lines in turn. Since everyone is fixed on a line, the speed of Internet access is limited by the bandwidth of the line.

Weight: weight can be understood as "proportion", which is only effective for IP shunting. Taking the environment where 12 people access the Internet in 3 extranets as an example, IP shunting owners are shunted to 3 extranets, with line 1 weighting 3, line 2 weighting 2, and line 3 weighting 1. As a result, 6 people will be awarded for line 1, 4 for line 2, and 2 for line 1.

(The weight is the proportion. For example, the weight of the three lines is 4, 2, 1, and the effect is 4:2:1)

Conclusion: IP shunting is applicable to the condition that there are a lot of lines, so as to reduce the IP of WAN ports being consumed by multiple people at the same time and improve the utilization of IP. It is mainly used to do Taobao in the community broadband, and Amazon e-commerce users are also used in some game studios (because too many people access from a WAN port, e-commerce may regard it as a swipe and hang up).

Session shunt is applicable to streaming multi-threaded download services that require extreme streaming, such as streaming P2P downloads and game update servers.

Source+Destination address shunt, is recommended by default to achieve better compatibility on the basis of session splitting.



Static Route

Generally, when using the private network, it is required to set the terminal to access the corresponding IP segment and forward it to the corresponding gateway.

1	System Status	V	Static routing	
	Network Configure	^	Static routing Routing information	
	WAN Configure		Add Delete	
	LAN/DHCP		SN Destination network Gateway	
	Physical Port Definition		1 192.168.12.0/255.255.255.0 192.168.1.1 Static routing config X	
	Subinterface Configure			
	Multi-line Diversion Rule	s	Destination address 192.168.12.0	
	Static Route		Netmask 255.255.255.0	
	DDNS		Gateway 192.168.1.1	
	NAT/Port Forwarding		Confirm Cancel	
2</td <td>Flow Control Policy</td> <td>\sim</td> <td></td> <td></td>	Flow Control Policy	\sim		
((;;	AC Management	v		
•	Auth Internet Access	\sim		
ģij	Behavior Control	\sim		
50	Object Management	\sim		
	Safety Protection	\sim		
₽	Log Record	V		
Ħ	VPN	\sim		
*	Device Maintenance	\sim		

Check static routing form

P	System Status	\sim	Statio	c routing					
	Network Configure	^		Static routing	Static routing				
	WAN Configure		SN			Destination address	Gateway	Interface	Routing type
	LAN/DHCP		1			127.0.0.0/255.0.0.0	220	WAN5	Network segment, local
	Physical Port Definition		2			127.0.0.0/255.0.0.0	-	WAN4	Network segment, local
	Subinterface Configure		3			172.22.0.0/255.255.0.0		EXT1	Network segment, local
	Multi-line Diversion Rule	s	4			172.23.0.0/255.255.0.0	-	EXT2	Network segment, local
	Static Route		5			192.168.0.0/255.255.255.0	-	WAN3	Network segment, local
	DDNS		6			192.168.1.0/255.255.255.0	-	LAN1	Network segment, local
	NAT/Port Forwarding		7			192.168.2.0/255.255.255.0		WAN2	Network segment, local
10	Flow Control Policy	v	8			192.168.8.0/255.255.255.0	-	WAN1	Network segment, local
0			9			192.168.12.0/255.255.255.0	192.168.1.1	LAN1	Network segment, forwarding





DDNS

The route is managed from the external network, that is, the dynamic domain name is accessed through the dynamic domain name, which is mainly provided by the dynamic domain name service provider.

P	System Status 🗸 🗸	DDNS
۲	Network Configure	WAN1 Dynamic domain name configure
	WAN Configure LAN/DHCP Physical Port Definition Subinterface Configure Multi-line Diversion Rules Static Route	WAN2 WAN3 WAN4 WAN5 Dynamic domain name: Account: Password:
	DDNS	
	NAT/Port Forwarding	
Ø	Flow Control Policy 🗸 🗸	

Marks:

1, Routing is only for IP reporting. The correctness and speed of the resolution depend on the 3322 service provider.

2, Some operators allocate the Internet access IP as a LAN IP, such as 10.10.99.99, which is a LAN IP and cannot be accessed by the external network. If it is a LAN IP, it is useless to configure a dynamic domain name.



NAT/Port Forwarding

Used to map LAN ports to the public network

*	System Status	\sim	N	AT/Po	ort forwarding				
	Network Configure	^		P	ort forwarding		DMZ host	s	Sic NAT Dst NAT
	WAN Configure			Add	Delete				
	LAN/DHCP			SN	Protocol	LAN IP	LAN port	WAN port	WAN
	Physical Port Definition			1	UDP	<mark>1</mark> 92.168.1.109	5060	5092	Port forwarding X
	Subinterface Configure			2	TCP	192.168.1.9	5080	5080	
	Multi-line Diversion Rules	s		3	TCP	192.168.1.9	10000-20000	10000-20000	0 Protocol: TCP 🗸
	Static Route			4	TCP	192.168.1.8	80	80	LAN IP: 192.168.1.100
	DDNS			5	TCP	192.168.1.185	8000	8000	LAN port range : 80 ~
	NAT/Port Forwarding			6	UDP	192.168.1.179	4569	4569	WAN port range: 80 ~
	Flow Control Deliay			7	TCP	192.168.1.181	8081	8081	WAN Interface selection
KD	Flow Control Policy	~		8	TCP	192.168.1.181	443	8082	
(in)	AC Management	V		9	TCP	192.168.1.109	5091	5091	Remark
9	Auth Internet Access	\sim		10	UDP	192.168.1.179	10000-20000	10000-20000	0
ţţļ	Behavior Control	\sim		11	TCP	192.168.1.181	13505	13505	Confirm Cancel
5	Object Management	V		12	TCP	192.168. <mark>1.11</mark> 8	5061	5061	WAN2,WAN1
D	Safety Protection	\sim		13	TCP	192.168.1.179	6040	6040	WAN1
₿	Log Record	~		14	TCP	192.168.1.140	443	4443	WAN2,WAN1

DMZ Host

To solve the problem that the external network cannot access the internal network server after the firewall is installed, click to open the DMZ host, and manually fill in the address and external network port to confirm that this function takes effect.





Src NAT

N K	AT/Port forwarding							
1				Src NAT				
	Add Delete							
	SN	Source network a	address			Destination network	address	
						Src NAT		X
						Source network address:	192.168.1.0	
						Netmask:	255.255.255.0	
						Destination network address:	192.168.1.0	
						Netmask:	255.255.255.0	
						Translation address:	192.168.1.200	1
						Remark:		
							Confirm	ancel

Dst NAT

Port forwarding DMZ host Sic NAT Det NAT Add Detelete	N N	AT/Port forwarding							
Add Delete SN Source network address Source network address: Source network address: Netmask: 255.255.255.0 Destination network address: Netmask: Netmask: 255.255.255.0 Translation address: Remark: Remark: Image: Remark	1					Dst NAT			
SN Source network address Destination network address: Source network address: Netmask: 255.255.255.0 Destination network address: Netmask: 255.255.255.0 Translation address: Remark:		Add Delete							
Det NAT > Source network address:		SN	Source network	k address			Destination network	address	
Source network address: Image: Source network address: Netmask: 255.255.255.0 Destination network address: Image: Source network address: Netmask: 255.255.255.0 Translation address: Image: Source network address: Remark: Image: Source network address:							Dst NAT		×
Netmask: 255.255.255.0 Destination network address:							Source network address:		
Destination network address: Netmask: 255.255.255.0 Translation address: Remark:							Netmask:	255.255.255.0	
Netmask: 255.255.255.0 Translation address:							Destination network address:		
Translation address: Remark:							Netmask:	255.255.255.0	
Remark:							Translation address:		1
							Remark:		
Confirm Cancel								Confirm	Cancel



3.3. Flow Control Policy

Manage the network speed of the terminal, and implement average bandwidth allocation or limit the bandwidth of the terminal.

Smart Flow Control

₹	System Status	V	Smart flow control	
	Network Configure	\sim	WAN1	One-key smart flow control
Ś	Flow Control Policy	^	WAN2	Function enable: Enabled, click to disable
	Smart Flow Control		WAN3	Upstream bandwidth 100000 KB 512Kbps 1Mbps 2Mbps 5Mbps 6Mbps 10Mbps
	Bandwidth Control		WAN5	Downstream bandwidth 100000 KB 4Mbps 5Mbps 10Mbps 20Mbps 200Mbps 200Mbps 200Mbps
	Free Flow Control			
()0	AC Management	V		💡 To ensure the excellent flow control effect, the WAN's upstream and downstream bandwidth must be configured correctly
9	Auth Internet Access	\sim		The bandwidth given by operators is usually in bit/s as unit: bps. The actual forwarding rate of the router is in bytes(BYTE/s): By So please pay attention to conversion. Suggest to use the bit rate give by the operator divided by 10.
	Difference and a			

For example, the uplink 20M and downlink 100M dial-up optical fiber can be configured with an uplink capacity of 2000KB and a downlink capacity of 10000KB. It is very important to configure the line bandwidth. The intelligent flow control automatically limits the speed according to the configured bandwidth. (You need to check the "Enable intelligent flow control" option to configure the bandwidth value.)

Bandwidth Control

Speed limit according to different source address rules

₩.	System Status	×	Bandwidth control			
	Network Configure	V	Add Delete			
k	Flow Control Policy	~	SN SN	Source address	Time	Bandwidth limited
_	Smart Flow Control				There is no policy bandwidth control rule defined yet. Please	Add
	Bandwidth Control				Bandwidth control rule	×
	Free Flow Control					
(i)o	AC Management	\sim				montment
•	Auth Internet Access	V			ANY 4 Adv	10
649	Behavior Control	V			Time: ANY 🗸 🌵 🗛	bi
- <u>-</u> 2	Object Management	\sim			Upstream limit: VINUMITED	
	Safety Protection	~			Downstream limit: VUNLIMITED	
0	Sulety Protection	•				
€	Log Record	V				
Ē	VPN	\sim				
*	Device Maintenance	V			Tips: Click icon to edite bandwidth Confirm	Cancel



Free Flow Control

The setting is not restricted by the overall network speed control of intelligent flow control, and its maximum bandwidth needs to be separately limited in the policy speed limit.

