

XT-1000AC



Wireless Access Point Controller & Multi-WAN Gateway

User Manual





Table of Contents

- 1 Log In
- 2 Status
- 3 Network
 - 3.1 Interface Setting
 - 3.2 Internet Setting
 - 3.3 Local Network Setting
 - 3.4 DNS Setting
 - 3.5 Balance
 - 3.6 VLAN Settings
 - 3.7 DNS Settings
 - 3.8 Static Route
 - **3.9 Directed Route**
 - 3.10 Timing Redial

4 AC Control

- 4.1 Group
- 4.2 Members
- 4.3 Batch Upgrade
- 4.4 Details

5 Authentication

- 5.1 Local Auth
- 5.1.1 OneKey Authentication
- 5.1.2 WeChat Authentication
- 5.1.3 Traffic Authentication
- 5.1.4 User Authentication
- 5.1.5 Password Authentication
- 5.2 Wifidog Auth





6 Bandwidth Control

6.1 QoS

- 6.2 IP Limit
- 6.3 Localnet Monitor

7 Firewall

- 7.1 IP Filter
- 7.2 MAC Filter
- 7.3 URL Filter
- 7.4 Port Filter
- 7.5 Port Mapping
- 7.6 DMZ settings
- 7.7 ARP Binding
- 7.8 Attack Protection

8 Service

- 8.1 DDNS Settings
- 8.2 Static DNS
- 8.3 Remote Management
- 8.4 VPN Client
- 8.4.1 PPTP Client
- 8.4.1 L2TP Client
- 8.5 VPN Server
- 8.5.1 PPTP Server
- 8.5.2 PPTP User
- 8.6 UPNP Settings

9 Log and Statistics

9.1 Log

9.2 Status Chart



KonTel



10 System Tools

- 10.1 System Upgarde
- 10.2 Manage Config

10.3 Reboot

- 10.3.1 Reboot Now
- 10.3.2 Timed Restart
- 10.4 Password Setting
- 10.5 Time Setting
- 10.6 PING







1 Log In

1. XT-1000AC is based on the browser's configuration interface. Open your browser, and input IP address as 192.168.1.1

🍯 New Tab	x +			 - 0 🗮
← → ♂ ŵ	Q 192.168.1.1			lin 🗉 🏽
				*
		G Search the Web	\rightarrow	
	E Top Sites >			
	EE TOP SIGN			
	🏷 Highlights →			

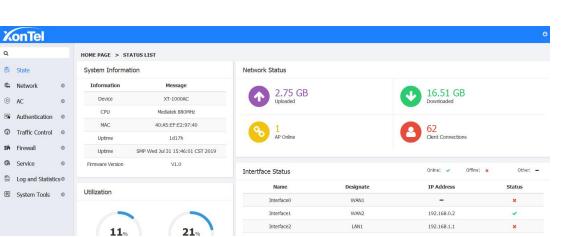
2. After finished the IP address and click Enter. Then it will get into XT-1000AC' LOGIN interface as below:

XonTel	x +		
(←) → ℃ @	👽 🔏 192.168.1.1/login.html		···· 🖂 🌣 🗎 🕲
		XonTel	
		L Username	
		Q. Password	
		LOGIN	
		Copyright © 2004-2019 By Xontel All Rights Reserved.	

2. Input user name "admin", Password "xontel". Then click LOGIN to get into the home page as below:

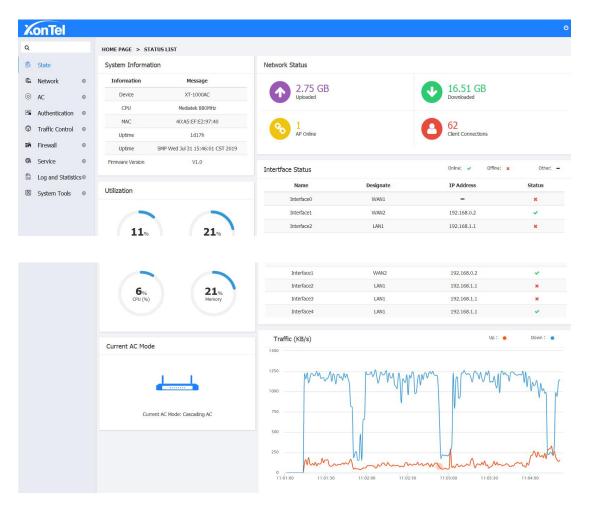






2 State

After login, it will get into the state information page directly. It will show you basic hardware information, CPU and Memory utilization, Ethernet status and Traffic rate data





زونت





3 Network

3.1 Interface Setting

The "eth0" is defaulted to be WAN port. "eth5" is defaulted to be LAN port and it cannot edit. The rest "eth1-eth4" is customized to be WAN port or LAN port. After designated the WAN port or LAN port, set up the internal network and outer network by "Local Network" and "WAN Settings".

1. Click "Interface Setting" and get into the its setting page as below:

L	HOME PAG	GE > NETWOR	C > INTERTFAC	E SETTING						
ð State	Extra Ir	nterface			Local Inter	face			Free Interfac	e
Network O	No.	Designate	Interface	Action	No.	Designate	Interface	Action	No.	Interface
Intertface Setting	1	WAN1	eth0.1		1	LAN1	eth0.5 eth0.3 eth0.4	1		
WAN Settings	2	WAN2	eth0.2							
LAN Settings										
DHCP Settings	1									
Balance	() infor	mation After Interfa	ice assign,please go	to < LAN Settings	s > or < WAN Setting	s > to add detail cont	iguration.			
VLAN Setup										
DNS Settings										
Static Route										

2. Click the "Edit" button to go into the "LAN1 Interface Settings" page, you can release free Ethernet ports. e.g eth0.4 is unchecked in below picture:

State Extra Interface sector physical interface status no. pesignate i id etho.5 Occupy no. interface no. interface id etho.4 Occupy id interface id	2	HOME PAG	GE > NETWORK	> LAN1 Interface S	etungs		×		
Network S No. Designate I Interface Setting 3 WANI Image: Constraint of the setting se	5 State	Extra In	terface	Select All	physical interface	Status		Free Interface	
Interface Setting 1 WAN1 WAN Settings 2 WAN2 LAN Settings	Network 🗢	No.	Designate	II II	eth0.5	Occupy	Action	No.	Interface
WAN Settings 2 WAI2 LAN Settings DHCP Settings	Intertface Setting	1	WAN1	V	eth0.3	Occupy	28		
DHCP Settings 0	WAN Settings	2	WAN2		eth0.4	Occupy			
A information that the interview descent to a 100 California on a 1000 California to add datal and such as the		1				sav			
Balance U minormation with interface assign please go to < Law Settings > to and detail conliguration.	Balance	() inform	mation After Interface	assign,please go to < LAN S	ettings > or < WAN Settings > to add detail co				

3. Click the "Add" button to get into the "Extra Interface", Then go into the newly increased Local Interface page,tick to choose the INTERFACE which you want to add,as below:

	HOME PAG	GE > NETWORK	> Add Local Interfa	aceLAN2	×			
State	Extra In	iterface	Select All	physical interface	Status	Add	Free Interfac	e
Network 🗢	No.	Designate	10	eth0.4	Free	Action	No.	Interface
Intertface Setting	1	WAN1			save	28	1	eth0.4
WAN Settings	2	WAN2	etno.2	_				
LAN Settings								
DHCP Settings								









4. Click "Save" and the INTERFACE list which you add will appear in the local Interface as new Interface.

2	HOME PA	GE > NETWORK	<pre>x > INTERTFAC</pre>	E SETTING						
5 State	Extra Ir	nterface			Local Inter	face			Free Interface	÷
🗈 Network 🔹 🗢	No.	Designate	Interface	Action	No.	Designate	Interface	Action	No.	Interface
Intertface Setting	1	WAN1	eth0.1	8	1	LAN1	eth0.5 eth0.3	28		
WAN Settings	2	WAN2	eth0.2	8	2	LAN2	eth0.4	28		
LAN Settings										
DHCP Settings 0 Balance	() infor	mation After interfa	ice assign,please go	to < LAN Settings	s > or < WAN Setting	js > to add detail config	uration.			
VLAN Setup										
DNS Settings										
Static Route										
Directed Route										

5. Click "LAN Settings" to set up the LAN2's IP Address and Subnet Mask parameter .

KonTel			ს
۹	HOME PAGE > NETWORK > LAN SETTINGS		
🕏 State	LAN1 LAN2		
C Network •			
Intertface Setting		40:A5:EF:E2:97:42	
WAN Settings		Static	
LAN Settings		192.168.2.1	0
DHCP Settings		ΙΡ Εχ: χοοιμοχωρούρος	
Balance	Subnet Mask	255.255.255.0	
VLAN Setup		Enter Subnet Mask Info	
DNS Settings	Allow access	Close	
Static Route		Save Cancel	1
Directed Route			

3.3 WAN Settings

In "WAN Settings" you can set up WAN Interface as DHCP Client, Static IP,PPPoE in connection types, it support Clone MAC address.

1. DHCP: If the WAN Port achieve the IP automatically by the DHCP, you can use this connection type.





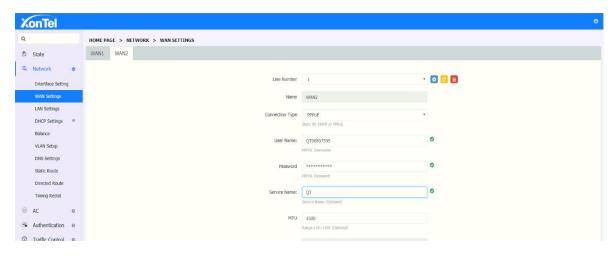


KonTel		ወ
Q	HOME PAGE > NETWORK > WAN SETTINGS	
🕏 State	WANI WAN2	
📽 Network 🛛 👁		
Intertface Setting	Line Number 1 💽 🖸 🕄 🗐	
WAN Settings	Name WWAVI	
LAN Settings	Connection Type DHCP Clent •	
DHCP Settings ® Balance	Static IP, DHCP or PPPuE	
VLAN Setup	Host Name	
DNS Settings	Host Name (Optional)	
Static Route	IP Address Auto IP	
Directed Route	Up 10	
Timing Redial	1-1000((Mbps))	
AC 0	Down 10	
Authentication @		

2. Static IP: Configure the Fixed IP, Subnet Mask, Default Gateway and DNS of the service.

7	onTel				Ċ
٩			HOME PAGE > NETWORK > WAN SETTINGS		
Ø	State		WAN1 WAN2		
C	Network	•			_
	Intertface Setting		Line Numbe	1	
	WAN Settings		Nam	WAN1	
	LAN Settings		Connection Type	Static IP	•
	DHCP Settings	Ø		Static IP, DHCP or PPPoE	
	Balance VLAN Setup		IP Addres	195.226.72.53	•
	DNS Settings			IP Ex: xoocaoocaoocaooc	
	Static Route		Subnet Masi		•
	Directed Route			Enter Subnet Mask Info	
	Timing Redial		Default Gateway	195.226.72.51 Enter Gateway Info	0
0	AC	0			
-	Authentication	0	main DN:	8.8.8.8 IP Ex: 100(200(200(200)	0

3. PPPoE: If choose this connection type,fill in the related User Name and Password of the service, the state will show connected after success authentication.









4. Click"+"to add multiple network connections on the same interface.

X	onTel				¢
٩			HOME PAGE > NETWORK > WAN SETTINGS		
¢.	State		WAN1 WAN2		
e.	Network	•			
4	Intertface Setting		Line Number	1	· 🙆 🖸
	WAN Settings		Name	WAN2	
	LAN Settings		Connection Type	PPPOE	*
	DHCP Settings	0		Static IP, DHCP or PPPoE	
	Balance		User Name:	QT96897595	0
	VLAN Setup DNS Settings			PPPOE Username	
	Static Route		Password		0
	Directed Route			PPPOE Pattword	
	Timing Redial		Service Name:	QT Service Name (Optional)	0
0	AC	0			
36	Authentication	0		1500 Range:128~1500 (Optional)	

5. Click "Redial" button to redial the network line

KonTel			¢
۹	HOME PAGE > NETWORK > WAN SETTINGS		
🖏 State	WAN1 WAN2		
C Network o			-
Intertface Setting	Line Number	1	
WAN Settings	Name	WANZ	
LAN Settings	Connection Type	PPPoE	
DHCP Settings 0		Static IP, DHCP or PPPoE	
Balance VLAN Setup	User Name:	QT96897595	0
DNS Settings		PPPOE Username	
Static Route	Password	*******	0
Directed Route		PPPOE Password	
Timing Redial	Service Name:	QT Service Name (Optional)	•
@ MC 0			

6. Click the delete button to delete unnecessary Internet lines. The first one cannot be deleted

2	onTel			0
٩		HOME PAGE > NETWORK > WAN SETTINGS		
8	State	WAN1 WAN2		
C	Network o			-
	Intertface Setting	Line Number	1 *	
	WAN Settings	Name	WAN2	
	LAN Settings	Connection Type	PPPoE *	
	DHCP Settings 0		Static IP, DHCP or PPPoE	
	Balance VLAN Setup		4100000000	9
	DNS Settings		PPPOE Utername	
	Static Route	Password	PPPOE Parsword	5
	Directed Route			
	Timing Redial	Service Name:	QT Service Name (Optional)	9
0	AC 0	MTU	1500	
B	Authentication 0		Ranpe:128-1500 (Optional)	





3.2 Local Network Settings

You can manually set each LAN Interface's IP Address and Subnet Mask, the default IP address is 192.168.1.1

KonTel		Ů
۹	HOME PAGE > NETWORK > LAN SETTINGS	
🕏 State	LAN1	
C Network •		
Intertface Setting	MAC	40:A5:EF:E2:97:40
WAN Settings		Static
LAN Settings	IP Address	192.168.1.1
DHCP Settings		1P Ex 3004004.004
Balance	Subnet Mask	255.255.255.0
VLAN Setup		Enter Subnet Mask Info
DNS Settings	Allow access	Close
Static Route		Save Cancel
Directed Route	-	Carce

3.5 DHCP Settings

DHCP Settings:Here you can set up DHCP as Server,start IP,Address number,DHCP Lease Time,Domain Name,Main DNS and Backup DNS. You can also disabled DHCP function. (Attention:At the situation of disabled DHCP function,the device will not offer IP to client,and client need to manual setting the IP address)

XonTel		Ċ
Q	HOME PAGE > NETWORK > DHCP SETTINGS > DHCP SERVICE	
🕏 State	LAN1	
📽 Network 🗢		
Intertface Setting	DHCP	Server •
WAN Settings	DHCP Starting IP	2
LAN Settings		Ex: 172.16.0.xxxx(Fill the last bit)
DHCP Settings	Max Clients	100
DHCP Service		Max Number of IPs to Alocate (1-32768)
Static List	DHCP Lease Time	120
Client List		(2 ~ 10080 Minutes)
Balance	Domain Name	XonTel
VLAN Setup		DHCP Domain (Ex : XonTel)
DNS Settings	Main DNS	192.168.1.1
Static Route		IP Ex xox.xox.xox.xox
Directed Route	Spare DNS	8.8.8.8

Static List:The DHCP service can always assign the same IP address to a specific computer on your LAN. To be more specific, the DHCP service assigns this static IP to a unique MAC address assigned to each NIC on your LAN.You can add it in this place. Here you can installed the compatible ARP binding information, and also can add the PC or mobile device IP address to static allocation, then those device will get the fixed IP.







onTel						
2	HOME PAGE > NETW	ORK > DHCP SE	TTINGS > STATICLIST			
State	Messages List			Number per P	age (10) 🔹 🕞 Delete ARP Binding 💽 🕂 Ad	dd 📗 💼 Delete Selected
Network •	Select All	No.	Client IP	Client MAC	Client Name	Edit
Intertface Setting						
WAN Settings						
LAN Settings						
DHCP Settings						
DHCP Service						
Static List						
Client List						

To add single static bind, click "Add" button in the static list and set up the Client IP and MAC.

