

## **CONFIGURATION ROUTEURS**

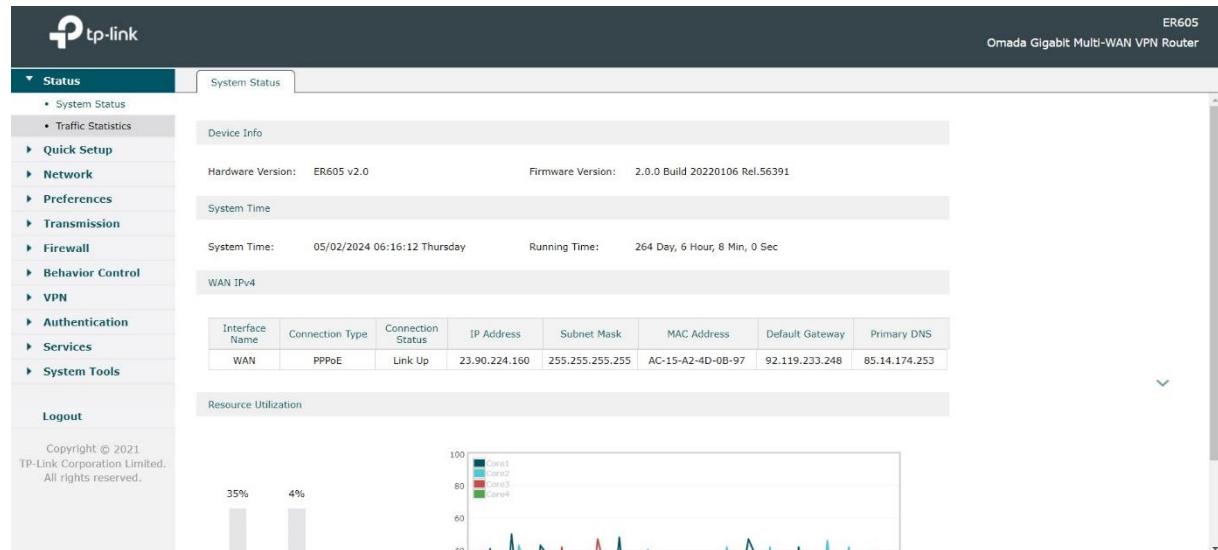
La configuration des routeurs est de 2 types : routeurs lien xDSL (ADSL, VDSL) ou lien fibre.

Nous retrouvons les configurations nécessaires au lien IP public de chaque solution sur les plateformes opérateurs dédiés (Snic Réseau Networth et Atlas par Unyc).

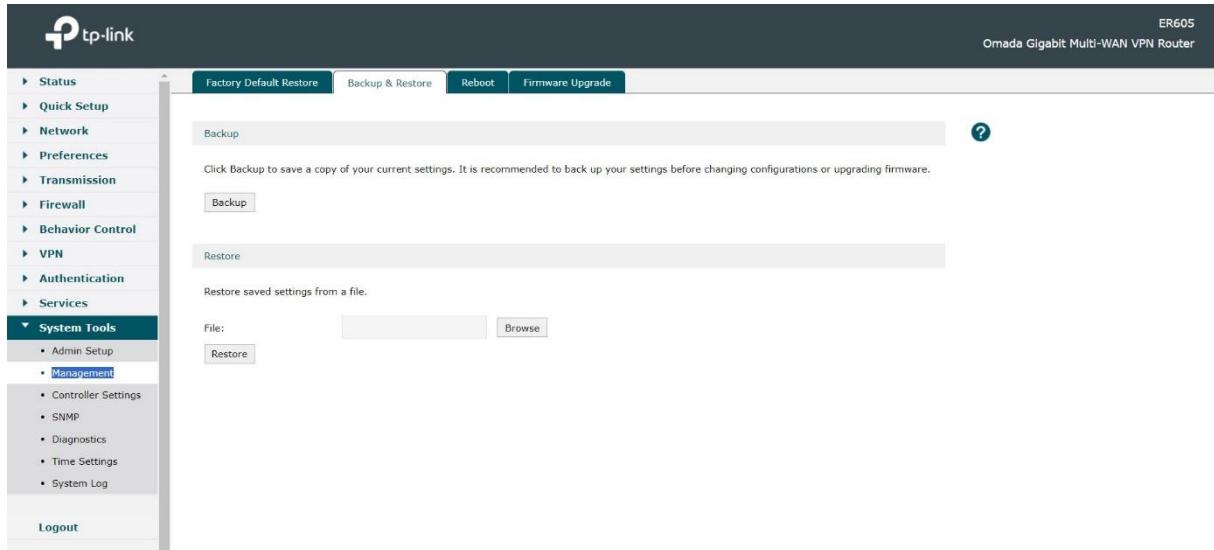
Ensuite, nous disposons de préconfiguration déjà établies, il suffit d'importer la configuration et d'effectuer les modifications nécessaires sur le nouveau réseau à venir de notre client.

Une chose très importante à faire avant tout cela est de récupérer la configuration sur le routeur déjà existant du client (s'il y en a un) et de conserver les paramétrages du LAN, DHCP, règles NAT notamment.