	System Status	V	Yree flow control					
	Network Configure	\sim	P Note: The free flow co	ntrol IP is not constrained by the smart flow	control. Please configure the bandwidth control to limit it maximum band	width.		
	Flow Control Policy	^	Add Delete					
	Smart Flow Control		SN SN	Source IP	Destination IP			Destination port
	Bandwidth Control				Free flow control re	ules	×	
	Free Flow Control				€ Enable O	Disable		
(10	AC Management	\sim						
٢	Auth Internet Access	\sim			Source IP	ANY	• 💠 <u>Add</u>	
649	Behavior Control	V			Destination IP	ANY	• 🗛 <u>Add</u>	
	Object Management	\sim			Destination port	ANY	Add	
D	Safety Protection	\sim						
₿	Log Record	\sim				Confirm	Cancel	



3.4. AC Management

AP List

Display all APs managed by AC, easy check and management.

	融合网关 convergence gelevaty					List									1		ogout i Language En	glish
	System Status	\sim	NP list							2	3			4	10	Online AP quantity/ Total AP:2 / 2,	AC service status: [or	iline]
	Network Configure	~	🗀 All AP	Res	start AP	Reset AP Delete AP	Country Code A	opply configuration template	e Set group Refresh	All device	✓ device more	del filte 🗸 Se	arch condit	ions: Device	FV	search		
K/3	Flow Control Policy	V			SN	AP name	Device IP	MAC address	\$\$ID(2.4G/5.8G)	User	Channel(2.4G/	Channel	Power	AP model	AP version	Status	AP remarks	Con
(00	AC Management	^									5.8G)	Analysis						
	AP List				1	Corridor	192.168.1.20	7C-27-3C-17-6B-84	XonTel2G 🚔 / XT16W 🚔	2 🚨	Auto[9]	2.4G 🖈	100%	XT-5400AX	V2.0-Build2024011213475	online 59	5	0
	AP Configure Template								XonTel5G 🕍		Auto[52]	5.8G 🐢	50%			14:4:0 up 46 days		-
	AP Group Definition				2	Office	192.168.1.21	7C-27-3C-17-6B-6C	XonTel2G 🚔 / XT16W 🚔	21 🙎	Auto[3]	2.4G 🔿	100%	XT-5400AX	V2.0-Build2024011213475	online 59		0
	AP Upgrade								XonTel5G 🚔		Auto[36]	5.8G 🞓	50%			14:3:59 up 46 days		
	Black and white list						8		7			~						
	Seamless Roaming								/			6						
	Auto Channel																	

- SN 1: View the number of online APs. Green represents the number of online APs, and red represents the total number of connected APs.
- SN 2: Filter displays only online or offline APs.
- SN 3: Filter displays by single model APs.+
- SN 4: Select to search according to the IP/MAC/name/model/version number of the AP device.
- SN 5: Edit the parameters and configuration of a single AP.
- SN 6: WIFI analyzer, used to scan WIFI of all channels in 2.4G or 5.8G frequency band of the AP.
- SN 7: The SSID (wireless WIFI name) and channel of 2.4G, 5.8G and 5.8G2 of the AP are displayed. Click the green villain to display the terminal connected to the AP.
- SN 8: AP server login address.



		کنوا	ـتـل تـ	ة زونـ	شرك
--	--	------	---------	--------	-----

للتجارة العامة ذ.م.م

Ð	System Status	~	MAP list												Onl	ine AP quantity/ Total AP:2 / 2
	Network Configure	~	C All AP	Res	tart AP	Reset AP Delete AP	Country Code	Apply configuration template	Set group Refresh	All device	✓ device mo	del filte 🗸	Search condition	s: Device IP	~	search
Ŵ	Flow Control Policy	~	l		SN	AP name	Device IP	MAC address	\$SID(2.4G/5.8G)	User	Channel(2.4G/	Channe	l Power	AP model	AP version	Status
()0	AC Management	^									5.8G)	Analysis				
	AP List		1		1	Corridor	192.168.1.20	7C-27-3C-17-6B-84	XonTel2G 🎍 / XT16W 🛔	12 💄	Auto[9]	2.4G	100%	(T-5400AX	/2.0-Build20240112134759	online
	AP Configure Template				_						Auto(52)	5.00	50%			2.40.49 up 45 days
	AP Group Definition				2	Office	192.168.1.21	7C-27-3C-17-6B-6C	XonTei2G @ 7XT16W @	41 👱	Auto[3]	2.4G 🐢	100%	T-5400AX	/2.0-Build20240112134759	online
	AP Upgrade								XonTel5G 🕍		Auto[36]	5.8G 🦛	50%			2:40:48 up 43 days
	Black and white list								Online terminal list						×	
	Seamless Roaming								SN	Terminal ma	IC .	Chann	el	Signal stren	gth	
	Auto Channel								1 4	A0-92-08-41-80	6-77	2.4G		(1:		
	Audit Configuration								2 7	E-68-A2-A0-70	C-82	2.4G		(
	Locating server								3 2	24-A1-60-37-18	B-91	2.4G		(î:		
9	Auth Internet Access	\sim							4 1	2-4F-22-3B-BI	E-66	2.4G		(1)		
64	Behavior Control	\sim							5 4	4-42-01-C2-B3	B-DA	2.4G		(It:		
D-1	Object Management	~							6 8	A-E6-A2-38-C	6-95	2.4G		(0		
		, ,							7 FI	E-8D-6D-BC-D	02-73	2.4G		(1:		
U	Safety Protection	\sim							8 C	E-76-79-B2-B	4-2F	2.4G		(0		
₽	Log Record	V							9 D	04-67-61-C8-0/	A-4B	2.4G		(
Ē	VPN	\sim							10 0	00-08-22-61-13	3-51	2.4G		();		
*	Device Maintenance	\sim							11 D	04-67-61-C8-0	A-19	2 4G		-	-	
															Disable	

Click for edit AP configs



Main editorial columns:

- SN 1: Select band need to edit (2.4G/5.8G).
- SN 2: Edit SSID name.
- SN 3: Encryption, WPA2PSK is recommended.
- SN 4: Edit wireless password. Click² to view password.
- SN 5: Select protocol mode.





Mode	802.11B/G/N 20MH 🗸
	default
WMM	802.11B/G
	802.11B
LANID	802.11G
	802.11B/G/N 20MHz
	802.11B/G/N 40MHz

Secondary columns:

AP name, AP remarks: It is used to distinguish all positions of the AP. Generally, it can be marked as installation position or coverage position.

Time restart: Set AP to auto-restart by hours/ days.

AP manage password: AP web login password.

Wireless status: Enable/ disable selected band (2.4G/5.8G).

Channel: Automatic channel can be selected. AP will automatically search for the optimal channel, or manually select the specified channel.

Broadcast SSID: Enable/ disable SSID broadcast.

User isolate: Enable/ disable the terminals under the AP to access each other. **Tx power:** default100%, optional: 75%/50%/25%/12%.

AP coverage threshold: If the connection strength of the detection terminal is weaker than the threshold value, the AP chooses to eliminate the terminal.

Access user number: Allowed accessed users quantity.

Virtual wireless: Up to 3 virtual WIFIs can be created in each frequency band, and different SSIDs and passwords can be set.

Virtual wireless						
Status	Disable	~	Broadcast SSID	Enable	~	
SSID	VAP_Wireless		User isolate	Disable	~	
Safe mode	OPEN	~	VLANID	0	(0,2~4095)	
Key	P		WMM	Enable	~	-
				Conf	firm Cance	el



AP Configure Template

Select a model to add a template, configure the SSID and password, and then select all APs of the same model in the AP to select the corresponding template for application configuration.

*	System Status	\sim	AP configuration template							
۲	Network Configure	V	Add template Delete template							
E.	Flow Control Policy	V	SN Template name							Device model
22	now control only		1 office							AX850-P2
6	AC Management	^	2 Config template							XT-5400AX
	AP List			AP template config					×	
	AP Configure Template			Template name	office		AP manage password		P	
	AP Group Definition			WIFI Time off	Close	~				
	AP Upgrade			Timed restart	Disabl V		LED	0		
	Black and white list			inited restart			LLD	Open		
	Seamless Roaming			User isolate	Disable	~	AP coverage threshold	-90 (-65dE	lm~-95dBm)	
	Auto Channel			LAN1	VLANID 0	(0,3~4094)	LAN2	VLANID 0	(0,3~4094)	
	Audit Configuration			LAN3	VLANID 0	(0,3~4094)	LAN4	VLANID 0	(0,3~4094)	
	Locating server				Select the band to b	e configured	2.4G Wireless device 🗸			-
2	Auth Internet Access	V		Wireless status	Enable	•	Channel	Auto	*	
44	Behavior Control	V		SSID	XonTel2G		Broadcast \$SID	Enable	•	
50	Object Management	V		Safe mode	WPA/WPA2PSK-TH	~	Key	•••••	P	
D	Safety Protection	\sim				Adva	anced			
₽	Log Record	\sim						Co	nfirm Cancel	

AP Upgrade

Upgrade online or upload firmware for local upgrade.

न्द्र	System Status	V	MAP	upgrad	e							
	Network Configure	v		Batch or	line upgrade	Batch local upgrade	Upload mirror Refresh	Search conditions:	Version	•	search Device model filt V	
Ŵ	Flow Control Policy	\sim		SN	AP name	IP	MAC	Stat	us	Device model	Current version	Online up
6	AC Management	~		1	Corridor	192.168.1.20	7C-27-3C-17-6B-84	Onli	ne	XT-5400AX	V2.0-Build20240112134759	22
	۵P List			2	Office	192.168.1.21	7C-27-3C-17-6B-6C	Onli	ne	XT-5400AX	V2.0-Build20240112134759	
	AP Configure Template AP Group Definition											
	AP Upgrade											
	Black and white list											
	Seamless Roaming											
	Auto Channel											
	Audit Configuration											
	Locating server											

(+965 1880005



Seamless Roaming

Automatic roaming is enabled by default.