K	onTel		r		-		
٩		HOME PAGE > NETWORK >	Single Static Bind		×		
Ē	State	Messages List	Client IP			C Delete ARP Binding	Ndd 🗎 Delete Selected
8	Network •	Select All No.	443.09200940	IP Ex: 3000.0001.000000		Client Name	Edit
	Intertface Setting		Client MAC				
	WAN Settings			MAC Ex. IXCONDUDIDIDIDIDIDI			
	LAN Settings		Clent Name				
	DHCP Settings			(Optional)			
	DHCP Service				save		
	Static List						
	Client List						
	Balance						
	VLAN Setup						

Client List:Here System will display the DHCP allocated CLIENT IP,CLIENT MAC,CLIENT NAME which are connected with the device.You can add any particular client IP to the static list by clicking "Add to Static List" button.

Messages List					Number	per Page (10)) 💽 🕈 🔿 Add to	Static List	C Refre
Select All	No. \$	Client IP 🔶	Client MAC	\$	Client Name	÷ R	Remaining Time	\$	Edit
	61	192.168.1.79					01:03:19		%
8	62	192.168.1.51					01:02:34		%
	63	192.168.1.2					01:02:16		%
	64	192.168.1.92					01:02:10		8
	65	192.168.1.4					00:03:22		8
			L				< 1 2 3	4 5	6 7
	Select All	Solicit All No. C I 61 62 I 63 63 I 64 100	No. Client IP Client IP 61 192.168.1.79 62 192.168.1.51 63 192.168.1.2 64 192.168.1.92	No. Client IP Client MAC 61 192.168.1.79 62 62 192.168.1.51 63 63 192.168.1.2 64	No. Client IP Client MAC 61 192.168.1.79 62 192.168.1.51 63 192.168.1.2 64 192.168.1.92	No. Client IP Client MAC Client Name 61 192.168.1.79 62 192.168.1.51 63 192.168.1.51 63 192.168.1.2 64 192.168.1.92 64 192.168.1.92	No. Client IP Client MAC Client Mame F 61 192.168.1.79 62 192.168.1.51 63 192.168.1.51 63 192.168.1.51 63 192.168.1.51 63 192.168.1.51 63 192.168.1.51 63 192.168.1.51 64 192.168.1.51 64 192.168.1.51 65 192.168.1.92 65 192.168.1.41 65 192.168.1.	Select All No. Client IP Client MAC Client MAme Remaining Time 6 192.168.1.79 01:03:19 01:03:39 01:02:34 6 192.168.1.51 01:02:34 01:02:34 6 192.168.1.92 01:02:10 01:02:10 6 192.168.1.92 00:03:22 00:03:22	No. Client IP Client MAC Client Name Remaining Time 61 192.168.1.79 01:03:19 62 192.168.1.51 01:02:34 63 192.168.1.2 01:02:16 64 192.168.1.92 01:02:10







3.5 Balance

Balance: When the multiple ISP lines connected, choose balance strategy, choose corresponding rate as per their speed. The same or different ISP line will allocate the bandwidth by balance strategy.

Balance			
	Wan line	Balance	Weight:
	WAN1		1 •
	WAN2		1 •
		Save	Cancel

Multiline Route: Install purpose-play Netcom game through Netcom, play Telecom game through Telecom.

tiline Route		Ann an the medical fact the	le different ICD have also a	nable multiline route,and load balan	eer in disklad \
	Mak	Enabled			ice is diabled.)
No.	Line	IP	ISP	Join miltiline route	Default Gateway
1	WAN1	192.168.0.2	MADA 👻	join 👻	22
2	WAN2		choose isp 👻	join 👻	
			Save	Cancel	

Custom ISP:If the list haven't corresponding broadband ISP,you can add custom ISP.Collect the full ISP IP,add it according to the format,then configure mutiline route.

	DHCP Settings		-	Save	Cancel		
	Balance		Custom ISP		×		
	VLAN Setup	Multiline Route					
	DNS Settings		ISP				
	Static Route			ISP Name	1	nce is diabled.)	
	Directed Route		ISP comment				
	Timing Redial			comment name not include chinese		Default Gateway	
0	AC O		Destination IP				
	Authentication 0						
Ø	Traffic Control			(Destination to format is:leagal ip address or ip address/netmask, each			
ΞÅ	Firewall O			line filled in one.)			
G	Service O				save		_
	Log and Statistics	Custom ISP				Number per Page (10) • • Add	🛱 Delete Selected
		Select All No. ≑	ISP			ISP comment	
14	System Tools						







Custom ISP			Number per Page (10) 🔻 🖨 Add 🗎 Delete Selected
Select All	No. \$	ISP	\$ ISP comment \$
	1	QQ	QQ

Port division

1. Traffic will go through the specific exit when the local network appointed IP wants to access some internet ports.

Choose the appointed wan line you need, and enter the appointed IP in SOURCE IP.Enter your DESTINATION PORT.

Attention:At the normal situation,you cannot enter the DESTINATION IP and SOURCE PORT.When your local internet IP is specific,you will need to enter the DESTINATION IP.

Example:Let 443 shutting into WAN1.

Port division						Number per	r Page (10)) Delete Selected
Select All	No.	Proto	Wan line	Source IP	Destination IP	Source port	Destination port	Edit

					Dicahl	ર્ત		-		
	Directed Route				Port division			×		
	Timing Redial							_		
0	AC	0			Proto	ТСР	•			
	Authentication	Θ	Custom ISP					1	lumber per Page (10) 🔹 🕒 Add	前 Delete Selected
Ø	Traffic Control	0			Wan line	WAN1 WAN2				
	Firewall	0	Select All	No, 🗘	Source IP	192.168.1.49	0		ISP comment	
6	Service	0		1		IP EX: X00L000.300L000			QQ	
	Dervice				Destination IP		0			
	Log and Statisti	cs0			Desunation IP	IP EX: X00.300.300.300				
图	System Tools	0				IP CA. AAA.AAA.MAA.AAA				
	System roois		Port division		Source port		•		lumber per Page (10) 🔹 💽 Add	Delete Selected
						Port (1~65535)				E Decte Decetto
			Select All	No.	Destination port	443	0	e po	ort Destination port	Edit
						Port (1~65535)				
								_		
								ave		
							_	-		

2. You can install local internet appointed IP in specific WAN line

Step:Protocol choose at random,Wan line choose appointed one you need,Source choose the appointed IP you need,Destination IP not need to write.







3.6 VLAN Settings

A VLAN is a group of devices on one or more LAN that are configured to communicate as if they were attached to the same wire, when in fact they are located on a number of different LAN segments. Because VLANs are based on logical instead of physical connections, they are extremely flexible.

VLAN SETUP;

Visit the VLAN SETUP page, click "add" on the upper right corner.Create a VLAN and set a virtual IP address.

VLAN ID: Virtual LAN ID number, used to distinguish between different VLANs

IP: This IP address is the address of this VLAN.

X	onTel													
٩		HOME PAGE > NETW	ORK > VLAN	SETUP										
勴	State	Messages List								Numbe	er per Page	(10)	▼ ⊕ Add	Delete Selected
G	Network •	Select All	No. \$	VLAN Name	÷	VLAN ID	¢	IP Address	\$ Subnet Mask	\$	Line	\$	Comments	Edit
	Intertface Setting	12	1	VLAN1		11		11.11.11.1	255.255.0.0		LAN1		Sales	
	WAN Settings													< 1 >
	LAN Settings													
	DHCP Settings													
	Balance													
	VLAN Setup													
	DNS Settings													
	Static Route													

Note: The VLAN ID must correspond to the VLAN ID in the switch. The LAN port of the router directly connect to the trunk of VLAN switch.

3.7 DNS Settings

DNS Settings: DNS, or Domain Name System, is the mechanism by which a network device resolves a name like www.example.com to an IP address such as 198.51.100.25, or viceversa. Clients must have functional DNS if they are to reach other devices such as servers using their hostnames or fully qualified domain names. At the Static IP Mode,need to manual set up Main DNS and Secondary DNS.If you don't know your local DNS address,you can contact with your Internet Service Provider.

1. On Homepage Click "Network - DNS Settings" to enter the DNS setting interface, turn on the DNS switch

15 | Page







KonTel					ტ
Q	HOME PAGE > NETWORK > DNS	SETTINGS			
🕏 State 📽 Network 🔹		DNS Switch	h ON O		
Intertface Setting WAN Settings	Multi line DNS				
LAN Settings	Name	Main DNS	Spare DNS	State	Edit
DHCP Settings	WAN1	192.168.0.1	8.8.8.8	Enabled	
Balance	WAN2	213.34.192.210	213.34.192.211	Disabled	
VLAN Setup					
DNS Settings					
Static Route					
Directed Route					
Timing Redial					

2. Select the need to set the DNS line, click the Edit button, you can select DNS Switch as On or Off, enter the main DNS or secondary DNS, click Save.

KonTel					ĥo	Ċ
۹	HOME PAGE > NETWORK >	DNS Setting		×		
🕏 State		DNS Status	Enabled			
C Network			Static IP cannot be turned off			
Intertface Setting	Multi line DNS	Main DNS	192.168.0.1			
WAN Settings			IP EX: X00.300.300.300			
LAN Settings	Name	Spare DNS	8.8.8.8		State	Edit
DHCP Settings	WAN1		IP Ex: x00.x00.x00.x00		Enabled	
Balance	WAN2	Apply to all			Enabled	
VLAN Setup		393500				
DNS Settings				save		
Static Route				_		
Directed Route						
Timing Redial						

3. Click "Apply to all lines" in the action box and click save to apply the current settings to all lines.

onTel					
L	HOME PAGE > NETWORK > DNS	SETTINGS			
State		DNS Switch			
Intertface Setting WAN Settings	Multi line DNS				
LAN Settings	Name	Main DNS	Spare DNS	State	Edit
DHCP Settings	WAN1	192.168.0.1	8.8.8	Enabled	
Balance	WAN2	192.168.0.1	8.8.8.8	Enabled	
VLAN Setup					
DNS Settings					
Static Route					

3.8 Static Route

Static Route is a form of routing that occurs when a router uses a manually-configured routing entry, rather than information from a dynamic routing traffic. In many cases, static routes are manually configured by a network administrator by adding in entries into a routing table, though this may not always be the case.



زونتــل



X	onTel									Q
Q			HOME PAGE > NETWORK >	• STATIC ROUTE						
Ø	State		Messages List					Number per Page (10)	▼ ⊕ Add	Delete Selected
G		0	Select All NO.	Target IP	Subnet Mask		Gatewa		Interface	Edit
	Intertface Setting		Select All HO.	Target IP	Subject Plask		Gatewa	1	Intendee	Lun
	WAN Settings	g								
	LAN Settings									
	DHCP Settings	Ø								
	Balance									
	VLAN Setup									
	DNS Settings									
	Static Route									
	Directed Route									
	Timing Redial									
X	onTel									Ċ
X	onTel		HOME PAGE > NETWORK >	Static Router Setting			×			ტ
۹			HOME PAGE > NETWORK >				×	Number per Dece (10)		
Q B	State		Messages List		192.168.0.0	Ø		Number per Page (10)	Add	前 Delete Selected
Q B		0			192.168.0.0 IP Ex x00.000.000		×		• • Add Interface	
Q B	State Network Intertface Setting		Messages List		IP Ex: x00.300.300.300	•				前 Delete Selected
Q B	State Network Interface Setting WAN Settings		Messages List	Target IP	IP EX: X00C000C00C00C					前 Delete Selected
Q B	State Network Interface Setting WAN Settings LAN Settings	J	Messages List	Target IP	IP Ex: xxx.xxxx.xxxx 255.255.255.0 Enter Subnet Mask Info 192.168.0.1					前 Delete Selected
Q B	State Network Intertface Setting WAN Settings LAN Settings DHCP Settings		Messages List	Target IP Subnet Mask	IP Ex: xxxx.xxxx.xxxx 255.255.255.0 Enter Subnet Mask Info	•				前 Delete Selected
Q B	State Network Intertface Setting WAN Settings LAN Settings DHCP Settings Balance	J	Messages List	Target IP Subnet Mask	IP Ex: xxx.xxxx.xxxx 255.255.255.0 Enter Subnet Mask Info 192.168.0.1	•				前 Delete Selected
Q B	State Network Interface Setting WAN Settings LAN Settings DHCP Settings Balance VLAN Setup	J	Messages List	Target IP Subnet Mask Gateway	IP EX: 30020020000 255.255.255.0 Enter Subnet Mask Info 192.168.0.1 Enter Gateway Info	•	va			前 Delete Selected
Q B	State Network Interface Setting WAN Settings LAN Settings Balance VLAN Setup DNS Settings	J	Messages List	Target IP Subnet Mask Gateway	IP EX: 30020020000 255.255.255.0 Enter Subnet Mask Info 192.168.0.1 Enter Gateway Info	•				前 Delete Selected
Q B	State Network Interface Setting WAN Settings LAN Settings DHCP Settings Balance VLAN Setup	J	Messages List	Target IP Subnet Mask Gateway	IP EX: 30020020000 255.255.255.0 Enter Subnet Mask Info 192.168.0.1 Enter Gateway Info	•	va			前 Delete Selected

3.9 Directed Route

Directed route means setting a fixed network flow direction and pointing data from one port to another fixed port instead of wide area.

1. Click on "Network- Directed Route" to enter the Directional Routing Settings page, click the "+Add" button, enter the start IP, end IP and destination line name, click Save.Set the start IP to end IP data. The flow direction is specified to wan1 and does not pass through other wan ports.







X	onTel								Ф
۹		HOME PAGE > NETWORK >	Directed Route Settings			×			
Ċ	State	Messages List	Start IP				Number per Page (10)	• 🔂 Add	Delete Selected
G	Network 4	Select All No.		IP Ex: x000000000000			Com	ments	Edit
	Intertface Setting		End IP						
	WAN Settings			IP EX: XXX.XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX		_			
	LAN Settings		Line Name	WAN1	•				
	DHCP Settings		Comments						
	Balance			Maximum 32 characters		_			
	VLAN Setup					ave			
	DNS Settings					ave			
	Static Route								
	Directed Route								
	Timing Redial								

3.9 Timing Redial

Auto Redial: Set a specific time or a specific interval to allow automatic redialing of a WAN line which is DHCP Client or PPPoE.

1. Click "Network - Timing Redial" to enter the Timing Redial page

	HOME PAGE > NETWORK	C > TIMING RE	DIAL				
State	Messages List						
Network o	Name	\$	Auto Redial	0	Interval Redial	\$ Timed Redial Settings	÷ Edit
Intertface Setting	WAN2		OFF		OFF		
WAN Settings							< 1
LAN Settings							
DHCP Settings 0							
Balance							
VLAN Setup							
DNS Settings							
Static Route							
Directed Route							

2. Click on the Edit button of one of the lines to pop up the operation box, enable the auto redial status, check the date, and click save after completing the time. As shown in the photo below, the WAN2 line automatically redials at 15:00hours every day.