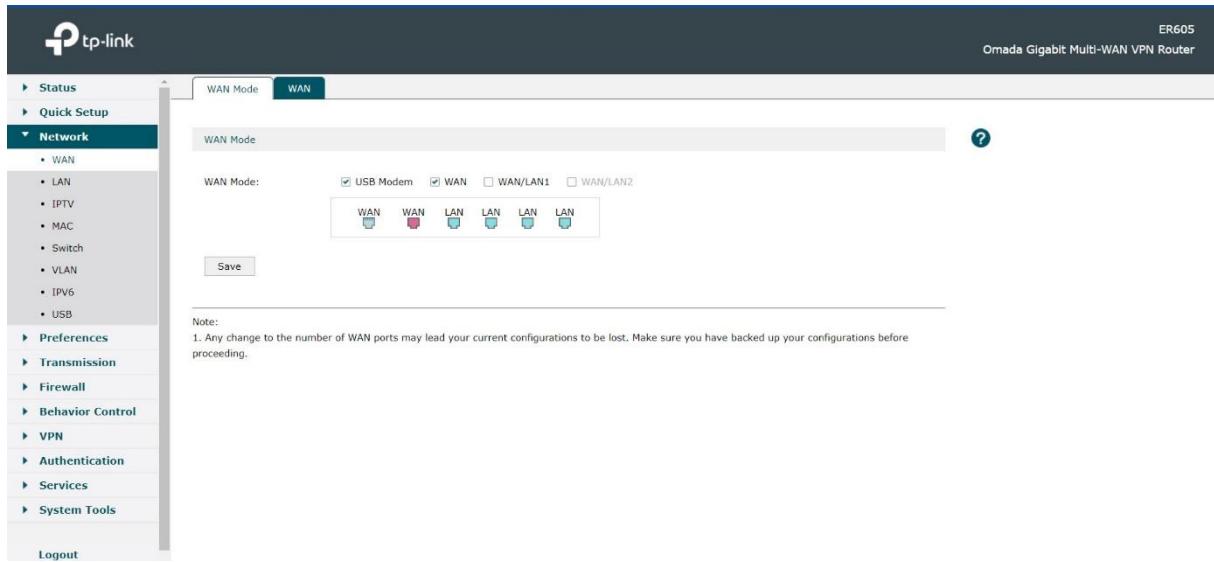
*Voici l'accueil d'un routeur ER605 :*



Je me rends dans System Tools puis dans Backup & Restore afin d'y uploader mon fichier de configuration déjà pré établi.



Ensuite, je peux me rendre dans WAN afin de vérifier les interfaces présentes. Je vois que le port 2 WAN et l'interface USB sont sélectionnés et donc activés.



J'indique les PPOE de la fibre contenant un Username et Password. Puis j'indique le VLAN de l'opérateur, ici 2900 correspond à une fibre SFR.

ER605  
Omada Gigabit Multi-WAN VPN Router

WAN Mode

Connection Configuration

Connection Type: PPPoE

Username: ip230126100395@ftth.umsy

Password: \*\*\*\*\*

Connection Mode: Connect Automatically

Upstream Bandwidth: 1000000 Kbps (100-1000000)

Downstream Bandwidth: 1000000 Kbps (100-1000000)

MTU: 1492 (576-1492)

Service Name: (1-128 characters, optional)

Primary DNS: (Optional)

Secondary DNS: (Optional)

Vlan:  Enable

Vlan ID: 2900 (1-4094)

Secondary Connection:  None  Dynamic IP  Static IP

Save Connect Disconnect

Au niveau de l'interface USB, je vois par « *disconnected* » qu'aucune clé n'est connectée ou alors elle n'est pas active.

ER605  
Omada Gigabit Multi-WAN VPN Router

USB Modem

USB Modem: No USB modem connected.

Config Type: Auto

Location: France

Mobile ISP: Bouygues Telecom

Connection Mode:  Connect Automatically  Connect Manually

Upload Bandwidth: 100000 Kbps (100-1000000)

Download Bandwidth: 100000 Kbps (100-1000000)

Authentication Type: Auto

MTU Size(in bytes): 1480

Use The following DNS Servers:  Enable

Connect Disconnect

Save

Je me rends ensuite dans le LAN afin de paramétrer le réseau voulu pour le client.

ER605  
Omada Gigabit Multi-WAN VPN Router

LAN

DHCP Client List

ID	Name	Vlan	IP Address	Subnet Mask	DHCP Server	DHCP Relay	Operation
1	LAN	1	192.168.1.1	255.255.255.0	Enabled	Disabled	...

Address Reservation

Name: LAN

IP Address: 192.168.1.1

Subnet Mask: 255.255.255.0

Vlan: 1 (1-4096)