	System Status	V	Seamless Roaming
æ	Network Configure	\sim	KVR parameter
Ó	Flow Control Policy	\sim	2G handover threshold: -75 (-55dBm ~ -94dBm)
(iộ	AC Management	^	5G handover threshold: -70 (-55dBm ~ -94dBm) Enable roaming ♥ ♥ When the roaming function is enabled, the WIFI names, encryption modes, and passwords of aps must be the same
	AP List		Enable 5G First: 🗹 💡 When 5G priority is enabled, the WIFI name, encryption mode, and password between 2G and 5G on the AP must be the same
	AP Configure Template		Save
	AP Group Definition		
	AP Upgrade		
	Black and white list		
	Seamless Roaming		
	Auto Channel		
	Audit Configuration		
	Locating server		

Auto Channel Select

2	System Status	\sim	Auto Channel
₩	Network Configure	v	Auto Channel Channel table
Ś	Flow Control Policy	\sim	Automatic channel switch
(î)	AC Management	^	Automatic channel assignment: Enabled, click to disable
	AP List		
	AP Configure Template		Turn on this feature when there is no channel available for intensive deployment
	AP Group Definition		Intensive deployment network optimization:
	AP Upgrade		Channel reallocation of ΔP on time
	Black and white list		
	Seamless Roaming		
	Auto Channel		Save
	Audit Configuration		

Channel table: View all APs SSID, channel, RSSI.

\$ +965 1880005



شركية زونيتال تكنولوجاي

للتجارة العامة ذ.م.م

₫.	System Status	V	Muto Channel				
۲	Network Configure	\sim	Auto Channel Channel table				
¢⁄ɔ	Flow Control Policy	\sim	AP_MAC	Wireless type	Auto Channel	Near AP_MAC	AP Name
()0	AC Management	^				24-FB-65-41-FB-06	
	AP List					7C-27-3C-17-6B-6E	Office
	AP Configure Template		7C-27-3C-17-69-E5 192.168.1.36	2G	8 Unassigned	82-27-3C-17-6B-6E	
	AP Group Definition					86-27-3C-17-6B-6E	
	AP Upgrade					E0-24-81-B3-D0-BE	
	Seamless Roaming					7C-27-3C-17-69-E6	
	Auto Channel					24-FB-65-41-FB-06	-
	Audit Configuration					7C-27-3C-17-6B-6E	Office
	Locating server		7C-27-3C-17-69-F1	2G	6 Unassigned	82-27-3C-17-6B-6E	
9	Auth Internet Access	\sim	192.168.1.38 			86-27-3C-17-6B-6E	
ŶŶĻ	Behavior Control	V				E0-24-81-B3-D0-BE	
60	Object Management	V				7C-27-3C-17-69-E7	
D	Safety Protection	V		5G	56 Unassigned	7C-27-3C-17-6B-6E	Office
-	Log Pacord						Onice



3.5. Auth Internet Access

Generally, Internet users can access the Internet directly by configuring the IP address of the network card or by routing DHCP to assign the address to obtain the IP address.

Authenticated Internet access means that you need to be a "user" before you can access the Internet.

Auth Configure

Control the authentication switch of the corresponding LNA port. Marks: As long as any one of the switches is turned on, it means that the LAN1 port is intercepted. Only authenticated users are allowed to access the Internet



PPPoE Auth

PPPoE authentication --- used for cell broadband. Intranet users can access the Internet through PPPoE dial-up. The dial-up account password is created on the route (for the connection with radius billing, it needs to be created on the radius billing system).

It is recommended to use the LAN address for the allocation of the address pool. The IP address of the LAN port must not be the same as the network segment. For example, the IP address of the LAN port is 192.168.1.1. The address pool here cannot be 192.168.1.xxx

DNS suggests to assign DNS of local operators.



شـركــة زونـتـل تـكنـولـوجـي للتجارة العامة ذ.م.م

	System Status	\sim	PPPoE Service											
	Network Configure	\sim	PPPoE Service	PPPoE advance option Access status										
Ś	Flow Control Policy	V	All Lan ports	Function enable: Enabled, Click to disable										
(;0	AC Management	\sim	LAN1	Service name. Q (Leave blank in default) after configure the service name, please input the service name to dial										
•	Auth Internet Access	^	EXT1	Assign IP address range										
	Auth Configure			Gateway IP: 10.0.0.1										
	PPPoE Auth			Start Address: 10.0.0.2 End address: 10.0.200.254										
	Portal Auth			Assign IP according to MAC Address:										
	Radius Billing			Please input IP and Mac assignment rules in the text box on the left, format is 1P address space MAC address' one for each line For example:										
	Auth User			10.10.1.2 AA.BB:CC:DD.EE.FF 10.10.1.3 BB:CC:DD.EE.FF:00 10.10.1.4 DD:EE.FF:001122										
	Auth User Status			10.10.14 DOLE.11.00.11.22										
	Department/Level Definit	ion		DNS Configuration										
4¢J	Behavior Control	v		Main DNS: 114.114.114 Alternate DNS: 8.8.8.8										
50	Object Management	\sim												
Ο	Safety Protection	\sim		Online detection time interval: 5 mins V 🖓 Recommend 5 min in defuit										
₽	Log Record	\sim		MTU: Enable custom MTU MRU: Enable custom MRU										
Ē	VPN	\sim												
*	Device Maintenance	\sim		 Tips: 1, after modifying the PPPoE dial-up configuration, the user who has already dialed will disconnect the network and need to dial again! 2, PPPoE dial-up users, unified in user management) authentication users 										
				Save										

Portal Auth

2	System Status	V	Vertal auth configure	
œ	Network Configure	~	Auth option Customize	ze auth page
¢)	Flow Control Policy	\sim	Portal authentified user timeout time: 0	minute 💡 The value range should be: 3-200 minutes
(i;o	AC Management	V		
۲	Auth Internet Access	^	Auth option Free auth: 〇 Ei	Enable 🐵 Disable
	Auth Configure		WEB auth: 💿 Er	Enable O Disable
	PPPoE Auth		Auth success URL redirect: Auth fail URL redirect:	
	Portal Auth			
	Radius Billing		Save	
	Auth User			
	Auth User Status			
	Department/Level Defini	ition		

Free auth: It is used in hotels to prevent pinhole cameras from linking to WIFI network. One more manual click step is required. Equivalent to self-service click to release. **WEB auth**: Users connected to the AP (such as mobile phones) can enter their username and password in the pop-up authentication window to access the Internet. The account password of the WEB password is created on the route (for the connection with radius billing, it needs to be created on the radius billing system)



Radius Billing

4	System Status	\sim	Nadius Billing	
	Network Configure	\sim	Function enable: Enable	ed,click to disable
Ś	Flow Control Policy	\sim	Billing outlet circuit:	Default V 🖓 Specify the billing exit line, and if the billing server is on the Intranet, you must select the default
()0	AC Management	\sim	Selection of docking type:	For PPPoE authentication For Portal authentication
•	Auth Internet Access	\sim	Authentication IP:	\bigtriangledown The IP address of the billing server
	Auth Configure		Shared key:	
	PPPoE Auth		Charging ID:	
	Portal Auth		Authentication Port:	0 ♀ The default radius authentication port for the server is: 1812
	Radius Billing		Charging port:	0 ♀ The default toll port of the Radius server is: 1813
	Auth User		Save	
	Auth User Status			
	Department/Level Defini	tion		

Auth User

The following figure shows five types of users.

MU	TI-FUNCTION GATEW	/AY	Curr	ent oper	ation Auth Intern	net Access														
₹	System Status	\sim	N/	Authenti	cation user	Total o														
	Network Configure	\sim		Add	Batch add	Enable all	Export user	Delete 🗸	User departm 🗸	User le	evel filte 🗸	User type	e filte 🗸	Stat 🗸	Acc	~			Exact	Search
Ś	Flow Control Policy	\sim		SN	Nar	me	Depa	artment	User lev	el	User tv	rpe		Notes		Creat ti	me↓	Due time	Ð	Operation
_							Authe	entication (user											
(î)	AC Management	\sim					_	Account:			Passw	ord: 442	24603				<u> </u>			
•	Auth Internet Access	\sim					De	partment:	default	~	Le	evel: def	fault		~					
	Auth Configure							Jser type:	PPPoE dial-up	~	Account t	ype: En	abl 🗸							
	PPPoE Auth						MAG	Binding:	PPPoE dial-up IP address auth	his	2									
	Portal Auth						Cr	eate time:	MAC address auth WEB password au	th	Expire t	ime:			A	dd time				
	Radius Billing							Name:	VPN dial-up			ID:								
	Auth User							Tel:			Addr	ess:								
	Auth User Status							Notes:												
	Department/Level Definit	tion																		
ţţţ	Behavior Control	\sim												Confin	m	Cancel				



Auth User Status

Users can be seen online, and the green icon represents the online users, allowing online access.

MUL	TI-FUNCTION GATEW	/AY	Current operation Auth Interne	t Access >> Aut	h User Status							
	System Status	\sim	Auth user status									
	Network Configure	\sim	Anonymous Us Online Total user quantity[0/0]	User level filte	er 🗸 User type fi	ilter 🗸	Due time filter	~	Status 🗸	Account	~	Search
Ń	Flow Control Policy	\sim	-	SN User	Level	Tel Add	dress/Remark	Due	e time	IP	Online status	Auth status
((;;	AC Management	\sim						No record of	currently			
9	Auth Internet Access	^										
	Auth Configure											
	PPPoE Auth											
	Portal Auth											
	Radius Billing											
	Auth User											
	Auth User Status											
	Department/Level Definit	tion										

Department/Level Definition

Management department and level, used to bind the Internet users

*	System Status	\sim	Department division	
۲	Network Configure	\sim	Department division Level division	
Ś	Flow Control Policy	\sim	P Department division purposes: User objects must choose the departments they belong to, so before defining users, they need to divide departments. For companies, department	ts are
(i ⁰	AC Management	\sim	of access users, such as: East 35 buildings, West 88 buildings. After dividing the departments, users can make various control rules according to the dividing departments.	ne location
9	Auth Internet Access		Add	
	Auth Configure		SN Department name	Operation
	PPPoE Auth		1 default	2 🔀
	Portal Auth			
	Radius Billing			
	Auth User			
	Auth User Status			
	Department/Level Definit	ion		



للتجارة العامة ذ.م.م

MUI	TI-FUNCTION GATEW	ΆY	Current operation Auth Internet Access >> Department/Level Definition	
1	System Status	\sim	User level division	
₩	Network Configure	\sim	Department division Level division	
κ'n	Flow Control Policy	\sim	Add	
(î)	AC Management	\sim	Seven-dividing purposes: User objects must select the level which they belong to, so they need to be graded before defining users; for companies, they are usually graded accertified the user's authority and position, such as senior executives, ordinary employees, etc. For residential area, it is usually classified according to the bandwidth purchased by the user	ording to r, such as
9	Auth Internet Access		2M, 4M. After grading, various control or speed limit rules can be made according to the grading.	
	Auth Configure		SN Name	Operation
	PPPoE Auth		1 default	2 🗶
	Portal Auth			
	Radius Billing			
	Auth User			
	Auth User Status			
	Department/Level Definit	ion		

3.6. Behavior Control

Application Firewall

Configure the required release and direct blocking destination IP, port and application according to the source and time.