KonTel					i -	Q
۹	HOME PAGE > NETWORK >	Timing Redial		×		
🕏 State	Messages List	Name	WAN2			
🖾 Network 🗢	Name	Name			Timed Redial Settings	≎ Edit
Intertface Setting	WAN2	Auto Redial				
WAN Settings		ALL MOI THU FR		ED V		< 1 >
LAN Settings						
DHCP Settings 0		Redial Time	15:00 ex.: 00:00	0		
Balance			· · · · · · · · · · · · · · · · · · ·			
VLAN Setup		Interval Redial	046			
DNS Settings Static Route		Interval		l.		
Directed Route			Interval(unit:m)			
Timing Redial				save		
KonTel						ల
Q	HOME PAGE > NETWORK >	TIMING REDIAL				
🕏 State	Messages List					
🕰 Network 🗢	Name	Auto Redial	Interval Redi	al ÷	Timed Redial Settings	≎ Edit
Intertface Setting	WAN2	ON	OFF		(Everyday)15:00Redial	
WAN Settings						< 1 >
LAN Settings						
DHCP Settings						
Balance VLAN Setup						
DNS Settings						
Static Route						
Directed Route						
Timing Redial						

3. To perform Interval Redial, Click on Edit button and Turn On Interval Redial, enter the interval restart time, click Save as shown below.After this setting WAN2 line will re-dial every 480 minutes (Every 8 Hours).

X	onTel					-		
Q		HOME PAGE > NETWORK >	Timing Redial			×		
¢	State	Messages List	Name	WAN2				
G	Network ©	Name	Auto Redial	OFF			Timed Redial Settings	≑ Edit
	Intertface Setting	WAN2	Interval Redial	ON ()			(Everyday)15:00Redial	
	WAN Settings							< 1 >
	DHCP Settings 0		Interval	480 Interval(unit:m)	0			
	Balance							
	VLAN Setup					save		
	DNS Settings							
	Static Route							
	Directed Route							
	Timing Redial							





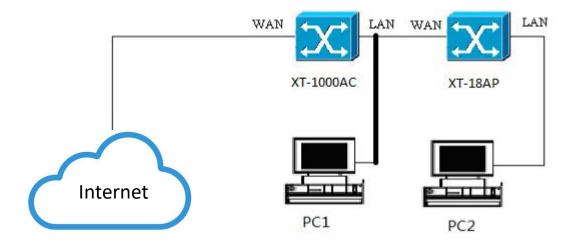


onTel								
	HOME PAGE > NETWORK	C > TIMING F	REDIAL					
b State	Messages List							
Network 🗢	Name	\$	Auto Redial	÷	Interval Redial	¢	Timed Redial Settings	\$ Edit
Intertface Setting	WAN2		OFF		480 min			
WAN Settings								1 >
LAN Settings								
DHCP Settings 0								
Balance								
VLAN Setup								
DNS Settings								
Static Route								
Directed Route								

4 AC Control

Cascading AC Mode

In Cascading AC mode, the Access Points(XT-18AP) connect with the XT-1000's internal network, and the connection way is XT-1000's LAN port connect with Access Point's WAN port as shown below:



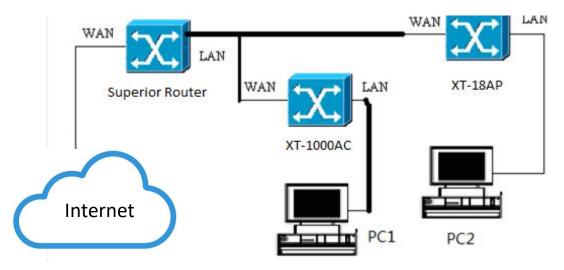






By-Pass AC Mode

In By-Pass AC Mode Access Points(XT-18AP) and XT-1000AC connects with the same network. The connection way is the Superior Router's LAN port connects with the WAN port of XT-1000AC and XT-18AP. After the XT-1000AC and Xt-18AP consult successfully, you can visit XT-1000AC management page through XT-1000AC's WAN port IP.



4.1 Group

Here you can use the default group (For Mass APs Config) or create a new group, can setup 2.4GHz and 5.8GHz SSID, wireless advanced parameters.

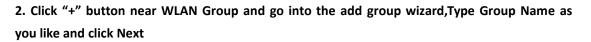
1. Open the XT-1000AC's home page,go into AC Control's "Group" page,as below:

		HOME PAGE > AC >	GROUP				
State				0 0 /			
Network	0	WLAN Group D	efault Group		2.4GHz 5.8GHz	Advanced	
AC	۲	2.4GHz WiFi					
AC Control		Client Network					
Group							
Members				Wireless			
Upgrade				Hide SSID	OFF		
Details				Hue 2210			
Authentication	0		Name/5	SID End	cryption Password	/Key VLAN	
Traffic Control	0		XonTel	WPA2-PS	sK vontel123	Disable	• 🕀
Firewall	0						
Service	Ø	Admin Network					
Log and Statis	ics Ø	Advanced					

21 | Page







Kon	Tel				٥
Q			HOME PAGE >	Add Group ×	
🕏 State	e		WLAN Group	Group Name 2.4GHz 3 5.8GHz Next	
📽 Netv	work	ø	WEAK GLOUP		
AC		۲	2.4GHz W	Group Name XonTel	
	Control	-	Client Ne	Group Name	-
Grou Men	nbers				
Upg	grade				
Deta	ais			Hide SSID	

3. Setup 2.4GHz relative parameter(SSID/Encryption Type/Password), click Next:

KonTel		
۹	HOME PAGE >	Add Group
🕏 State		Group Name 2.4GHz 5.8GHz Back Next
C Network O	WLAN Group	SSID XonTel
◎ AC	2.4GHz W	
AC Control	Client Ne	Encryption WPA2-PSK •
Group		
Members		Password 12345678 Password 8-32 Characters
Upgrade		Password ev-sz. Unalaciels
Details		
Authentication O		Name/SSID Encryption Password/Key VLAN
Traffic Control 0		XonTel WPA2-PSK • xontel123 Disable •

4. Setup 5.8GHz relative parameter(SSID/Encryption Type/Password)

KonTel			
Q	A HOME PAGE >	Add Group X	
🕏 State		Group Name 2.4GHz 5.8GHz Back Apply	
C Network O	WLAN Group	SSID XonTeEGHz	
⊙ AC ⊙	2.4GHz W	SID	
AC Control	Client Ne	Encryption WPA2-PSK •	-
Group			
Members		Password 12345678 Password 8-32 Characters	
Upgrade		r bornen oʻdu, sinindikora	
Details			
Authentication •		Name/SSID Encryption Password/Key VLAN	
Traffic Control		XonTel WPA2-PSK 🔹 xonteli23 Disable 🔹 🕂	

5. Click "Apply" and it will go to "GROUP" page. Choose the group name which you set in wizard and you can view detail setup of that group.

1: Client Network: You can setup the NAME/SSID and PASSWORD/KEY for End Users.







K	onTel							
۹			HOME PAGE > AC > GROUP					
6) 6	State Network	0	WLAN Group XonTel		/	2.4GHz 5.8GHz Adv	vanced	
0	AC	0	2.4GHz WiFi					
	AC Control		Client Network					
	Group							
	Members Upgrade				Wireless	ON O		
	Details				Hide SSID	OFF		
.	Authentication	0		Name/SSID	Encryption	Password/Key	VLAN	
0	Traffic Control	0		XonTel	WPA2-PSK	• 12345678	Disable	• 🕀
BÅ I	Firewall	0	Admin Network		_	_	_	_
6	Service	Ø	Advanced					
	Log and Statistic	so	Auvanceu			_		
8	System Tools	Ø			Apply	Reset		

2: Admin Network: You can setup the NAME/SSID and PASSWORD/KEY for Admin Network.

onTel		
ι.	HOME PAGE > AC > GROUP	
b State	WLAN Group XonTel	2.4GHz 5.8GHz Advanced
Network O		
AC O	2.4GHz WIFI	
AC Control	Client Network	+
Group	Admin Network	-
Members		
Upgrade	Wireless	OFF
Details		
Authentication ©	Hide Admin SSID	
Traffic Control	Name/SSID	XonTel_ADMIN_2G
Firewall O		Name/SSID
Service Ø	Encryption	WPA2-PSK •
Log and Statistics	Password/Key	12345678
System Tools 🛛 💿		8~32 Characters
	Advanced	+

3: Advanced-Here you can setup Country, Channel, Transmit Power etc. relative parameters.





0	AC	•	2.4GHz WIFI
	AC Control	_	Client Network +
	Group		Admin Network +
	Members		
	Upgrade		Advanced –
	Details		Country: Europe •
	Authentication	0	Channel auto
0	Traffic Control	0	Claime aud
EA	Firewall	ø	Transmt Power 100%
•	Service	0	Bandwidth 20MHz -
	Log and Statisti	cs©	Rekey 86400
然	System Tools	0	Units(600-604800) 0 to shut down
			Max WFI Connections 256
			Nax WHI Connectors 1~256
			Shortgi:
			Apply Reset

6. Inside Client Network click "+" sign to add multiple SSID. You can add extra 7 SSID both in 2.4GHz and 5.8GHz.

2.4G Multiple -SSID:

ent Network					
		Wireless			
		Hide SSID	OFF		
	Name/SSID	Encryption	Password/Key	VLAN	
	XonTel	WPA2-PSK	▼ xontel123	Disable	• 🕀
	2	WPA2-PSK	• 123123123	Disable	• 🖯
	3	NONE	•	Disable	• 😑
	4	NONE	•	Disable	• 😑
	5	NONE	•	Disable	• 😑
	6	NONE	•	Disable	• 😑
	7	NONE	-	Disable	• 🖯



زونتل





5.8GHz Multiple -SSID:

.8GHz WiFi					
Client Network					
		Wireless	OFF		
		Hide SSID	OFF		
	Name/SSID	Encryption	Password/Key	VLAN	
	XonTel5G	WPA2-PSK	xontel123	Disable	• 🛨
	2	WPA2-PSK		Disable	• 😑
	3	NONE		Disable	• 😑
	4	NONE		Disable	• 😑
	5	NONE		Disable	• 😑
	6	NONE		Disable	• 😑
	7	NONE		Disable	• 🖯

7. Click Advanced on top of the page, Advance WIFI Settings will open. Here you can Enable/Disable Wireless User Isolation to isolate wireless users. Also can setup Timed Restart or Interval Restart of the Access Points in that group.

WLAN Group	Default Group	• 🖸 🗖 🖌	2.4GHz 5.8GHz Advanced
Advanced			
Advanced Wil	Fi Settings		-
		Isolate	017
		RTS:	
		Beacon:	Untcbyte(0-2347) 100
			Unitms(15~65535)
		DTIM	2 Units(1~255)
WiFi Roaming) Settings	_	+
Timed Restar	t		+

4.2 Members

If there multiple Access Points connect with XT-1000AC network, the managed device information will be shown on the Performance page. Click Managementand here you can modify the corresponding device's wireless SSID, country, channel, transmitted power, wireless bandwidth, max-awaiting amount and alias.







1. Open WEB home page and go into AC Control's "Members" page, as below:

۹			HOME PAG	E > AC > MEMBERS									
Đ	State						erformance Managem	ant		Disable au	to flush 🔹 🕫	Number per Pag	je (10)
C	Network	Θ					enormance managen	ient.		Disable au		Number per Pag	Je (10)
0	AC	0	No. *	MAC	IP Address	Client	Up/Down	SSID VLAN	Uptime	Status 🗘	Current Group	AP Location	State
	AC Control		1	D4:67:61:18:04:EC	192.168.1.5	25/0/25	21 GB/122 GB	Support	21d12h	Online	Default Group	Corridor_IN	۲ <mark>۵</mark> :
	Group		2	40:A5:EF:B2:E9:80	172.16.0.106	1/0/1	0 B/64 B	Support	37s	Offline	XonTel	Corridor_Out	:Q:
	Members												1 2
	Upgrade												
	Details												
ų	Authentication	Θ											
3	Traffic Control	0											
ah.	Firewall	0											

2. Click on above picture's "Management" button and go into the managing page, as below:

X	onTel																¢
Q			HOME PAGE	> A	C > MEMBERS												
₿	State							0-6					Disable a		- 0	Number on Deer	(10)
C.	Network	0						Perio	rmance Ma	anagement			DisdDie d	uto nusn		Number per Page	• (10)
۲	AC	•						Default	Group	Move Group					Turn of	f LED light 👻	Reboot
	AC Control		Select All	No.	MAC	0 2	2.4GHz SSID®	5.8GHz SSID	Capability	Transmit Power	Channel	Device 🖗	SW Version	Status	Current Group	AP Location ©	Edit
	Group		B	1	D4:67:61:18:04:E	С	XonTel	XonTel5G	256/256	50%/100%	auto/auto	XT-18AP	V1.0	Online	Default Group	Corridor_IN	28
	Members			2	40:A5:EF:B2:E9:8	D	XonTel	XonTel5G	255/256	50%/100%	6/auto	XT-18AP	V1.0	Offline	XonTel	Corridor_Out	2 💼
	Upgrade															<	1 >
	Details																
	Authentication	0															
Ø	Traffic Control	Ø															
EA	Firewall	0															
œ	Service	0															

3. Click below picture's "Edit"button so you can reconfigure the device's SSID,Country,Channel and TX Power etc.details as below:

2	onTel									-				Ċ
Q			HOME PAGE	> A	.C > MEMBE	Single Device Setting			×					
Ċ	State						2.4GHz 5.8GH	tz Advanced		Disable	auto flush	• 0	Number per Pag	
C	Network	0				2.4GHz WiFi				Disdule	auto nusri		Number per Pag	e (10)
0	AC	•					_	_				Turn o	ff LED light 👻	Reboot
	AC Control		Select All	No.	MAC	Client Network			-	Version	Status	Current Group	AP Location	Edit
	Group			1	D4:67:61:18:		Wireless	ON O		V1.0	Online	Default Group	Corridor_IN	
	Members			2	40:A5:EF:B2:			_		V1.0	Offine	XonTel	Corridor_Out	
	Upgrade						Hide SSID	OFF						1 2
	Details					Name/SSID	Encryption	Password/Key	VLAN					
8	Authentication	0				XonTel	WPA2-PSK	xontel123	Disable 🔸 🛨					
0	Troffic Control	0												

4. Click Admin Network







X	onTel			· · · · · · · · · · · · · · · · · · ·						
Q			HOME PAGE > AC > MEME	Single Device Setting	×					
Ē	State			2.4GHz	5.8GHz Advanced					
G	Network	0		2.4GHz WiFi		Disable	e auto flush		Number per Page	
0	AC	0		Client Network	+			Turn of	f LED light 👻	Reboot
	AC Control		Select All No. ⁴ MA			N Versior	Status	Current Group	AP Location	Edit
	Group		🗐 1 D4:67:61:1	Admin Network ٤	-	V1.0	Online	Default Group	Corridor_IN	
	Members		🖾 2 40:A5:EF:E	2 Wireless	OFF	V1.0	Offine	XonTel	Corridor_Out	
	Upgrade								<	1 >
	Details			Hide Admin SSID						
	Authentication	0		Name/SSID	XonTel_ADMIN_2G					
Ø	Traffic Control	0			Name/SSID					
ЕŅ	Firewall	0		Encryption	WPA2-PSK					
6	Service	0		Password/Key	12345678					
	Log and Statistic	s0			8~32 Characters					