DHCP

DHCP Mode:  DHCP Server  DHCP Relay

Status:  Enable

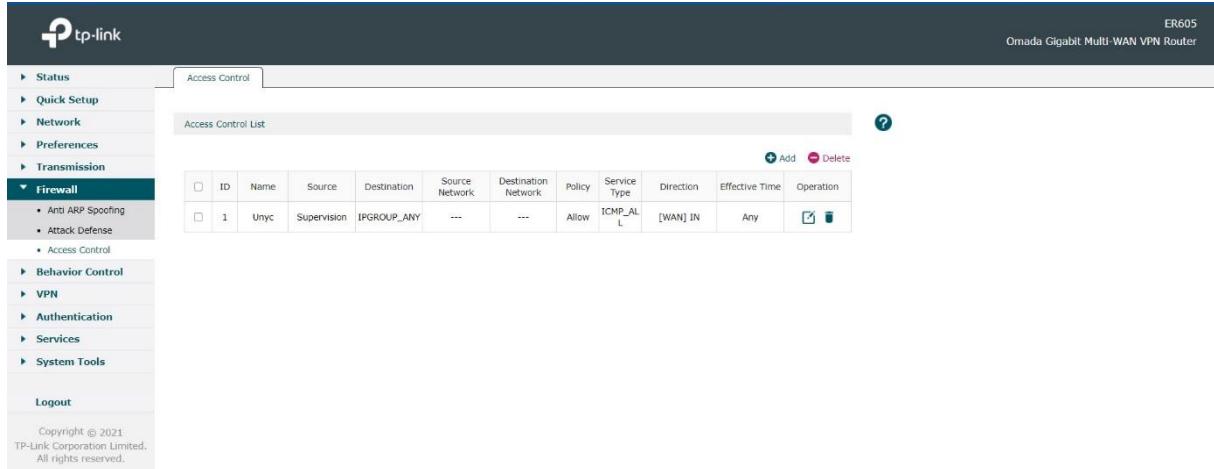
Starting IP Address: 192.168.1.100

Ending IP Address: 192.168.1.199

Lease Time: 120 minutes (1-2880. The default value is 120)

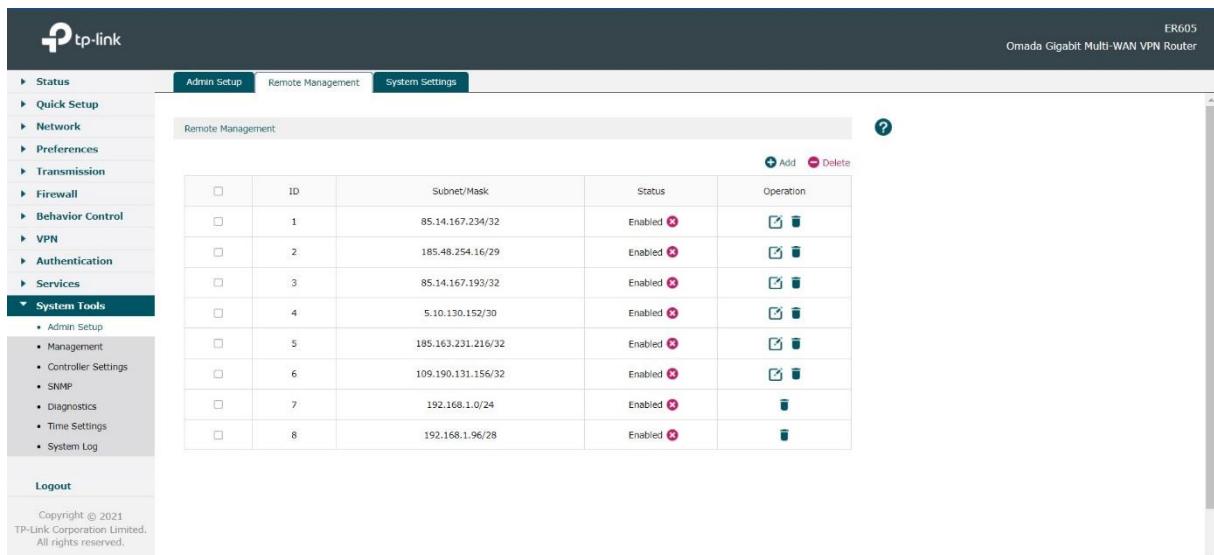
Default Gateway: (Optional)

Je peux aller dans *firewall* et *access control* vérifier si les règles de la configuration sont bien en place. La supervision est paramétrée pour les serveurs d'Unyc.



ID	Name	Source	Destination	Source Network	Destination Network	Policy	Service Type	Direction	Effective Time	Operation
1	Unyc	Supervision	IPGROUP_ANY	---	---	Allow	ICMP_ALL	[WAN] IN	Any	<input checked="" type="checkbox"/> 

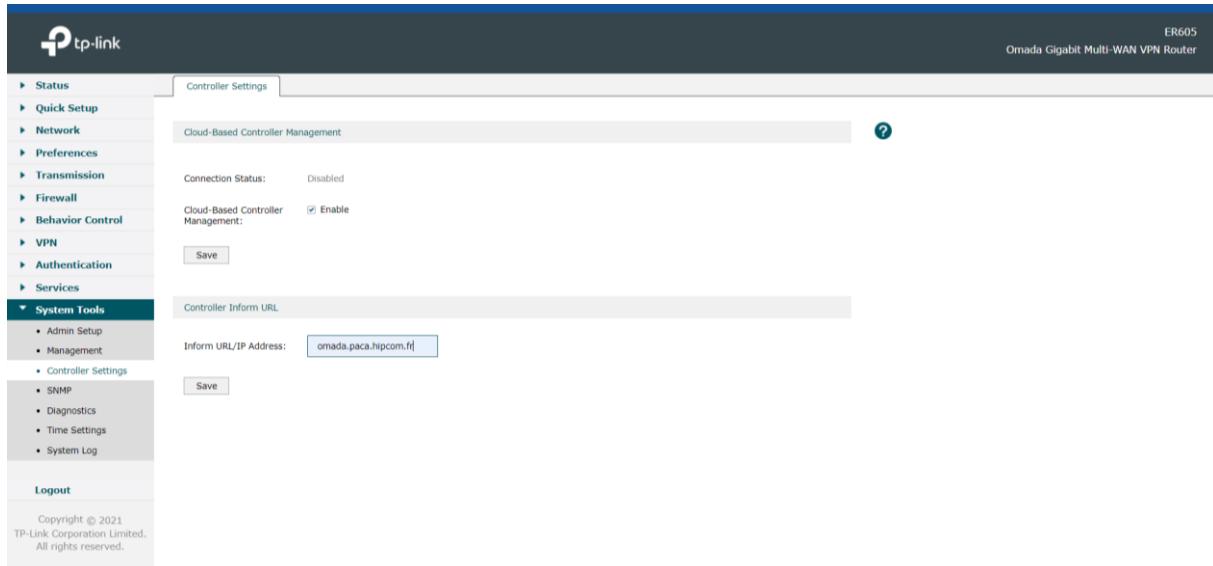
Ensuite, je vérifie dans *System Tools* puis *Remonte Management* si notre adresse IP publique apparaît bien afin d'avoir accès au routeur à distance. Je vois que l'adresse est présente c'est donc bon.