₫	System Status	\sim	Application firewall					
	Network Configure	\sim	Function enable: Enabled,click to disable					
¢	Flow Control Policy	\sim	Add Delete	Firewall rules		×		
((;;	AC Management	~	SN Source address object Time		able	~	Action	Operatio
•	Auth Internet Access	\sim		Source address:				
4¢4	Behavior Control	^		oource address.	ANY ·	Add		
	Application Firewall			Time	ANY	Add		
	URL Redirect			Destination IP:	ANY	Add		
	Domain Redirect			Destination port:		Add		
5	Object Management	\sim		Policy:	Release			
D	Safety Protection	\sim			Release Block directly			
₽	Log Record	\sim						
Ħ	VPN	~			Con	ofirm Cancel		
-	Device Maintenance	\sim			CO	Cancer		

🕻 +965 1880005 🛛 🌐 www.xontel.com 👘 🐼 kuwait@xontel.com



URL Redirect

When the terminal accesses the original website, it will automatically jump to the destination website. (Takes effect after clearing the browser cache)

MUI	TI-FUNCTION GATEW	AY	Current operation Behavior Control >> URL Redirect		Refresh Change password Logout
*	System Status	\sim	URL redirect		
	Network Configure	\sim	Add Batch add Delete		
ś	Flow Control Policy	\sim	SN Original URL	Redirected URL	Operation
((;0	AC Management	\sim		ect demnation	
9	Auth Internet Access	\sim	Orig	inal URL: www.google.com Such as:www.aaa.com(Don't contain*http://*)	
φ¢\$	Behavior Control	^	Destina	tion URL: www.xxx.com	
	Application Firewall			Such as: www.aaa.com/a.htm (Do not contain http://, but can be with path)	
	URL Redirect			Confirm Cancel	
	Domain Redirect				
6	Object Management	\sim			
D	Safety Protection	\sim			
₽	Log Record	\sim			
Ē	VPN	\sim			
*	Device Maintenance	\sim			

Domain Redirect

(+965 1880005

Set that when the terminal accesses the domain name, it automatically resolves to the specified IP (takes effect after clearing the browser cache)

MUL	TI-FUNCTION GATEW	VAY	Current operation Behavior Control >> Domain Redirect		Refresh Change password Logout
	System Status	\sim	Y Domain redirect		
(Network Configure	\sim	Add Batch add Delete The below defined domain name will be resolved directly to corresponding IP a	address without th	e DNS server
(Z)	Flow Control Policy	\sim	C SN Domain name I	P	Operation
6	AC Management	~	Domain name resolution definition	×	
•• •	Auth Internet Access	v	Domain name:		
4¢4	Behavior Control	^	IP:		
	Application Firewall				
	URL Redirect		Confirm	Cancel	
	Domain Redirect				
	Object Management	\sim			
D	Safety Protection	\sim			
₽	Log Record	\sim			
Ē	VPN	\sim			
*	Device Maintenance	\sim			

(
www.xontel.com

kuwait@xontel.com



3.7. Object Management

Time Object

1	System Status	\sim	Т	'ime ob	ject						
	Network Configure	\sim		Add	Delete						
64	Flow Control Policy	~		SN	Name	D	ate			Time period	Operation
(7)	Flow Control Folicy	~	-	1	ANY	Time object			X	Any time	8 X
(ijo	AC Management	\sim									
•	Auth Internet Access	\sim				Nam	e:				
ţţţ	Behavior Control	\sim				Sun D	Mon 🗆 Tue 🗆 Wed	□Thu □Fri	□Sat		
	Object Management	^					Start time	End time			
	Time Object					-					
	Source IP Object					-					
	Port Object										
	Destination IP Object					-					
	Build-in Application Object	t				Time format	: 24 hour, (HH:mm), suc	ch as 13:10			
	Custom Application Objec	:t						Carfir	Canad		
Ο	Safety Protection	\sim						Confirm	Cancel	1	

Source IP Object

Here you can define the range of IP addresses which you can use for example for multi diversion rules

MUL	MULTI-FUNCTION GATEWAY Current operation Object Management >> Source IP Object Refresh Change password Logout											
	System Status	\sim	N S	ource IF	object							
	Network Configure	\sim	8	Add	Delete							
Ø	Flow Control Policy	\sim		SN	Name			Address range		Operation		
			-	1	ANY	Any addr	Address object		×	Ø 18		
10	AC Management	\sim		2	FASTTELCO	172.16.4	Name: EAS			2 🕱		
•	Auth Internet Access	\sim				192.168.:	Name. FAS	TIELCO				
ţţţ	Behavior Control	\sim		3	Zain5G	172.16.4	IP Start IP	End IP				
	Object Management	^				172.16.10	172.16.41.2	172.16.41.254				
	Time Object											
	Source IP Object											
	Port Object											
	Destination IP Object											
	Build-in Application Object	ct										
	Custom Application Obje	ct										



شركــة زونـتـل تـكنـولـوجـي للتجارة العامة ذ.م.م

Port Object

₫	System Status	\sim	N P	ort objec	t						
æ	Network Configure	\sim		Add	Delete						
	Flow Control Boliov			SN	Name			Content dis	cription		Operation
(7)	Flow Control Folicy	v	-	1	ANY	Protocol:TCP&UDP Port:Ar	Port object			Ø 🗶	
(;;	AC Management	\sim		2	DNS	Protocol:UDP Port:53	News				2
9	Auth Internet Access	\sim		3	HTTP	Protocol:TCP Port:80	Name:	ниг			2 ×
4¢1	Behavior Control	\sim		4	ICMP	Protocol:ICMP Port:1	Protocol	Start Port	End Port		2 🔀
	Object Management	^		5	SSL	Protocol:TCP Port:443	TCP 🗸	80	80		2
	Time Object			6	TCP	Protocol:TCP Port:Any port	~				2
	Source IP Object			7	UDP	Protocol:UDP Port:Any port	~				2 🗙
							~				
	Port Object						~				
	Destination IP Object						~				
	Build-in Application Object	t					~				
	Custom Application Object	ct					~				

Destination IP Object

*	System Status	\sim	Des	tination IP object		
@	Network Configure	\sim	A	dd		
50	Eleve Control Boliov		ID	Name	Remark	Operation
(A)	Flow Control Folicy	~	4	Fasttelco range	Destination IP object X	X
(;0	AC Management	\sim	5	merge		لۍ ۲
•	Auth Internet Access	\sim			Name: Fastteico range	
ţţţ	Behavior Control	\sim			Remark: Fasttelco range	
0-2 0	Object Management	^			Click the button to obtain the online destination address table, and modify the destination address table	
	Time Object				format to IP/netmask numbers, such as 1.25.0.0/15	
	Source IP Object				Select online address table : Obtain the address table 🗸 Obtain the latest	
	Port Object				172.16.41.0/24	
	Destination IP Object					
	Build-in Application Object	ct				
	Custom Application Obje	ct				



Built-in Application Object



Custom Application Object

1	System Status	\sim	ИС	ustom	ize app object								
	Network Configure	\sim		Custo	mize app object		Define app	by IP + port					
Ś	Flow Control Policy	\sim		Add									
()0	AC Management	\sim		SN	App name	App type	Customize app			X		Operation	i ^
	A with Internet Access			1	11dota	Online game	App Name:	11dota				Z 🗶	
6	Auth Internet Access	~		2	175pt	Online game	App type:	Online game	~	•		2	
ŶţŶ	Behavior Control	\sim		3	300hero	Online game	Description:					2	
	Object Management	^		4	360-speed	Madsl						2	
	Time Object			5	360safe	Software Update	L					2	
	Source IP Object			6	3guohero	Online game			Confirm	Cancel		2	
	Port Object			7	3guohero2	Online game						2	
	Destination IP Object			8	6rooms	Web Video						2	
	Build-in Application Object	t		9	7fame	Online game						2	
	Custom Application Object	t		10	acfun	Web Video						2	
σ	Safety Protection	\sim		11	aion	Online game						2	



Define applications according to domain name or destination IP+port as shown in the figures below

MUL	TI-FUNCTION GATEW	AY	Current operation Object Management >> Custom Application O		Refresh Change password Logout
Ŧ	System Status	\sim	Sustomize app object		
	Network Configure	\sim	Customize app object Define app by domain	Define app by IP + port	
ý	Flow Control Policy	\sim	Add	Petino ann hu domain	
(ij)	AC Management	\sim	Domain	ame	Operation
•	Auth Internet Access	\sim		Domain:	
ţţţ	Behavior Control	\sim		App name: 11dota	
	Object Management	^			
	Time Object			Confirm Cancel	
	Source IP Object				
	Port Object				
	Destination IP Object				
	Build-in Application Obje	ct			
	Custom Application Obje	ct			

MUI	TI-FUNCTION GATEW	/AY	Current operation Object Managerr	nent >> Custom Application O	bject				Refresh Change password Logout
	System Status	\sim	Customize app object						
@	Network Configure	\sim	Customize app object	Define app by domain	Define app b	y IP + port			
κ/̈́́́	Flow Control Policy	\sim	Add					~	
();0	AC Management	\sim	SN	App name	Define app by IP	+ роп		×	Operation
9	Auth Internet Access	\sim			Start address:				
ţţţ	Behavior Control	\sim			Protocol:	TCP/UDP	~		
50	Object Management	\sim			Start port:				
	Time Object				End port:				
	Source IP Object				App name:	11dota	~		
	Port Object								
	Destination IP Object						Confirm Cancel		
	Build-in Application Obje	ect							
	Custom Application Obie	ect							



3.8. Safety Protection

IP-MAC Banding

After the IP-MAC is bound, the IP address cannot be modified at will, so it can avoid IP conflicts that affect other users' normal Internet access.