5.Click Advanced:

X	onTel		ტ
Q		Single Device Setting	*
Ø	State	2.4GHz 5.8GHz Advanced	
G	Network O		Disable auto flush
0	AC o	2.4GHz WiFi	Turn off LED light 👻 Reboot
	AC Control	Select All No.* MAC	V Version⊕ Status⊕ Current Group⊕ AP Location⊕ Edit
	Group	1 D4:67:61:12	V1.0 Online Default Group Corridor_IN 🖉 📴
	Members	Advanced –	V1.0 Offine XonTel Corridor_Out 🖉 🗐
	Upgrade	Country: Europe	
	Detais	Channel auto 🗸	
	Authentication O	Channel auto 💌	
Ø	Traffic Control 0	Transmit Power 50%	
ШŅ	Firewall O	Bandwidth 40MHz •	
G	Service 0	Max WFI Connections 256	
	Log and Statistics®	Max WIFI Connections 1~256	
X	System Tools 🛛 🛛 🛛 🛛 🛛 🔍	Shortgi:	

6. Move a device to different group: Select the devices you want to move to different group and choose the group name(XonTel)from the drop-down menu near "Move Group" button and then click on Move Group.

	onTel																
۹			HOME PAGE	> A	C > MEMBERS												
B	State																
2	Network	Ø						Perfor	mance M	lanagement			Disable a	auto flush	• 0	Number per Pag	e (10)
0	AC	0						XonTel	-	Move Group					Turn of	f LED light 👻	Reboot
	AC Control		Select All	No.	MAC	2.4GHz SSID	5.8GF	Default G XonTel	roup	Transmit Power	Channel	Device 🗘	SW Version	Status	Current Group	AP Location	Edit
	Group		8	1	D4:67:61:18:04:EC	XonTel	Xon	Tel5G	256/256	50%/100%	auto/auto	XT-18AP	V1.0	Online	Default Group	Corridor_IN	1
	Members			2	40:A5:EF:B2:E9:80	XonTel	Xon	Tel5G	255/256	50%/100%	6/auto	XT-18AP	V1.0	Offline	XonTel	Corridor_Out	28
	Upgrade																1 >
	Details																
	Authentication	0															

7. Click the LED light control button to turn off the LED light of the Access Points. Click again to open the LED light of the Access Points.









X	onTel															e
Q			HOME PAGE	> A	C > MEMBERS											
勴	State						Perfo	rmance Ma	nagement			Dicable :	auto flush	• 0	Number per Pag	e (10) 🔻
C	Network	0					, reno	manec ne	indgemene			Disciple c	10100 110311		number per rag	
0	AC	•					Default	Group	Move Group					Turn o	off LED light 👻	Reboot
	AC Control		Select All	No.	MAC	2.4GHz SSID	5.8GHz SSID	Capability	Transmit Power	Channel	Device 🗘	SW Version	Status	Turn	on the LED light	Edit
	Group			1	D4:67:61:18:04:EC	XonTel	XonTel5G	256/256	50%/100%	auto/auto	XT-18AP	V1.0	Online	Default Group	Corridor_IN	2 📋
	Members		8	2	40:A5:EF:B2:E9:80	XonTel	Comfast5G	255/256	50%/100%	6/auto	XT-18AP	V1.0	Offline	XonTel	Corridor_Out	
	Upgrade															1 >
	Details															
	Authentication	0														

4.3 Upgrade

Upgrade option can upgrade all Access Points at same time. You have to upload a firmware file and select the devices you upgrade.

1. Open XT-1000AC's Upgrade page, as below:

X	onTel														
۹			HOME PAGE > AC	> UPGRADE											
Đ	State		Upload												
¢,	Network	0					Status :		Firmware is not uploade	d					
0	AC	•													
	AC Control						Select		Browse No file sele	cted.					
	Group						Upk	ad		Cancel					
	Members														
	Upgrade		Upgrade									Number per	Page (10)	🔹 🔅 Upgr	rade
	Details											number per			
-1	Authentication	Θ	Cancel All	No. 🗘	Device	÷	SW Version	÷	MAC	\$	SSID	\$ Group	4	AP Location	
Ð	Traffic Control	Ø	12	1	XT-18AP		V1.0		D4:67:61:18:04:EC		XonTel5G	Default Group		Corridor_IN	
	Firewall	0												< 1	×

2. Click above picture's "Browse" button, choose the newest firmware which you want to upgrade for the Access Points, click "Upload" button "Firmware has been uploaded", as below:

KonTel	ڻ ف
۹	HOME PAGE > AC > UPGRADE
🕏 State	Upload
Network	Status : Firmware has been uploaded
 AC AC Control 	firmware name : XT-184P VL0.bn
Group	Select Browse No file selected.
Members	Upbad Cancel
Upgrade	
Details	
Authentication O	Upgrade Number per Page (10) 🔻 🗘 Upgrade
C Traffic Control O	Select All No.
👪 Firewall 🛛 🛛	1 XT-18AP V1.0 D4:67:61:18:04:EC XonTeBG Default Group Corridor_JN
Service O	

4. Choose the AP devices which you want to upgrade, click the "Upgrade" button on the right, then the devices are on upgrading.









X	onTel														Q
Q			HOME PAGE > AC	> UPGRADE											
₿	State		Upload												
¢.	Network	0				Status :		Firmware has been uplo	aded						
0	AC	۰													
	AC Control					firmware name		XT-18AP V1.0.bin							
	Group					Select		Browse No file sele	cted.						
	Members					Upk	oad		ancel						
	Upgrade									_					
	Details														
-	Authentication	0	Upgrade									Number per	Page (10)	🔹 🔅 Upgr	ade
Ø	Traffic Control	0	Cancel All	No. 🗘	Device	\$ SW Version	\$	MAC	÷	SSID	*	Group	٢	AP Location	0
EA	Firewall	0	122	1	XT-18AP	V1.0		D4:67:61:18:04:EC		XonTel5G		Default Group		Corridor_IN	
G	Service	Θ												~ 1	

4.4 Details

This function displays all terminal entries under XT-1000AC, including Access Points and wireless terminals connected to Access Points.

1. Login, enter the menu, AC Control-> Details.

KonTel									
۹		HOME PAGE >	AC > DETAILS						
🕏 State		Details							
C Network	0	No.	MAC	IP Address	Client	Uptime	Device	SW Version	Current Group
⊚ AC	•	1	D4:67:61:18:04:EC	192.168.1.5	29/0/29	22d7h	XT-18AP	V1.0	Default Group
AC Control									
Group									
Members									
Upgrade									
Details									
Authentication	0								
Traffic Control	0								

2. Click on the AP entry, the details of the wireless terminals connected to the AP is displayed below







C	Network	0	No.	MAC	IP Address	Client	Uptime	Device	SW Version	Current Group
0	AC	•	1	D4:67:61:18:04:EC	192.168.1.5	23/0/23	22d8h	XT-18AP	V1.0	Default Group
	AC Control		Terminal IP	Terminal MAC	SSID	type	Signal(dBm)	Link time	Total Tx	Total Rx
	Group		192.168.1.72	D4:67	XonTel	2G	-46	4h39m	755 KB	429 KB
			192.168.1.18	D4:67	XonTel	2G	-44	2h32m	1 MB	888 KB
	Members		192.168.1.95	C8:3D	XonTel	2G	-42	2h	13 MB	30 MB
	Upgrade	_	192.168.1.40	C0:B6	XonTel	2G	-47	1h53m	4 MB	9 MB
	Details		192.168.1.24	34:2E	XonTel	2G	-50	1h32m	537 KB	939 KB
	Authentication	0	192.168.1.30	D8:C4	XonTel	2G	-52	1h30m	587 KB	957 KB
~	-		192.168.1.63	40:B8	XonTel	2G	-52	1h24m	6 MB	47 MB
Ø	Traffic Control	0	192.168.1.33	D4:67	XonTel	2G	-50	59m56s	114 KB	67 KB
EÅ	Firewall	0	192.168.1.3	D4:67	XonTel	2G	-33	58m14s	528 KB	324 KB
G	Service	Θ	192.168.1.94	7C:67	XonTel	2G	-59	56m29s	4 MB	12 MB
FD			192.168.1.93	90:32	XonTel	2G	-51	40m23s	1 MB	2 MB
	Log and Statistic	SO	192.168.1.8	04:D3	XonTel	2G	-50	27m1s	898 KB	988 KB
<u> </u>	System Tools	Θ	192.168.1.42	4C:74	XonTel	2G	-58	19m31s	2 MB	2 MB
			192.168.1.36	0C:9D	XonTel	2G	-55	15m44s	323 KB	686 KB
			192.168.1.10	D4:67	XonTel	2G	-60	1m43s	20 KB	17 KB
			192.168.1.16	4C:3B	XonTel	2G	-32	14m23s	225 KB	27 KB
			192.168.1.59	D4:67	XonTel	2G	-32	13m50s	25 KB	34 KB

5 Authentication

5.1 Local Auth.

5.1.1 OneKey Authentication

Onekey Authentication to authenticate online by clicking on the authentication button on the page

1. Login XT-1000AC and go into the home page,"Network "-->"Interface Setting".

		HOME PAG	e > Network	<pre>x > INTERTFAC</pre>	E SETTING						
b State		Extra Inf	terface			Local Inter	face			Free Interfac	e
Network	۰	No.	Designate	Interface	Action	No.	Designate	Interface	Action	No.	Interface
Intertface Setti	ng	1	WAN1	eth0.1	8	1	LAN1	eth0.5 eth0.3 eth0.4 eth0.2	22		
WAN Settings LAN Settings DHCP Settings	Ð	1 inform	nation After interfa	ice assign, please go	to < LAN Settings	> or < WAN Setting	s > to add detail con	figuration.			
UTICP Setungs		6									
Balance		-									

2. In the Local Interface, click "Edit" button, uncheck the eth0.2 from the LAN1 Interface Settings page, then the eth0.2 port will be freed, later click "Save".







XonTel		LAN1 Interface	Settings	×	ტ
۹	HOME PAGE > NETWORK >		Settings		
🕏 State	Extra Interface	Select All	physical interface	Status	Free Interface
C Network o	No. Designate	Cr	eth0.5	Occupy	Action No. Interface
Intertface Setting	1 WAN1	V	eth0.3	Occupy	
WAN Settings			eth0.4	Occupy	
LAN Settings		10	eth0.2	Occupy	
DHCP Settings	() information After interface as	s		save	
Balance					
VLAN Setup					

3.Add a New Local Interface: Click "Add" in the local interface, and select the port you need to allocate to Interface LAN2 then click save.

	HOME	PAGE > NETWORK	Add Local Interf	aceLANZ	· · · · · · · · · · · · · · · · · · ·	<		
b State	Extra	Interface	Cancel All	physical interface	Status	O Add	Free Interfac	e
Network	No.	Designate	II III	eth0.2	Free	Action	No.	Interface
Intertface Setting WAN Settings	1	WAN1			save	28	1	eth0.2
LAN Settings DHCP Settings	• 0 in	formation After interfa	ice assign, please go to < LAN S	Settings > or < WAN Settings > to add detai co	nfiguration.			

4.Go into Network--Local Network to setup LAN2's local address.

KonTel		Q
۹	HOME PAGE > NETWORK > LAN SETTINGS	
💩 State	LAN1 LAN2	
🕼 Network 🔹		
Intertface Setting	MAC 40:A5:EF:E2:97:43	
WAN Settings	Static	
LAN Settings	IP Address 192.168.2.1.	
DHCP Settings 0		
Balance	Subnet Mask 255.255.255.0 -	
VLAN Setup	Enter Subnet Mask Info	
DNS Settings	Alow access Close •	
Static Route	Save Cancel	
Directed Route		

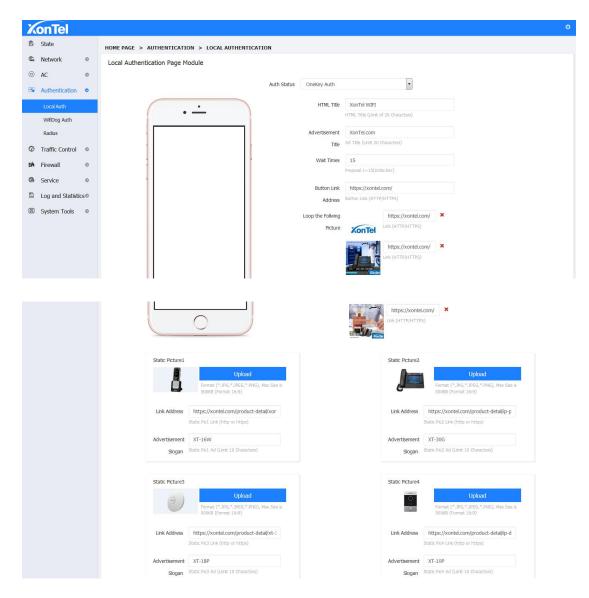
5. Click "Authentication Settings - Local Authentication" and select "Onekey Auth" from the authentication status.

X	onTel			<u>ە</u>
ß	State		HOME PAGE > AUTHENTICATION > LOCAL AUTHENTICATION	
G.	Network	0	Local Authentication Page Module	
0	AC	0		
	Authentication		Auth Status	OneKey Auth
	Authentication	•		Disabled
				OneKey Auth
			• —	WeChat Auth
	WifiDog Auth			Traffic Auth
	Radius			User Auth
				Password Auth
0	Traffic Control	0		





6. After you choose the Authentication type as One Key Auth, you can upload the ad image and fill in the link address(the link address need to fill in the full network address, such as https://xontel.com/).



7. Go to "Bind local interface" below the and select the newly created LAN2 to bind with Authentication and then Save.



زونت





Bind local interface	LAN2
Authentication time	720 Mnute(1~1080)
MAC WhiteIst	Judd MAC address does not require authentication, multiple MAC addresses with a comma "," plasse do not enter the space particlo., for example, 00:E0:6F:29:46:46;00:E0:6F:29:46:47
	Save

8. After finishing setup, clients connected with LAN2 Port(Direct with LAN2 or through Access Point connected on LAN2) when open any website in browser local portal page will appear and click for "Internet Access" button , wait for 10 seconds, and system will allow access for internet.



5.1.2 WeChat Authentication

WeChat Authentication is authenticating through WeChat function.

1. Please refer to 5.1.1 1-4 steps to complete the follow-up operation, choose WeChat Authentication and go to WeChat authentication page, setup HTML title, ad title and static pic, then click save button.