ID	Subnet/Mask	Status	Operation
1	85.14.167.234/32	Enabled 	<input checked="" type="checkbox"/> 
2	185.48.254.16/29	Enabled 	<input checked="" type="checkbox"/> 
3	85.14.167.193/32	Enabled 	<input checked="" type="checkbox"/> 
4	5.10.130.152/30	Enabled 	<input checked="" type="checkbox"/> 
5	185.163.231.216/32	Enabled 	<input checked="" type="checkbox"/> 
6	109.190.131.156/32	Enabled 	<input checked="" type="checkbox"/> 
7	192.168.1.0/24	Enabled 	<input checked="" type="checkbox"/> 
8	192.168.1.96/28	Enabled 	<input checked="" type="checkbox"/> 

Antoine Gargi  
Aristee Formation  
2022-2024

Enfin, je me rends dans Controller Settings afin d'activer le Cloud management et j'ajoute l'adresse URL correspondant au domaine Cloud.



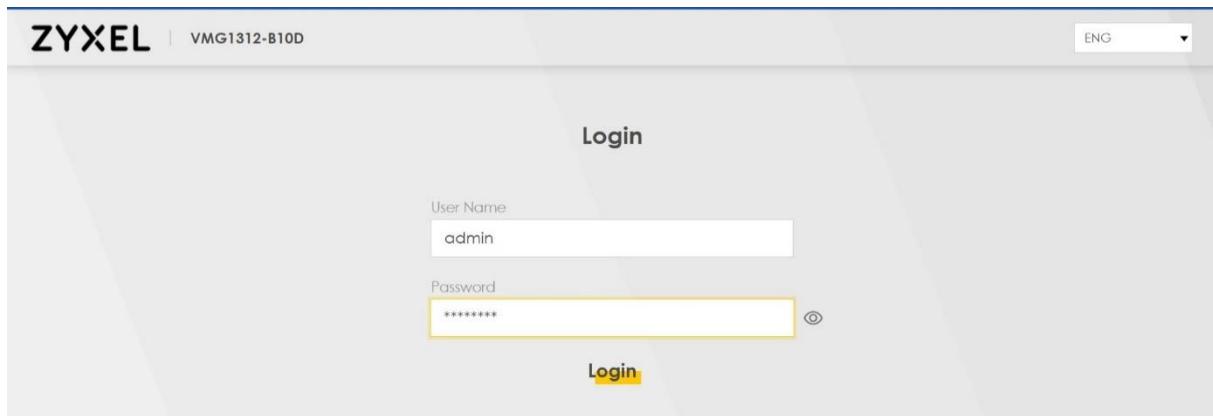
ER605  
Omada Gigabit Multi-WAN VPN Router

Status Quick Setup Network Preferences Transmission Firewall Behavior Control VPN Authentication Services System Tools Admin Setup Management Controller Settings SNMP Diagnostics Time Settings System Log Logout

Copyright © 2021 TP-Link Corporation Limited. All rights reserved.

## Paramétrage routeur Zyxel :

Voici la page de connexion d'un Zyxel VLG1312-B10D :



Je me rends dans *backup/restore* afin d'uploader mon fichier de configuration correspondant au modèle.

**Backup/Restore**

You can save the current settings in a backup file on your computer, or restore previous settings from a backup file. You can also reset the device back to its factory default state.

**Backup Configuration**

Click Backup to save the current configuration of your system to your computer.

**Backup**

**Restore Configuration**

To restore a previously saved configuration file to your system, browse to the location of the configuration file and click Upload.

File Path  Choisir un fichier Aucun fichier choisi **Upload**

Je me rends ensuite dans *Broadband* afin de configurer les identifiants radius du lien xDSL client. Je dois faire la manipulation sur les 2 interfaces ADSL et VDSL.

**Broadband**

Broadband Cellular Backup Advanced Ethernet WAN

You can configure the Internet settings of this device. Correct configurations build successful Internet connection.

**Add New WAN Interface**

#	Name	Type	Mode	Encapsulation	802.1p	802.1q	IGMP Proxy	NAT	Default Gateway	IPv6	MLD Proxy	Modify
1	ADSL	ATM	Routing	PPPoE	N/A	N/A	N	Y	Y	N	N	
2	VDSL	PTM	Routing	PPPoE	0	835	N	Y	Y	N	N	

J'entre les identifiants fournis par l'opérateur du client puis je valide.