	System Status	\sim	IP-MAC bind								
æ	Network Configure	\sim	Add Del	ete Ba	atch add One-click	to bind all Cancel all bind	Only MAC-bound terminals are all	owed to access	the Internet	Display curre	ent IP-MAC
428	guro		SN SN			User		IP Address	MAC ac	ldress	Enable Op
Ś	Flow Control Policy	\sim		IP-MAC	address list					×	
(î)	AC Management	\sim		O No	ting, click R to hind the l	P address and MAC address alick	A to Liphinda aliak		abiaatl		
•	Auth Internet Access	\sim		A NO			to onbindy, click			-	
IāI	Pabayiar Control			User	~	Search					
φĨ¢	Benavior Control	~		SN	IP	User	MAC	Auth method	Connection time	Operation	
D-j	Object Management	\sim		1 :	172.16.40.101	-	F8-0D-AC-BE-90-65		03-19 17:38:42	24 🙈	
Ο	Safety Protection	^		2	172.16.40.103		CC-D2-81-5B-AD-7C	-	03-21 02:01:41	<mark>2</mark> 4 🙈	
	IP-MAC Binding			3	172.16.40.105 🕑		4E-7D-3D-4B-D4-E2		03-21 02:19:31	<mark>2</mark> , 🔒	
	Connection Quantity Lim	nit		4	172.16.40.109 🕑	2	56-57-E8-4D-A1-42		03-21 02:18:54	<mark>2</mark> 4 🔒	
	LAN Abnormal Detection	1		5	172.16.41.103 🕑	-	78-C8-81-E0-98-C0		03-19 17:45:05	<mark>2</mark> ₀ 🔒	
	LAN Attack Protection			6	172.16.41.104 🕑	-	80-60-B7-1B-2C-C7		03-20 23:26:33	<mark>&</mark> 🕹	
	WAN Ping Forbid/WAN L	_ogin									
₿	Log Record	\sim							C	lose	
Ē	VPN	\sim									

Connection Quantity Limit

Limit the maximum number of TCP and UDP connections of the source object.

*	System Status	\sim	onnect	control rule								
	Network Configure	\sim	Add	Delete	_							
Ś	Flow Control Policy	\sim	SN	Source address object	Time	TCP	connectio	n quantity	UDP o	connection quantity	Enable	Operation
(); ;	AC Management	v	1	ANY	Enable Ox Disat	ble				×	~	×, ×
9	Auth Internet Access	\sim			Source address of	hiect: C			Department			
4¢1	Behavior Control	\sim				bjeet. e	ANY	v	Add			
- -	Object Management	\sim			1	Time:	ANY	~	4 Add			
Ο	Safety Protection	^			Maximum quantity of TC	CP con	nections:	5000				
	IP-MAC Binding				maximum quantity of or	DI CON	neotiono.	3000				
	Connection Quantity Lim	iit						C	Confirm Ca	ncel		
	LAN Abnormal Detection											

(+965 1880005



LAN Abnormal Detection

Enable DHCP detection to search whether there are other DHCP servers in the LAN that cause IP address assignment conflicts.

It is normal for the AC gateway to find the main route when it is used as by pass mode. Turn on loop detection to determine whether there is link loopback in the LAN switch, which causes a network broadcast storm and slow and unstable Internet access quality.



LAN Attack Protection

	System Status	\sim	Intranet attack protection
	Network Configure	\sim	Function enable: Enabled, click to disable
Ś	Flow Control Policy	\sim	Select the interface to protect
((;0	AC Management	\sim	
9	Auth Internet Access	\sim	Parameter settings
ţţŶ	Behavior Control	\sim	Package threshold: 0 (Number of packets / per second)
	Object Management	\sim	Package threshold: The maximum number of packets allowed to be sent per second for a single IP. The reference value is between 5000 and 10000.
Ο	Safety Protection	^	Whether the LAN port is connected to the Layer 3 switch 💡 Do not select it if there is no layer 3 switch.
	IP-MAC Binding		
	Connection Quantity Lim	iit	Save
	LAN Abnormal Detection		
	LAN Attack Protection		
	WAN Ping Forbid/WAN L	ogin	



WAN Ping Forbid/WAN Login

View remote login parameters and configurations.

	System Status	\sim	Section 21 Extranet prohibited to PING/ Extra	anet login		
ŧ	Network Configure	\sim	Host security			
¢۶	Flow Control Policy	\sim		Prohibit ping router from Allow administrator to lo	n extranet	tranet IP
()	AC Management	\sim	WED service parts		g in remotely via extra	
9	Auth Internet Access	\sim	WEB service port:	2011		
ţţ	Behavior Control	\sim	Master DNS:	114.114.114.114	The DNS server a	address is needed as a network terminal by the local computer(router)
	Object Management		Update line options:	Default 🗸	Specify device s	system upgrades and protocol update lines!
-ċ	Object Management	~	Remote management	www.demo.yowifi.net	Remote access rout	uting link address:http://Y24190000467.demo.yowifi.net:20110
Ο	Safety Protection	^	Server.			
	IP-MAC Binding		Device name:			Display on the login page
	Connection Quantity Lim	nit				Save
	LAN Abnormal Detection	ı				
	LAN Attack Protection					
	WAN Ping Forbid/WAN L	ogin				

3.9. Log Record

User Auth Log

View users online/ offline records.

*	System Status	\sim	Ŋuser auth log		
	Network Configure	\sim	© Search		
6	Flow Control Policy	V	SN Time	Description	
(7)	Flow control Folicy	v		There are no records currently	
÷0	AC Management	\sim	Home Pre page Next page Last Page Turn to	page GO Total 0.Current page 1	
2	Auth Internet Access	\sim			
ţţ	Behavior Control	\sim			
	Object Management	\sim			
Ο	Safety Protection	\sim			
₽	Log Record	^			
	User Auth Log				
	Online User Log				
	Interface Flow Log				
	System Log				
	AC Operation Log				
	AP Event log				



Online User Log



Interface Flow Log

MUL	MULTI-FUNCTION GATEWAY Current operation Log Record >> Interface Flow Log Refresh Change password Logout											
\$	System Status	\sim	Interface flow log									
	Network Configure	\sim	All ports			— Upstream rate	— Downstream rate	History flow detail				
	Flow Control Boliov		MAN1	Г								
(7)	Flow Control Folicy	v	MAN2			Please sele	ct the detailed area to view tr	nrough the following general pict	ure.			
(in)	AC Management	\sim	WAN3									
•	Auth Internet Access	\sim	LAN3	(KB/S								
ļţļ	Behavior Control	\sim	LAN2	Speed								
50	Object Management	\sim	LAN1									
Ο	Safety Protection	\sim										
₽	Log Record	\sim										
	User Auth Log			Period	of time: 20	24-03-14 ~ 2024-03-2	21 Inquire <u>Today Yes</u>	sterday The day before yesterda	<u>y Nearly two days Near</u>	iy three days Nearly on	e week	
	Online User Log					20	024-03-14 ~ 2024-03-21Flo	w graph (Select an area by m	ouse to view details)			
	Interface Flow Log				14648 -					1		
	System Log			5	(S/8)							
	AC Operation Log			-	eed (
	AP Event log				<mark>ዓ 4882</mark> -							
-										ім. և п.	.	



System Log

2	System Status	\sim	System log											
æ	Network Configure	\sim	© Search											
	Flow Control Boliou		SN Time	Description										
Ś	Flow Control Policy	~	1 2024-03-19 17:36:03	Interface:WAN3 online, ip:192.168.202.2										
(10	AC Management	\sim	2 2024-03-19 17:34:49	Interface:WAN2 online,Ip:172.16.20.4										
9	Auth Internet Access	\sim	3 2024-03-19 17:32:53	Interface:WAN1 online, ip:178.61.168.14										
ţţţ	Behavior Control	\sim	4 2024-03-19 17:32:13	Interface:WAN3 online										
	Object Management	\sim	5 2024-03-19 17:32:13	Interface:WAN2 online										
Q	Safety Protection	\sim	Home Pre page Next page Last P	age Turn to page GO Total 1,Current page 1										
Ð	Log Record	^												
	User Auth Log													
	Online User Log													
	Interface Flow Log													
	System Log													
	AC Operation Log													
	AP Event log													

3.10. VPN

PPTP

To use this function, AC is required as the primary route, and the WAN interface is connected to the public IP provided by the external network for the operator.

Gateway IP and address pool are set according to the actual needs of DNS.

MUL	TI-FUNCTION GATEW	VAY	Current operation VPN >> PPTP	Refresh Change password Logout
*	System Status	\sim	N PPTP	
	Network Configure	\sim	PPTP VPN server PPTP VPN access status	
٢́٨	Flow Control Policy	\sim	Function enable: Enabled, click to disable	
(10	AC Management	\sim	Client IP address range	
•	Auth Internet Access	\sim	Gateway IP 0.0.0.0	
	Behavior Control	\sim	Start IP address: 0.0.0.0 End IP address: 0.0.0.0	
°2	Object Management	\sim	DNS configure	
Ο	Safety Protection	\sim	Master DNS: 0.0.0.0 Auxiliary DNS : 0.0.0.0	
Ð	Log Record	V		
Ē	VPN	^	Detect the online time:	
	PPTP		MTU: Denable customer MTU	
	L2TP		MRU: Enable customer MRU MPPE-128: Support MPPE-128	
	VTUNS Configure		S Tips: point-to-net VPN dialing users, are unified in Auth Internet Access. User Management, Auth user	8
	VTUNS Status		Save	





Click Authentication User to jump to Create VPN Authentication User

1	System Status	\sim	N N	uthentio	ation user	Total	0											
	Network Configure	\sim		Add	Batch ac	dd Enable	all Export use	Delete 🗸	User departm 🗸	User I	evel filte 🗸 🛛	Jser type filte 🥆	Stat 🗸	Acc 🗸			Exact	Search
Ø	Flow Control Policy	\sim		SN		Name	De	epartment	User lev	vel	User tvi	be	Notes		Creat ti	me↓ D	ue time	Operation
							Au	thentication u	user						×			
(î0	AC Management	\sim						Account:			Passwor	d:			-			
•	Auth Internet Access							Department:	default	~	Leve	el: default		~				
	Auth Configure							User type:	VPN dial-up	~	Account typ	e: Enabl 🗸						
	PPPoE Auth							Upstream broadband:	UNLIMITED		Downstrea broadban	m d:						
	Portal Auth						м	AC Binding:	Disable	~								
	Radius Billing							Create time:			Expire tim	e:		Add	time			
	Auth User							Name:			П	D:						
	Auth User Status							Tel:			Addres	s:						
	Department/Level Definiti	ion						Notes:							*			
ţţ	Behavior Control	\sim											Confirm	m Ca	ancel			
- i	Object Management	\sim																

L2TP

To use this function, AC is required as the primary route, and the WAN interface is connected to the public IP provided by the external network for the operator.