State	HOME PAGE > AUTHENTICATION > LOCAL AUTHENTICATION		
Network 0	Local Authentication Page Module		
⊙ AC ⊘			
	Auth Status	WeChat Auth	
Authentication		Disabled	
Local Auth	•	OneKey Auth	
	•	WeChat Auth	
WifiDog Auth		Traffic Auth	
Radius		User Auth	
		Password Auth	
Traffic Control		Password Audi	



33 | Page



2. Setup relative parameters, choose LAN2(It has already been set at local portal), then click save button, as below:

3. Once the setting is complete, use router's WAN port to connect with LAN2 of AC, setup obtain an IP address automatically, connect the router's WiFi by cellphone, after connection, open the browser and click any website then it will popping the WeChat Authentication page, as below:

Bind local interface	LAN2
Shop_id	
Appid	
Secretkey	
Authentication time	720
	Minute(1~10080)
MAC Whitelst	Add MAC address does not require authentication, multiple MAC addresses with a comma "," please do not enter the space partition, for example, 00:E0:6Fi:29:46:46;00:E0:6Fi:29:46:47
_	Save Cancel
	Cancei

4.Click "A Key to open the WeChat connect with Wi-Fi" on the screen, then it will go into WeChat connecting Wi-Fi page.

5.Click on "Connect immediately"button, then it will show connecting Wi-Fi successfully and WeChat Authentication is finished, and the cellphone can surf the Internet normally. All devices which connect through LAN2(such as the example's configuration is the physical port eth0.2) need to authenticate then only access the Internet.

5.1.3 Traffic Authentication

Traffic Authentication: Restrict user re-authentication by restricting traffic

1. Please refer to **5.1.1 1-4** steps to complete the follow-up operation, choose Traffic Authentication and go to traffic authentication page, setup HTML title, ad title and static pic, then click save button.







X	onTel			Ċ
B	State		HOME PAGE > AUTHENTICATION > LOCAL AUTHENTICATION	
¢.	Network	0	Local Authentication Page Module	
0	AC	0		
	Authentication	•	Auth Status	Traffic Auth
	and a second			Disabled OneKey Auth
	Local Auth		-	WeChat Auth
	WifiDog Auth			Traffic Auth
	Radius			User Auth
~				Password Auth
Ø	Traffic Control	Ø		Mark Theorem 19

2. Setup relative parameters, choose LAN2(It has already been set at local portal), fill in the restricted traffic (e.g.: 1024), then click save button, as below:

Bind local interface	LAN2	·
Limitation of delivery	1024	0
	Unit:MB	
Authentication time	720	
	Minute(1~10080)	
MAC WhiteIst	Add MAC address does not require authentication, multiple MAC addresses with a comma ";"please do not enter the space partition, for example, 00:E0:6F:29:46:46;00:E0:6F:29:46:47	
	Save	

3. Once the setting is complete, after connection thought Interface LAN2, open the browser and click any website then it will pop up the traffic authentication page, after the authentication Internet can be accessed. When the user uses more than 1024M of traffic, it will re-jump to the authentication page to re-authenticate.

5.1.4 User Authentication

User Authentication: Authentication by account and password

1. Please refer to **5.1.1 1-4** steps to complete the follow-up operation, choose User Authentication and go to user authentication page, setup HTML title, ad title and static pic, then click save button.

X	onTel				Q
₿	State		HOME PAGE > AUTHENTICATION > LOCAL AUTHENTICATION		
¢.	Network	0	Local Authentication Page Module		
0	AC	0			
-	Authentication		Auth Status	OneKey Auth	
C36	Authentication	0		Disabled	
	Local Auth			OneKey Auth	
			• —	WeChat Auth	
	WifiDog Auth			Traffic Auth	
	Radius			User Auth	
				Password Auth	
0	Traffic Control	0			

2. Bind local interface LAN2 port (LAN2 has already been set at local portal), set the authentication duration, and then click the save button, as below:



35 | Page

KonTel



Firewall Service Log and Statisti System Tools	admin	Button Link Address Loop the Folwing Picture	Ntps://xonte.com/ Button Link (HTTP:/HTTPS) X X X X X X X X X X X X X
	Bind local inte	erface LAN2	•
	Authentication	1 time 720 Minute(1~10080)	
	MAC WI	Add MAC address authentication, m comma ";" please partition, for exam	ultiple MAC addresses with a do not enter the space

3. Add authentication user information at the bottom of the page, click the "+Add" button, enter the account username and password in the pop-up input box (e.g: ali/123456), click "Save"

				CADE _ PARTY OF	Provide State		
Add authen	tication info					×	
	Username	ali					
	Password	1234	56				
					Ĩ	save	
-	MAC WI	nitelist	authenticat	ddress does not n ion, multiple MAC please do not enl	addresses wit	th a	1
Messages List			Number p	ver Page (10) 🔹 🕂 Add	Delete Selected	圙 Import	前 Export
Select All No.	Username		*	Password		÷	Edit
1	ali			123456			
							< 1 >

4.Once the setting is complete, after connection through LAN2, open the browser and click any website then it will pop up the Authentication page, as below:









5. Enter the correct authentication password (such as: ali/123456), click on the login, automatically jump to the page after successful login, this time the certification is completed, you can normally access the Internet

6. You can import account information in batches by importing files. The file content format is:

username1 passwd1

username2 passwd2



www.xontel.com





The file is encoded as ANSI or UTF-8 and does not support the Unicode format. Save as .txt suffix file. As shown below:

·*
*
н. 4

Click the Import File button and select the file account.txt.

Import		×
	Select Browse account.txt	
		Upload

You can see that the user name and password were imported successfully, and the previously added account configuration will be overwritten, so before you import, you can export the previously added accounts in advance.

lessages Lis	st		Number	r per Page (10) 🔹 🕒 Add 🛍 Delete Selec	ted 🗎 Import	j Expor
Select All	No. \$	Username	\$	Password	≑ Ed	lit
	1	username1		passwd1	2	Û
	2	al		123456		1
	3	fouad		654321		Û
					<	1 >

Click Export File to export the current account information to the account.txt file.





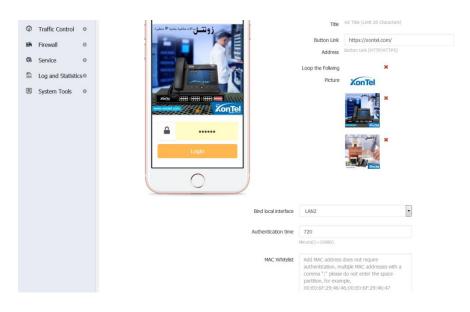


5.1.4 Password Authentication

1. Please refer to **5.1.1 1-4** steps to complete the follow-up operation, choose Password Authentication and go to password authentication page, setup HTML title, ad title and static pic.

X	onTel				ወ
₿	State		HOME PAGE > AUTHENTICATION > LOCAL AUTHENTICATION		
¢,	Network	0	Local Authentication Page Module		
0	AC	0			
	Authentication	•	Auth Status	User Auth Disabled	
-	Local Auth			OneKey Auth	
	WifiDog Auth		•-	WeChat Auth Traffic Auth	
	Radius		XonTel.com	User Auth	
0	Traffic Control	0	زونتسل دار الد دیما اسلاد معامل	Password Auth	
EA	Firewall	0		Button Link https://xontel.com/	
-				Address Button Link (HTTP/HTTPS)	

2. Bind local interface- Select LAN2 port, set the authentication duration.



3. Add the authentication password at the bottom of the page, click the "+Add" button, enter the authentication password in the pop-up input box (e.g: 123456), click "Save"

Add authentication info		×
Password	123456	
		save









Messages List			Number per Page (10)	前 Delete Selected	圖 Import 圖 Export
Select All	No.	÷	Password	\$	Edit
	1		123456		
					< 1 >

4.Once the setting is complete, after connection through LAN2, open the browser and click any website then it will pop up the Authentication page, as below:



5. Enter the correct password (such as: 123456), click on the login, automatically jump to the page after successful login, this time the authentication is completed, you can normally access the Internet.

6. You can import account information in batches by importing files. The file content format is:

passwd1

passwd2

The file is encoded as ANSI or UTF-8 and does not support the Unicode format. Save as .txt suffix file. As shown below:



40 | Page







Click the Import File button and select the file passwd.txt:

Import		×
	Select Browse passwd.txt	
		Upload

You can see that the passwords were imported successfully, and the previously added account configuration will be overwritten, so before you import, you can export the previous useful account in advance.

essages List		Number per Page (10) 🔽 🗲 Add 🗎 🗎 De	lete Selected 🛛 🛍 Import 🗍 🛍 Expor
Select All	No. ÷	Password	≑ Edit
	1	passwd1	2 🗎
	2	123456	
	3	654321	
			< 1 >

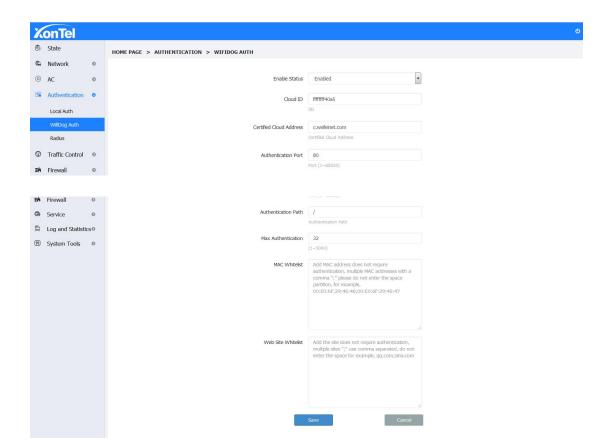
Click Export File to export the current account information to the passwd.txt file.

5.2 WifiDog Auth

1. Go to" Authentication" ---" Wifidog Auth", then choose the status as Enable, setup relative parameters, click save button.







2.Open the browser in the local computer,open the other website which are not in the "Website White list",system will pop up the authentication page.

3.Use device's MAC address to add to white list to open the browser, and system will not pop up the authentication page in any websites.

6 Traffic Control

6.1 QoS

When there are many ISP lines connect to the device, open the traffic switch, setup every ISP line's upstream and downstream bandwidth by the real network situation.

1. Go to QoS page, setup the relative parameters, fill in the actual UP/Down bandwidth according to the bandwidth of each external network, and click save button, as below:



42 | Page





KonTel								
٩	HOME PAGE > TRAFFIC CONTROL > QOS							
🖏 State								
C Network ©			QoS		CIN 🜔			
◎ AC ●	Bandwidth Setting							
B Authentication ©	banawath setung							
Traffic Control			Qos Model B	lance			•	
QoS		Wan line		Up			Down	
IP Limit		WANL	Up	1000	Mbps	Down	1000	Mbps
LocalNet Monitor		WANZ	Up	1000	Mbps	Down	1000	Mbps
HA Firewall 0			1			-	_	
G Service 0			Saw	·		Cance		
Log and Statistics e								
System Tools 0								

2. The line flow control mode can be adjusted according to the actual usage of the clients:

X	onTel											٥
۹			HOME PAGE > TRAFFIC CONTROL > QOS									
ß	State											
6	Network	0			QoS		<u>()</u>					
0	AC	0										
8	Authentication	0	Bandwidth Setting									
0	Traffic Control	•			Qos Model	Surff						
	QoS			Wan line		Balance			own			
	IP Limit					Surff			-			
	LocalNet Monitor			WAN1	U¢	Down or Video			000	Mbps		
				WAN2	Up	Custom 1000	Mbps	Down	1000	Mbps		
зA	Firewall	0										
G	Service	0				Save		Cancel				
۵	Log and Statistic	50										
医	System Tools	0										

6.2 IP Limit

System can control the uplink and downlink traffic of single user according to the IP address.

1. Go into the IP LIMIT page, add a single IP speed limit information, e.g. IP: 192.168.1.30, up and down rate are 256 and 256, then the user's uplink and downlink speed values should be same.

		_	Terminal Speed Limit			×	_			
l III	HOME PAGE > TRAF	FIC CONT								
b State	Messages List		Status	Enabled	•		Number per	Page (10)	🕒 Add 📋 🗊)elete Selecte
🗅 Network 🛛 🔍	Select All	No.			-		ontrol Mode 🗢	Comments	Status 🗢	Edit
AC o		1	IP	192.168.1.25 P or P Range(172.16.0.10-172.16.0.100)			Shared	Waleed	Enabled	
Authentication O		2	Upload Rate(KB/s)	256	0		Shared		Enabled	
Traffic Control		3	upidau kate(KB/S)	236 Ex:100, Limit 100(KB/s)			Shared		Enabled	
QoS IP Limit		4	Download Rate(KB/s)	256	0		Shared		Enabled	
LocalNet Monitor		5		Ex:100, Limit 100(KB/s)			Shared		Enabled	
Firewall O		6	Control Mode	Shared	•		Shared		Enabled	
Service 0		7	Comments				Shared		Enabled	
Log and Statistics®		8		Maximum 32 characters			Shared		Enabled	
System Tools 🛛 🛛 🔍		9				save	Shared		Enabled	
	m	10	192.168.1.25	350	350	_	Shared		Enabled	

2. Speed Limit for Range of IPs: Go to the IP Limit page and add the IP range limit information,





e.g.IP: 192.168.1.11-192.168.1.20, with 128 and 256 upstream and downstream respectively. The exclusive bandwidth is the independent speed limit setting for all users in the network segment. The bandwidth and the shared bandwidth are the bandwidths shared by all users in the network segment. In this case, the user's uplink and downlink rates are consistent with the speed limit values.

X	onTel							_			Q
Q			HOME PAGE > TRAFFIC	CONT	Terminal Speed Limit			×			
₿	State		Messages List		Status	Enabled	1		Number per Page (10)	▼ 🔂 Add 👔 D	elete Selected
C .	Network	0			Status	Liabed					
	AC	Θ	Select All	No.	Ib		0		Control Mode 🚊 Comme		Edit
लिय	Authentication	0		1		IP or IP Range(172.16.0.10-172.16.0.100)			Shared Wale	ed Enabled	
			8	2	Upload Rate(KB/s)	128			Shared	Enabled	
3	Traffic Control	0		3		Ex:100, Limit 100(KB/s)			Shared	Enabled	
	QoS			4	Download Rate(KB/s)	256		- 1	Shared	Enabled	
	IP Limit			5		Ex:100, Limit 100(KB/s)			Shared	Enabled	
	LocalNet Monitor			6	Control Mode	Exclusive			Shared	Enabled	
EA	Firewall	0		0)				
G	Service	Ø	8	7	Comments				Shared	Enabled	
	Log and Statistic	cs O		8		Maximum 32 characters			Shared	Enabled	
8	System Tools	ø	8	9			sav	e	Shared	Enabled	
				10	192.168.0.20-192.168.1.11	128	256		Exclusive	Enabled	
										<	1 2 >

ConTel									
	HOME PAGE > TRA	FFIC CONTROL >	IP LIMIT						
State	Messages List				IP Limit Switch 💿 🕻	Number per Page	e (10) 🔹 🔂	Add 🗎 De	elete Selecter
Network ©	Select All	No. 🗘	IP	Upload Rate(KB/s)	Download Rate(KB/s)	Control Mode ≑	Comments \$	Status 🔅	Edit
AC O		1	192.168.1.54	350	350	Shared	Waleed	Enabled	
Authentication 0	E	2	192.168.1.34	350	350	Shared		Enabled	
Traffic Control	8	3	192.168.1.53	350	350	Shared		Enabled	1
QoS IP Limit		4	192.168.1.55	350	350	Shared		Enabled	 8
LocalNet Monitor	8	5	192.168.1.75	350	350	Shared		Enabled	28
Firewall 0		6	192.168.1.78	350	350	Shared		Enabled	2 💼
Service Ø	E	7	192.168.1.243	350	350	Shared		Enabled	20
Log and Statistics®	E	8	192.168.1.30	350	350	Shared		Enabled	2 💼
System Tools Ø	8	9	192.168.1.45	350	350	Shared		Enabled	20
	12	10	192.168.1.11-192.168.1.20	128	256	Exclusive		Enabled	1

6.3 LocalNet Monitor

Real-time monitoring of each user's uplink and downlink rates and uplink and downlink total traffic, and will automatically update real-time, you can manually add each user to a single IP speed limit list to control a single user speed.