**Edit WAN Interface**

**General**

Name: ADSL  
Type: ADSL over ATM  
Mode: Routing  
Encapsulation: PPPoE  
IPv4/IPv6 Mode: IPv4 Only

**PPP Information**

PPP User Name: ip230524105489@srvc  
PPP Password:    
PPP Connection Trigger: PPPoE Passthrough  
Auto Connect:  On Demand

**ATM PVC Configuration**

VPI [0-255]: 8  
VCI [32-65535]: 35  
Encapsulation: VC/MUX  
Service Category: UBR Without PCR

**VLAN**

802.1p: 0  
802.1q: (1-4094)

**MTU**

MTU: 1492

Je peux désormais paramétrer le LAN et le Wifi client (se trouvant tous deux dans l'accueil de l'interface).

**WiFi Settings**

2.4G WiFi Name: **LTI\_Telecom**

WiFi Password: **.....**

**LAN**

IP Address: **192.168.1.1**

Subnet Mask: **255.255.255.0**

IP Address Range: **192.168.1.10 ~ 192.168.1.60**

DHCP: **Enabled**

Lease Time: **1 days 0 hours 0 mins**

Enfin, j'effectue une vérification au niveau des règles de Firewall, dans Access Control pour m'assurer d'avoir l'accès distant au routeur. Je vois que l'adresse est bien présente c'est donc bon.

**Firewall**

General Protocol **Access Control** Dos

An ACL rule is a manually defined rule to accept, reject, or drop the incoming or outgoing data of your network. You may need to create at least one Protocol entry in order to add an ACL rule.

Rules Storage Space Usage: 25%

**Add New ACL Rule**

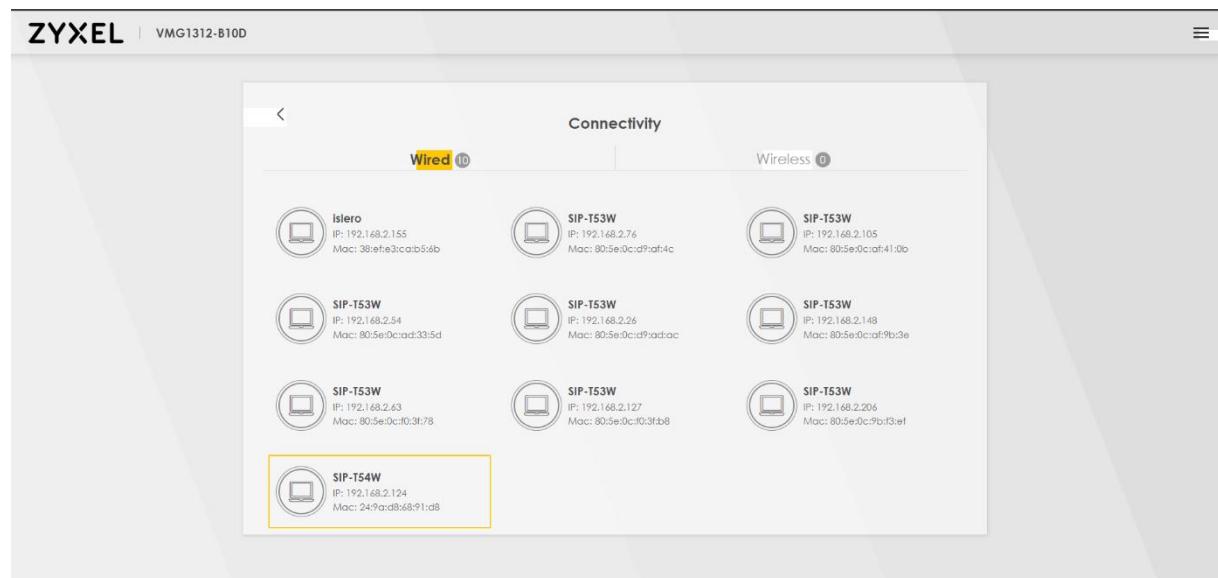
#	Name	Src IP	Dest IP	Service	Action	Modify
1	Eqinote_5	185.197.109.16/28	Any/32	ALL	Accept	
2	Eqinote_4	185.163.212.64/28	Any/32	ALL	Accept	
3	Eqinote_3	185.163.212.48/28	Any/32	ALL	Accept	
4	Eqinote_2	185.48.254.0/28	Any/32	ALL	Accept	
5	Eqinote_1	185.48.253.0/27	Any/32	ALL	Accept	
6	Acces Bureau	85.14.167.234/32	Any/32	ALL	Accept	
7	Acces distant	85.31.110.71/32	Any/32	ALL	Accept	
8	Acces distant1	46.18.122.39/32	Any/32	ALL	Accept	

Voici l'exemple d'une règles de NAT effectuée sur un routeur Zxyel :

Je me rends sur Atlas pour récupérer l'adresse MAC du téléphone enregistré sur la licence.



Je me rends ensuite dans les clients du routeur du client, j'aperçois bien le téléphone T54W portant l'adresse MAC en question.