Gateway IP and address pool are set according to the actual needs of DNS.

₫	System Status	\sim	L2TP	
	Network Configure	\sim	L2TP VPN server	L2TP VPN access status
Ś	Flow Control Policy	\sim	All WAN ports	Function enable: Enabled, click to disable
((;;	AC Management	\sim	WAN2	Client IP address range
9	Auth Internet Access	\sim	WAN1	Gateway IP:
ţţţ	Behavior Control	\sim		Start address: End address:
	Object Management	\sim		
D	Safety Protection	\sim		
₽	Log Record	\sim		Master DNS: Secondary DNS:
Ē	VPN	^		
	PPTP			Port number: 1701
	L2TP			MTU: _ Enable custom MTU
	VTUNS Configure			MPPE-128: Support MPPE-128
	VTUNS Status			Point-to-network VPN dial-up users, unified in Auth Internet Access, User Management, Auth user
*	Device Maintenance	\sim		Save



VTUNS

The network to network virtual channel over TCP/IP is established for the combination of two LANs. The one with good performance is set as the server. The LAN segments on both sides cannot be the same. The server needs to have a public IP address.

1	System Status	\sim	VTUNS
	Network Configure	\sim	Parameter settings Tunnel management
Ś	Flow Control Policy	\sim	Function enable: Enabled, click to disable
();0	AC Management	\sim	Parameter settings
•	Auth Internet Access	\sim	• Set this device as VPN center server O Set this device as VPN Dialing client
Į.	Behavior Control	\sim	Password: ••••• Protocol: Tcp v
0-2 0	Object Management	\sim	Whether encryption: Yes No
Ο	Safety Protection	\sim	compression: Yes No
₽	Log Record	\sim	Save
Ħ	VPN	\sim	
	PPTP		
	L2TP		
	VTUNS Configure		
	VTUNS Status		

Tunnel management: Add the custom tunnel name and tunnel ID, and fill in the intranet segment of the VPN client, such as 192.168.1.0 and 255.255.255.0. Note that the tunnel name and tunnel ID must be consistent between the server and the client

MUL	TI-FUNCTION GATEW	AY	Current operation VPN >> VTUNS Configure		
	System Status	\sim	VTUNS		
	Network Configure	\sim	Parameter settings Tunnel management		
(j)	Flow Control Policy	\sim	VPN Tunnel configure		
();e	AC Management	\sim	Add Delete	VPN lunnel configure	Operation
9	Auth Internet Access	\sim		Tunnel ID:	Operation
ţţţ	Behavior Control	\sim			
	Object Management	\sim		Opposite side network segment IP address Netmask	
Ο	Safety Protection	\sim			
₽	Log Record	\sim			
Ē	VPN				
	PPTP				
	L2TP				
	VTUNS Configure			· · · · · · · · · · · · · · · · · · ·	
	VTUNS Status			Save Cancel	
-					



3.11. Device Maintenance

Firmware Upgrade

Online upgrade, or select a specific local firmware upgrade





Modify Password

Here you modify administrator user login password

Auth Internet Access	\sim	Modify password
Behavior Control	\sim	Or Modify the system password, please remember the new password, the default password is: admin
Object Management	\sim	Old password:
Safety Protection	\sim	New password:
∟og Record	~	Confirm password:
/PN	\sim	Modify password
Device Maintenance	^	
Firmware Upgrade		
Modify Password		
Authority Management		
Ping Detection		
Configure File Maintenan	се	
	ehavior Control bject Management afety Protection og Record PN evice Maintenance irmware Upgrade idolfy Password uthority Management ing Detection configure File Maintenan	ehavior Control bject Management afety Protection og Record PN evice Maintenance imware Upgrade timware Upgrade timo Detection configure File Maintenance

Authority Management

Here you can create multiple users with custom permissions as shown below

9	Auth Internet Access	\sim	Nuthority Management				
ţţ	Behavior Control	\sim	Add				
	Object Management	\sim	Account		Remarks		
D	Safety Protection	\sim		Administrators		×	
Ē	Log Record	\sim		Account			
	VPN	\sim		Password		2	
*	Device Maintenance	^		Remarks			
	Firmware Upgrade					Authority	
	Modify Password					Confirm Cancel	
	Authority Management						
	Ping Detection						
	Configure File Maintenar	nce					
	Restart Device						
	Timed Task						

🔇 +965 1880005 🛛 🍥 www.xontel.com 🔹 kuwait@xontel.com



9	Auth Internet Access	\sim	Managemer	nt				
ļå	Behavior Control	\sim	Add					
	Object Management	\sim	Account			Remarks		
Ο	Safety Protection	\sim		Administrator Permissi	on Settings			×
				Module	Authority			-
f≣}	Log Record	\sim		All Authority	Set Authority	If no permissions are set, all func	tions are read-only	
Ē	VPN	\sim		System Status	Device Info	□Interface Status	LAN IP Flow	
\$	Device Maintenance	^		Network Configure	 WAN Configure Subinterface Configure DDNS 	LAN/DHCP Multi-line Diversion Rules NAT/Port Forwarding	 Physical Port Definition Static Route 	
	Firmware Upgrade			Flow Control Policy	Smart Flow Control	Bandwidth Control	Free Flow Control	
	Modify Password			□AC Management	□AP List □AP Upgrade □Auto Channel	AP Configure Template Black and white list Audit Configuration	□AP Group Definition □Seamless Roaming □Locating server	
	Ping Detection			Auth Internet Access	□Auth Configure □Radius Billing □Department/Level Definition	PPPoE Auth Auth User	□Portal Auth □Auth User Status	
	Configure File Maintenan	ice		Behavior Control	Application Firewall	URL Redirect	Domain Redirect	
	Restart Device			Object Management	Time Object	Source IP Object	Port Object Custom Application Object	
	Timed Task			□Safety Protection	IP-MAC Binding LAN Attack Protection	Connection Quantity Limit	LAN Abnormal Detection	
	Time Synchronization			Log Record	User Auth Log	Online User Log	AC Operation Log	

Ping Detection

Use to check whether there is a path between AC and the specified IP.

9	Auth Internet Access	Ping inspection - single ping
ţţţ	Behavior Control	✓ Single ping Multi ping
°2	Object Management	✓ WAN1 ✓ ping IP: 62.215.1.162 Start
D	Safety Protection	PING 62.215.1.162 (62.215.1.162) from 178.61.168.14: 56 data bytes
Ē	Log Record	 ✓ 64 bytes from 62.215.1.162: seq=0 ttl=255 time=2.497 ms 64 bytes from 62.215.1.162: seq=1 ttl=255 time=2.411 ms
Ŧ	VPN	✓ 64 bytes from 62.215.1.162: seq=2 ttl=255 time=2.342 ms 64 bytes from 62.215.1.162: seq=3 ttl=255 time=3.783 ms
*	Device Maintenance	▲ 64 bytes from 62.215.1.162: seq=4 ttl=255 time=2.276 ms
	Firmware Upgrade	64 bytes from 62.215.1.162: seq=5 ttl=255 time=2.260 ms
	Modify Password	62.215.1.162 ping statistics 6 packets transmitted, 6 packets received, 00x96e1b30acket loss
	Authority Management	round-trip min/avg/max = 2.260/2.594/3.783 ms
	Ping Detection	



Multi Ping



Configure File Maintenance

Export and import the configuration information of the gateway and restore it to the factory.

9	Auth Internet Access	~	S Configuration file maintenance	
ţţļ	Behavior Control	\sim	Configuration file maintenance Email backup	
	Object Management	\sim	Export cofiguration	
D	Safety Protection	\sim	P Export and save the configuration file, which can be imported and recovery later	
ŧ	Log Record	\sim	Export cofiguration	
Ē	VPN	\sim		
10	Device Maintenance	~	Import configuration	
-			Image: Select configuration file, import to recover the configuration	
	Firmware Upgrade		File path: Chaose File No file chaose Import configuration	
	Modify Password			
	Authority Management		Restore to factory setting	
	Ping Detection		Restore to factory setting, all previous configuration will be lost	
	Configure File Maintena	nce	Restore to factory setting	
	Restart Device			
	Timed Task			
	Time Synchronization			



Restart Device

From here you can restart XT-2500AC or shutdown the device

C,	Auth Internet Access	\sim	Reboot device
ţţ	Behavior Control	\sim	P Before reboot the device, make sure that the device is not in the process of upgrading, otherwise the device may not be able to start and repair!
0-2 0	Object Management	\sim	Reboot device Power off
Ο	Safety Protection	\sim	
₽	Log Record	\sim	
Ē	VPN	\sim	
\$	Device Maintenance	^	
	Firmware Upgrade		
	Modify Password		
	Authority Management		
	Ping Detection		
	Configure File Maintenar	nce	
	Restart Device		
	Timed Task		

Time Task

Set the timing operation of the gateway

MUL	MULTI-FUNCTION GATEWAY Current operation Device Maintenance >> Timed Task Refresh Change password Logout						
٩	Auth Internet Access	\sim	Timed task				
ļţļ	Behavior Control	\sim	Timed task Temporary task				
- <u>-</u>	Object Management	\sim	Add Delete				
Ο	Safety Protection	\sim	SN Type Execution ti	Enable	Operation		
₽	Log Record	\sim					
÷.	VPN	\sim	Cycle execution ✓ <u>Select all</u> ✓Sun ♥Mon ♥Tue ♥Wed ♥Thu ♥Fr	i √ Sat			
*	Device Maintenance	^	Start time:				
	Firmware Upgrade		Execution command (One command per line, up	io 100)			
	Modify Password		reboot				
	Authority Management			1			
	Ping Detection		Time format: 24-hour system, (HH: mm), such as 1	3:10			
	Configure File Maintenar	nce		Confirm Cancel			
	Restart Device						
	Timed Task						
	Time Synchronization						
	Cloud Configure						
			965 1880005 🛞 www.xontel.com 💌	kuwait@xontel.	 com		



Time Synchronization

Different time zones and main time servers can be selected

Q	Auth Internet Access	\sim	Time synchronization			
ţţ	Behavior Control	\sim	P Configure the correct network	ork time server domain name or IP, the device	will be timed (30 minutes) synchronize with the server.	
0-2 0	Object Management	\sim	time zone :	(GMT+03:00)Baghdad, Kuwait, Riyadh	~	
Ο	Safety Protection	\sim	Master time server:	ntp.api.bz		
₽	Log Record	\sim	Alternate time server:	time.windows.com		
ŧ.	VPN	\sim	Save configuration			
*	Device Maintenance					
	Firmware Upgrade		Current device time:	2024-03-21 02:49		
	Modify Password		Local computer time:	2024-03-21 02:48		
	Authority Management		Synchronize time			
	Ping Detection		Cynonionize ane			
	Configure File Maintenar	nce				
	Restart Device					
	Timed Task					
	Time Synchronization					
	Cloud Configure					



Cloud Configure

Cloud configuration will allow you to manage your XT-2500AC remotely.