1.Go into LocalNet monitor page, each user corresponding to the uplink and downlink rate and the total flow is of the same line with the actual value.







	onTel									
۹			HOME PAGE	> TRAFFIC CO	ONTROL > LOCALNET MONITOR					
鹍	State		Messages	s List					Number per Page (100)	C Refresh
2	Network	0	No. 🗖	ІР	Upload Rate(KB/s)	Download Rate(KB/s)	Upload Bytes	Download Bytes 🔅	Online Time 💠	Edit
0	AC	0	1	192.168.1.30	8.24 KB	11.56 KB	45.87 MB	68.63 MB	2019-12-09 09:19:31	20
T.	Authentication	0	2	192.168.1.200	5.28 KB	4.63 KB	862.14 MB	501.59 MB	2019-12-02 17:09:10	20
0	Traffic Control	•	3	192.168.1.45	3.28 KB	10.09 KB	347.05 MB	2.51 GB	2019-12-04 09:42:58	20
	QoS		4	192.168.1.232	3.06 KB	729.00 B	1.71 GB	413.25 MB	2019-12-02 17:09:10	20
	IP Limit		5	192.168.1.56	1.93 KB	20.52 KB	14.39 MB	121.50 MB	2019-12-09 09:08:18	20
	LocalNet Monitor		6	192.168.1.27	1.28 KB	16.74 KB	12.78 MB	227.02 MB	2019-12-09 08:32:22	20
	Firewall	0	7	192.168.1.36	1.25 KB	22.92 KB	10.57 MB	176.37 MB	2019-12-09 09:19:55	2 0
8	Service	0	8	192.168.1.95	1.22 KB	3.49 KB	20.23 MB	319.90 MB	2019-12-09 08:57:07	20
	Log and Statistic		9	192.168 <mark>.1</mark> .54	1.14 KB	3.76 KB	11.66 MB	58.55 MB	2019-12-09 09:01:06	20
<u></u>	System Tools	0	10	192.168.1.93	849.00 B	989.00 B	6.74 MB	11.88 MB	2019-12-09 09:22:27	20
			11	192.168.1.52	816.00 B	14.00 KB	189.05 MB	4.86 GB	2019-12-04 08:53:54	20
			12	192.168.1.3	789.00 B	4.08 KB	7.63 MB	25.93 MB	2019-12-09 08:55:21	20
			13	192.168.1.19	705.00 B	2.57 KB	5.09 MB	28.18 MB	2019-12-09 09:00:53	

2. Click on the 'Edit' icon of any user, to setup single IP speed limit of that user:

K	onTel					ć					
Q			HOME PAGE	> TRAFFIC CON	Terminal Speed Limit			×			
₿	State		Messages	s List	Upload Rate(KB/s)	100	•			Number per Page (100)	• C Refresh
C	Network	0	No. 🔺	ID 💠	56 USC 68400	Ex:100, Limit 100(KB/s)			load Bytes 🔅	Online Time	¢ Edit
0	AC	Θ	1	192.168.1.30	Download Rate(KB/s)	100	0		3.63 MB	2019-12-09 09:19:31	
	Authentication	Θ	2	192.168.1.200		Ex:100, Limit 100(KB/s)			1.59 MB	2019-12-02 17:09:10	
0	Traffic Control	0	3	192.168.1.45				save	.51 GB	2019-12-04 09:42:58	
	QoS		4	192.168.1.232	3.06 KB	729.00 B	1.71 GB	41	3.25 MB	2019-12-02 17:09:10	
	IP Limit		5	192.168.1.56	1.93 KB	20.52 KB	14.39 MB	12	1.50 MB	2019-12-09 09:08:18	
	LocalNet Monitor		6	192.168.1.27	1.28 KB	16.74 KB	12.78 MB	22	7.02 MB	2019-12-09 08:32:22	

3. An abnormal traffic user can be added to the black list to prevent the user from accessing the Internet.

ξ			HOME DAG		Terminal Speed Limit			×		
			HOME PAG	E > TRAFFIC CONT						
6			A Warning Are you sure you can add" 0C:9D:92:99:C1:9A to the black list ?				Number per Page (100)	C Refrest		
6	Network	Ø	No. 🔦	Ib 👌				load Bytes	Online Time	≑ Edit
	AC	0	1	192.168.1.30				3.63 MB	2019-12-09 09:19:31	20
9	Authentication	Θ	2	192.168.1.200				save 1.59 MB	2019-12-02 17:09:10	
9	Traffic Control	۲	3	192.168.1.45	3.28 KB	10.09 KB	347.05 MB	2.51 GB	2019-12-04 09:42:58	
	QoS		4	192.168.1.232	3.06 KB	729.00 B	1.71 GB	413.25 MB	2019-12-02 17:09:10	
	IP Limit		5	192.168.1.56	1.93 KB	20.52 KB	14.39 MB	121.50 MB	2019-12-09 09:08:18	
			6	192.168.1.27	1.28 KB	16.74 KB	12.78 MB	227.02 MB	2019-12-09 08:32:22	





7 Firewall

7.1 IP Filter

Here you must know the IP of the computer achieved and the device allocated, and confirm that which computer achieved IP or IP segment need to filter forbid visit network base on the practical situation.

1. Click the home page "Firewall" and go into the IP Filter page, as below:

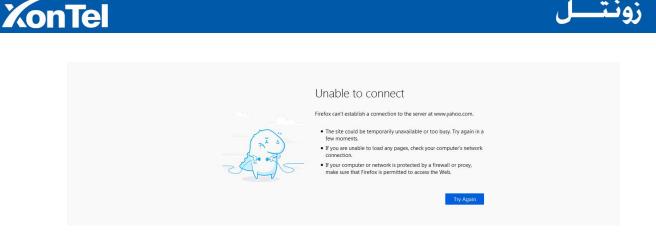
KonTel							
۹	HOME PAGE > FIREWALL	> IP FILTER					
🕏 State		3	Use IP Blackist				
Network O			Use IP Whitelist				
AC Ø							
Authentication Ø	Messages List				Nur	mber per Page (10) 🔹 🕒	Add 🗎 Delete Selecte
Traffic Control	Select All	No.	Protocol	Start IP	End IP	Comments	Edit
Firewall O							
IP Filter							
MAC Filter							
URL Filter							
Port Filter							
Port Mapping							
DMZ Setting							
ARP Binding							
Attack Protection							

2.Click "Add" and go into IP Filter's detail setup page, setting the Black List IP segment range which you need, then click "Save" as below:

X	onTel						-		ው
Q			HOME PAGE > FIREWALL >	Single IP Filtering			×		
Ø	State			Protocol	ALL	•			
¢.	Network	0							
	AC	0		Start IP	192.168.1.11	0			
			Messages List		IP Ex: 3000.0000.0000			Number per Page (10)	dd 🛙 🛍 Delete Selected
	Authentication	0		End IP	192.168.1.50	۲			
Ø	Traffic Control	Θ	Select All		IP Ex: 200.200.200			Comments	Edit
=h	Firewall	0		700 IZ					
				Comments					
	IP Filter				Maximum 32 characters				
	MAC Filter								
	URL Filter						save		
	Port Filter								
	Port Mapping								
	DMZ Setting								
	ARP Binding								

3.Open the native's browser, and it can not open the website normally, because the native IP:192.168.1.11 is in the IP Black List range:





4. Switch to the White list. Only users in the White list can access the Internet. Other users cannot access the Internet. (Use this option with caution)

K	onTel								3
۹			HOME PAGE > FIREWALL >	IP FILTER					
₿	State				Use IP Blacklist				
C .	Network	0		121	Use IP Whitelist				
0	AC	0	Managana						
-	Authentication	0	Messages List				Num	nber per Page (10)	Add 🗍 Delete Selected
0	Traffic Control	0	Select All	No.	Protocol	Start IP	End IP	Comments	Edit
BÅ	Firewall	0							
	IP Filter								
	MAC Filter								
	URL Filter								
	Port Filter								
	Port Mapping								

7.2 MAC Filter

Here you must know the computer LAN card's MAC address, then enter the corresponding computer MAC address to block Internet in MAC Filter.

1. Login the router's WEB page,go into the "MAC Filter" page in Firewall,setup PC's MAC address which you want block and save the setting.

KonTel		(-	°				
۹	HOME PAGE > FIREWALL >	Single MAC Filtering			×					
🕏 State		MAC Address	00:25:64:C6:7E:D0	•						
C Network O			MAC Ex. 100300300300300							
◎ AC ●		Comments	MyPC	۲						
Authentication	Messages List		Maximum 32 characters			Number per Page (10)	d 👔 Delete Selected			
Traffic Control	Select All No.				save	Comments	Edit			
EA Firewall •			_							
IP Filter										
MAC Filter										
URL Fiter										
Port Filter										



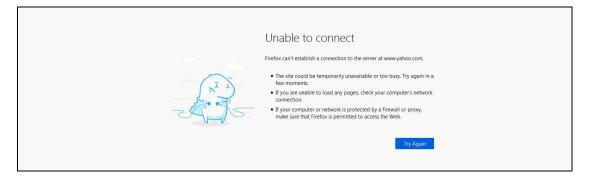
47 | Page





X	onTel									Q
٩			HOME PAGE > FIRE	EWALL > MA	C FILTER					
B	State					Use MAC Blacklist				
6	Network	0				Use MAC Whitelist				
0	AC	0	Manager 11a							
	Authentication	0	Messages List					Number per Page (10)		Delete Selected
0	Traffic Control	0	Select All	No.	\$	MAC Address	÷	Comments	0	Edit
EN	Firewall	•	(m)	1		00:25:64:C6:7E:D0		MyPC		
	IP Filter									< 1 >
	MAC Filter									

2. Open the local browser. The filtered device cannot access the Internet normally.



3. Modify the MAC address whitelist mode. Only devices in the whitelist can access the Internet. Other devices cannot access the Internet. (Use this option with caution)

X	onTel					ወ
۹			HOME PAGE > FIREWALL > MAC FILT	ER		
₿	State			Use MAC Blacklist		
¢.	Network	0		Use MAC Whiteist		
0	AC	0				
-	Authentication	0	Messages List		Number per Page (10) Add	Delete Selected
Ø	Traffic Control	0	Select All No.	MAC Address	Comments	Edit
EŃ	Firewall	۰				
	IP Filter					
	MAC Filter					
	URL Filter					
	Port Filter					
	Port Mapping					

7.3 URL Filtering

Here you can setup the website address to filter which you need, and the saved address(URLs) can not be accessed.

1. Login the router's WEB page,click URL Filter in Firewall and enter "www.youtube.com" in the website filter.







Z	onTel							Q
٩			HOME PAGE > FIR	ewall > u	RL FILTER			
Ċ	State		Messages List			Number per Page (10)	d 🛛 🛍 Delete Sele	ected
C.	Network	0	Select All	No.	•	URL Address	÷ Edit	
0	AC	0		1		www.youtube.com	2 💼	ĺ.
	Authentication	0					< 1	1
C	Traffic Control	0						
EX	Firewall	0						
	IP Filter							
	MAC Filter							
	URL Filter							
	Port Filter							
	Port Mapping							

2.Open browser and try to visit <u>www.youtube.com</u>, the PC cannot access the website, but can visit other websites.

← → ♂ ŵ	0 0 https://www.youtube.com	… ⊠ ☆	± ⊪\	•	® Ξ
	Secure Connection Failed				
	An error occurred during a connection to www.youtube.com. PR_END_OF_FILE_ERROR				
	 The page you are trying to view cannot be shown because the authenticity of the received data could not be verified. 				
	Please contact the website owners to inform them of this problem.				
	Learn more				
	Try Again				

(←) → ℃ 6		🛛 🔒 https://www.skynewsaral	ia.com/search?q=er	nglish&sort=DAT	E					☑ ☆	∓ IIV	▣ :
F 🌲 💿	У 🛛 f								~	17°C ≎ الكويت	مبر 2019	الأحد 29 ديس
Q	بحث في المحتوى				sky news	عربية					الدخول	🕒 تسجيل
ادیو مباشر	م) عاجل 🕼	مزید ب	فيديو ~	برامجنا 🗸	منوعات 🗸	اقتصاد 🗸	علوم 🗸	رياضة 🗸	عالم 🗸	شرق أوسط 🗸	أخبار 🗸	الرئيسية
		حسب القسم	×							english	Q	
		🗵 جميع الأقسام	بخ حسب الصلة	حسب التاري					"englis	لعثور على 3 أخبار "h	تم ال	
	0	🗵 شرق أوسط						منوعات	i.			
	0	🗵 عالم			ہ یتعلمھ <mark>ا</mark>	هارة الجديدة التر	اؤلات ما المو	بورة أثارت التسا بريم		1		
	1	🗵 رياضة					2019	ى لاح؟ السبت 26 أكتوبر (5	A Second		
	0	🗵 اقتصاد									-	
	0	🗵 علوم				ل	تلاحق إسطنبو	ىنوعات ينة "الإنجليزية" i	and the second se			
	2	🗵 منوعات						الثلاثاء 26 يونيو 8	STRANGE .		and the second se	
	0	🗵 برامجنا							and the second diversion of th	The second s		
	0	🗵 راديو سکاي نيوز عربية						ياضة			-	
	_					ية بحق زيدان		كاميرا ترصد ألفا				
		ىحث متقدم					2016	الإثنين 26 سبتمبر	° di			





7.4 Port Filter

XonTel

When in actual use, certain ports need to be filtered, the port filtering module allows some internal services to be used or prohibited by internal users by opening or closing some ports.

1. On home page click on "Firewall-Port Filter" to enter the port filter page, click on the "+ Add" button to pop up into the port filter settings box:

X	onTel									Q
Q			HOME PAGE > FIREWALL	> PORT FILTER						
勴	State		Messages List					Number per Page (10)	• 🔂 Add	Delete Selected
¢.	Network	0		No. Protocol	Source Start Port	Source Send Port	Destination Start Port	Destination Send Port		Edit
0	AC	Ø								
	Authentication									
Ø		Ø								
EM	Firewall	0								
		20								
	IP Filter MAC Filter									
	URL Filter									
	Port Fiter									
	Port Mapping									
	DMZ Setting									
1	onTel			-						ψ
Q			HOME PAGE > FIREWALL	Single Port Filter	ing		×			
	State		Messages List						• • • • • •	Delete Selected
		0			Protocol	BOTH BOTH / UDP / TCP	•	Number per Page (10)		
	Network		Select All N	0.				Destination Send Port	Comments	Edit
	AC	0				100 Source Start Port	0			
	Authentication						0			
	Traffic Control	Ð			Source Send Port	150 Source Send Port	0			
- Sh	Firewall	0			estination Start Port	300	0			
	IP Filter					Destination Start Port				
	MAC Filter			Di	estination Send Port	400	0			
	URL Filter					Destination Send Port				
	Port Mapping				Comments	My	0			
	DMZ Setting					Maximum 32 characters				
	ARP Binding						save			
	Attack Protection			-						
6	Service	Ð								

2. Fill in the source port and the destination port (set according to the actual situation). The source port refers to the local port and the destination port is the remote port. Then click Save. After the setting is successful, filter the local port 100-150, remote port 300-400







K	onTel										¢
٩			HOME PAGE > FIRE	WALL > P	ORT FILTER						
₿	State		Messages List						Number per Page (10)	▼ 🔁 Add	🛍 Delete Selected
¢.	Network	0	Select All	No.	Protocol	Source Start Port	Source Send Port \Rightarrow	Destination Start Port 🔅	Destination Send Port	Comments	Edit
0	AC	Θ	E	1	BOTH	100	150	300	400	My	28
	Authentication	0									< 1 >
0	Traffic Control	0									
Шİ	Firewall	•									
	IP Filter										
	MAC Filter										
	URL Filter										
	Port Filter										

7.5 Port Mapping

Port Mapping or **Port Forwarding** is an application of network address translation (NAT) that redirects a communication request from one address and **port** number combination to another while the packets are traversing a network gateway, such as XonTel XT-1000AC.