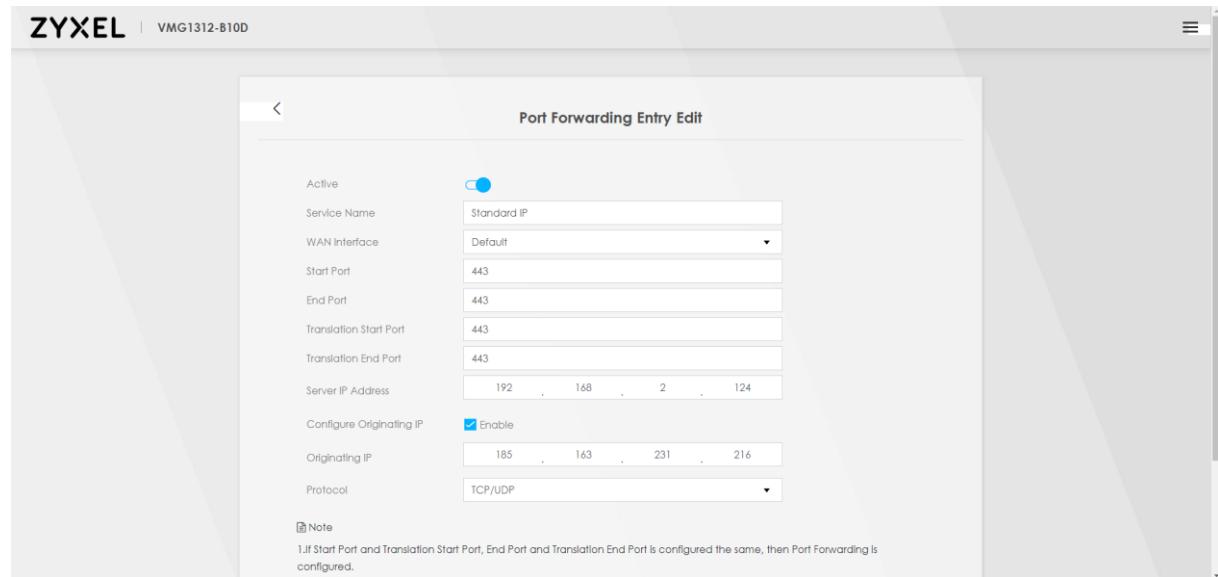


Je me rends dans *Port Forwarding* afin de paramétrer la règle de NAT.

Je choisis l'interface WAN par défaut, les ports start/end 443 et la même chose pour les ports de translation.

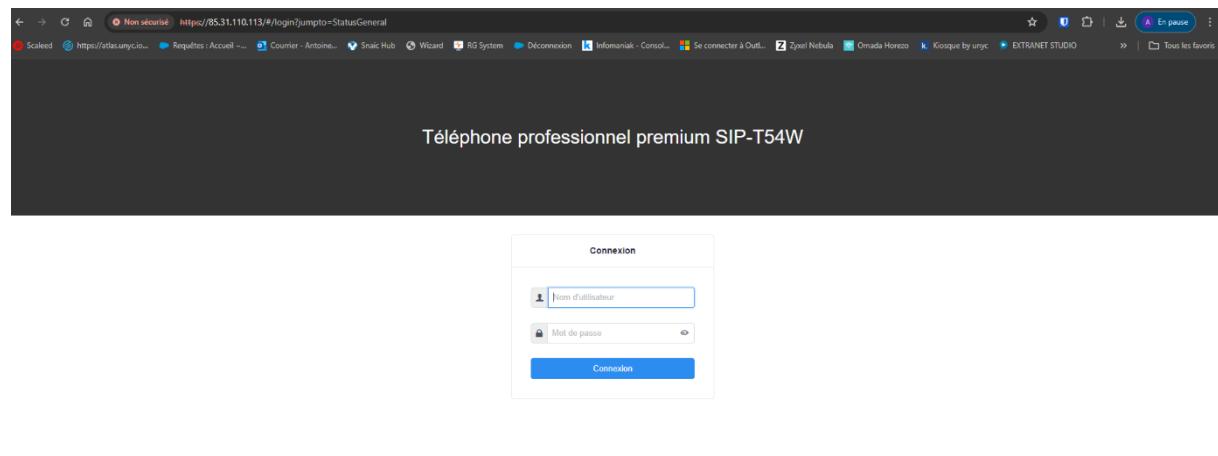
Il est important de ne pas oublier de préciser l'adresse IP de l'adresse MAC : 192.168.2.124

Je coche également l'adresse IP d'origine, donc celle de notre bureau support, qui est autorisée à atteindre le routeur.



Je tape l'adresse IP publique du routeur en https pour le port 443 et j'atteins bien le téléphone en question.

Je me connecte via admin et le mot de passe correspondant au T54W (récupérable dans cockpit d'Atlas ci-dessous)



*Mot de passe de sécurité d'un T54W*



Enfin, j'accède au téléphone en dur afin d'effectuer les paramétrages ou vérifications nécessaires pour notre client.

The screenshot shows the Yealink TS4W router's status page. The left sidebar has a tree structure with 'Etat' selected. The main content area is divided into sections: 'Version' (firmware 96.06.254.850, hardware 96.1.2.0.2.1.2), 'Certificats d'appareil' (Certificates installed), 'Réseau' (Port Internet: IPv4), 'IPv4' (WAN settings: DHCP, IP 192.168.2.124, Subnet 255.255.255.0, Gateway 192.168.2.1, Primary DNS 105.48.254.18, Secondary DNS 85.14.174.253), and 'Réseau commun' (MAC address 24:9A:D8:68:91:D8, machine ID 301081F061211505, SSID N/A, MAC Wi-Fi 24:9A:D8:77:DC:3F, VLAN ID 0, MAC Bluetooth 24:9A:D8:68:91:D9, WAN port state 1000Mbps Full Duplex, PC port state Disconnected).