Create account in the cloud management (<u>http://97.74.85.146:9090/</u>) and Configure cloud management in controller.

MUL	TI-FUNCTION GATEW	AY	Current operation Device Maintenance >> Cloud Configure
9	Auth Internet Access	\sim	Cloud platform configure
ţţţ	Behavior Control	\sim	Function enable: Enabled, click to disable
	Object Management	\sim	
D	Safety Protection	\sim	Cloud server address: http://97.74.85.146:9090 Register
₿	Log Record	\sim	Save configuration
ţ.	VPN	\sim	
*	Device Maintenance	^	
	Firmware Upgrade		
	Modify Password		
	Authority Management		
	Ping Detection		
	Configure File Maintenand	ce	
	Restart Device		
	Timed Task		
	Time Synchronization		
	Cloud Configure		



After logging successfully to your cloud management account successfully click on binding device as shown below.







Copy the active LAN MAC address from controller to setup in cloud management as shown in the figures below.

MU	LTI-FUNCTION GATEW	/AY	Current operation System S	tatus >> Device Info				Refresh Change	e password
2	System Status	^	Network interface statu	IS					
	Device Info								
	Interface Status								
	LAN IP Flow		LAN1 LAN2	LAN3 WAN3 WAN2 WAN1					
	Application Flow		Interface	Туре	Link mode	IP address	MAC address	Receive speed	Send s
	Network Configure	\sim	WAN1	WAN port Online	1000M/Full duplex	89.203.21.208	94-09-D3-12-7F-A5	0.08 KB/S	0.01
(v)	Flow Control Policy	\sim	WAN2	WAN port Online	1000M/Full duplex	172.16.20.4	94-09-D3-12-7F-A4	0.12 KB/S	0.09
6	AC Management	~	WAN3	WAN port Online	1000M/Full duplex	192.168.202.2	94-09-D3-12-7F-A3	1.37 KB/S	0.981
	AC Management	~	LAN3	LAN port	Disconnect	172.18.0.1	94-09-D3-12-7F-A2	0.00 KB/S	0.00
(Auth Internet Access	\sim	LAN2	LAN port	Disconnect	172.17.0.1	94-09-D3-12-7F-A1	0.00 KB/S	0.00
ţţţ	Behavior Control	\sim	LAN1	LAN port	Disconnect	172.16.40.1	94-09-D3-12-7F-A0	0.00 KB/S	0.00
	Object Management	\sim	Device basic information	on					
D	Safety Protection	\sim	Device ID:	Y24190000467, Max Users:1024 , Max AP	can be managed:1024				
₽	Log Record	\sim	Uptime:	4:35:3 up 0 days					
÷	VPN	\sim	Memory utilization:	19% 350.36MB/1.82G	В			2ª	
			07 74 05 146:0000 (-1				0-	A (1)	
		IN	etlot	Home Device	Project Maintenance	Auth	Account	8	
•	Project List		All (5) G	ateway (4) AP (1) CPE (0) 4	G (0) 5G (0)	lotal Device:5	Online:3	Alarm:0	Offlin
	SMy Project(5)		• De •	Binding Device		×	e Name 🔍	×	V= ~
				Binding Device	Batch Bin	ding	Version Access	Time 👘 Status	Config
					controller userna	me and password	AX850-P2 2023-1	2-25 💿	
				Device Account admin		ine una pussiona	V20221125 2022.1	2.25	
				Device Password ••••••		Ø	V20231125 2023-12	2-25 🤍	
				MAC 94:09:D3:12:	7F:A0 Controller LA	N MAC Address	V20231125 2023-12	2-18 📀	
			4	Rinding Project			V20231125 2023-1	2-18 📀	
				My Pi	roject				
						2			
			Tot					Go to 1	/1



After binding controller successfully, you can manage the settings remotely as shown below

	ot				E	7										P	
	υı		Ho	ome	Devi	ice	Pr	oject	Ma	aintenance		Auth	Account			0	
Project List		All (5)	Gat	eway (4)	AP (1)	CPE (0)	4G	(0)	5G (0)			Total Device:5	Online	e:3	l Ala	rm:0	Offline
My Project(5)		Dev	vice Lis	t			660	All	~	All Mod	~	MAC/Type/Devi	ce Name	Q	[y .	∑ ≡
			SN	MAC		IP			Name 🌲	Туре	÷	Mode	Version	Access T	ime	Status	Config
			1	7C:27:3C	:17:6B:6C	192.16	8.1.18		ap-xontel	AX850-	P2	AP	AX850-P2	2023-12-	25	0	
			2	94:09:D3	:12:7F:A0	172.16	.40.1		A_latifMUk	AC-BW	1000	GateWay	V20231125	²⁰² =	Info)	: E
			3	7C:27:3C	:48:B3:FE	192.16	8.8.1		hassanh	AC-BW	520	GateWay	V20231125	2023 =	Unt	bind	
	d.		4	7C:27:3C	:48:B4:06	192.16	8.1.1		office	AC-BW	520	GateWay	V20231125	2023-12-	18	0	***
			5	94:09:D3	:11:70:06											0	
		Tota	15									7 / pag	e v <	1 >	Go t	o 1	/1

← → C ▲ Not secure 97.74.85.146	5:9090/cloudnetlot/frontend/home/ind	dex.html#/device/managemen	t		©	r ☆ Ď	■ ●
Z CloudNetlot	Home Device	Project N	faintenance	Auth /	Account	P	
Project List Ver	rsion: V20231125			CPU	0%	Memory 🔴	17%
My Project(5)	Uptime 00:00:35	//AC 94:09:D3:12:7F:A0 //ode GateWay	Name Type	A_latifMUK)	Info	AP
	User List Alarm setting Other	set 🗸					
•	SN Name	MAC	IP Empty Data		↑ Up	↓ Down	Config