X	onTel														
۹			HOME PAGE > FIRE	ewall > por	RT MAPPIN	IG									
₿	State		Messages List								Number per	Page (10)	• 🔂 Add	<u>ش</u> ۵	elete Selected
¢.	Network	0	Select All	No.	¢	Port Mapping Name	\$ Protocol	¢	Outer Port	¢	Inner Ip	\$	Inner Port	¢	Edit
0	AC	0													
	Authentication	0													
Ø	Traffic Control	0													
EM	Firewall	0													
	IP Filter														
	MAC Filter														
	URL Filter														
	Port Filter														
	Port Mapping														
	DMZ Setting														
	Attack Protection	6													

2. Click above picture's "+add" button,go into the Single Port Filtering page,setup the relative parameters.







X	onTel			á			_			Q
Q			HOME PAGE > FIRE	VALL >	Port Mapping Settings		×			
₿	State		Messages List		Port Mapping Name	SIP		Number per Page	(10) 🔽 🖸 Add	🛍 Delete Selected
8	Network	Ð	Select All	No.	Porc Mapping Name	SIF		Inner Ip 🗧	Inner Port	¢ Edit
0	AC	ø		1	Protocol	BOTH		92.168.1.200	5060	
	Authentication	Ð	6	2	Outer Port	5060		92.168.1.200	10000-20000	
Ø	Traffic Control	Θ		3		1-65535		92.168.1.200	6040	
зk	Firewall	O		4	Inner Ip	192.168.1.200 IP Ex: 100.100.100.100		92.168.1.200	5061	
	IP Filter			5	Inner Port	5060		192.168.1.25	8090	
	MAC Filter					1-65535				
	URL Filter					_				
	Port Filter					sav	e			
	Port Mapping									
	DMZ Setting									
	ARP Binding									
	Attack Protection									

3. Click save and go into the Massages List page, and the port forwarding function is successfully configured (the port is mapped to the external network port 5060 to the internal network port 5060 on IP Address 192.168.1.200).

X	onTel										
۹			HOME PAGE > FIRE	WALL > PORT	MAPPING						
₿	State		Messages List					N	mber per Page	(10) 🔹 🔂 Add	间 Delete Selected
C	Network	0	Select All	No. \$	Port Mapping Name	Protocol	Outer Port	\$ Inn	er Ip 🗢	Inner Port	÷ Edit
0	AC	0		1	SIP	BOTH	5060	192.16	8.1.200	5060	2 🗎
	Authentication	0									
	Traffic Control	0									
ΞŅ	Firewall	•									
	IP Filter										
	MAC Filter										< 1 >
	URL Filter										
	Port Filter	-									
	Port Mapping DMZ Setting										
	ARP Binding										

7.6 DMZ settings

A *DMZ* or *demilitarized zone* (sometimes referred to as a perimeter network or screened Subnet) is a physical or logical sub-network that contains and exposes an organization's external-facing services to an untrusted network, usually a larger network such as the Internet.You can place some server facilities which needs to be public in this small web area, such as enterprise Web server,FTP server and forum, etc. On the other hand, through this DMZ area, it is more effectively to protect the internal network.







X	onTel		Ö
Q			HOME PAGE > FIREWALL > DMZ
ß	State		
¢.	Network	0	DMZ Feature Enabled
0	AC	0	Host IP 192.168.1.240
B	Authentication	0	IP Ex xxx.xxx.xxxxxxxxxx
Ø	Traffic Control	0	Save
ΞŇ	Firewall	•	
	IP Filter		
	MAC Filter		
	URL Filter		
	Port Filter		
	Port Mapping	_	

7.7 ARP Binding

The Address Resolution Protocol is a communication protocol used for discovering the link layer address, such as a MAC address, associated with a given internet layer address, typically an IPv4 address.

Attention:ARP Binding isn't a option of your device can receive the static IP, it can only receive it when you tick to choose compatible ARP binding list in DHCP static allocation.

xon		HOME PAGE > FIRE	WALL > AR	P BINDING									
State	2	Messages List							Nur	nber per Page ((100) 💌	🕂 Add	Delete Selecte
Netw	vork Ø	Select All	No.	IP Address	÷	MAC	÷	Network		Comments	0	Status	≑ Edit
D AC	Θ	Statistics and statistics	1	192.168.1.66		00:C0:EE:37:A6:16		LAN1				Jnbound	28
	entication 0		2	192.168.1.47		D4:67:61:F3:01:9B		LAN1				Jnbound	20
	fic Control O		3	192.168.1.99		30:24:32:95:9D:BD		LAN1)	Jnbound	28
Firev	vall 🗢		4	192.168.1.48		D8:C4:6A:C8:F3:CF		LAN1				Jnbound	28
IP Fi	iter Filter		5	192.168.1.29		00:25:64:9A:1A:E6		LAN1				Unbound	
	. Filter		6	192.168.1.81		D4:67:61:C8:07:25		LAN1			1	Jnbound	2 😒
Port	Filter		7	192.168.1.11		4C:3B:74:01:BD:E4		LAN1				Jnbound	2 😒
Port	Mapping		8	192.168.1.95		00:25:64:C6:7E:D9		LAN1			į.	Jnbound	28
DMZ	2 Setting		9	192.168.1.26		0C:89:10:C7:4F:61		LAN1			9	Inbound	2 😒
	Binding		10	192.168.1.8		0C:CD:ED:35:38:91		LAN1			Q	Jnbound	28
Atta	ck Protection		11	192 168 1 74		48-BA-4E-37-D4-6D		LAN1				Inhound	

7.8 Attack Protection

A distributed denial-of-service (DDoS) attack is a malicious attempt to disrupt normal traffic of a targeted server, service or network by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic. Attack Protection can effectively protect the network from attacks and protect the network security.







X	onTel					ڻ
٩			HOME PAGE > FIREWALL > ATTACK PROTECTION			
酌	State					
¢.	Network	0	Anti ICMP Attack	~	Anti UDP Attack	~
0	AC	0				
	Authentication	0	Anti SYN Attack	~	Anti NULL Scan	~
Ø	Traffic Control	Ø				
ΞŃ	Firewall	•	Anti FIN Scan	~	Anti Xmas Tree	✓
	IP Filter		Anti Sumrf	~	Anti Ping	
	MAC Filter		And Summ	×	And Ping	
	URL Filter		ICMP Rate Threshold	1000		
	Port Filter			1-5000		
	Port Mapping		UDP Rate Threshold	2000		
	DMZ Setting			1-5000		
	ARP Binding		SYN Rate Threshold	200		
	Attack Protection			1-5000		
•	Service	0		Save	Cancel	1
	Log and Statistic	sØ				

8 Service

8.1 DDNS Settings

DDNS supports dyndns, 3322, Oray three ways of domain name resolution. (Note: If the device is used as the primary router for PPPoE dial up, the source of the IP address is selected to resolve the network adapter. If you are using as the secondary or lower route, the source of the IP address here is to select the network) Add your domain name and password here:

onTel		warmen gen en som		Maria Maria										
		HOME PAGE > SERV	TCE > DE	ONS SETTINGS										
State		Messages List							Number	r per Page (10)	•	🕀 Add	💼 Delete S	Selecte
Network	Ø	Select All	No.	DDNS Enable	Provider	Domain 🗘	User Name	Password/M	tey 🗘	IP Source	\$	Interface	÷	dit
AC	0	22	1	Enabled	dyndns.org	falan@xontel.com	user	pass		Interface		WAN1	1	1
Authentication	0												<	1
Traffic Control	0												1.1	1
Firewall	0													
Service	•													
DDNS Settings														
Static DNS														

8.2 Static DNS

Sometimes it required to use some service from your home/office device through Mobile App, locally and remote. Static DNS useful in that case. Static DNS can map a local IP address of the



54 | Page



device with a Domain name. So the mobile app can work with that domain name either in private WiFi network or on public network (4G/5G, Public WiFi)

KonTel							Q
Q		HOME PAGE > SER	VICE > STATIC DNS				
🕏 State		Messages List				Number per Page (10) 🗸 🕂 Add	Delete Selected
C Network	0	Select All	No. \$	Domain	÷	IP Address	\$
◎ AC	0		1	kuwait.gulfgate.com		192.168.1.200	
Authentication	0						< 1 >
Traffic Control	Θ						
H Firewall	0						
Service	•						
DDNS Settings							
Static DNS							
Remote Manage	ment						
VPN Client	0						

8.3 Remote Management Setting

Enterprise network administrators want to manage routers from anywhere on the network, allowing them to be managed and configured in real time and securely. Remote WEB management function can allow remote management of routers in the place of access to the Internet.

1. Click "Service - Remote Management" on the main interface of the XT-1000AC to enter the remote setup page, as shown below:

2. Enable the service, the port enters 1-65535 any one port, IP address default to remain empty, enter the specific IP only allow that particular IP remote access, do not enter any external network IP remote access, and then click Save.

X	onTel		٥
٩			HOME PAGE > SERVICE > REMOTE MANAGEMENT
₿	State		Remote Management
¢.	Network	0	Switch Enabled
0	AC	Θ	Port 80
-	Authentication	0	Port 80 Port (1~65335)
0	Traffic Control	0	IP Address
ыk	Firewall	0	IP Ex. xooucoucousous (Only this IP will have Remote Access)
6	Service	0	
	DDNS Settings		Save Cancel
	Static DNS		
	Remote Managerr	ient	Remote Control

3. Enter the gateway of the upper-level route to set up the virtual server, IP is the WAN port IP of the XT-1000AC, and the port number of the external network port and internal network port is the same as the port number set on the remote management page.





tertface Status		Online: 🗹 Offline:	× Other: -
Name	Designate	IP Address	Status
Interface0	WAN1	192.168.22.106	~
Interface1	LAN2	192.168.3.3	~
Interface2	LAN1	172.16.0.1	×
Interface3	LAN1	172.16.0.1	×
Interface4	LAN1	172.16.0.1	×

4.After added, connect to the upper-level route, enter the WAN port address of the device in the browser: port number (such as "192.168.22.106:80"), press Enter, you can access the gateway of the device remotely.

8.4 VPN Client

8.4.1 PPTP Client

PPTP Client:PPTP is Point to Point Tunneling Protocol.This protocol is a new enhanced security protocol which base on the PPP protocol, it support VPN,PAP and EAP,etc.enhanced security.It can also let the remote clients safety visit the enterprise network through dial-in ISP, directly connect the Internet or other network.

Use the PPTP client function, enabled the PPTP switch, enter the Username, Password and Server/IP, click "save" and finish the setting.

X	onTel				ტ
Q			HOME PAGE > SERVICE > VPN CLIENT > PPTP CLIENT		
₿	State				
C	Network	0	PPTP Switch	Enabled	
0	AC	0	Username	ai	0
-	Authentication	0		Usemame	
Ø	Traffic Control	0	Password	123456 Password	0
BÅ	Firewall	0			0
G	Service	0	Server/IF	62.132.45.48 Server/IP	~
	DDNS Settings		Link Status	Disabled	
	Static DNS		IP Address	Other	
	Remote Manager		IP Address	oule	
	VPN Client	•		Save Cancel	l

8.4.2 L2TP Client

L2TP Client: L2TP is an industrial standard Internet tunneling protocol, the function is the same as PPTP protocol, such as it can also encryption for the network traffic. But it also have the different, such as PPTP require the network as the IP network, L2TP require point to point







connection for the data packet. PPTP use the single tunnel, L2TP use multi-tunnels. L2TP provide header compression and tunnel verify, but PPTP not support it.

Use L2TP Client, enabled L2TP Switch, enter the username, password and server/IP, click save then finish the L2TP client function setting.

X	onTel				ڻ
۹			HOME PAGE > SERVICE > VPN CLIENT > L2TP CLIENT		
₿	State				_
¢.	Network	ø	L2TP Swite	h Enabled	-
0	AC	0	Usernan		0
	Authentication	0		Username	
Ø	Traffic Control	0	Passwo	d 123456 Password	•
EÅ	Firewall	0			
6	Service	0	Server/	P 62.125.215.37 Server/JP	0
	DDNS Settings Static DNS		Link State	is Disabled	
	Remote Manager	nent	IP Addre	is Other	
	VPN Client	•		Save Cancel	
	PPTP Client		-		-

8.5 VPN Server

VPN is Virtual Private Network, it built up a temporary, safety and simulated point to point connection through a public network (such as Internet). This is an information tunnel which pass through the public network, the data can safety transmitting in the public network through this tunnel. So the user can vividly call it "Network of Network".

8.5.1 PPTP Server

1.Go into PPTP Server setting page, enter VPN account and password, as below:

7	onTel				
Q			HOME PAGE > SERVICE > VPN SERVER > PPTP SERVER		
₿	State				
C.	Network	0	PPTP server switch	Enabled ~	-
0	AC	0			
	Authentication	0	ServerIP	192.168.0.1 IP Ex: x0x.x0x.x0x.x0x	0
0	Traffic Control	0			0
EA	Firewall	0	Start IP	192.168.0.20 IP Ex: x00.400.300.300	~
G	Service	0	End IP	192.168.0.30	
	DDNS Settings			IP Ec xocuoocuoocuooc	
	Static DNS		Main DNS	192.168.0.1	0
	Remote Manager	ment		IP Ex: xox.xox.xox.xox	
	VPN Client	Ø	Secondary DNS		
	VPN Server	0		IP Ex: xox.xox.xox.xox (Optional)	
	PPTP Server		MTU		
	PPTP User			Optional/range value(128-1500)	
	UPNP Setup		MRU		
	Log and Statisti	ics©		Optional/range value(128-1500)	_







2.Go into PPTP USER page, set up the user

X	onTel								0
۹			HOME PAGE > SERV	ICE > VPN S	SERVER > PPTP USER				
₿	State		Messages List				Number per Page (10) 🛛 👻 🔂 Add	🗎 Del	ete Selected
C.	Network	0	Select All	No.	\$ Username	÷	Password	¢	Edit
0	AC	0		1	youruser		yourpass		
	Authentication	0							1 >
0	Traffic Control	0							10-01
ΞÅ	Firewall	0							
6	Service	0							
	DDNS Settings								
	Static DNS								
	Remote Manager	nent							
	VPN Client	0							
	VPN Server	0							
	PPTP Server								
	PPTP User								

3. Setup a VPN connection in laptop which is on different network, enter the user name and password added by PPTP, test the connection, and get the specified IP address.