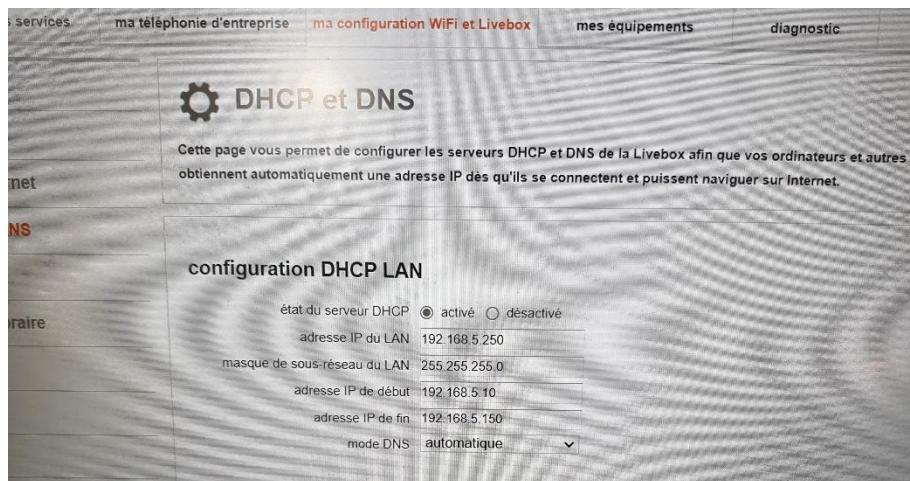
Il est important de préciser que la règle de NAT sur un routeur de la gamme Omada est quasi similaire. Seulement le nom de l'interface change « *virtual servers* » au lieu de « *port forwarding* ». Il n'y a ici pas de start/end port à renseigner, on indiquerait seulement 443 pour le port https et l'adresse IP de l'équipement souhaité.

The screenshot shows the TP-Link ER605 router's configuration interface. The left sidebar has a tree structure with 'Transmission' selected, then 'NAT'. The main content area shows a 'Virtual Server List' table with one entry (ID 1, Name vs1, Interface WAN1, External Port 50, Internal Port 6050, Internal Server IP 192.168.0.10, Protocol TCP, Status Disabled). Below the table is a 'Virtual Server' configuration dialog with fields: Name (vs1), Interface (WAN1), External Port (50), Internal Port (6050), Internal Server IP (192.168.0.10), Protocol (TCP), and Status (Enable checked). Buttons for 'OK' and 'Cancel' are at the bottom.

**Voici un exemple d'une connexion sur une box Orange d'un client afin de récupérer sa configuration existante :**

(Certains de nos clients choisissent par eux-mêmes de conserver certains liens Internet xDSL et nous pouvons être amenés à paramétriser sur un nouveau routeur xDSL que nous leur fournissons. De plus, certains liens Fibre SFR ou Orange disposent d'une box avec un ONT (boîtier optique) intégré à la Box. Ce qui signifie que les interfaces de connexion sur ces routeurs sont relativement similaires à ceux xDSL).

*Sur cette photo, nous retrouvons les informations du serveur DHCP que nous allons configurer sur notre nouveau routeur.*



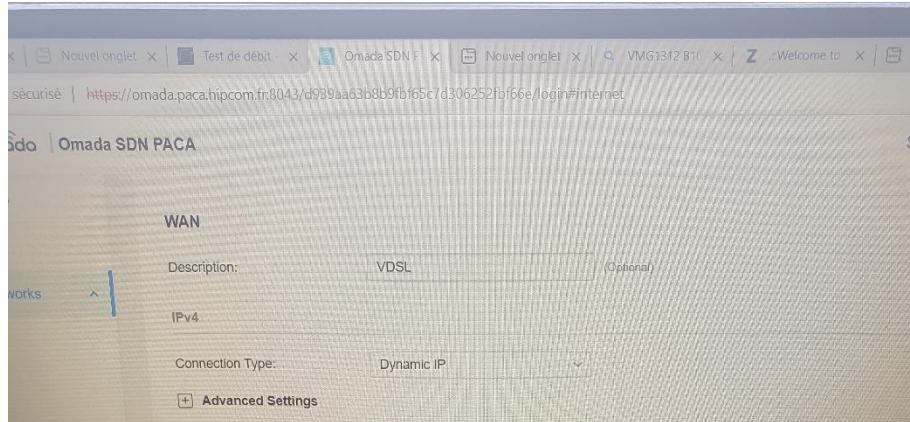
*Règles de redirections de ports (NAT) sur cette même Box Orange :*

table de redirections							
application / service	protocole	adresse IP externe autorisée	masque réseau externe	port externe	port interne	équipement / adresse IP	activer
SSH	TCP		255.255.255.255	22	22	192.168.0.5	<input checked="" type="checkbox"/>
VNV	TCP		255.255.255.255	5900	5900	192.168.0.5	<input checked="" type="checkbox"/>

**! La création d'une règle sur le port 53 (service DNS) est fortement déconseillée.**  
La création d'une règle en UDP sur le port **5050** et dans les plages **6070 à 6080** et **10000 à 20000** est susceptible d'entrer en conflit avec la téléphonie IP de la Livebox.

Nous voici sur notre interface Cloud Omada (TPLink). Nous disposons de cette plateforme pour assurer la configuration en cloud des équipements.

L'interface présentée sur la photo est la pat WAN permettant de faire transiter les flux du routeur VDSL via notre routeur TPLink Omada. Etant donné que les routeurs Omada sont routables pour des connexions Fibre, la communication sur le port WAN s'effectue ici de façon Dynamic, c'est-à-dire en mode Bridge.