L +965 1880005

kuwait@xontel.com

شركـة زونـتـل تـكنـولـوجـي

_ للتجارة العامة ذ.م.م



شركـة زونـتـل تـكنـولـوجـي

للتجارة العامة ذ.م.م

7 Clou	dNe	tlot				E						2 6	র 🛛 ।
	unte			Home		Device	Pro	ject Mainter	nance	Auth	Account	0.0	
Project List		Ve	rsion: V202	31125						CPU	0%	Memory 🔵	17
📚 My Project(5)					. 0								
				io "Ö	J	MA	AC 94	:09:D3:12:7F:A0	Name	A_latifMU	K 🖸		D
			Uptime	00:00:35		Mo	de Ga	tevvay	Type	AC-RM 100	50	Info	AP
			User Li	st Ala	rm setting	Other set	t v						
						•	Remote Ma	nagement					
		4											
							Remote Ma	nagement Enable		7	1 4		
							Remote	connection			\vee		
							If no new w	indow pop up after cli	ck the blue bu	utton, pleas <mark>e co</mark>	py address h		
							nacto it inte	the hrowcer addreed	nar to open fr	na ramota mana	agament link		
✓ Z CloudNetiot		×	Converge	d Gateway		× +	naeta it inte	the hrowcer addrecs	bar to open tr	na ramota mana	anamant link	_	D
✓ Z CloudNetlot		× =	Converge	d Gateway	20110/inc	× +	nacta it inte	tha hrowcar addraec l	har to open tr	na ramota mana	mement link	-	
 ✓ Z CloudNetlot ← → C ▲ Not 	t secure	× =	Converge	d Gateway rowifi.net:2	20110/inc	× + dex.htm	nacta it inte	the hrowcer addreed	par to open tr	na ramota mana	namant link	- * छ।	□ ■ B
 ✓ Z CloudNetlot ← → C ▲ Not MULTI-FUNCTION GATE 	t secure	x = y241900004	Converge 167.demo.y	d Gateway rowifi.net:2 Status >> I	20110/inc Device Info	× + Jex.htm	nacta it inte	the hrowcer addreed	nar to onen tr	na ramota mana	mamant link	- ☆ ♪ Refresh Change	D B password L
 ✓ Z CloudNetlot ← → C ▲ Not MULTI-FUNCTION GATI ☑ System Status 	t secure	x y241900004 Surrent operation Network in	Converge 167.demo.y tion System nterface stat	d Gateway rowifi.net:2 Status >> I tus	20110/inc	× + dex.htm	nacta it inte	Domoin fro	nar to onen tr	na ramota mana	noment link	→ ♪ Refresh Change	D D password L
 ✓ Z CloudNetIot ← → C ▲ Not MULTI-FUNCTION GATI ☑ System Status □evice Info 	t secure y	× = y241900004 surrent opera	Converge 167.demo.y tion System	d Gateway rowifi.net: Status >> I tus	20110/inc	× + dex.htm		b the hrowcer addreed b Domain from	m cloud ma	nagement rer	notely	- ★ ♪ ↓ Refresh Change	D D Password L
 ✓ Z CloudNetlot ← → C ▲ Not MULTI-FUNCTION GATI ④ System Status Device Info Interface Status 	EWAY c	x = y241900004 Current operations Network into LAN1	Converge	d Gateway rowifi.net: Status >> I tus	20110/inc Device Info	× + dex.htm	pacta it inte	Domain fro	m cloud ma	nagement ret	notely	 ★ ♪ ↓ Refresh Change	D D password L
 ✓ Z CloudNetlot ← → C ▲ Not MULTI-FUNCTION GATI ☑ System Status □ Device Info Interface Status LAN IP Flow Application Flow 	EWAY C	x 241900004 Current operat Network in LAN1	Converge	d Gateway rowifi.net:2 Status >> I tus LAN3	20110/inc Device Info	× + dex.htm WAN2	pacta it inte	b the hrowcer addrece i Domain from	m cloud ma	nagement rer	notely MAC address	← ★ ♪ ↓ Refresh Change	D D password L Send spe
 ✓ Z CloudNetIot ← → C ▲ Not MULTI-FUNCTION GATI ☑ System Status □ Device Info □ Interface Status □ LAN IP Flow Application Flow ■ Network Configure 	EWAY c	x	Converge	d Gateway rowifi.net.: Status >> 1 tus LAN3	20110/inc Device Info WAN3	× + dex.htm WAN2 Type	parta it inte	Domain froi Link mode	m cloud mat	nagement rer P address .203.21.208	notely MAC address 94-09-D3-12-7F-A5	Refresh Change	Dessword L Send spec 0.06 KB
 ✓ Z CloudNetlot ← → C ▲ Not MULTI-FUNCTION GATION GATION ✓ System Status ✓ Device Info ✓ Interface Status ✓ LAN IP Flow ✓ Application Flow ✓ Network Configure 	EWAY C	x = y241900004 Surrent operat Network in LAN1 Inte WW	Converge	d Gateway rowifi.net:2 Status >> I tus LAN3	20110/inc Device Info WAN3	x + dex.htm wanz Type V port Online	pacta it inte	Domain from Link mode 1000M/Full duplex	m cloud mat s la sea la s a sea la sea la sea la s a sea la sea la sea la sea la sea la sea la s a sea la sea la s a sea la sea la s a sea la	nagement ren Paddress .203.21.208 72.16.20.4	MAC address 94-09-D3-12-7F-A4	Refresh Change Receive speed 0.13 KB/S 0.10 KB/S	
✓ ✓ ✓ CloudNetlot ← → C ▲ Not MULTI-FUNCTION GATI ☑ System Status ☑ Device Info Interface Status LAN IP Flow Application Flow ④ ●	t secure	x = y241900004 Surrent operation Network in LAN1 inte WW WW	Converge	d Gateway vowifi.net: Status >> 1 tus LAN3	20110/inc Device Info WAN3 WAN3 WAN WAN	× + dex.htm wax2 Type A port Online A port Online	pacta it inte	Domain froi Link mode 1000M/Full duplex 1000M/Full duplex	m cloud ma:	nagement rer Paddress 1.203.21.208 72.16.20.4 2.168.202.2	MAC address 94-09-D3-12-7F-A4 94-09-D3-12-7F-A3		
✓ ✓ CloudNetlot ← → Cl ▲ Nor MULTI-FUNCTION GATION Image: System Status Image: Device Info Image: LAN IP Flow Application Flow Application Flow Image: Flow Control Policy Image: Status Image: Plow Control Policy Image: Status	EWAY C	× = y241900004 Surrent operations Network in LAN1 Inte W W W W L	Converge 167.demo.y 160 System Interface star LAN2 erface AN1 AN2 AN3	d Gateway rowifi.net:: Status >> I tus LAN3	20110/inc Device Info WAN3 WAN WAN	x + dex.htm wanz Type N port Online N port Online N port Online	parta it inte	Domain from Link mode 1000M/Full duplex 1000M/Full duplex 1000M/Full duplex	m cloud mat 8 89 4 19 4 9	nagement rer Paddress .203.21.208 72.16.20.4 2.168.202.2 172.18.0.1	MAC address 94-09-D3-12-7F-A5 94-09-D3-12-7F-A3 94-09-D3-12-7F-A3 94-09-D3-12-7F-A3		
✓ ✓ ✓ CloudNetlot ← → Cl ▲ Not MULTI-FUNCTION GATI ☑ System Status ☑ Device Info Interface Status LAN IP Flow Application Flow ④ Interface Status LAN IP Flow Application Flow Image: A C Management Image: A C Management	t secure	x	Converge	d Gateway vowifi.net: Status >> I tus LAN3	20110/inc Device Info WAN3 WAN3 WAN WAN	x + dex.htm wanz Type N port Online N port Online N port Online An port -AN port	pacta it inte	Domain froi Link mode 1000M/Full duplex 1000M/Full duplex 1000M/Full duplex 1000M/Full duplex	m cloud mat s a 19 s	P address 0.203.21.208 72.16.20.4 12.168.202.2 172.18.0.1	MAC address 94-09-D3-12-7F-A5 94-09-D3-12-7F-A4 94-09-D3-12-7F-A3 94-09-D3-12-7F-A2 94-09-D3-12-7F-A2		
✓ ✓ CloudNetlot ← → Cl ▲ Nor MULTI-FUNCTION GATE ✓ System Status Imerface Status LAN IP Flow Application Flow ● Flow Control Policy ● Act Management ● Auth Internet Access ● ●	t secure	× =	Converge	d Gateway owifi.net:: Status >> I tus LAN3	20110/inc Device Info WAN3 WAN3 WAN WAN WAN	× + dex.htm	parta it inte	Domain from Link mode 1000M/Full duplex 1000M/Full duplex 1000M/Full duplex 1000M/Full duplex Disconnect Disconnect	m cloud ma: 8 89 1 19 1 19 1 1 1 1 1 1 1 1 1 1	nagement rer Paddress .203.21.208 72.16.20.4 2.168.202.2 172.18.0.1 172.17.0.1 72.16.40.1	MAC address 94-09-D3-12-7F-A5 94-09-D3-12-7F-A4 94-09-D3-12-7F-A3 94-09-D3-12-7F-A2 94-09-D3-12-7F-A1 94-09-D3-12-7F-A1	Refresh Change 0.13 KB/S 0.13 KB/S 0.13 KB/S 0.10 KB/S 1.34 KB/S 0.00 KB/S 0.00 KB/S 0.00 KB/S	
✓ ✓ ✓ CloudNettot ← → CloudNettot Mod MULTI-FUNCTION GATI ☑ System Status ☑ System Status ☑ Device Info Interface Status Interface Status IAN IP Flow Application Flow Image: A C Management	s secure	× =	Converge	d Gateway rowifi.net: Status >> I tus LAN3	20110/inc Device Info WAN3 WAN3 WAN UVAN UVAN	x + dex.htm dex.htm WAN2 Type N port Online N port Online A port Online An port LAN port	pacta it inte	Domain froi Link mode 1000M/Full duplex 1000M/Full duplex 1000M/Full duplex 1000M/Full duplex 1000M/Full duplex Disconnect Disconnect	m cloud mat s and a second se	Paddress 1203.21.208 72.16.20.4 172.16.8.01 172.16.40.1	MAC address 94-09-D3-12-7F-A3 94-09-D3-12-7F-A3 94-09-D3-12-7F-A3 94-09-D3-12-7F-A3 94-09-D3-12-7F-A1 94-09-D3-12-7F-A0		Send spec O.06 KB O.07 KB O.09 KB O.00 KB O.00 KB O.00 KB O.00 KB O.00 KB
✓ ✓ CloudNetlot ← → CloudNetlot MULTI-FUNCTION GATION Image: System Status Image: System Status Image: Device Info	EWAY C	× =	Converge Conve	d Gateway cowifi.net:: Status >> I tus LAN3 LAN3 Lion tion	20110/inc Device Info WAN3 WAN WAN UVAN UVAN L L L	× + dex.htm	pacta it into	b the browcer addrees b Domain from Link mode 1000M/Full duplex 1000M/Full duplex 1000M/Full duplex Disconnect Disconnect Disconnect sconnect	m cloud mat s 89 1 3 4 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5	Paddress .203.21.208 72.16.20.4 172.16.0.1 172.17.0.1 72.16.40.1	MAC address 94-09-D3-12-7F-A5 94-09-D3-12-7F-A3 94-09-D3-12-7F-A3 94-09-D3-12-7F-A1 94-09-D3-12-7F-A1 94-09-D3-12-7F-A0	► ► − Refresh Change Receive speed 0.13 KB/S 0.13 KB/S 0.13 KB/S 0.10 KB/S 0.00 KB/S 0.00 KB/S	Send spe 0.06 KB 0.39 KB 0.30 KB 0.00 KB
✓ ✓	EWAY C	x	Converge	d Gateway vowifi.net.: Status >> 1 tus LAN3 LAN3 tion y Y241900 e: 4:39:3 IU	20110/inc Device Info WAN3 WAN3 WAN UAN UAN UAN UAN UAN UAN UAN UAN UAN U	x + dex.htm dex.htm WAN2 Type N port Online N port Online AN port AN port AN port AN port AN port AN port AN port	Pacta it inte WAN1	be the browser address of the browser address	m cloud mat a la la a la	nagement rer Paddress 1.203.21.208 72.16.20.4 12.168.202.2 172.18.0.1 172.17.0.1 72.16.40.1	MAC address 94-09-D3-12-7F-A5 94-09-D3-12-7F-A4 94-09-D3-12-7F-A3 94-09-D3-12-7F-A2 94-09-D3-12-7F-A0	► ► − Refresh Change Refresh Change Refresh Change 0.13 KB/S 0.10 KB/S Refresh Change 0.10 KB/S 0.00 KB/S Refresh Change 0.00 KB/S 0.00 KB/S Refresh Change	
✓ ✓ CloudNetlot ← → CloudNetlot MULTI-FUNCTION GATE Image: System Status Image: System Status Image: Device Info Ima	EWAY C	× •	Converge	d Gateway owifi.net:: Status >> 1 tus LAN3	20110/inc Device Info WAN3 WAN3 WAN WAN UAN UAN UAN UAN UAN UAN UAN UAN UAN U	× + dex.htm dex.htm wanz Type N port Online N port Online A port Online A port Online An port An port An port ax Users:102-	Pacta it into WAN1 4 , Max AP can	be herowear addrace by Domain from Domain from Link mode 1000M/Full duplex 1000M/Full duplex 1000M/Full duplex 1000M/Full duplex Disconnect Disconnect Disconnect	m cloud mat s 89 s 1 s 89 s 1 s 1 9 s 1 1 9 s 1 1	nagement rer Paddress .203.21.208 72.16.20.4 2.168.202.2 172.18.0.1 172.17.0.1 72.16.40.1	MAC address 94-09-D3-12-7F-A5 94-09-D3-12-7F-A4 94-09-D3-12-7F-A3 94-09-D3-12-7F-A1 94-09-D3-12-7F-A1 94-09-D3-12-7F-A0	► ► Refresh Change Receive speed 0.13 KB/S 0.10 KB/S 1.34 KB/S 0.00 KB/S 0.00 KB/S 0.00 KB/S	