8.6 UPNP Settings

UPnP is a variety of intelligent devices, wireless devices and PC to realize peer to peer network connection (P2P) structure throughout the world. UPnP is a distributed and open network structure.

	HOME PAGE >	SERVICE > UPNP SET	UP						
State	Messages Lis	t						Num	ber per Page (100) VPNP Feature
Network ©	No.	Protocol	\$	IP Address	÷	External Port	Inter	rnal Port 🗦	Description
AC O	1	TCP		192.168.1.44		34001	3	8341	DIRECT_REVERSE_SERVER
Authentication 0	2	UDP		192.168.1.38		56066	5	6066	WhatsApp
Traffic Control	3	UDP		192.168.1.38		45874	4	5874	WhatsApp
	4	UDP		192.168.1.65		51500	5	1500	WhatsApp
Firewall O	5	UDP		192.168.1.95		63314	6	3314	WhatsApp
Service o	6	UDP		192.168.1.70		58618	5	8618	WhatsApp
DDNS Settings									< 1
Static DNS									
Remote Management									
VPN Client O									
VPN Server 0									







9 Log and Statistics

9.1 Log

Here you can view the system's working status when the device is working.

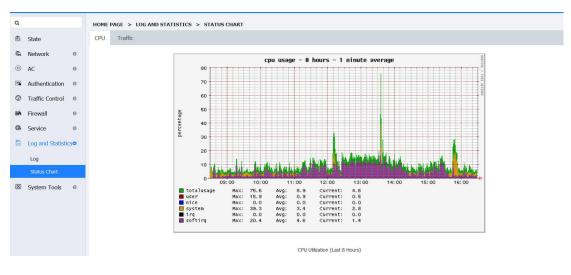
1.Go to WEB Interface and go to Log and Statistics-Log page,click "GET LOG" button, then the page will refresh the log details every moments, as below:

KonTel			Q
۹	HOME PAGE > LOG AND STATISTICS	> L0G	
🕏 State			
C Network O		GET LOG	
AC	Date Leve	l Log	
Authentication 0	2020/1/6 16:25:31 Info	DHCPREQUEST for 192.168.1.87 (192.168.1.1) from d4:67:61:c8:07:03 via br-lan: database update failed	
Traffic Control	2020/1/6 16:25:31 Info	Wrote 93 leases to leases file.	
BM Firewall ©	2020/1/6 16:25:29 Info	DHCPACK on 192.168.1.22 to d4:67:61:c8:06:f8 via br-lan	
	2020/1/6 16:25:29 Info	DHCPREQUEST for 192.168.1.22 (192.168.1.1) from d4:67:61:c8:06:f8 (android-cc8faa0cee33eae7) via br-lan	
Service 0	2020/1/6 16:25:29 Debu	g reuse_lease: lease age 3 (secs) under 25% threshold, reply with unaltered, existing lease	
Log and Statistics	2020/1/6 16:25:26 Info	DHCPREQUEST for 192.168.1.22 (192.168.1.1) from d4:67:61:c8:06:f8 via br-lan: database update failed	
	2020/1/6 16:25:26 Info	Wrote 93 leases to leases file.	
Status Chart	2020/1/6 16:24:38	CGI error: -32601/Method not found	
System Tools O	2020/1/6 16:24:37 Info	User admin/xontel authorized OK	
	2020/1/6 16:24:37 Info	DHCPACK on 192.168.1.10 to 00:08:7b:16:af:a4 via br-lan	
	2020/1/6 16:24:37	R Action (Construction of the Action of the Construction of the Landback on Action of the Action of	
	2020/1/6 16:24:37 Debu		
	2020/1/6 16:24:36		
	2020/1/6 16:24:16 Info		
	2020/1/6 16+24+0E	DUCDACK on 100 160 1 17 to ad-36-16/02-76-00 uis brillion	

9.2 Status Chart

Historical Statistics

1.CPU: here record the CPU usage information when the devise working 8 hours, one day and one week.

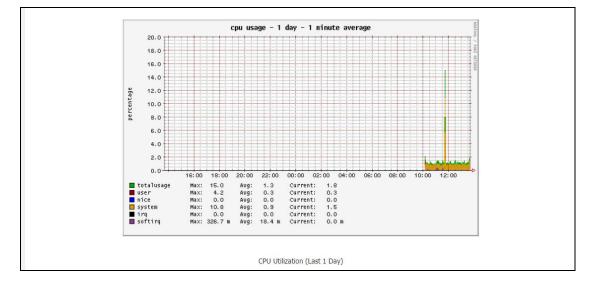


<8 Hours>

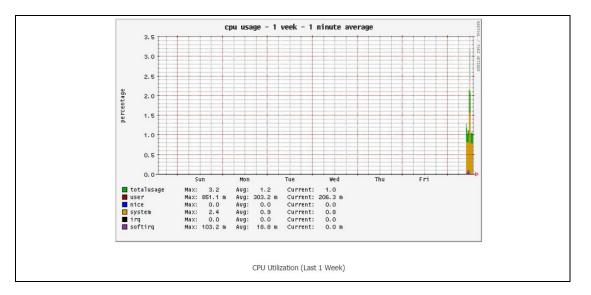


59 | Page





<One Day>



<One Week>

2.Traffic: Here record the traffic status information when the devise working 8 hours, one day and one week.

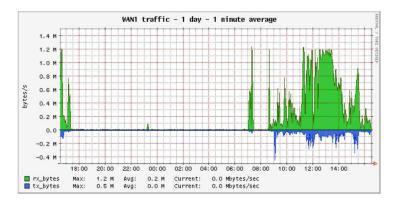






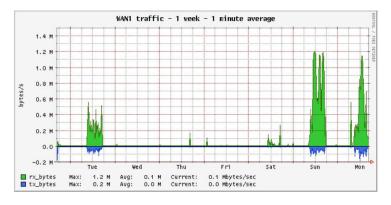






Bandwidth (Last 1 Day)





Bandwidth (Last 1 Week)

<One Week>





10 System Tools

10.1 System upgrade

Download the latest XT-1000AC firmware from the website <u>https://xontel.com</u>, download and save it on the computer. Go into the system upgrade page,click Browse to choose the firmware file you had downloaded in this page. Then click "Upgrade Firmware" button to upgrade.

KonTel	ڻ ن
Q	HOME PAGE > SYSTEM TOOLS > SYSTEM UPGRADE
🕏 State	Local upgrade
C Network O	Firmware Version XT-1000AC-V1.0
• AC •	Select Browse No file selected.
Authentication	No file selected.
Ø Traffic Control ◎	Upgrade Firmware Cancel
₩ Firewall ©	
CB Service 0	
Log and Statistics	
🗷 System Tools 🗢	
System Upgrade	
Manage Config	

10.2 Manage Config

Backup Config: After you configure the device's parameters, you can click "download" button to save the configure parameters in file to be used later.

KonTel		0
Q		HOME PAGE > SYSTEM TOOLS > MANAGE CONFIG
🕏 State		Backup Config File
C Network	0	Download
◎ AC	0	
Authentication	0	() information Press' Download' Button. Choose File Location.
C Traffic Control	0	
Hirewall	0	Update Config
Service	0	Select Browse No file selected.
Log and Statistics	50	Upload Cancel
System Tools	0	
System Upgrade		information Press button, the system will restore the configuration to the upbaded backup file.
Manage Config		
Reboot		Restore Factory Settings
Password Setting		Kesure ratury seturitys
Time Setting		Restore Factory Settings
PING		A information Pressing the 'Restore Factory Settings' Button will Reset Device.







HOME PAGE > SYSTEM TOOLS > MANAGE CONFIG					
Backup Config File					
	Download				
information Press 'Download' Button. Choose File Location.					

2. Select the path to save the configuration, and then click OK, the current configuration has been saved on the local computer.

Update Config: If you need to change the configure temporary or the device was restored the default settings, you can select to choose the configure file that you save before.

1. Choose the configure file that you save before, Click "Upload" button to restore.

Update Config		
	Select	Browse bakup.file
	Upload	Cancel
() information Press button, the system will restore the configu	ration to the uploaded backup	fie.

2. Click "Upload" and after a while system will popping the interface to login again.

(←) → C ⁴ ⁽¹⁾	0 🔏 192.168.1.1/login.html		Q v A	<u>⊀</u> III\ ⊡ ®* ≡
		XonTel		
		🖾 Username		
		Q Password		
		LOGIN		
		Copyright © 2004-2019 By Xontel All Rights Reserved.		

Restore Factory Settings: If you want to reset the device to its factory default, you can click "Restore Factory Settings" button at the bottom of the Manage Config page.

1. Go to the Manage Config page, click "Restore Factory Settings"







Restore Factory Settings	
	Restore Factory Settings
A information Pressing the 'Restore Factory Settings' Button will Reset Device.	

2. System will pop the notice information, configuration will set to factory defaults, please wait for <180> seconds and Do Not disconnect the power.

3. 3 minutes later system will automatic interface to login again, it is success to restore factory settings.



10.3 System Reboot

10.3.1 Timed Restart

1. Go into the System Tools- Reboot page, you can On or Off scheduled reboot, select or remove the restart days of week, input the restart time click Save.







K	onTel			ڻ
۹			HOME PAGE > SYSTEM TOOLS > REBOOT	
₿	State		Timed Restart	
¢,	Network	0	Timed Restart Switch	
0	AC	0		WED 🗹
-	Authentication	0		SUN 2
0	Traffic Control	0	Restart Time 04:00	
BÅ	Firewall	0	ex. : 00:00	
•	Service	0	Interval Restart O OFF	
	Log and Statistic	so	Save Cano	4
8	System Tools	۲		_
	System Upgrade			
	Manage Config		Reboot Now	
	Reboot		Reboot Now	
Password Setting				
	Time Setting		Warning Pressing the 'Reboot' Button will Reboot Device.	
	PING			

2. After this setup the device will restart automatically on the days and time your setup above.

Interval Restart: Go into the System Tools-reboot page, you can set up an interval Restart. Turn On the Interval Restart, input the interval restart time, click Save. As shown below the device restarts every 6 hours.

X	onTel			đ
۹			HOME PAGE > SYSTEM TOOLS > REBOOT	
勴	State		Timed Restart	
C.	Network	0	Timed Restart Switch	
0	AC	0		
	Authentication	0	Interval Restart	
Ø	Traffic Control	0	Interval 6	
EÁ	Firewall	Θ	Internal(untch)	
6	Service	Θ	Save Cancel	
	Log and Statisti	cs Ø		
	System Tools	0	Reboot Now	
	System Upgrade		Reboot Now	
	Manage Config			
	Reboot		Warning Pressing the 'Reboot' Button will Reboot Device.	

10.3.2 Reboot Now

1. If system required immediate restart go into the System Tools-Reboot page,click "Reboot Now" button.







KonTel	Ö
٩	HOME PAGE > SYSTEM TOOLS > REBOOT
🕏 State	Timed Restart
C Network O	Timed Restart Switch
◎ AC Ø	
Authentication ©	Interval Restart 🛛 🔍
Traffic Control	Interval 6
BN Firewall ©	Interva(unith)
C Service 0	Save Cancel
Log and Statistics Ø	
🗷 System Tools 🔹	Reboot Now
System Upgrade	Reboot Now
Manage Config	
Reboot	A Warning Pressing the 'Reboot' Button will Reboot Device.
Password Setting	

2. Wait for 1 minute for the system to come up again.

10.4 Password Setting

Here you can change the Admin Password. After setting you need to use the new password to login.

1. Go into System home page and go to System Tools "Password Setting" page as below:

K	onTel			
Q			HOME PAGE > SYSTEM TOOLS > PASSWORD SETTING	
₿	State			
C	Network	ø	Old Password	Old Password
0	AC	0	New Password	
-	Authentication	0		New Password
Ø	Traffic Control	0	Confirm Password	
EA	Firewall	0		Confirm Password
6	Service	0		Save
	Log and Statisti	sø		
团	System Tools	0		
	System Upgrade			
	Manage Config			
	Reboot			
	Password Setting			

- 2. Enter the new password two times and click Save:
- 3. After setting you need to use the new password to login again.





10.5 Time Setting

Here you can the sync the system time with Computer time from where you logged in,Enable/Disable Internet Sync time. The device will be automatic sync system time with NTP server configured.

1.Go into System home page and go to System Tools -"Time Setting" page as below:

X	onTel			
۹			HOME PAGE > SYSTEM TOOLS > TIME SETTING	
ß	State			
C.	Network	Θ	Computer Time 20	020-01-07 15:55:14
0	AC	0	Internet Sync D	Disabled V
	Authentication	0	Save	e Cancel
0	Traffic Control	0		
BÅ	Firewall	0		
6	Service	0		
	Log and Statisti	cs€		
浽	System Tools	0		
	System Upgrade			
	Manage Config			
	Reboot			
	Password Setting	1		
	Time Setting			

2. Click Internet Sync switch's button, choose "Enabled" then click Save.

X	onTel			Ø
٩			HOME PAGE > SYSTEM TOOLS > TIME SETTING	
B	State			
¢.	Network	0	Computer Time	2020-01-07 15:42:40
0	AC	0	Internet Sync	Enabled
	Authentication	0	Current Time Zone	(UTC+03:00)Kuwait, Riyadh 🖌
0	Traffic Control	0	NTP Server	pool.ntp.org
ВÅ	Firewall	0		r.g : 0.openwrt.pool.ntp.org
•	Service	0		Save Cancel
	Log and Statistic	cs0		
図	System Tools	0		
	System Upgrade			
	Manage Config			
	Reboot			
	Password Setting	1		
	Time Setting			

3. Wait for 5 seconds, the system time will be synchronized with the network time.

4. Disable the Internet Sync, use the option to sync time from the computer from which you logged in. This will be a onetime sync.







10.6 PING (Diagnostic Tool)

Here you can PING any IP address or Domain name to confirm the connectivity of the system to Internet.

1. Go into system home page and go to the System Tools "PING" page as below:

KonTel	୦ ୦
Q	HOME PAGE > SYSTEM TOOLS > PING
🕏 State	
C Network O	Host Name PING Please Input: IP Address/Doman Itame
Authentication Ø	
Traffic Control	
🖬 Firewall 🛛 🛛	
C Service 0	
Log and Statistics O	
🗷 System Tools 🔹	
System Upgrade	
Manage Config	
Reboot	
Password Setting Time Setting	
PING	

2. Enter IP address of google.com as 8.8.8.8 or the domain google.com itself, click "PING" button, wait some seconds, it will show the result as below:

X	onTel				ტ		
Q			HOME PAGE > SYSTEM TOOLS > PING				
₿	State						
¢.	Network	0		Host Name	google.com PING		
0	AC	0			Please Input IP Address/Domain Name		
	Authentication	0			14: seq=0 ttl=54 time=62.162 ms		
Ø	Traffic Control	0		64 bytes from 172.217.19.14: seq=1 ttl=54 time=50.006 ms 64 bytes from 172.217.19.14: seq=2 ttl=54 time=43.711 ms			
EA	Firewall	0		64 bytes from 172.217.19.14: seq=3 ttl=54 time=35.461 ms google.com ping statistics			
6	Service	0		4 packets transmitted, 4 packets received, 0% packet loss round-trip min/avu/max = 35.461/47.835/62.162 ms			
8	Log and Statistic	s⊚			Å		
8	System Tools	0					
	System Upgrade						
	Manage Config						
	Reboot						
	Password Setting						
	Time Setting						
	PING						