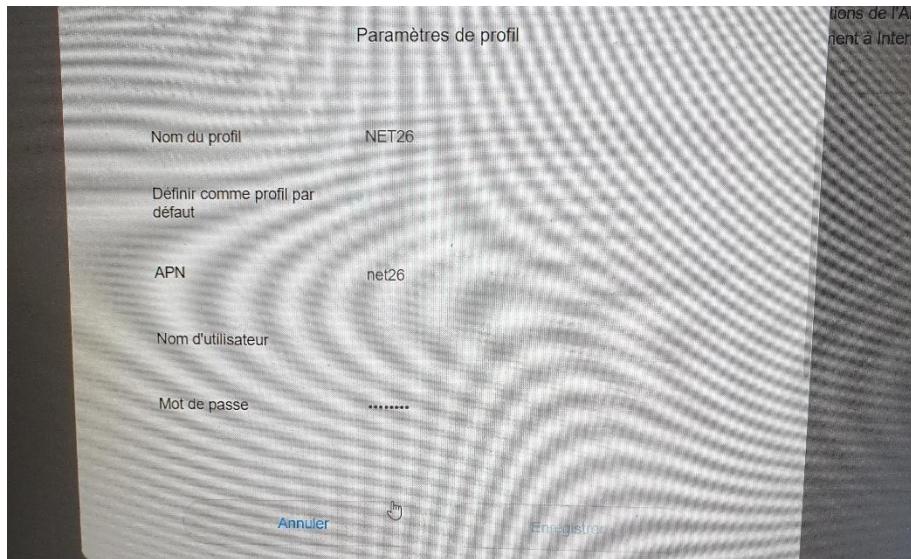


### Configuration Réseau Backup (Clé 4g Lien de Secours) :

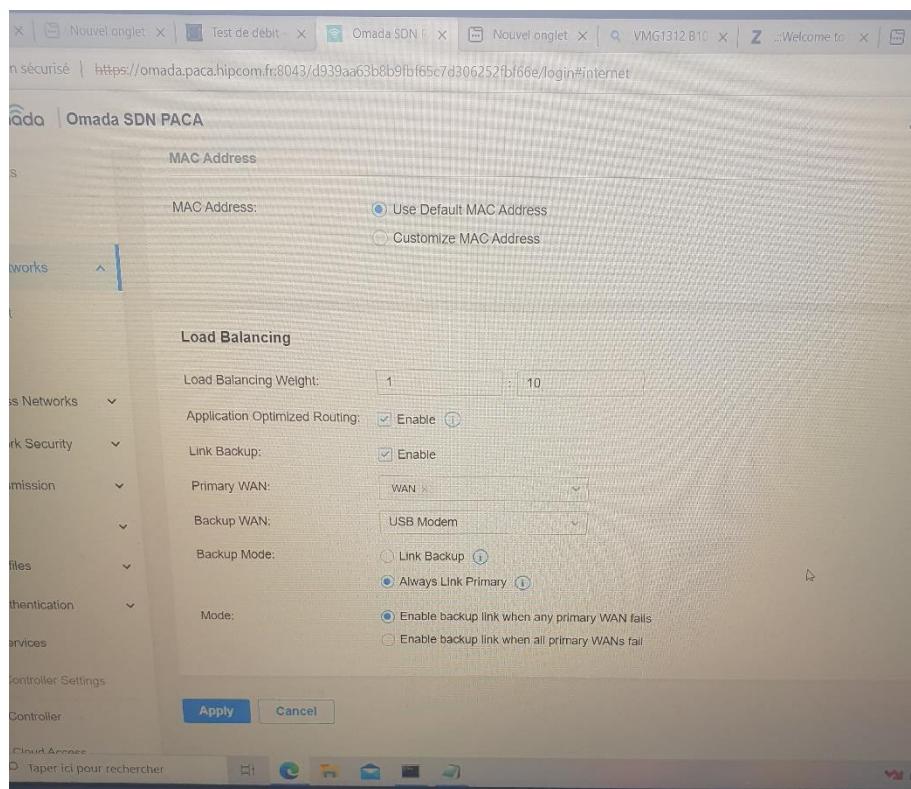
Dans les contrats clients, très souvent, des liens de secours sont choisis : nous devons fournir un accès à internet à l'entreprise en cas de coupure du lien principal (fibre ou xDSL)

Ces clés sont paramétrables via une SIM mobile activable sur Atlas.

La photo ci-dessous présente le déblocage de la SIM sur une clé 4g. Il est essentiel de la déverrouiller dans un premier temps puis d'ajouter le point d'accès (APN) NET26 permettant de transiter les connexions réseaux en itinérances plus facilement quelque soit la localisation du client.



Ensuite, nous revenons sur notre interface cloud Omada afin de configurer le WAN de la clé 4g en lien backup load balancing. C'est-à-dire que si la connexion au lien principal se coupe, nous paramétrons cette solution de sorte qu'elle prenne immédiatement le relais.



Voici le rendu d'une clé USB Huawei sur le routeur TP-Link Omada ER605.

Les 3 voyants indiquent sur le routeur qu'il fonctionne électriquement (PWR), que sa configuration est bien stable (SYS) et que la clé USB est détectable.

Le voyant rouge de la clé USB indique cependant une erreur sur la carte SIM (probablement l'APN qui n'est pas valide ou le code PIN de la clé USB qui n'est pas désactivé).

